Dokumentation von SolidFire und Element Software

Element Software

NetApp
November 13, 2025

This PDF was generated from https://docs.netapp.com/de-de/element-software/index.html on November 13, 2025. Always check docs.netapp.com for the latest.

Inhalt

Dokumentation von SolidFire und Element Software . . . 1
Versionshinweise . . . 2
Aktuelle und frühere Release-Informationen . . . 2
NetApp Element Software . . . 2
Management Services . . . 2
NetApp Element Plug-in für vCenter Server . . . 2
Storage-Firmware . . . 3
Weitere Informationen . . . 3
Neuerungen bei Element Software . . . 3
Element 12.9 . . . 4
Element 12.8 . . . 4
Element 12.7 . . . 5
Element 12.5 . . . 6
Weitere Informationen . . . 7
Konzepte . . . 8
Produktübersicht . . . 8
Funktionen der SolidFire . . . 8
SolidFire Implementierung . . . 8
Weitere Informationen . . . 8
Architektur und Komponenten . . . 9
Erfahren Sie mehr über die SolidFire -Architektur. . . . 9
SolidFire-Softwareschnittstellen . . . 10
SolidFire Active IQ . . . 12
Management-Node für Element Software . . . 13
Managementservices für SolidFire All-Flash-Storage . . . 13
Knoten . . . 14
Management-Node . . . 14
Storage-Node . . . 14
Fibre Channel-Node . . . 14
Node-Status des Vorgangs . . . 15
Weitere Informationen . . . 15
Cluster . . . 15
Autorisierende Storage-Cluster . . . 16
Drittelregel . . . 17
Ungenutzte Kapazität . . . 17
Storage-Effizienz . . . 17
Storage Cluster Quorum . . . 17
Sicherheit . . . 17
Verschlüsselung für Daten im Ruhezustand (Hardware) . . . 17
Verschlüsselung für Daten im Ruhezustand (Software) . . . 18
Externes Verschlüsselungskeymanagement . . . 18
Multi-Faktor-Authentifizierung . . . 18
FIPS 140-2 für HTTPS und Verschlüsselung von Daten im Ruhezustand . . . 19

Finden Sie weitere Informationen . . . 19
Konten und Berechtigungen . . . 19
Konten für Storage-Cluster-Administratoren . . . 19
Benutzerkonten . . . 20
Autorisierende Cluster-Benutzerkonten . . . 20
Volume-Konten . . . 21
Storage . . . 21
Volumes . . . 21
Virtuelle Volumes (VVols) . . . 22
Volume-Zugriffsgruppen . . . 23
Initiatoren . . . 24
Datensicherung . . . 24
Typen der Remote-Replizierung . . . 24
Volume Snapshots zur Datensicherung . . . 26
Volume-Klone . . . 26
Übersicht über Backup- und Restore-Prozesse für Element Storage . . . 27
Sicherungsdomänen . . . 27
Benutzerdefinierte Schutzdomänen . . . 28
Hochverfügbarkeit mit Double Helix . . . 28
Leistung und Servicequalität . . . 28
Parameter für die Servicequalität . . . 29
QoS-Wertbegrenzungen . . . 30
QoS-Performance . . . 30
QoS-Richtlinien (QoS . . . 31
Weitere Informationen . . . 31
Anforderungen . . . 32
Netzwerkbetrieb . . . 32
Finden Sie weitere Informationen . . . 32
Switch-Konfiguration für Cluster mit Element Software . . . 32
Finden Sie weitere Informationen . . . 33
Anforderungen an Netzwerk-Ports . . . 33
Finden Sie weitere Informationen . . . 37
Probieren Sie es aus . . . 38
Storage-Funktionen mit Element Demo-Node testen . . . 38
Unterstützte Funktionen: . . . 38
VM-Anforderungen erfüllt . . . 39
Host-Anforderungen erfüllt . . . 39
Laden Sie Den Element Demo-Node Herunter . . . 39
Installieren Sie Element Demo Node auf VMware ESXi . . . 39
Support-Hilfe . . . 40
Weitere Informationen . . . 40
Installation und Wartung von Hardware . . . 41
H410S und H610S Hardware-Informationen . . . 41
Storage-Nodes der H-Series installieren . . . 41
Einen H410S Node austauschen . . . 49

Austausch eines H610S Nodes . . . 54
Ersetzen Sie Laufwerke . . . 56
Ersetzen Sie ein Netzteil . . . 59
Hardwareinformationen zur SF-Series . . . 62
Ein Chassis austauschen . . . 62
Ersetzen von Laufwerken für SF-Series Storage-Nodes . . . 65
Ersetzen Sie ein Netzteil . . . 68
Kehren Sie zur Factory Image Information zurück . . . 69
Konfigurieren Sie die Rückkehr zum Werkbild . . . 70
RTFI-Bereitstellungs- und Installationsoptionen . . . 70
Das RTFI-Verfahren . . . 71
Menü RTFI-Optionen . . . 73
Storage-Nodes . . . 76
H610S . . . 76
H410S . . . 98
SF38410, SF19210, SF9605 und SF4805 . . . 101
Storage einrichten . . . 106
Erfahren Sie mehr über die Einrichtung von Speichersystemen. . . . 106
Weitere Informationen . . . 106
Richten Sie ein Cluster mit Storage-Nodes ein . . . 107
Konfigurieren Sie einen Storage-Node . . . 107
Erstellen eines Storage-Clusters . . . 109
Greifen Sie auf die Benutzeroberfläche der Element Software zu . . . 111
Fügen Sie Laufwerke zu einem Cluster hinzu . . . 111
Richten Sie ein Cluster mit Fibre Channel Nodes ein . . . 112
Konfigurieren Sie einen Fibre Channel-Node . . . 112
Erstellen Sie ein neues Cluster mit Fibre Channel Nodes . . . 113
Fügen Sie einem Cluster Fibre Channel Nodes hinzu . . . 114
Einrichten von Zonen für Fibre Channel-Nodes . . . 114
Erstellen einer Volume-Zugriffsgruppe für Fibre Channel-Clients . . . 115
Ermitteln der zu installierenden SolidFire-Komponenten . . . 115
Finden Sie weitere Informationen . . . 116
Richten Sie einen Management-Node ein . . . 116
Weitere Informationen . . . 116
Konfigurieren Sie vollständig qualifizierten Domänennamen Web UI-Zugriff . . . 117
Konfigurieren Sie den FQDN-Web-UI-Zugriff mit NetApp Hybrid Cloud Control . . . 117
Konfigurieren Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API . . . 118
Entfernen Sie FQDN Web-UI-Zugriff mit NetApp Hybrid Cloud Control . . . 119
Entfernen Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API . . . 119
Fehlerbehebung . . . 120
Weitere Informationen . . . 121
Was kommt als Nächstes . . . 121
Weitere Informationen . . . 121
Storage-Management mit Element Software . . . 122
Storage-Management mit Element Software . . . 122

Weitere Informationen . . . 122
Greifen Sie auf die Benutzeroberfläche der Element Software zu . . . 122
Weitere Informationen . . . 123
Konfigurieren Sie nach der Bereitstellung die SolidFire Systemoptionen . . . 123
Konfigurieren Sie nach der Bereitstellung die SolidFire Systemoptionen . . . 123
Anmeldedaten in NetApp HCI und NetApp SolidFire ändern . . . 123
Ändern Sie das Standard-SSL-Zertifikat der Element Software . . . 128
Ändern Sie das Standard-IPMI-Passwort für Nodes . . . 129
Verwenden Sie grundlegende Optionen in der UI für Element Software . . . 130
Verwenden Sie grundlegende Optionen in der UI für Element Software . . . 130
API-Aktivität . . . 130
Symbole in der Element-Schnittstelle . . . 131
Feedback mitteilen . . . 132
Konten verwalten . . . 133
Konten verwalten . . . 133
Arbeiten Sie mit Konten, die CHAP verwenden . . . 133
Verwalten von Benutzerkonten für Cluster-Administratoren . . . 136
LDAP verwalten . . . 139
Management des Systems . . . 147
Management des Systems . . . 148
Multi-Faktor-Authentifizierung aktivieren . . . 148
Konfigurieren Sie Cluster-Einstellungen . . . 149
Erstellen eines Clusters, das FIPS-Laufwerke unterstützt . . . 166
Sichere Kommunikation herstellen . . . 169
Erste Schritte mit externem Verschlüsselungsmanagement . . . 172
Management von Volumes und virtuellen Volumes . . . 177
Erfahren Sie mehr über die Verwaltung von Volumen und virtuellen Volumen. . . . 177
Arbeiten mit Volumes . . . 179
Arbeiten mit virtuellen Volumes . . . 188
Arbeiten Sie mit Volume-Zugriffsgruppen und -Initiatoren . . . 196
Sichern Sie Ihre Daten . . . 203
Sichern Sie Ihre Daten . . . 203
Nutzen Sie Volume Snapshots zur Datensicherung . . . 204
Remote-Replizierung zwischen Clustern mit NetApp Element Software . . . 218
SnapMirror Replizierung zwischen Element und ONTAP Clustern (Element UI) verwenden . . . 232
Replizierung zwischen NetApp Element Software und ONTAP (ONTAP CLI) . . . 243
Backup und Restore von Volumes . . . 265
Konfigurieren Sie benutzerdefinierte Sicherungsdomänen . . . 269
Fehler im System beheben . . . 270
Systemereignisse . . . 270
Status der ausgeführten Aufgaben anzeigen . . . 275
Systemwarnungen . . . 275
Zeigen Sie die Node-Performance-Aktivitäten an . . . 294
Volumenleistung . . . 294
iSCSI-Sitzungen . . . 296

Fibre Channel-Sitzungen . . . 297
Fehlerbehebung bei Laufwerken . . . 298
Fehlerbehebung für Nodes . . . 302
Storage-Nodes: Dienstprogramme pro Node unterstützen . . . 303
Erläuterung der Cluster-Auslastungsebenen . . . 311
Management und Monitoring von Storage mit NetApp Hybrid Cloud Control . . . 313
Fügen Sie Storage-Cluster mit NetApp Hybrid Cloud Control hinzu und managen Sie sie . . . 313
Fügen Sie einen Storage-Cluster hinzu . . . 313
Bestätigen des Storage-Cluster-Status . . . 314
Bearbeiten der Anmeldedaten für das Storage-Cluster . . . 314
Entfernen eines Storage-Clusters . . . 314
Aktivieren und deaktivieren Sie den Wartungsmodus . . . 315
Konfigurieren Sie vollständig qualifizierten Domänennamen Web UI-Zugriff . . . 317
Konfigurieren Sie den FQDN-Web-UI-Zugriff mit NetApp Hybrid Cloud Control . . . 318
Konfigurieren Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API . . . 318
Entfernen Sie FQDN Web-UI-Zugriff mit NetApp Hybrid Cloud Control . . . 319
Entfernen Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API . . . 320
Fehlerbehebung . . . 320
Weitere Informationen . . . 321
Erstellen und managen Sie Benutzerkonten mit NetApp Hybrid Cloud Control . . . 321
Aktivieren Sie LDAP . . . 322
Managen von autorisierenden Cluster-Konten . . . 322
Volume-Konten verwalten . . . 324
Erstellen und managen Sie Volumes mit NetApp Hybrid Cloud Control . . . 325
Erstellen eines Volumes . . . 326
Wenden Sie eine QoS-Richtlinie auf ein Volume an . . . 327
Bearbeiten Sie ein Volume . . . 327
Volumes klonen . . . 329
Hinzufügen von Volumes zu einer Volume-Zugriffsgruppe . . . 330
Löschen Sie ein Volume . . . 330
Wiederherstellen eines gelöschten Volumes . . . 331
Löschen Sie ein gelöschtes Volume . . . 331
Erstellung und Management von Volume-Zugriffsgruppen . . . 332
Fügen Sie eine Zugriffsgruppe für Volumes hinzu . . . 332
Bearbeiten Sie eine Zugriffsgruppe für Volumes . . . 333
Löschen Sie eine Zugriffsgruppe für Volumes . . . 333
Erstellen und Verwalten von Initiatoren . . . 334
Erstellen eines Initiators . . . 334
Fügen Sie Initiatoren zu einer Volume-Zugriffsgruppe hinzu . . . 335
Ändern eines Initiator-Alias . . . 336
Löschen Sie Initiatoren . . . 336
Erstellung und Management von QoS-Richtlinien für Volumes . . . 337
Erstellen einer QoS-Richtlinie . . . 337
Wenden Sie eine QoS-Richtlinie auf ein Volume an . . . 338
Ändern der QoS-Richtlinienzuweisung eines Volumes . . . 338

Bearbeiten einer QoS-Richtlinie . . . 339
Löschen einer QoS-Richtlinie . . . 339
Überwachen Sie Ihr SolidFire System mit NetApp Hybrid Cloud Control . . . 340
Überwachen Sie die Speicherressourcen über das Hybrid Cloud Control Dashboard . . . 340
Zeigen Sie Ihren Bestand auf der Seite Knoten an . . . 345
Überwachung von Volumes auf Ihrem Storage-Cluster . . . 347
Sammelt Protokolle für die Fehlerbehebung . . . 348
Storage-Management mit Element API . . . 353
Element API-Software . . . 353
Erfahren Sie mehr über die Speicherverwaltung mit der Element API. . . . 353
Fordern Sie Objektmitglieder an . . . 357
Mitglieder des Antwortobjekts . . . 358
Endpunkte anfordern . . . 358
API-Authentifizierung . . . 359
Asynchrone Methoden . . . 359
Merkmale . . . 360
Gemeinsame Objekte . . . 361
Konto . . . 361
AuthSessionInfo . . . 362
BulkVolumeJob . . . 364
Bindung (virtuelle Volumes) . . . 365
ZertifikateDetails . . . 366
Cluster . . . 367
ClusterAdmin . . . 369
ClusterKapazität . . . 370
Cluster-Konfiguration . . . 373
ClusterInfo . . . 374
Cluster-Paar . . . 376
ClusterStatistik . . . 377
ClusterStructure . . . 381
Laufwerk . . . 381
Fahrstollen . . . 384
Fehler . . . 386
Ereignis . . . 387
Fehler . . . 389
Fibre Channel-Port . . . 392
FipsErrorNodeReport . . . 393
FipsNodeReport . . . 394
FipsReport . . . 395
GroupSnapshot . . . 395
HardwareInfo . . . 396
Host (virtuelle Volumes) . . . 398
IdpConfigInfo . . . 399
Initiator . . . 400
ISCSIAuthentifizierung . . . 401

KeProviderKmip . . . 402
KeyServerkmip . . . 403
LdapKonfiguration . . . 404
LoggingServer . . . 406
Netzwerk (verbundene Schnittstellen) . . . 406
Netzwerk (alle Schnittstellen) . . . 411
Netzwerk (Ethernet-Schnittstellen) . . . 412
Netzwerk (lokale Schnittstellen) . . . 414
Netzwerk (SNMP) . . . 416
Netzwerkschnittstelle . . . 417
NetworkSchnittstellenStats . . . 418
Knoten . . . 419
NodeProtectionDomains . . . 422
KnotenStatistiken . . . 422
OntapVersionInfo . . . 424
HängenActiveNode . . . 425
Hängende Knoten . . . 427
ProtectionDomain . . . 428
SchutzDomainLevel . . . 429
SchutzDomaininAusfallsicherheit . . . 430
SchutzDominToleranz . . . 430
SicherungAusfallsicherheit . . . 431
SchutzSchemeToleranz . . . 432
ProtocolEndpoint . . . 432
QoS . . . 433
QoSPolicy . . . 434
EntfernteClusterSnapshotStatus . . . 435
Zeitplan . . . 436
Sitzung (Fibre Channel) . . . 440
Sitzung (iSCSI) . . . 441
SnapMirror Aggregat . . . 444
SnapMirror Clusteridentität . . . 444
SnapMirror Endpoint . . . 445
SnapMirrorJobeCronInfo . . . 446
SnapMirrorLunInfo . . . 446
SnapMirror Netzwerkschnittstelle . . . 447
SnapMirror Node . . . 448
SnapMirror Richtlinie . . . 449
SnapMirror PolicyRule . . . 450
SnapMirror Beziehung . . . 451
SnapMirror Volume . . . 454
SnapMirrorVolumeInfo . . . 455
SnapMirrorVServer . . . 456
SnapMirrorVserveraggregateInfo . . . 457
snapshot . . . 457

SnmpTrapEmpfänger 460
Storage Container 461
SyncJob 462
Aufgabe (virtuelle Volumes) 465
UsmUser 467
VirtualNetwork 468
VirtualVolume 469
Datenmenge 471
VolumeAccessGroup 475
Volumepaar 476
VolumeStatistik 477
Gängige Methoden 482
GetAPI 482
GetAsyncResult 490
GetCompleteStats 495
GetLimits 495
GetOrigin 497
GetRawStats 498
ListeAsyncResults 499
Account-API-Methoden 502
AddAccount 502
GetAccountByID 505
GetAccountByName 506
GetAccountEffizienz 508
Listenkonten 509
ModifyAccount 512
RemoveAccount 514
Administrator-API-Methoden 516
AddClusterAdmin 516
GetCurrentClusterAdmin 518
GetLoginBanner 519
ListenClusteradministratoren 520
ModifyClusterAdmin 523
RemoveClusterAdmin 524
SetLoginBanner 525
Cluster-API-Methoden 528
AddNodes 528
ClearClusterStandards 531
CreateClusterSchnittstellenPräferenz 533
DeleteClusterSchnittstellenPräferenz 534
DisableFeature 535
EnableFeature 536
GetClusterCapacity 538
GetClusterFullThreshold 540
GetClusterHardware-Informationen 546

GetClusterInfo . . . 548
GetClusterSchnittstellenPräferenz . . . 550
GetClusterMasterNodeID . . . 551
GetClusterStats . . . 552
GetClusterVersionInfo . . . 553
GetFeatureStatus . . . 557
GetLoginSessionInfo . . . 559
GetNodeHardwareInfo . . . 561
GetNodeStats . . . 562
ListenActiveNodes . . . 565
ListenAllNodes . . . 565
ListenClusterstandards . . . 567
ListenClusterSchnittstelleneinstellungen . . . 571
ListEvents . . . 572
ListNodeStats . . . 576
ListISSessions . . . 578
ListServices . . . 580
ListenPendingKnoten . . . 582
ListPendingActiveNodes . . . 584
ModifyClusterFullThreshold . . . 586
ModifyClusterSchnittstellenPräferenz . . . 594
RemoveNodes . . . 595
SetLoginSessionInfo . . . 597
Herunterfahren . . . 599
API-Methoden zur Clustererstellung . . . 600
CheckeAngebot für Cluster . . . 600
CreateCluster erstellen . . . 602
GetBootstrapConfig . . . 605
Drive-API-Methoden . . . 609
AddDrives . . . 609
GetDriveHardwareInfo . . . 611
GetDriveStats . . . 613
ListenLaufwerke . . . 616
ListDriveStats . . . 618
RemoveDrives . . . 620
SecureEraseDrives . . . 622
Fibre Channel-API-Methoden . . . 624
GetVolumeAccessGroupLunAssignments . . . 624
ListFiberChannelPortInfo . . . 625
ListFiberChannelSessions . . . 629
ListNodeFiberChannelPortInfo . . . 630
ModifyVolumeAccessGroupLunAssignments . . . 632
Initiator-API-Methoden . . . 634
CreateInitiatoren . . . 635
DeleteInitiatoren . . . 639

ListenInitiatoren . . . 641
ModifyInitiatoren . . . 642
LDAP-API-Methoden . . . 646
AddLdapClusterAdmin . . . 646
EnableLdapAuthentifizierung . . . 648
DisableLdapAuthentifizierung . . . 653
GetLdapConfiguration . . . 654
TestLdapAuthentifizierung . . . 656
Multi-Faktor-Authentifizierungs-API-Methoden . . . 658
AddIdpClusterAdmin . . . 658
CreateIdpConfiguration . . . 660
DeleteAuthSession . . . 662
DeleteAuthSessionByClusterAdmin . . . 664
DeleteAuthSessionsByUsername . . . 665
DeleteIdpKonfiguration . . . 668
DisableIdpAuthentifizierung . . . 669
EnableIdpAuthentifizierung . . . 669
GetIdpAuthenticationState . . . 671
ListActiveAuthSessions . . . 672
ListIdpConfigurations . . . 673
UpdateIdpKonfiguration . . . 675
API-Methoden für die Sitzungsauthentifizierung . . . 678
ListAuthSessionByClusterAdmin . . . 678
ListAuthSessionsByBenutzername . . . 680
Node-API-Methoden . . . 683
CheckPingOnVlan . . . 683
CheckeAngebot NodeAdditions . . . 686
CreateClusterSupportBundle . . . 689
CreateSupportBundle . . . 692
DeleteAllSupportBundles . . . 695
Instandhaltungmodus . . . 696
DisableSsh . . . 699
Instandhaltungmodus . . . 700
EnableSsh . . . 703
GetClusterConfig . . . 704
GetClusterStatus . . . 706
Getconfig . . . 707
GetDriveConfig . . . 708
VMware HardwareConfig . . . 711
GetHardwareInfo . . . 713
GetIpmiConfig . . . 715
GetIpmiInfo . . . 720
GetNetworkConfig . . . 723
GetNetworkInterface . . . 724
GetNodeActiveTlsCiphers . . . 728

GetNodeFipsDrivesReport . . . 729
GetNodeSSLZertifikat . . . 730
GetNodeSupportedTlsCiphers . . . 732
GetPatchInfo . . . 734
GetPendingOperation . . . 736
GetSshInfo . . . 737
ListDriveHardware . . . 738
ListNetworkInterfaces . . . 741
ListNetworkSchnittstellenStats . . . 743
ListTruhen . . . 745
ListenUtilities . . . 746
RemoveNodeSSLZertifikat . . . 747
Erneutes Ansetzen von Laufwerken . . . 748
ResetNode neu . . . 750
ResetNodeErgänzungTlsCiphers . . . 753
Netzwerk neu starten . . . 753
RestartServices neu starten . . . 754
SetClusterConfig . . . 756
SetConfig . . . 758
SetNetworkConfig . . . 760
SetNodeSSLZertifikat . . . 762
SetNodeSupplementalTlsCiphers . . . 765
Herunterfahren . . . 766
TestConnectEnsemble . . . 768
TestConnectMvip . . . 770
TestConnectSvip . . . 774
TestDrives . . . 779
TestHardwareConfig . . . 780
TestLocateCluster . . . 782
TestLocalConnectivity . . . 783
TestNetworkConfig . . . 786
TestPing . . . 789
TestRemoteConnectivity . . . 793
Replizierungs-API-Methoden . . . 795
Reihenfolge der Vorgänge für die Cluster-Paarung . . . 795
Reihenfolge der Vorgänge für die Volume-Kopplung . . . 796
Unterstützte Replikationsmodi für gepaarte Cluster . . . 797
CompleteClusterPairing . . . 797
CompleteVolumePairing . . . 798
ListenClusterpaare . . . 800
ListeActivePairedVolumes . . . 801
ModifyVolumePair . . . 804
RemoveClusterPair . . . 806
RemoveVolumePair . . . 807
StartClusterPairing . . . 808

StartVolumePairing . . . 810
Sicherheits-API-Methoden . . . 814
AddKeyServerToProviderKmip . . . 814
CreateKeyProviderKmip . . . 815
CreateKeyServerkmip . . . 817
CreatePublicPrivateKeyPair . . . 820
DeleteKeyProviderKmip . . . 822
DeleteKeyServerkmip . . . 823
UnbeständigkeitVerverschlüsselungAttest . . . 824
EnableVerschlüsselungAtZiel . . . 825
GetClientCertificateSignRequest . . . 828
GetKeyProviderKmip . . . 829
GetKeyServerkmip . . . 830
GetSoftwareVerschlüsselungAtRestInfo . . . 832
ListKeyProvidersKmip . . . 833
ListKeyServersKmip . . . 836
ModifyKeyServerkmip . . . 840
RekeySoftwareVerschlüsselungAtRestMasterKey . . . 843
RemoveKeyServerFromProviderKmip . . . 846
Signalschlüssel . . . 847
TestKeyProviderKmip . . . 852
TestKeyServerkmip . . . 853
SnapMirror API-Methoden . . . 854
AbortSnapMirrorBeziehung . . . 854
BreakSnapMirrorBeziehung . . . 855
BreakSnapMirrorVolume . . . 856
CreateSnapMirrorEndpoint . . . 858
CreateSnapMirrorEndpointnicht verwaltet . . . 859
CreateSnapMirrorBeziehung . . . 860
CreateSnapMirrorVolume . . . 861
LöteSnapMirrorEndpunkte . . . 863
DeleteSnapMirrorRelationships . . . 863
GetOntapVersionInfo . . . 864
GetSnapMirrorClusteridentität . . . 865
InitializeSnapMirrorRelationship . . . 866
ListSnapMirrorAggregates . . . 867
ListSnapMirrorEndpunkte . . . 868
ListSnapMirrorLuns . . . 869
ListSnapMirrorNetworkInterfaces . . . 870
ListSnapMirrorNodes . . . 871
ListSnapMirrorPolicies . . . 872
ListSnapMirrorSchedules . . . 872
ListSnapMirrorBeziehung . . . 873
ListSnapMirrorVolumes . . . 875
ListSnapMirrorVserver . . . 876

ModifySnapMirrorEndpoint . . . 877
ModifySnapMirrorEndpoint (nicht gemanagt) . . . 878
ModifySnapMirrorRelationship . . . 879
UpdateSnapMirrorRelationship . . . 881
QuiesceSnapMirrorBeziehung . . . 882
ResummeSnapMirrorBeziehung . . . 882
ResyncSnapMirrorRelationship . . . 883
Methoden für die Systemkonfiguration-API . . . 884
DisableBmcColdReset . . . 884
DisableClusterSsh . . . 885
AbleSnmp . . . 887
EnableBmcColdReset . . . 888
EntleClusterSsh . . . 889
EnableSnmp . . . 891
GetBinAssignmentProperties . . . 892
GetClusterSshInfo . . . 895
GetClusterStructure . . . 896
GetFipsReport . . . 897
GetLldpConfig . . . 899
GetLldpInfo . . . 900
GetNodeFipsDrivesReport . . . 901
GetNtpInfo . . . 902
GetNvramInfo . . . 904
GetProtectionDomainLayout . . . 905
GetRemoteLoggingHosts . . . 907
GetSnmpACL . . . 908
GetSnmpInfo . . . 909
GetSnmpState . . . 911
GetSnmpTrapInfo . . . 913
GetSSLZertifikat . . . 914
ListeProtectionDomainLevels . . . 916
RemoveSSLZertifikat . . . 918
NetworkConfig erneut verwenden . . . 919
RücksetzenErgänzungTlsCiphers . . . 920
SetClusterStructure . . . 921
SetLldpConfig . . . 922
SetNtpInfo . . . 923
SetProtectionDomainLayout . . . 925
SetRemoteLoggingHosts . . . 929
SetSnmpACL . . . 931
SetSnmpInfo . . . 932
SetSnmpTrapInfo . . . 935
SetSSLZertifikat . . . 937
SnmpSendTestTraps . . . 939
TestAddressAvailability . . . 940

Mandantenfähige Netzwerk-API-Methoden . . . 942
Namenskonventionen für virtuelle Netzwerke . . . 942
AddVirtualNetwork . . . 942
ModifyVirtualNetwork . . . 945
ListVirtualNetworks . . . 950
RemoveVirtualNetwork . . . 952
Volume-API-Methoden . . . 953
CancelClone . . . 953
GruppenClone abbrechen . . . 954
CloneMultipleVolumes . . . 955
KlonVolume . . . 959
CopyVolume . . . 964
CreateQoSPolicy . . . 966
CreateVolume . . . 968
CreateBackupTarget . . . 977
DeleteQoSPolicy . . . 978
DeleteVolume . . . 979
DeleteVolumes . . . 982
GetBackupTarget . . . 985
GetVolumeStats . . . 987
GetDefaultQoS . . . 989
GetQoSPolicy . . . 991
GetVolumeCount . . . 993
GetVolumeEffizienz . . . 994
ListeActiveVolumes . . . 996
ListBackupTargets . . . 998
ListBulkVolumeJobs . . . 999
ListDeletedVolumes . . . 1001
ListQoSPolicies . . . 1004
ListSyncJobs . . . 1006
ListVolumeQoSHistogramme . . . 1008
ListVolumes . . . 1010
ListVolumeStats . . . 1015
ListVolumesForAccount . . . 1017
ListVolumeStatsByKonto . . . 1020
ListVolumeStatsByVirtualVolume . . . 1022
ListVolumeStatsByVolume . . . 1024
ListVolumeStatsByVolumeAccessGroup . . . 1026
ModifyBackupTarget . . . 1028
ModifyQoSPolicy . . . 1030
UmfyVolume . . . 1032
ModifyVolumes . . . 1042
PurgeDeletedVolume . . . 1052
PurgeDeletedVolumes . . . 1053
RemoveBackupTarget . . . 1055

RestoreDeletedVolumen . . . 1056
SetdefaultQoS . . . 1057
StartBulkVolumeRead . . . 1059
StartBulkVolumeWrite . . . 1062
UpdateBulkVolumeStatus . . . 1065
API-Methoden für Volume-Zugriffsgruppen . . . 1068
AddInitiatorsToVolumeAccessGroup . . . 1068
AddVolumesToVolumeAccessGroup . . . 1070
CreateVolumeAccessGroup . . . 1072
DeleteVolumeAccessGroup . . . 1075
ListVolumeAccessGroups . . . 1078
EntfernenVolumeFromVolumeAccessGroup . . . 1080
RemoveInitiatorsFromVolumeAccessGroup . . . 1082
ModifyVolumeAccessGroup . . . 1085
GetVolumeAccessGroupEffizienz . . . 1089
Volume Snapshot-API-Methoden . . . 1091
Snapshots – Überblick . . . 1091
CreateGroupSnapshot . . . 1091
Erstellen Sie einen Zeitplan . . . 1098
Erstellen von Snapshot . . . 1111
DeleteGroupSnapshot . . . 1117
LöschSnapshot . . . 1119
GetSchedule . . . 1120
ListenSnapshots . . . 1122
ListSchedules . . . 1125
ListenSnapshots . . . 1127
ModifyGroupSnapshot . . . 1129
ModifySchedule . . . 1133
UmfySnapshot . . . 1140
RollbackToGroupSnapshot . . . 1144
RollbackToSnapshot . . . 1149
API-Methoden für virtuelle Volumes . . . 1152
CreateStorageContainer . . . 1152
DeleteStorageContainers . . . 1153
GetStorageContainerEffizienz . . . 1154
GetVirtualVolumeCount . . . 1156
ListProtocolEndpunkte . . . 1157
ListStorageContainer . . . 1160
ListVirtualVolumeBindungen . . . 1161
ListVirtualVolumeHosts . . . 1163
ListVirtualVolumes . . . 1165
ListVirtualVolumeTasks . . . 1169
ModifyStorageContainer . . . 1170
Zugriffssteuerung . . . 1172
Konten . . . 1172

Verwalter 1173
ClusterAdmin 1173
Laufwerke 1176
Knoten 1176
Lesen 1177
Berichterstellung 1178
Repositorys 1180
Volumes 1180
Schreiben 1181
Antwortbeispiele 1182
Getconfig 1182
GetClusterHardware-Informationen 1185
GetLldpInfo 1199
GetNetworkConfig 1228
GetNodeHardwareInfo (Ausgabe für iSCSI) 1232
GetNodeHardwareInfo (Ausgabe für Fibre Channel Nodes) 1234
GetNvramInfo 1242
ListenActiveNodes 1250
ListeActiveVolumes 1254
TestHardwareConfig 1263
NetApp Element Plug-in für vCenter Server 1269
Finden Sie weitere Informationen 1269
Monitoring von Storage mit SolidFire Active IQ 1270
Finden Sie weitere Informationen 1270
Arbeiten Sie mit dem Management-Node 1271
Übersicht über Management-Nodes 1271
Installation oder Wiederherstellung eines Management-Node 1272
Installieren Sie einen Management-Node 1272
Erstellen einer NetApp HCC-Rolle in vCenter 1279
Konfigurieren eines Speicher-Netzwerkschnittstellentoncontrollers (NIC) 1284
Wiederherstellung eines Management-Node 1286
Greifen Sie auf den Management-Node zu 1291
Greifen Sie über die UI auf den Management-Node zu 1292
Greifen Sie auf DIE REST-API-UI für den Management-Node zu 1293
Ändern Sie das Standard-SSL-Zertifikat für den Management-Node 1294
Weitere Informationen 1294
Arbeiten Sie mit der Management-Node-UI 1294
Übersicht über die Management-Node-UI 1294
Konfigurieren der Meldungsüberwachung 1295
Ändern und Testen der Netzwerk-, Cluster- und Systemeinstellungen des Management-Node 1295
Führen Sie Systemdienstprogramme vom Management-Node aus 1297
Arbeiten mit DER REST-API des Management-Node 1298
Übersicht über DIE REST-API-UI für den Management-Node 1298
Autorisierung zur Verwendung VON REST-APIs 1299
Monitoring von Active IQ und NetApp 1300

Konfiguration von NetApp Hybrid Cloud Control für mehrere vCenter . . . 1303
Fügen Sie dem Management-Node eine Controller-Ressource hinzu . . . 1304
Erstellen und Managen von Storage-Cluster-Assets . . . 1306
Vorhandene Controller-Assets können angezeigt oder bearbeitet werden . . . 1311
Konfigurieren Sie einen Proxyserver . . . 1313
Überprüfen Sie die Betriebssystem- und Servicestversionen der Management-Nodes . . . 1314
Abrufen von Protokollen von Managementservices . . . 1315
Managen von Supportverbindungen . . . 1317
Zugriff auf Storage-Nodes mithilfe von SSH für die grundlegende Fehlerbehebung . . . 1317
Starten Sie eine Remote NetApp Support Sitzung . . . 1321
Verwalten der SSH-Funktionalität auf dem Management-Node . . . 1322
Upgrade für Ihr NetApp SolidFire All-Flash-Storage-System . . . 1326
Übersicht der Aktualisierungssequenz . . . 1326
Systemaktualisierungssequenz . . . 1327
Verfahren für System-Upgrades . . . 1328
Integritätsprüfungen von Element Storage vor einem Storage Upgrade durchführen . . . 1328
Upgrade eines Management-Node . . . 1333
Managementservices aktualisieren . . . 1337
Upgrade der Element Software . . . 1340
Firmware für Storage-Upgrades . . . 1351
Aktualisieren Sie das Element Plug-in für vCenter Server . . . 1361
Aktualisieren Sie Ihre vSphere Komponenten für ein NetApp SolidFire Storage-System mit dem Element Plug-in für vCenter Server . . . 1369
Weitere Informationen . . . 1370
Frühere Versionen der Dokumentation zu SolidFire und NetApp Element . . . 1371
Finden Sie weitere Informationen . . . 1371
Rechtliche Hinweise . . . 1372
Urheberrecht . . . 1372
Marken . . . 1372
Patente . . . 1372
Datenschutzrichtlinie . . . 1372
Open Source . . . 1372

Dokumentation von SolidFire und Element Software

Versionshinweise

Aktuelle und frühere Release-Informationen

Links zu den neuesten und früheren Versionshinweisen für verschiedene Komponenten der Element Storage-Umgebung finden Sie.

Sie werden aufgefordert, sich mit Ihren NetApp Support-Anmeldedaten einzuloggen.

NetApp Element Software

- "NetApp Element Software 12.9 – Versionshinweise"*Neu*
- "Versionshinweise zu NetApp Element Software 12.8"
- "Versionshinweise zu NetApp Element Software 12.7"
- "Versionshinweise zu NetApp Element Software 12.5"
- "Versionshinweise zu NetApp Element Software 12.3.2"
- "Versionshinweise zu NetApp Element Software 12.3.1"
- "Versionshinweise zu NetApp Element Software 12.3"
- "Versionshinweise zu NetApp Element Software 12.2.1"
- "Versionshinweise zu NetApp Element Software 12.2"
- "Versionshinweise zu NetApp Element Software 12.0.1"
- "Versionshinweise zu NetApp Element Software 12.0"
- "Versionshinweise zu NetApp Element Software 11.8.2"
- "Versionshinweise zu NetApp Element Software 11.8.1"
- "Versionshinweise zu NetApp Element Software 11.8"
- "Versionshinweise zu NetApp Element Software 11.7"
- "Versionshinweise zu NetApp Element Software 11.5.1"
- "Versionshinweise zu NetApp Element Software 11.3P1"

Management Services

- "Versionshinweise Für Management Services"

NetApp Element Plug-in für vCenter Server

- "Versionshinweise zum vCenter Plug-in 5.5"
- "Versionshinweise zu vCenter Plug-in 5.4"
- "Versionshinweise zu vCenter Plug-in 5.3"
- "Versionshinweise zu vCenter Plug-in 5.2"
- "Versionshinweise zu vCenter Plug-in 5.1"
- "VCenter Plug-in 5.0 – Versionshinweise"

- "VCenter Plug-in 4.10 – Versionshinweise"
- "VCenter Plug-in 4.9 – Versionshinweise"
- "VCenter Plug-in 4.8 – Versionshinweise"
- "VCenter Plug-in 4.7 – Versionshinweise"
- "VCenter Plug-in 4.6 – Versionshinweise"
- "VCenter Plug-in 4.5 – Versionshinweise"
- "VCenter Plug-in 4.4 – Versionshinweise"
- "VCenter Plug-in 4.3 – Versionshinweise"

Storage-Firmware

- "Speicher-Firmware-Paket 2.182.0 – Versionshinweise" *NEU*
- "Speicher-Firmware-Paket 2.175.0 – Versionshinweise"
- "Versionshinweise Zum Speicher-Firmware-Bundle 2.164.0"
- "Versionshinweise Zum Speicher-Firmware-Bundle 2.150"
- "Versionshinweise Zum Speicher-Firmware-Bundle 2.146"
- "Versionshinweise Zum Speicher-Firmware-Bundle 2.99.2"
- "Versionshinweise Zum Speicher-Firmware-Bundle 2.76"
- "Versionshinweise Zum Speicher-Firmware-Bundle 2.27"
- "H610S BMC 3.84.07 – Versionshinweise"
- "Unterstützte Firmware- und ESXi-Treiberversionen"

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Neuerungen bei Element Software

NetApp aktualisiert regelmäßig die SolidFire und Element-Software, um Ihnen neue Funktionen, Verbesserungen und Fehlerbehebungen bereitzustellen. Element 12.9 ist die neueste Version und beinhaltet Sicherheits- und Systemkomponenten-Updates, betriebliche Verbesserungen und behobene Probleme.

Die kumulativen Software- und Firmware-Updates werden im Rahmen eines Element 12.9-Upgrades auf Basis der aktuell auf einem Speichercluster laufenden Element-Version installiert. Wenn beispielsweise auf einem Cluster derzeit Element 12.5 ausgeführt wird, können Sie direkt auf Element 12.9 aktualisieren, um die kumulativen Updates von Element 12.7, 12.8 und 12.9 zu erhalten. Informationen zu unterstützten Upgrade-Pfaden finden Sie im Knowledge-Base-Artikel. "Welche Upgrade-Matrix enthält die Storage Cluster, auf denen NetApp Element Software ausgeführt wird" Die

Element 12.9

Erfahren Sie mehr über die Neuerungen in Element 12.9.

Unterstützung für FQDN in "SetRemoteLoggingHosts"

Ab Element 12.9 können Sie die `SetRemoteLoggingHosts` Methode zum Konfigurieren eines vollqualifizierten Domänennamens (FQDN) oder einer IP-Adresse als Protokollierungshostwert für einen Speichercluster. Sie können den FQDN-Hostwert in der Antwort für die `GetRemoteLoggingHosts` Verfahren. Bei Element 12.8 und älteren Versionen kann nur eine IP-Adresse als Wert für den Protokollierungshost konfiguriert werden.

"Erfahren Sie mehr über die Konfiguration des Protokollierungshosts."

Element 12.8

Erfahren Sie mehr über die Neuerungen in Element 12.8.

Volume-Lastausgleich

In Element 12.8 wird die Funktion zum Lastausgleich von Volumes eingeführt. Mithilfe dieser Funktion können Sie Volumes über Nodes hinweg basierend auf dem tatsächlichen IOPS-Level jedes Volumes ausgleichen, anstatt wie in der QoS-Richtlinie konfiguriert zu sein. Sie können die Volume Load Balancing-Funktion nur zum Ausgleich von Volumes verwenden. Sie können es nicht zum Ausbalancieren virtueller Volumes verwenden. Die Volume Load Balancing-Funktion ist standardmäßig deaktiviert. Sie können sie aktivieren und deaktivieren, indem Sie den `VolumeLoadBalanceOnActualIOPS` API-Parameter mit den "EnableFeature"Methoden und "DisableFeature" API verwenden oder die Option in der Element UI verwenden"Volume-Lastausgleich".

Zeigt Informationen zur Node-Auslastung an

Mit Element 12.8 können Sie Informationen zur Node-Auslastung mithilfe der `GetNodeStats` und `ListNodeStats` API-Methoden anzeigen `nodeHeat`. Das `nodeHeat` Objekt ist Mitglied des `nodeStats` Objekts und zeigt Informationen zur Node-Auslastung basierend auf dem Verhältnis der primären gesamten IOPS oder der gesamten IOPS zu den im Zeitverlauf konfigurierten IOPS an.

Darüber hinaus können Sie die Node-Auslastung als Prozentsatz von `recentPrimaryTotalHeat` in der Anzeige Details anzeigen für einen Node in der Element-Benutzeroberfläche anzeigen.

Anzeigen von I/O-Statistiken für ein Volume

Mit Element 12.8 können Sie Statistiken zur I/O-Nutzung für ein Volume anhand der `GetVolumeStats` API-Methoden und `ListVolumeStatsByVolume` anzeigen `sliceIopsStats`. Die I/O-Statistiken werden mithilfe der Lese- und Schreib-IOPS-Informationen für das Volume berechnet und über zwei Zeiträume, die letzten 24 Stunden und die letzte Stunde, gemessen. "Weitere Informationen .".

CHAP-Algorithmus für iSCSI-Sitzung

Ein Host-iSCSI-Initiator fordert eine Liste der CHAP-Algorithmen (Challenge-Handshake Authentication Protocol) an, die verwendet werden sollen, wenn eine iSCSI-Sitzung mit einem Element-iSCSI-Ziel erstellt wird. Ab Element 12.8 können Sie den unterstützten CHAP-Algorithmus anzeigen, den das Element iSCSI-Ziel für eine iSCSI-Sitzung verwendet.

Upgrade der VM-Hardwareversion

Wenn Sie ein in-Place-Upgrade eines vorhandenen Management-Node auf Element 12.8 durchführen, müssen Sie vor dem Upgrade sicherstellen, dass die VM-Hardwareversion auf dem Management-Node je nach Umgebung mit ESXi 6.7 (VM-Hardwareversion 14) oder höher kompatibel ist. "Weitere Informationen .".

Element 12.7

Erfahren Sie mehr über die Neuerungen in Element 12.7.

Sichere CHAP-Algorithmen

Element 12.7 bietet Unterstützung für sichere FIPS-konforme CHAP-Algorithmen (Challenge-Handshake Authentication Protocol) SHA1, SHA-256 und SHA3-256. "Weitere Informationen .".

Dynamische Blocksynchronisation (bin)

Cluster-Vorgänge wie Ergänzungen, Upgrades oder Wartungen von Nodes oder das Hinzufügen von Laufwerken usw. lösen Block-Sync (bin) aus, um Block-Daten an die neuen oder aktualisierten Nodes in einem Cluster-Layout zu verteilen. Die Verwendung einer einzigen, langsamen Geschwindigkeit als Standard-Synchronisationsrate führt dazu, dass diese Vorgänge viel Zeit in Anspruch nehmen, und nutzt nicht die höhere Verarbeitungsleistung größerer Nodes. Ab Element 12.7 wird die Sync-in-Rate basierend auf der Anzahl der Kerne im Storage-Node dynamisch optimiert, sodass diese Vorgänge deutlich schneller ablaufen.

Wenn Sie beispielsweise großen 28-Core Storage-Nodes (H610S, SF19210 und SF38410) mit Element 12.7 zu einem vorhandenen Cluster hinzufügen, wird die Synchronisationsrate für Daten automatisch auf 110 MB/s anstatt 60 Mbps eingestellt. Wenn Sie diese großen Storage-Nodes zusätzlich aus dem Wartungsmodus für den Node-Wartungsmodus bringen, beispielsweise bei einem Upgrade von Element 12.3.x oder höher zu Element 12.7 mit NetApp Hybrid Cloud Control, wird die Sync-in-Rate für geänderte Block-Datenraten automatisch auf 110 MB anstatt 20 MB/s eingestellt.

Wenn Sie einem Element 12.7 Cluster die mittleren 16-Core Storage-Nodes (H410S) und kleinen 12-Core Storage-Nodes (SF4805) hinzufügen, bleibt die Synchronisationsrate für Daten mit 60 MB/s; Wenn geänderte Blöcke jedoch synchronisiert werden, wenn Sie sie während einer Aktualisierung von Element 12.3.x zu Element 12.7 aus dem Wartungsmodus des Node verlassen, wird die Sync-in-Rate für mittelgroße Storage-Nodes automatisch von 20 Mbit/s bis 60 Mbit/s und für kleinere Storage Nodes mit 40 Mbit/s synchronisiert.

Wenn Sie Storage-Nodes entfernen, wird die Synchronisationsrate des Blocks nicht beeinträchtigt, sodass Performance-Beeinträchtigungen für Client-I/O vermieden werden

Verbesserung der Speicherbereinigung

Bei Clustern mit größeren Storage-Nodes beispielsweise führt ein H610S-4 mit einem belegten Speicherplatz von 1 PB sehr hohe Workloads mit Überschreibungen aus, Dank hoher Deduplizierung und Komprimierung kann der Speicherbereinigung jetzt mithalten, da die standardmäßige Bloom-Filtergröße für die größeren Nodes von 700 GB oder mehr Speicher auf 1048576 Bit erhöht wurde. Diese Änderung wird automatisch wirksam, wenn Sie Ihre Storage-Nodes auf Element 12.7 aktualisieren. Es hat keine Auswirkungen auf kleinere Nodes.

Verbesserung der Skalierbarkeit

Bei Element 12.7 sind keine spezifischen Sequenzen mehr nötig, wenn einem vorhandenen Cluster mehrere Storage-Nodes mit Block- und Metadatenlaufwerken hinzugefügt werden müssen. Über die Element UI oder API können Sie einfach alle verfügbaren Laufwerke auswählen und dann alle Massenvorgänge gleichzeitig hinzufügen. Element 12.7 verwaltet die Datensynchronisierung automatisch, sodass alle Block-Services

gleichzeitig synchronisiert werden. Wenn die Block-Services für jeden Node die Synchronisierung abgeschlossen haben, kann das Metadatenlaufwerk dieses Node den Host-Volumes zugewiesen werden. Diese Verbesserung durch Skalierung reduziert deutlich die Latenz bei der Lesereaktionszeit und verhindert eine Verschlechterung der Performance, während Daten zwischen neu hinzugefügten Storage-Nodes synchronisiert werden.

Updates der Storage Node-Firmware

Element 12.7 enthält das Storage-Firmware-Bundle Version 2.164.0, das auch die Unterstützung neuer Systemkomponenten bietet. "Weitere Informationen .".

> In Element 12.7 sind keine neuen Firmware-Updates vorhanden. Basierend auf dem aktuellen Firmware-Bundle, das auf den Storage-Nodes ausgeführt wird, werden jedoch die kumulativen Updates beim Upgrade auf Element 12.7 installiert.

SolidFire Active IQ-Dokumentation

In der SolidFire Active IQ-Benutzeroberfläche können Sie jetzt auf der Seite QoS-Management navigieren, um Empfehlungen und Informationen zur Knotendrosselung für das Cluster anzuzeigen. Darüber hinaus wird auf dem Cluster-Dashboard jetzt die Gesamtanzahl der Snapshots angezeigt. Weitere aktuelle Verbesserungen sind das Hinzufügen primärer und sekundärer Node-Informationen für aktive Volumes und des durchschnittlichen Durchsatzes, der IOPS-Werte und der durchschnittlichen Latenz der letzten 30 Minuten auf primären Volumes auf einem Node.

Sie haben jetzt über die Dokumentation der Element Software Zugriff auf die SolidFire Active IQ Dokumentation. "Weitere Informationen .".

NetApp Bugs Online enthält gelöste und bekannte Probleme

Gelöste und bekannte Probleme sind im NetApp Bugs Online-Tool aufgeführt. Sie können diese Themen für Element Software und andere Produkte hier durchsuchen "NetApp Bugs Online".

Element 12.5

Erfahren Sie mehr über die Neuerungen in Element 12.5.

Verbesserter Zugriff auf Storage-Nodes

Element 12.5 bietet mithilfe signierter SSH-Zertifikate einen verbesserten Remote-Zugriff auf einzelne Knoten. Für sicheren Remote-Zugriff auf Storage-Nodes wird ein neues lokales Benutzerkonto mit beschränkter Berechtigung aufgerufen `sfreadonly` Wird jetzt während RTFI eines Speicherknotens erstellt. Der `sfreadonly` Account ermöglicht den Zugriff auf das Backend des Storage-Nodes zu grundlegenden Wartungs- oder Fehlerbehebungszwecken. Sie können nun die konfigurieren `supportAdmin` Zugriffstyp für Cluster-Administratorbenutzer, damit der NetApp Support nach Bedarf auf das Cluster zugreifen kann

Verbessertes Management individueller Sicherungsdomänen

Element 12.5 verfügt über eine neue Benutzeroberfläche, mit der Sie vorhandene benutzerdefinierte Schutz-Domains schnell und einfach anzeigen und neue benutzerdefinierte Schutz-Domains konfigurieren können.

Neue und verbesserte Fehler, Ereignisse und Warnmeldungen im Cluster

Element 12.5 verbessert die Fehlerbehebung im System durch die Einführung der neuen Cluster-Fehlercodes

`BmcSelfTestFailed` Und `CpuThermalEventThreshold`. Element 12.5 enthält auch Verbesserungen der Robustheit bei vorhandenen Cluster-Ereignissen und Warnungen, z. B. `nodeOffline`, `volumeOffline`, `driveHealthFault`, `networkEvent`, und `cSumEvent`.

Aktivieren Sie die Softwareverschlüsselung im Ruhezustand über die Benutzeroberfläche Cluster erstellen

Durch Hinzufügen eines neuen Kontrollkästchens in der Benutzeroberfläche „Cluster erstellen“ bietet Element 12.5 die Möglichkeit, während der Cluster-Erstellung Cluster-übergreifende Softwareverschlüsselung für SolidFire All-Flash-Storage-Cluster zu aktivieren.

Updates der Storage Node-Firmware

Element 12.5 umfasst Firmware-Updates für Storage-Nodes. "Weitere Informationen .".

Erhöhte Sicherheit

Element 12.5 enthält die Minderung, die das Risiko der Element Software gegenüber der Apache Log4j-Sicherheitsanfälligkeit schließt. NetApp SolidFire Storage-Cluster mit aktivierter Funktion Virtual Volumes (VVols) sind der Apache Log4j Sicherheitsanfälligkeit ausgesetzt. Informationen zum Workaround für die Sicherheitsanfälligkeit von Apache Log4j in der NetApp Element-Software finden Sie im KB-Artikel.

Wenn Sie Element 11.x, 12.0 oder 12.2 verwenden oder sich Ihr Storage-Cluster bereits bei Element 12.3 oder 12.3.1 befindet und die VVols-Funktion aktiviert ist, sollten Sie ein Upgrade auf 12.5 durchführen.

Element 12.5 umfasst außerdem mehr als 120 CVE-Sicherheitsvorkehrungen.

Weitere Informationen

- "Versionshinweise zu NetApp Hybrid Cloud Control and Management Services"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Dokumentationszentrum für frühere Versionen"
- "NetApp HCI-Dokumentation"
- "Unterstützte Storage-Firmware-Versionen für SolidFire Storage-Nodes"

Konzepte

Lernen Sie grundlegende Konzepte in Bezug auf Element Software kennen.

- "Produktübersicht"
- Übersicht über die Architektur von SolidFire
- Knoten
- Cluster
- "Sicherheit"
- Konten und Berechtigungen
- "Volumes"
- Datensicherung
- Leistung und Servicequalität

Produktübersicht

Ein SolidFire All-Flash-Storage-System besteht aus separaten Hardwarekomponenten (Laufwerke und Nodes), die in einem einzelnen Pool der Storage-Ressourcen kombiniert werden. Dieser Unified Cluster stellt ein einziges Storage-System zur Verwendung durch externe Clients dar und wird mit der NetApp Element Software gemanagt.

Mit der Element Schnittstelle, der API oder anderen Managementtools können Sie die Kapazität und Performance des SolidFire Cluster-Storage überwachen und Storage-Aktivitäten in einer mandantenfähigen Infrastruktur managen.

Funktionen der SolidFire

Ein SolidFire System umfasst folgende Funktionen:

- Bietet hochperformanten Storage für Ihre große Private-Cloud-Infrastruktur
- Flexible Skalierung bei sich ändernden Storage-Anforderungen
- Verwendet eine API-gestützte Softwareschnittstelle für Storage-Managementelemente
- Garantierte Performance dank Quality of Service-Richtlinien
- Umfasst einen automatischen Lastausgleich über alle Nodes im Cluster hinweg
- Automatische Ausbalancierung von Clustern beim Hinzufügen oder Entfernen von Nodes

SolidFire Implementierung

Verwenden Sie von NetApp bereitgestellte und in NetApp Element Software integrierte Storage-Nodes.

"Übersicht über die All-Flash-Storage-Architektur von SolidFire"

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"

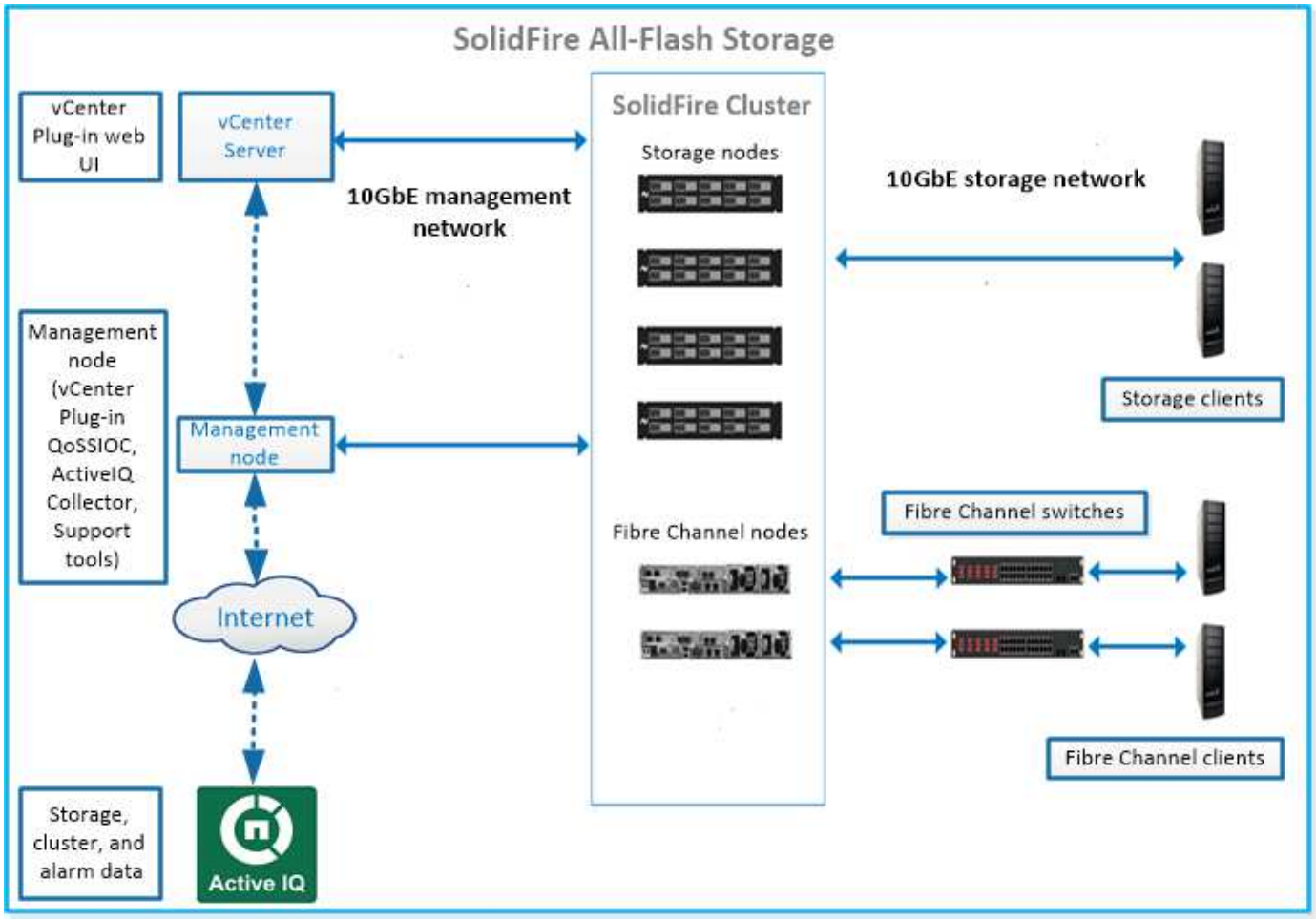
Architektur und Komponenten

Erfahren Sie mehr über die SolidFire -Architektur.

Ein SolidFire All-Flash-Storage-System besteht aus separaten Hardwarekomponenten (Laufwerk und Nodes), die in einem Pool von Storage-Ressourcen kombiniert werden. Dabei wird die NetApp Element Software unabhängig auf jedem Node ausgeführt. Dieses einzelne Storage-System wird als Einheit über die UI, die API und andere Managementtools von Element Software gemanagt.

Ein SolidFire Storage-System umfasst die folgenden Hardwarekomponenten:

- **Cluster**: Der Hub des SolidFire Speichersystems, das eine Ansammlung von Knoten ist.
- **Knoten**: Die Hardware-Komponenten in einem Cluster gruppiert. Es gibt zwei Node-Typen:
  - Storage-Nodes: Bei Servern handelt es sich um eine Sammlung von Laufwerken
  - Fibre Channel-Nodes (FC), die Sie zum Herstellen einer Verbindung mit FC-Clients verwenden
- **Laufwerke**: Wird in Speicherknoten verwendet, um Daten für den Cluster zu speichern. Ein Storage-Node enthält zwei Laufwerkstypen:
  - Volume-Metadaten speichern Informationen, die Volumes und andere Objekte innerhalb eines Clusters definieren.
  - Block-Laufwerke speichern Datenblöcke für Volumes.



Sie können das System über die Element Web-UI und andere kompatible Tools verwalten, überwachen und aktualisieren:

- "SolidFire-Softwareschnittstellen"
- "SolidFire Active IQ"
- "Management-Node für Element Software"
- "Management Services"

Allgemeine URLs

Dies sind die allgemeinen URLs, die Sie mit einem SolidFire All-Flash-Storage-System verwenden:

URL	Beschreibung
`https://[storage cluster MVIP address]`	Zugreifen auf die Benutzeroberfläche der NetApp Element Software
`https://activeiq.solidfire.com`	Überwachen Sie Ihre Daten und erhalten Sie Warnmeldungen zu Performance-Engpässen oder potenziellen Systemproblemen.
`https://[management node IP address]`	Der Zugriff auf NetApp Hybrid Cloud Control ermöglicht Ihnen, Ihre Services für die Storage-Installation und -Aktualisierung zu aktualisieren.
`https://[IP address]:442`	Greifen Sie über die UI pro Node auf Netzwerk- und Cluster-Einstellungen zu und nutzen Sie Systemtests und Dienstprogramme. "Weitere Informationen ."
`https://[management node IP address]/mnode`	Nutzen Sie DIE REST-API für Managementservices und andere Funktionen vom Management-Node."Weitere Informationen ."
`https://[management node IP address]:9443`	Registrieren Sie das vCenter Plug-in-Paket im vSphere Web Client."Weitere Informationen ."

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

SolidFire-Softwareschnittstellen

Sie können ein SolidFire Storage-System mit verschiedenen NetApp Element Software-Schnittstellen und Integrations-Utilities verwalten.

Optionen

- Benutzeroberfläche der NetApp Element Software
- NetApp Element Software-API
- NetApp Element Plug-in für vCenter Server
- NetApp Hybrid Cloud Control

- UIs für Managementknoten
- Zusätzliche Integrations-Tools

Benutzeroberfläche der NetApp Element Software

Ermöglicht die Einrichtung von Element Storage, die Überwachung von Cluster-Kapazität und -Performance und das Management von Storage-Aktivitäten in einer mandantenfähigen Infrastruktur. Element ist das Storage-Betriebssystem, das Herzstück eines SolidFire Clusters ist. Element Software wird unabhängig auf allen Nodes im Cluster ausgeführt und ermöglicht den Nodes des Clusters die Kombination der Ressourcen, die externen Clients als einzelnes Storage-System präsentiert werden. Element Software ist für die gesamte Clusterkoordination, den Umfang und das Management des Systems verantwortlich. Die Softwareschnittstelle basiert auf der Element API.

"Storage-Management mit Element Software"

NetApp Element Software-API

Ermöglicht die Verwendung einer Reihe von Objekten, Methoden und Routinen zum Storage Management. Die Element-API basiert auf dem JSON-RPC-Protokoll über HTTPS. Sie können API-Vorgänge in der Element-UI überwachen, indem Sie das API-Protokoll aktivieren. Dadurch können Sie die Methoden anzeigen, die an das System ausgegeben werden. Sie können sowohl Anfragen als auch Antworten aktivieren, um zu sehen, wie das System auf die ausgestellten Methoden antwortet.

"Storage-Management mit der Element API"

NetApp Element Plug-in für vCenter Server

Ermöglicht die Konfiguration und das Management von Storage-Clustern mit Element Software über eine alternative Schnittstelle für die Element UI in VMware vSphere.

"NetApp Element Plug-in für vCenter Server"

NetApp Hybrid Cloud Control

Ermöglicht die Aktualisierung von Element-Storage- und Managementservices sowie das Management von Storage-Ressourcen über die NetApp Hybrid Cloud Control Schnittstelle.

"Management und Monitoring von Storage mit NetApp Hybrid Cloud Control"

UIs für Managementknoten

Der Managementknoten enthält zwei UIs: Eine Benutzeroberfläche zur Verwaltung VON REST-basierten Diensten und eine Benutzeroberfläche pro Node zur Verwaltung von Netzwerk- und Clustereinstellungen sowie Betriebssystemtests und Dienstprogrammen. Über DIE REST-API-UI steht ein Menü mit Service-bezogenen APIs zur Verfügung, die die Service-basierte Systemfunktionalität vom Management-Node aus steuern.

Zusätzliche Integrations-Tools

Obwohl Sie Ihren Storage in der Regel mit NetApp Element, der NetApp Element API und dem NetApp Element Plug-in für vCenter Server managen, können Sie auf den Storage mithilfe weiterer Integrationstools und -Tools zugreifen.

Element CLI

"Element CLI" Ermöglicht die Steuerung eines SolidFire Storage-Systems über eine Befehlszeilenschnittstelle, ohne die Element API verwenden zu müssen.

Element PowerShell Tools

"Element PowerShell Tools" Aktivieren Sie die Verwendung einer Sammlung von Microsoft Windows PowerShell Funktionen, die die Element API zum Managen eines SolidFire Storage-Systems verwenden.

Element-SDKs

"Element-SDKs" Ermöglichen Sie die Verwaltung Ihres SolidFire-Clusters mithilfe folgender Tools:

- Element Java SDK: Ermöglicht Programmierern die Integration der Element-API in die Java-Programmiersprache.
- Element .NET SDK: Ermöglicht Programmierern die Integration der Element-API in die .NET-Programmierplattform.
- Element Python SDK: Ermöglicht Programmierern die Integration der Element-API in die Programmiersprache Python.

SolidFire Postman API Testsuite

Ermöglicht Programmierern, eine Sammlung von zu verwenden "Postman" Funktionen, die Element-API-Aufrufe testen.

SolidFire Storage Replication Adapter

"SolidFire Storage Replication Adapter" Die Integration in VMware Site Recovery Manager (SRM) ermöglicht die Kommunikation mit replizierten SolidFire Storage-Clustern und ermöglicht die Ausführung unterstützter Workflows.

SolidFire VRO

"SolidFire VRO" Einfache Möglichkeit, die Element API für das Management Ihres SolidFire Storage-Systems mit VMware vRealize Orchestrator zu verwenden

SolidFire VSS Provider

"SolidFire VSS Provider" Integriert VSS-Schattenkopien in Element Snapshots und Klonen.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

SolidFire Active IQ

"SolidFire Active IQ" Ist ein webbasiertes Tool, das kontinuierlich aktualisierte historische Ansichten von clusterweiten Daten bietet. Sie können Benachrichtigungen für bestimmte Ereignisse, Schwellenwerte oder Metriken einrichten. Mit SolidFire Active IQ können Sie die Performance und Kapazität des Systems überwachen und über den Cluster-Zustand auf dem Laufenden bleiben.

Folgende Informationen zu Ihrem System finden Sie im SolidFire Active IQ:

- Anzahl der Nodes und Status der Nodes: Ordnungsgemäß, offline oder Fehler
- Grafische Darstellung der CPU-, Speichernutzung und Knotendrosselung
- Details zum Node, z. B. Seriennummer, Steckplatz im Chassis, Modell und Version der NetApp Element Software, die auf dem Storage-Node ausgeführt wird
- CPU- und Storage-bezogene Informationen zu Virtual Machines

Weitere Informationen zu SolidFire Active IQ finden Sie im "SolidFire Active IQ-Dokumentation".

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"
- "NetApp Support-Website gt; Tools für Active IQ"

Management-Node für Element Software

Der "Management-Node (mNode)" Ist eine Virtual Machine, die mit einem oder mehreren auf Element basierenden Storage-Clustern parallel ausgeführt wird. Er dient als Upgrade und zur Bereitstellung von Systemservices wie Monitoring und Telemetrie, zum Management von Cluster-Ressourcen und -Einstellungen, zur Ausführung von Systemtests und Dienstprogrammen und zur Aktivierung des NetApp Support-Zugriffs zur Fehlerbehebung.

Der Management-Node interagiert mit einem Storage-Cluster, um Managementaktionen auszuführen, ist jedoch nicht Mitglied des Storage-Clusters. Managementknoten erfassen regelmäßig über API-Aufrufe Informationen über das Cluster und melden diese Informationen zur Remote-Überwachung an Active IQ (sofern aktiviert). Management-Nodes sind auch für die Koordinierung von Software-Upgrades der Cluster-Nodes verantwortlich.

Ab Element 11.3 fungiert der Management Node als Microservice-Host, wodurch sich ausgewählte Softwareservices schneller außerhalb der Hauptversionen aktualisieren lassen. Diese Microservices oder "Management Services" Werden häufig als Service-Bundles aktualisiert.

Managementservices für SolidFire All-Flash-Storage

Ab der Version von Element 11.3 werden **Management Services** auf dem gehostet "Management-Node", Ermöglicht schnellere Updates von ausgewählten Software-Dienstleistungen außerhalb der Hauptversionen.

Managementservices bieten zentrale und erweiterte Managementfunktionen für SolidFire All-Flash-Storage. Hierzu zählen auch diese Services "NetApp Hybrid Cloud Control", Active IQ Systemtelemetrie, Protokollierung und Service-Updates sowie der QoSSIOC-Service für das Element Plug-in für vCenter.

Weitere Informationen zu "Management Services-Releases".

Knoten

Nodes sind Hardware- oder virtuelle Ressourcen, die in einem Cluster gruppiert werden, um Block-Storage- und Computing-Funktionen bereitzustellen.

NetApp Element Software definiert verschiedene Node-Rollen für ein Cluster. Die Typen der Node-Rollen sind die folgenden:

- Management-Node
- Storage-Node
- Fibre Channel-Node

Nodes-Status Abhängig von Cluster-Zuordnung.

Management-Node

Ein Management-Node ist eine Virtual Machine, mit der Systemservices wie Monitoring und Telemetrie aktualisiert und bereitgestellt, Cluster-Ressourcen und -Einstellungen gemanagt, Systemtests und Dienstprogramme ausgeführt und der NetApp Support-Zugriff zur Fehlerbehebung aktiviert werden."Weitere Informationen ."

Storage-Node

Ein SolidFire-Storage-Node ist ein Server, der eine Sammlung von Laufwerken enthält, die über die Bond10G-Netzwerkschnittstelle miteinander kommunizieren. Laufwerke im Node enthalten Block- und Metadatenspeicherplatz für den Daten-Storage und das Datenmanagement. Jeder Node enthält ein Factory Image der NetApp Element Software.

Storage-Nodes weisen folgende Merkmale auf:

- Jeder Node hat einen eindeutigen Namen. Wenn ein Node-Name nicht von einem Administrator angegeben wird, ist er standardmäßig SF-XXXX, wobei XXXX vier zufällige Zeichen enthält, die vom System generiert werden.
- Jeder Node verfügt über einen eigenen hochperformanten NVRAM-Schreib-Cache (Non-Volatile Random Access Memory), um die Systemperformance insgesamt zu verbessern und die Schreiblatenz zu reduzieren.
- Jeder Node ist mit zwei Netzwerken verbunden, Storage und Management, jedes mit zwei unabhängigen Links, um für Redundanz und Performance zu sorgen. Jeder Node benötigt in jedem Netzwerk eine IP-Adresse.
- Sie können mit neuen Storage-Nodes ein Cluster erstellen oder einem vorhandenen Cluster Storage Nodes hinzufügen, um die Storage-Kapazität und Performance zu steigern.
- Nodes können jederzeit ohne Serviceunterbrechung zum Cluster hinzugefügt oder aus dem Cluster entfernt werden.

Fibre Channel-Node

SolidFire Fibre Channel Nodes stellen Konnektivität zu einem Fibre Channel Switch bereit, den Sie mit Fibre Channel Clients verbinden können. Fibre Channel Nodes fungieren als Protokollkonverter zwischen den Fibre Channel- und iSCSI-Protokollen. So können Sie jedem neuen oder vorhandenen SolidFire Cluster Fibre Channel-Konnektivität hinzufügen.

Fibre-Channel-Nodes weisen folgende Merkmale auf:

- Fibre Channel Switches managen den Zustand der Fabric und bieten optimierte Verbindungen.
- Der Datenverkehr zwischen zwei Ports fließt nur durch die Switches; er wird nicht an einen anderen Port übertragen.
- Der Ausfall eines Ports ist isoliert, hat keine Auswirkungen auf den Betrieb anderer Ports.
- Mehrere Ports können gleichzeitig in einem Fabric kommunizieren.

Node-Status des Vorgangs

Je nach Konfigurationsstufe kann ein Node in einem von mehreren Status vorhanden sein.

- **Verfügbar**

  Dem Node ist kein Cluster-Name zugewiesen, der noch nicht Teil eines Clusters ist.

- **Ausstehend**

  Der Node ist konfiguriert und kann einem zugewiesenen Cluster hinzugefügt werden.

  Für den Zugriff auf den Node ist keine Authentifizierung erforderlich.

- **Ausstehend Aktiv**

  Das System installiert gerade kompatible Element Software auf dem Node. Nach Abschluss der Migration wird der Node in den Status „aktiv“ verschoben.

- * Aktiv*

  Der Knoten ist an einem Cluster beteiligt.

  Zum Ändern des Node ist eine Authentifizierung erforderlich.

In jedem dieser Zustände werden einige Felder schreibgeschützt.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Cluster

Ein Cluster ist der Hub eines SolidFire Storage-Systems und besteht aus einer Sammlung von Nodes. Sie müssen mindestens vier Nodes in einem Cluster aufweisen, damit die SolidFire Storage-Effizienz realisiert werden kann. Ein Cluster wird im Netzwerk als einzelne logische Gruppe angezeigt und kann dann als Block-Storage genutzt werden.

Durch das Erstellen eines neuen Clusters wird ein Node als Kommunikationsinhaber für ein Cluster initialisiert und stellt die Netzwerkkommunikation für jeden Node im Cluster her. Dieser Prozess wird nur einmal für jedes neue Cluster durchgeführt. Sie können ein Cluster mithilfe der Element UI oder der API erstellen.

Sie können ein Cluster horizontal skalieren, indem Sie weitere Nodes hinzufügen. Wenn Sie einen neuen Node hinzufügen, wird der Service nicht unterbrochen, und der Cluster nutzt die Performance und Kapazität des neuen Node automatisch.

Administratoren und Hosts können über virtuelle IP-Adressen auf das Cluster zugreifen. Jeder Node im Cluster kann die virtuellen IP-Adressen hosten. Die Management Virtual IP (MVIP) ermöglicht das Clustermanagement über eine 1-GbE-Verbindung, während die Speicher-virtuelle IP (SVIP) den Host-Zugriff auf Speicher über eine 10-GbE-Verbindung ermöglicht. Diese virtuellen IP-Adressen ermöglichen konsistente Verbindungen unabhängig von der Größe oder dem Aufbau eines SolidFire Clusters. Wenn ein Node, der eine virtuelle IP-Adresse hostet, ausfällt, beginnt ein anderer Node im Cluster mit dem Hosten der virtuellen IP-Adresse.

Ab Element Version 11.0 können Nodes mit IPv4, IPv6 oder beiden Adressen für ihr Managementnetzwerk konfiguriert werden. Dies gilt sowohl für Storage-Nodes als auch für Management-Nodes, mit Ausnahme von Management-Node 11.3 und höher, der IPv6 nicht unterstützt. Beim Erstellen eines Clusters kann nur eine einzelne IPv4- oder IPv6-Adresse für den MVIP verwendet werden, und der entsprechende Adresstyp muss auf allen Knoten konfiguriert werden.

Mehr auf Clustern

- Autorisierende Storage-Cluster
- Drittelregel
- Ungenutzte Kapazität
- Storage-Effizienz
- Storage Cluster Quorum

Autorisierende Storage-Cluster

Der Storage-Cluster ist der Storage-Cluster, mit dem NetApp Hybrid Cloud Control Benutzer authentifizieren kann.

Wenn der Management-Node nur über einen Storage-Cluster verfügt, dann ist er das autorisierende Cluster. Wenn der Management-Node zwei oder mehr Storage-Cluster umfasst, wird einem dieser Cluster als autorisierende Cluster zugewiesen. Nur Benutzer dieses Clusters können sich bei NetApp Hybrid Cloud Control anmelden. Um herauszufinden, welcher Cluster der maßgebliche Cluster ist, können Sie den verwenden `GET /mnode/about` API: In der Antwort die IP-Adresse im `token_url` Feld ist die virtuelle Management-IP-Adresse (MVIP) des autorisierenden Storage-Clusters. Wenn Sie versuchen, sich bei NetApp Hybrid Cloud Control als Benutzer anzumelden, der sich nicht auf dem autorisierenden Cluster befindet, schlägt der Anmeldeversuch fehl.

Viele Funktionen von NetApp Hybrid Cloud Control wurden für den Einsatz mit mehreren Storage-Clustern entwickelt. Allerdings schränkteutig die Authentifizierung und Autorisierung sein. Die Authentifizierung und Autorisierung im Zusammenhang mit der Authentifizierung besteht darin, dass der Benutzer aus dem autorisierenden Cluster Aktionen auf anderen Clustern ausführen kann, die an NetApp Hybrid Cloud Control gebunden sind, auch wenn diese nicht Anwender in den anderen Storage-Clustern sind.

Bevor Sie mit der Verwaltung mehrerer Storage-Cluster fortfahren, sollten Sie sicherstellen, dass die auf den Standards definierten Benutzer auf allen anderen Storage-Clustern mit denselben Berechtigungen definiert sind. Sie können Benutzer über das verwalten "Benutzeroberfläche von Element Software".

Siehe "Erstellen und Managen von Storage-Cluster-Assets" Weitere Informationen zur Arbeit mit den Management-Node-Storage-Cluster-Assets.

Drittelregel

Bei einer Kombination von Storage-Node-Typen in einem NetApp SolidFire Storage Cluster kann kein einzelner Storage-Node mehr als 33 % der gesamten Storage Cluster-Kapazität enthalten.

Ungenutzte Kapazität

Wenn ein neu hinzugefügter Node mehr als 50 % der gesamten Cluster-Kapazität beträgt, wird einige der Kapazitäten dieses Node unbrauchbar („ungenutzt“) gemacht, sodass die Kapazitätsregel eingehalten wird. Dies bleibt der Fall, bis mehr Storage-Kapazität hinzugefügt wird. Wenn ein sehr großer Node hinzugefügt wird, der auch die Kapazitätsregel nicht befolgt, kann der zuvor isolierte Node nicht mehr ungenutzt bleiben, während der neu hinzugefügte Node ungenutzt ist. Kapazität sollte immer paarweise hinzugefügt werden, um dies zu vermeiden. Wenn ein Node ungenutzt wird, ist ein geeigneter Cluster-Fehler zu werfen.

Storage-Effizienz

NetApp SolidFire Storage Cluster nutzen Deduplizierung, Komprimierung und Thin Provisioning, um den physischen Storage-Bedarf für das Speichern eines Volumes zu verringern.

- **Komprimierung**

  Bei der Komprimierung wird der physische Storage-Bedarf eines Volumes reduziert, indem Datenblöcke in Komprimierungsgruppen kombiniert werden, die jeweils als einzelne Blöcke gespeichert werden.

- **Deduplizierung**

  Dank der Deduplizierung wird die Menge des für ein Volume erforderlichen physischen Storage reduziert, indem doppelte Datenblöcke verworfen werden.

- **Thin Provisioning**

  Ein Thin Provisioning-Volume oder eine LUN ist eine LUN, bei der kein vorab reservierter Storage reserviert wird. Stattdessen wird der Storage dynamisch nach Bedarf zugewiesen. Freier Speicherplatz wird wieder dem Storage-System freigegeben, wenn die Daten vom Volume oder von der LUN gelöscht werden

Storage Cluster Quorum

Element Software erstellt ein Storage-Cluster von ausgewählten Nodes, wobei eine replizierte Datenbank der Clusterkonfiguration erhalten bleibt. Zur Teilnahme am Cluster-Ensemble sind mindestens drei Nodes erforderlich, um das Quorum für die Cluster-Ausfallsicherheit zu erhalten.

Sicherheit

Wenn Sie Ihr SolidFire All-Flash-Storage-System nutzen, werden Ihre Daten durch branchenübliche Sicherheitsprotokolle geschützt.

Verschlüsselung für Daten im Ruhezustand (Hardware)

Alle Laufwerke in Storage-Nodes können verschlüsselt werden. Dazu wird die AES 256-Bit-Verschlüsselung auf Laufwerksebene verwendet. Jedes Laufwerk verfügt über einen eigenen Verschlüsselungsschlüssel, der beim ersten Initialized des Laufwerks erstellt wird. Wenn Sie die Verschlüsselungsfunktion aktivieren, wird ein

Cluster-weites Passwort erstellt und Datenblöcke des Passworts werden dann auf alle Nodes im Cluster verteilt. Kein Single Node speichert das gesamte Passwort. Das Passwort wird dann verwendet, um den gesamten Zugriff auf die Laufwerke kennwortgeschützt zu machen. Das Kennwort ist erforderlich, um das Laufwerk zu entsperren und wird dann nur benötigt, wenn die Stromversorgung vom Laufwerk entfernt oder das Laufwerk gesperrt ist.

"Aktivieren der Hardware-Verschlüsselung für Daten im Ruhezustand" Beeinträchtigt die Performance oder Effizienz des Clusters nicht. Wenn ein verschlüsselungsfähiges Laufwerk oder Node mit der Element API oder der Element UI aus der Cluster-Konfiguration entfernt wird, wird die Verschlüsselung im Ruhezustand auf den Laufwerken deaktiviert. Nachdem das Laufwerk entfernt wurde, kann das Laufwerk mit dem sicher gelöscht werden `SecureEraseDrives` API-Methode. Wenn ein physisches Laufwerk oder ein Knoten gewaltsam entfernt wird, bleiben die Daten durch das Cluster-weite Passwort und die individuellen Verschlüsselungsschlüssel des Laufwerks geschützt.

Verschlüsselung für Daten im Ruhezustand (Software)

Bei einem anderen Verschlüsselungstyp, der Softwareverschlüsselung im Ruhezustand, können alle Daten, die in einem Storage-Cluster auf SSDs geschrieben wurden, verschlüsselt werden. "Wenn aktiviert", Es verschlüsselt alle Daten geschrieben und entschlüsselt alle Daten automatisch in der Software gelesen. Softwareverschlüsselung im Ruhezustand spiegelt die SED-Implementierung (Self-Encrypting Drive) in der Hardware, um Datensicherheit ohne SED zu gewährleisten.

Bei SolidFire All-Flash-Storage-Clustern muss die Softwareverschlüsselung im Ruhezustand während der Cluster-Erstellung aktiviert sein und nach dem Erstellen des Clusters nicht deaktiviert werden können.

Sowohl die Software- als auch die Hardware-basierte Verschlüsselung im Ruhezustand können unabhängig voneinander oder kombiniert werden.

Externes Verschlüsselungskeymanagement

Sie können Element Software für das Management der Storage-Cluster-Verschlüsselungen konfigurieren, indem Sie einen KMIP-konformen (Key Management Service) eines Drittanbieters verwenden. Wenn Sie diese Funktion aktivieren, wird der Schlüssel für den Zugriff auf das Passwort für den gesamten Laufwerkszugriff des Storage-Clusters von einem von Ihnen angegebenen KMS gemanagt.

Element kann die folgenden wichtigen Managementservices nutzen:

- Gemalto SafeNet KeySecure
- SafeNet BEI KeySecure
- HyTrust KeyControl
- Vormetric Data Security Manager
- IBM Security Key Lifecycle Manager

Weitere Informationen zur Konfiguration der externen Schlüsselverwaltung finden Sie unter "Erste Schritte mit externem Verschlüsselungsmanagement" Dokumentation.

Multi-Faktor-Authentifizierung

Multi-Faktor-Authentifizierung (MFA) ermöglicht es Benutzern, bei der Anmeldung mehrere Arten von Beweisen zur Authentifizierung bei der NetApp Element Web-UI oder der Storage-Node-UI vorzulegen. Sie können Element so konfigurieren, dass nur Multi-Faktor-Authentifizierung für Anmeldungen akzeptiert wird, die

sich in Ihr vorhandenes Benutzerverwaltungssystem und Ihren Identitäts-Provider integrieren lassen. Sie können das Element so konfigurieren, dass es sich in einen vorhandenen SAML 2.0-Identitätsanbieter integrieren lässt, der mehrere Authentisierungsschemata wie Passwort- und Textnachricht, Passwort- und E-Mail-Nachricht oder andere Methoden durchsetzen kann.

Sie können Multi-Faktor-Authentifizierung mit gängigen SAML 2.0-kompatiblen Identitäts-Providern (IDPs) wie Microsoft Active Directory Federation Services (ADFS) und Shibboleth kombinieren.

Informationen zur Konfiguration der Multi-Faktor-Authentifizierung finden Sie unter "Die Multi-Faktor-Authentifizierung aktivieren" Dokumentation.

FIPS 140-2 für HTTPS und Verschlüsselung von Daten im Ruhezustand

NetApp SolidFire Storage-Cluster unterstützen eine Verschlüsselung, die die Anforderungen des Federal Information Processing Standard (FIPS) 140-2 an kryptografische Module erfüllt. Sie können die Compliance mit FIPS 140-2 auf Ihrem SolidFire Cluster sowohl für HTTPS-Kommunikation als auch für Laufwerksverschlüsselung aktivieren.

Wenn Sie den FIPS 140-2 Betriebsmodus auf dem Cluster aktivieren, aktiviert das Cluster das NetApp Cryptographic Security Module (NCSM) und nutzt die zertifizierte Verschlüsselung nach FIPS 140-2 Level 1 für die gesamte Kommunikation über HTTPS mit der NetApp Element UI und den API. Sie verwenden das `EnableFeature` Element API mit dem `fips` Parameter zur Aktivierung der Verschlüsselung nach FIPS 140-2 HTTPS. Auf Storage-Clustern mit FIPS-kompatibler Hardware lässt sich mithilfe des auch FIPS-Laufwerksverschlüsselung für Daten im Ruhezustand aktivieren `EnableFeature` Element API mit dem `FipsDrives` Parameter.

Weitere Informationen zur Vorbereitung eines neuen Storage-Clusters auf die Verschlüsselung nach FIPS 140-2 finden Sie unter "Erstellen eines Clusters, das FIPS-Laufwerke unterstützt".

Weitere Informationen über die Aktivierung von FIPS 140-2 auf einem vorhandenen, vorbereiteten Cluster finden Sie unter "Die API für das EnableFeature-Element".

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Konten und Berechtigungen

Um die Storage-Ressourcen in Ihrem System zu verwalten und Zugriff zu gewähren, müssen Sie Konten für Systemressourcen einrichten.

Mit Element Storage können Sie folgende Typen von Konten erstellen und verwalten:

- Administratorkonten für das Storage-Cluster
- Benutzerkonten für Storage-Volume-Zugriff
- Maßgebliche Cluster-Benutzerkonten für NetApp Hybrid Cloud Control

Konten für Storage-Cluster-Administratoren

In einem Storage-Cluster mit NetApp Element Software können zwei Arten von Administratorkonten vorhanden sein:

- **Primary Cluster Administrator Account**: Dieses Administratorkonto wird beim Erstellen des Clusters erstellt. Dieses Konto ist das primäre administrative Konto mit der höchsten Zugriffsebene auf das Cluster. Dieses Konto ist analog zu einem Root-Benutzer in einem Linux-System. Sie können das Kennwort für dieses Administratorkonto ändern.
- **Cluster-Administratorkonto**: Sie können einem Cluster-Administratorkonto eine begrenzte Anzahl von Administratorzugriff zur Ausführung bestimmter Aufgaben innerhalb eines Clusters gewähren. Die jedem Cluster-Administratorkonto zugewiesenen Zugangsdaten werden zur Authentifizierung von API- und Element-UI-Anforderungen innerhalb des Storage-Systems verwendet.

Ein lokales (nicht-LDAP)-Cluster-Administratorkonto ist erforderlich, um über die UI pro Node auf aktive Knoten in einem Cluster zuzugreifen. Kontoanmeldeinformationen sind für den Zugriff auf einen Node, der noch nicht Teil eines Clusters ist, nicht erforderlich.

Das können Sie "Verwalten von Cluster-Administratorkonten" Indem Sie Cluster-Administratorkonten erstellen, löschen und bearbeiten, das Kennwort für den Cluster-Administrator ändern und LDAP-Einstellungen konfigurieren, um den Systemzugriff für Benutzer zu verwalten.

Benutzerkonten

Über Benutzerkonten werden der Zugriff auf die Storage-Ressourcen in einem softwarebasierten Netzwerk von NetApp Element gesteuert. Mindestens ein Benutzerkonto ist erforderlich, bevor ein Volume erstellt werden kann.

Wenn Sie ein Volume erstellen, wird es einem Konto zugewiesen. Wenn Sie ein virtuelles Volume erstellt haben, ist das Konto der Speichercontainer.

Folgende Aspekte sollten zusätzlich berücksichtigt werden:

- Das Konto enthält die CHAP-Authentifizierung, die für den Zugriff auf die ihm zugewiesenen Volumes erforderlich ist.
- Einem Konto können bis zu 2000 Volumes zugewiesen sein, aber ein Volume kann nur zu einem Konto gehören.
- Benutzerkonten können über den Erweiterungspunkt für die NetApp Element-Verwaltung verwaltet werden.

Autorisierende Cluster-Benutzerkonten

Autorisierte Cluster-Benutzerkonten können sich gegen alle Storage-Ressourcen authentifizieren, die mit der NetApp Hybrid Cloud Control Instanz der Nodes und Cluster verbunden sind. Mit diesem Konto können Sie Volumes, Konten, Zugriffsgruppen und mehr über alle Cluster hinweg verwalten.

Maßgebliche Benutzerkonten werden über die obere rechte Menü-Option „Benutzermanagement“ in der NetApp Hybrid Cloud Control gemanagt.

Der "Autorisierende Storage-Cluster" Ist der Storage-Cluster, den NetApp Hybrid Cloud Control zur Authentifizierung von Benutzern verwendet.

Bei der NetApp Hybrid Cloud Control können sich alle Benutzer, die auf dem autorisierenden Storage-Cluster erstellt wurden, anmelden. Benutzer, die auf anderen Storage Clustern erstellt wurden, können sich bei Hybrid Cloud Control nicht anmelden.

- Wenn der Management-Node nur über einen Storage-Cluster verfügt, dann ist er das autorisierende Cluster.

- Wenn der Management-Node zwei oder mehr Storage-Cluster umfasst, wird einem dieser Cluster als autorisierende Cluster zugewiesen. Nur Benutzer dieses Clusters können sich bei NetApp Hybrid Cloud Control anmelden.

Viele NetApp Hybrid Cloud Control Funktionen funktionieren zwar mit mehreren Storage-Clustern, jedoch bringen Authentifizierung und Autorisierung erforderliche Einschränkungen mit sich. Die Einschränkung der Authentifizierung und Autorisierung besteht darin, dass Benutzer aus dem autorisierenden Cluster Aktionen auf anderen Clustern ausführen können, die an NetApp Hybrid Cloud Control gebunden sind, auch wenn diese nicht in den anderen Storage-Clustern ausgeführt werden. Bevor Sie mit der Verwaltung mehrerer Storage-Cluster fortfahren, sollten Sie sicherstellen, dass die auf den Standards definierten Benutzer auf allen anderen Storage-Clustern mit denselben Berechtigungen definiert sind. Benutzer können über NetApp Hybrid Cloud Control gemanagt werden.

Volume-Konten

Volume-spezifische Konten gelten nur für den Storage Cluster, auf dem sie erstellt wurden. Mit diesen Konten können Sie Berechtigungen für bestimmte Volumes im Netzwerk festlegen, haben aber keine Auswirkungen außerhalb dieser Volumes.

Volume-Konten werden in der Tabelle „NetApp Hybrid Cloud Control Volumes“ gemanagt.

Storage

Volumes

Das Storage-System NetApp Element stellt Storage mithilfe von Volumes bereit. Volumes sind Blockgeräte, auf die über das Netzwerk von iSCSI- oder Fibre Channel-Clients zugegriffen wird.

Element Storage ermöglicht Ihnen das Erstellen, Anzeigen, Bearbeiten, Löschen, Klonen Sichern Sie Volumes für Benutzerkonten oder stellen Sie sie wieder her. Außerdem lassen sich Volumes in einem Cluster managen und Volumes in Volume-Zugriffsgruppen hinzufügen oder entfernen.

Persistente Volumes

Mithilfe persistenter Volumes können Management-Node-Konfigurationsdaten nicht lokal mit einer VM in einem bestimmten Storage-Cluster gespeichert werden, damit Daten auch bei Verlust oder Entfernung von Management-Nodes erhalten bleiben. Persistente Volumes sind eine optionale, jedoch empfohlene Management-Node-Konfiguration.

Eine Option zum Aktivieren persistenter Volumes ist in den Installations- und Upgrade-Skripten bei enthalten "Implementieren eines neuen Management-Node". Persistente Volumes sind Volumes auf einem Element Software-basierten Storage-Cluster, die Konfigurationsinformationen für die Host-Management-Node-VM enthalten, die über den Lebenszyklus der VM hinaus bestehen bleiben. Wenn der Management-Node verloren geht, kann eine VM mit dem Ersatz-Management-Node eine Verbindung herstellen und Konfigurationsdaten für die verlorene VM wiederherstellen.

Persistente Volume-Funktion, sofern diese während der Installation oder des Upgrades aktiviert ist, erstellt automatisch mehrere Volumes. Diese Volumes können, wie jedes softwarebasierte Element Volume, je nach Ihren Vorliebe und Installation über die Web-UI in Element Software, das NetApp Element Plug-in für vCenter Server oder die API angezeigt werden. Persistente Volumes müssen mit einer iSCSI-Verbindung zum Management-Node in Betrieb sein, um die aktuellen Konfigurationsdaten beizubehalten, die für eine Recovery verwendet werden können.

Persistente Volumes, die mit Managementservices verbunden sind, werden bei der Installation oder bei einem Upgrade einem neuen Konto erstellt und zugewiesen. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie die Volumes oder ihr zugehörigem Konto nicht

Virtuelle Volumes (VVols)

VSphere Virtual Volumes ist ein Storage-Paradigma für VMware, das einen Großteil des Storage-Managements für vSphere vom Storage-System in VMware vCenter verschiebt. Mit Virtual Volumes (VVols) können Sie Storage den Anforderungen einzelner Virtual Machines zuweisen.

Bindungen

Der NetApp Element Cluster wählt einen optimalen Protokollendpunkt, erstellt eine Bindung, die den ESXi Host und das virtuelle Volume dem Protokollendpunkt zugeordnet und die Bindung an den ESXi Host zurückgibt. Nach der Bindung kann der ESXi Host I/O-Vorgänge mit dem gebundenen virtuellen Volume ausführen.

Protokollendpunkte

VMware ESXi Hosts verwenden logische I/O-Proxys – als Protokollendpunkte bezeichnet –, um mit virtuellen Volumes zu kommunizieren. ESXi Hosts binden virtuelle Volumes an Protokollendpunkte, um I/O-Vorgänge durchzuführen. Wenn eine virtuelle Maschine auf dem Host einen I/O-Vorgang durchführt, leitet der zugehörige Protokollendpunkt den I/O-Vorgang an das virtuelle Volume, mit dem sie gekoppelt wird.

Protokollendpunkte in einem NetApp Element-Cluster funktionieren als logische SCSI-Verwaltungseinheiten. Jeder Protokollendpunkt wird automatisch vom Cluster erstellt. Für jeden Node in einem Cluster wird ein entsprechender Protokollendpunkt erstellt. Ein Cluster mit vier Nodes verfügt beispielsweise über vier Protokollendpunkte.

ISCSI ist das einzige unterstützte Protokoll für die NetApp Element-Software. Das Fibre Channel-Protokoll wird nicht unterstützt. Protokollendpunkte können nicht von einem Benutzer gelöscht oder geändert werden, sind keinem Konto zugeordnet und können nicht einer Volume-Zugriffsgruppe hinzugefügt werden.

Storage-Container

Storage-Container sind logische Konstrukte, die NetApp Element-Konten zugewiesen werden und für die Berichterstellung und Ressourcenzuweisung verwendet werden. Sie bilden die Brutto-Storage-Kapazität oder aggregierte Storage-Funktionen, die das Storage-System virtuellen Volumes zur Verfügung stellen kann. Ein VVol Datastore, der in vSphere erstellt wird, wird einem einzelnen Storage-Container zugeordnet. Ein einzelner Storage-Container verfügt standardmäßig über alle verfügbaren Ressourcen des NetApp Element-Clusters. Falls mehr granulare Governance für Mandantenfähigkeit erforderlich ist, können auch mehrere Storage Container erstellt werden.

Storage-Container funktionieren wie herkömmliche Konten und können sowohl virtuelle Volumes als auch herkömmliche Volumes enthalten. Pro Cluster werden maximal vier Storage-Container unterstützt. Zur Nutzung der VVols Funktionen ist mindestens ein Storage-Container erforderlich. Sie können Storage-Container bei der VVols Erstellung in vCenter erkennen.

VASA-Provider

Um vSphere auf die vVol Funktion im NetApp Element Cluster aufmerksam zu machen, muss der vSphere Administrator den NetApp Element VASA Provider mit vCenter registrieren. Der VASA Provider ist der Out-of-

Band-Kontrollpfad zwischen vSphere und dem Element Cluster. Er ist verantwortlich für die Ausführung von Anfragen im Element Cluster im Auftrag von vSphere, z. B. die Erstellung von VMs, die Bereitstellung von VMs für vSphere und die Werbung für Storage-Funktionen für vSphere.

Der VASA Provider wird als Teil des Cluster-Master in der Element Software ausgeführt. Der Cluster-Master ist ein hochverfügbarer Service, der bei Bedarf ein Failover auf jeden Node im Cluster ermöglicht. Bei einem Failover des Cluster-Master übernimmt der VASA Provider die Lösung und stellt damit die Hochverfügbarkeit für den VASA-Provider sicher. Alle Provisionierungs- und Storage-Managementaufgaben verwenden den VASA-Provider, der alle erforderlichen Änderungen am Element Cluster übernimmt.

Registrieren Sie bei Element 12.5 und früheren Versionen nicht mehr als einen NetApp Element VASA Provider in einer einzelnen vCenter Instanz. Wenn ein zweiter NetApp Element VASA Provider hinzugefügt wird, macht das alle VVOL Datastores unzugänglich.

VASA-Unterstützung für bis zu 10 vCenters steht als Upgrade-Patch zur Verfügung, wenn Sie bereits einen VASA Provider bei vCenter registriert haben. Folgen Sie zur Installation den Anweisungen im VASA39-Manifest und laden Sie die Datei .tar.gz aus dem herunter "NetApp Software-Downloads" Standort. Der NetApp Element VASA Provider verwendet ein NetApp Zertifikat. Bei diesem Patch wird das Zertifikat von vCenter nicht verändert, um mehrere vCenters für die Verwendung von VASA und VVols zu unterstützen. Ändern Sie das Zertifikat nicht. Benutzerdefinierte SSL-Zertifikate werden von VASA nicht unterstützt.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Volume-Zugriffsgruppen

Durch die Erstellung und Nutzung von Volume-Zugriffsgruppen können Sie den Zugriff auf eine Gruppe von Volumes steuern. Wenn Sie einen Satz von Volumes und einen Satz von Initiatoren einer Volume-Zugriffsgruppe zuordnen, gewährt die Zugriffsgruppe diesen Initiatoren Zugriff auf diese Gruppe von Volumes.

Volume-Zugriffsgruppen im NetApp SolidFire Storage ermöglichen den Zugriff auf eine Sammlung von Volumes durch iSCSI-Initiator-IQNs oder Fibre Channel-WWPNs. Jeder IQN, den Sie einer Zugriffsgruppe hinzufügen, kann ohne CHAP-Authentifizierung auf jedes Volume in der Gruppe zugreifen. Jeder WWPN, den Sie einer Zugriffsgruppe hinzufügen, ermöglicht den Fibre-Channel-Netzwerkzugriff auf die Volumes in der Zugriffsgruppe.

Volume-Zugriffsgruppen verfügen über die folgenden Grenzen:

- Maximal 128 Initiatoren pro Volume-Zugriffsgruppe.
- Maximal 64 Zugriffsgruppen pro Volume.
- Eine Zugriffsgruppe kann aus maximal 2000 Volumes bestehen.
- Ein IQN oder WWPN kann nur zu einer Volume-Zugriffsgruppe gehören.
- Bei Fibre Channel Clustern kann ein einzelnes Volume zu maximal vier Zugriffsgruppen gehören.

Initiatoren

Initiatoren ermöglichen den Zugriff auf externe Clients auf Volumes in einem Cluster. Diese dienen als Einstiegspunkt für die Kommunikation zwischen Clients und Volumes. Sie können Initiatoren für CHAP-basierten Zugriff anstelle von kontenbasierten Speichervolumes verwenden. Wenn ein einzelner Initiator einer Volume-Zugriffsgruppe hinzugefügt wird, können die Mitglieder der Volume-Zugriffsgruppen auf alle der Gruppe hinzugefügten Storage Volumes zugreifen, ohne dass eine Authentifizierung erforderlich ist. Ein Initiator kann nur einer Zugriffsgruppe angehören.

Datensicherung

Zu den Datensicherungsfunktionen gehören Remote-Replizierung, Volume Snapshots, Volume-Klonen, Protection Domains und Hochverfügbarkeit mit Double Helix Technologie.

Element Storage-Datensicherung umfasst folgende Konzepte:

- Typen der Remote-Replizierung
- Volume Snapshots zur Datensicherung
- Volume-Klone
- Übersicht über Backup- und Restore-Prozesse für Element Storage
- Sicherungsdomänen
- Benutzerdefinierte Sicherungsdomänen
- Hochverfügbarkeit mit Double Helix

Typen der Remote-Replizierung

Die Remote-Replikation von Daten kann folgende Formen annehmen:

- Synchrone und asynchrone Replizierung zwischen Clustern
- Reine Snapshot Replizierung
- Replizierung zwischen Element und ONTAP Clustern mit SnapMirror

Weitere Informationen finden Sie unter "TR-4741: NetApp Element Software Remote Replication".

Synchrone und asynchrone Replizierung zwischen Clustern

Für Cluster mit NetApp Element Software ermöglicht Echtzeitreplizierung die schnelle Erstellung von Remote-Kopien von Volume-Daten.

Ein Storage-Cluster kann mit bis zu vier anderen Storage-Clustern gekoppelt werden. Sie können Volume-Daten für Failover- und Failback-Szenarien synchron oder asynchron von einem Cluster in einem Cluster-Paar replizieren.

Synchrone Replizierung

Die synchrone Replizierung repliziert die Daten kontinuierlich vom Quell-Cluster zum Ziel-Cluster und wird von Latenz, Paketverlust, Jitter und Bandbreite beeinträchtigt.

Synchrone Replizierung eignet sich für die folgenden Situationen:

- Replizierung mehrerer Systeme über kurze Entfernungen
- Ein Disaster-Recovery-Standort lokal an der Quelle
- Zeitkritische Applikationen und der Schutz von Datenbanken
- Business-Continuity-Applikationen, bei denen der sekundäre Standort als primärer Standort fungieren muss, wenn der primäre Standort ausfällt

Asynchrone Replizierung

Die asynchrone Replikation repliziert kontinuierlich Daten von einem Quellcluster zu einem Zielcluster, ohne auf die Bestätigungen aus dem Zielcluster zu warten. Während der asynchronen Replizierung werden Schreibvorgänge dem Client (Applikation) bestätigt, nachdem sie im Quell-Cluster durchgeführt wurden.

Asynchrone Replizierung eignet sich für die folgenden Situationen:

- Der Disaster-Recovery-Standort ist weit von der Quelle entfernt und die Applikation toleriert keine durch das Netzwerk verursachten Latenzen.
- Das Netzwerk, das die Quell- und Ziel-Cluster verbindet, weist Bandbreiteneinschränkungen auf.

Reine Snapshot Replizierung

Bei der Datensicherung nur mit Snapshots werden geänderte Daten zu einem bestimmten Zeitpunkt in ein Remote-Cluster repliziert. Es werden nur die Snapshots repliziert, die auf dem Quellcluster erstellt wurden. Aktive Schreibvorgänge vom Quell-Volume sind nicht.

Sie können die Häufigkeit der Snapshot Replikationen festlegen.

Die Snapshot Replizierung hat keine Auswirkungen auf die asynchrone oder synchrone Replizierung.

Replizierung zwischen Element und ONTAP Clustern mit SnapMirror

Mit der NetApp SnapMirror Technologie können Snapshots repliziert werden, die mit NetApp Element Software für Disaster Recovery-Zwecke in ONTAP erstellt wurden. In einer SnapMirror Beziehung stellt Element einen Endpunkt dar, und ONTAP ist der andere.

SnapMirror ist eine NetApp Snapshot Replizierungstechnologie für Disaster Recovery, die für das Failover von primärem Storage auf sekundärem Storage an einem externen Standort ausgelegt ist. Die SnapMirror Technologie erstellt ein Replikat bzw. eine Spiegelung der Arbeitsdaten im sekundären Storage, von dem aus Sie bei einem Ausfall am primären Standort weiterhin Daten bereitstellen können. Daten werden auf Volume-Ebene gespiegelt.

Die Beziehung zwischen dem Quell-Volume im primären Storage und dem Ziel-Volume im sekundären Storage wird als Datensicherungsbeziehung bezeichnet. Die Cluster werden als Endpunkte bezeichnet, in denen sich die Volumes befinden und die Volumes, die die replizierten Daten enthalten, müssen peed sein. Eine Peer-Beziehung ermöglicht einen sicheren Datenaustausch zwischen Clustern und Volumes.

SnapMirror wird nativ auf den NetApp ONTAP Controllern ausgeführt und ist in Element integriert, das auf NetApp HCI und SolidFire Clustern ausgeführt wird. Die Logik zur Steuerung von SnapMirror befindet sich in

ONTAP Software. Daher müssen alle SnapMirror Beziehungen mindestens ein ONTAP System erfordern, um die Koordination durchzuführen. Benutzer managen die Beziehungen zwischen Element- und ONTAP-Clustern. Dies erfolgt hauptsächlich über die Element UI. Einige Managementaufgaben befinden sich jedoch im NetApp ONTAP System Manager. Benutzer können SnapMirror auch über die CLI und die API managen, die sowohl in ONTAP als auch in Element verfügbar sind.

Siehe "TR-4651: NetApp SolidFire SnapMirror Architektur und Konfiguration" (anmeldung erforderlich)

Sie müssen die SnapMirror Funktion auf Cluster-Ebene manuell mit der Element Software aktivieren. Die SnapMirror Funktion ist standardmäßig deaktiviert und wird nicht automatisch im Rahmen einer neuen Installation oder eines Upgrades aktiviert.

Nach der Aktivierung von SnapMirror können Sie SnapMirror Beziehungen über die Registerkarte Datensicherung in der Element Software erstellen.

NetApp Element Software 10.1 und höher unterstützt SnapMirror Funktionen zum Kopieren und Wiederherstellen von Snapshots mit ONTAP Systemen.

Systeme mit Element 10.1 und höher beinhalten Code, der direkt mit SnapMirror auf ONTAP Systemen mit 9.3 oder höher kommunizieren kann. Die Element API bietet Methoden zur Aktivierung der SnapMirror Funktion in Clustern, Volumes und Snapshots. Zudem umfasst die Element UI Funktionen zum Managen von SnapMirror Beziehungen zwischen Element Software und ONTAP Systemen.

Beginnend mit Element 10.3 und ONTAP 9.4 Systemen können ONTAP-basierte Volumes in Element Volumes repliziert werden, und zwar in bestimmten Anwendungsfällen mit eingeschränkter Funktionalität.

Weitere Informationen finden Sie unter "Replizierung zwischen NetApp Element Software und ONTAP (ONTAP CLI)".

Volume Snapshots zur Datensicherung

Ein Volume Snapshot ist eine zeitpunktgenaue Kopie eines Volumes, mit der Sie später ein Volume auf diesen speziellen Zeitpunkt wiederherstellen können.

Während Snapshots einem Volume-Klon ähneln, sind Snapshots lediglich Replikate von Volume-Metadaten. Sie können also nicht mounten oder darauf schreiben. Das Erstellen eines Volume-Snapshots nimmt ebenfalls nur eine geringe Menge an Systemressourcen und Platz in Anspruch, sodass die Snapshot-Erstellung schneller als das Klonen erfolgt.

Sie können Snapshots in einem Remote-Cluster replizieren und als Sicherungskopie des Volumes verwenden. Dadurch können Sie ein Rollback eines Volumes zu einem bestimmten Zeitpunkt mit dem replizierten Snapshot durchzuführen. Sie können auch einen Klon eines Volumes aus einem replizierten Snapshot erstellen.

Sie können ein Backup von Snapshots aus einem Element Cluster auf einem externen Objektspeicher oder auf einem anderen Element Cluster erstellen. Wenn Sie einen Snapshot in einem externen Objektspeicher sichern, müssen Sie über eine Verbindung zum Objektspeicher verfügen, der Lese-/Schreibvorgänge ermöglicht.

Sie können einen Snapshot eines einzelnen Volumes oder mehrerer zur Datensicherheit erstellen.

Volume-Klone

Ein Klon eines einzelnen oder mehrerer Volumes ist eine zeitpunktgenaue Kopie der Daten. Wenn Sie ein Volume klonen, erstellt das System einen Snapshot des Volume und erstellt dann eine Kopie der Daten, auf

die der Snapshot verweist.

Dies ist ein asynchroner Prozess und die erforderliche Zeit hängt von der Größe des zum Klonen benötigten Volumes und der aktuellen Cluster-Last ab.

Das Cluster unterstützt bis zu zwei aktuell laufende Klonanforderungen pro Volume und bis zu acht aktive Volume-Klonvorgänge gleichzeitig. Anforderungen, die über diese Grenzen hinausgehen, werden zur späteren Verarbeitung in die Warteschlange gestellt.

Übersicht über Backup- und Restore-Prozesse für Element Storage

Backups und Restores von Volumes mit anderen SolidFire Storage-Systemen sowie in sekundären Objektspeichern mit Amazon S3 oder OpenStack Swift möglich.

Sie können ein Volume unter folgender Adresse sichern:

- Ein SolidFire Storage-Cluster
- Ein Amazon S3-Objektspeicher
- OpenStack Swift Objektspeicher

Wenn Sie Volumes aus OpenStack Swift oder Amazon S3 wiederherstellen, benötigen Sie Manifest-Informationen aus dem ursprünglichen Backup-Prozess. Wenn Sie ein Volume wiederherstellen, das auf einem SolidFire Storage-System gesichert wurde, sind keine Manifest-Informationen erforderlich.

Sicherungsdomänen

Eine Protection Domain ist ein Knoten oder eine Gruppe von Knoten, die so gruppiert sind, dass ein Teil oder sogar alle Knoten ausfallen könnten, ohne dass die Datenverfügbarkeit beeinträchtigt wird. Protection-Domänen ermöglichen es einem Storage-Cluster, automatisch den Verlust eines Chassis (Chassis-Affinität) oder einer gesamten Domäne (Chassis-Gruppe) zu heilen.

Sie können die Überwachung der Schutzdomäne manuell mit dem Erweiterungspunkt für die NetApp Element-Konfiguration im NetApp Element-Plug-in für vCenter Server aktivieren. Sie können einen Schutz-Domain-Schwellenwert basierend auf Node- oder Chassis-Domänen auswählen. Sie können die Überwachung von Schutzdomänen auch über die Element-API oder die Web-Benutzeroberfläche aktivieren.

Ein Protection Domain-Layout weist jeden Knoten einer bestimmten Protection Domain zu.

Es werden zwei unterschiedliche Protection Domain Layouts unterstützt, sogenannte Protection Domain Levels.

- Auf Node-Ebene befindet sich jeder Node in einer eigenen Protection Domain.
- Auf Chassis-Ebene befinden sich nur Nodes, die sich ein Chassis teilen, in derselben Protection Domain.
  - Das Layout auf Chassis-Ebene wird automatisch von der Hardware bestimmt, wenn der Node zum Cluster hinzugefügt wird.
  - In einem Cluster, in dem sich jeder Node in einem separaten Chassis befindet, sind diese beiden Ebenen funktional identisch.

Wenn Sie ein neues Cluster erstellen und Storage-Nodes verwenden, die sich in einem gemeinsam genutzten Chassis befinden, sollten Sie möglicherweise über die Protection Domains-Funktion einen Ausfallschutz auf Chassis-Ebene in Betracht ziehen.

Benutzerdefinierte Schutzdomänen

Sie können ein benutzerdefiniertes Schutz-Domain-Layout definieren, das Ihrem spezifischen Gehäuse- und Node-Layout entspricht und wo jeder Knoten mit einer und nur einer benutzerdefinierten Schutzdomäne verknüpft ist. Standardmäßig ist jeder Knoten derselben benutzerdefinierten Standard-Schutzdomäne zugewiesen.

Falls keine benutzerdefinierten Sicherungsdomänen zugewiesen sind:

- Der Cluster-Vorgang wird nicht beeinträchtigt.
- Die benutzerdefinierte Ebene ist weder tolerant noch widerstandsfähig.

Wenn Sie benutzerdefinierte Protection Domains für einen Cluster konfigurieren, gibt es drei mögliche Schutzstufen, die Sie im Element Web UI Dashboard sehen können:

- Nicht geschützt: Das Speicher-Cluster ist nicht vor dem Ausfall einer seiner benutzerdefinierten Schutz-Domains geschützt. Um dies zu beheben, fügen Sie dem Cluster zusätzliche Speicherkapazität hinzu oder konfigurieren Sie die benutzerdefinierten Schutz-Domains des Clusters neu, um das Cluster vor möglichen Datenverlusten zu schützen.
- Fehlertolerant: Der Speicher-Cluster verfügt über genügend freie Kapazität, um Datenverlust nach dem Ausfall einer seiner benutzerdefinierten Schutz-Domains zu verhindern.
- Fehler ausfallsicher: Der Speicher-Cluster verfügt über genügend freie Kapazität, um sich nach dem Ausfall einer seiner benutzerdefinierten Schutz-Domains selbst zu heilen. Nach Abschluss des Heilungsprozesses wird das Cluster vor Datenverlust geschützt, wenn weitere Domänen ausfallen sollten.

Wenn mehr als eine benutzerdefinierte Schutzdomäne zugewiesen wird, weist jedes Subsystem Duplikate zu separaten benutzerdefinierten Schutzdomänen zu. Ist dies nicht möglich, so wird das Zuweisen von Duplikaten zu separaten Nodes rückgängig gemacht. Jedes Subsystem (z. B. Behälter, Schichten, Protokollendpunktanbieter und Ensemble) erledigt dies unabhängig voneinander.

Über die Element-UI lassen sich "Konfigurieren Sie benutzerdefinierte Sicherungsdomänen", Oder Sie können die folgenden API-Methoden verwenden:

- "GetProtectionDomainLayout" - Zeigt an, in welchem Gehäuse und in welcher benutzerdefinierten Schutzdomäne sich jeder Knoten befindet.
- "SetProtectionDomainLayout" - Ermöglicht die Zuweisung einer benutzerdefinierten Schutzdomäne zu jedem Knoten.

Hochverfügbarkeit mit Double Helix

Die Double Helix Datensicherung ist eine Replizierungsmethode, die mindestens zwei redundante Datenkopien auf alle Laufwerke innerhalb eines Systems verteilt. Der Ansatz „RAID-less“ ermöglicht es einem System, mehrere gleichzeitige Ausfälle auf allen Ebenen des Storage-Systems zu absorbieren und schnell zu reparieren.

Leistung und Servicequalität

Ein SolidFire Storage Cluster bietet QoS-Parameter (Quality of Service) für einzelne Volumes. Sie können die Cluster-Performance, die in ein- und Ausgaben pro Sekunde (IOPS) gemessen wird, mit drei konfigurierbaren Parametern garantieren, die QoS definieren: Das IOPS-Minimum, das IOPS-Maximum und die Burst-IOPS.

SolidFire Active IQ verfügt über eine Seite mit QoS-Empfehlungen zur optimalen Konfiguration und Einrichtung von QoS-Einstellungen.

Parameter für die Servicequalität

IOPS-Parameter werden folgendermaßen definiert:

- **Minimum IOPS** - die Mindestanzahl kontinuierlicher ein- und Ausgänge pro Sekunde (IOPS), die der Storage Cluster einem Volume zur Verfügung stellt. Die für ein Volume konfigurierten IOPS-Mindestwerte sind das garantierte Performance-Niveau für ein Volume. Die Performance sinkt nicht unter dieses Niveau.
- **Maximale IOPS** - die maximale Anzahl an anhaltenden IOPS, die der Storage Cluster einem Volume zur Verfügung stellt. Wenn Cluster-IOPS-Niveaus kritisch hoch sind, wird diese IOPS-Performance nicht überschritten.
- **Burst IOPS** - die maximale Anzahl von IOPS in einem kurzen Burst Szenario erlaubt. Wenn ein Volume unter dem IOPS-Maximum ausgeführt wurde, werden Burst Credits gesammelt. Wenn Performance-Level sehr hoch sind und auf ein Maximum geschoben werden, sind kurze Anstiegen von IOPS auf dem Volume zulässig.

  Element Software verwendet Burst IOPS, wenn ein Cluster eine niedrige IOPS-Auslastung aufweist.

  Ein einzelnes Volume kann die Burst-IOPS erhalten und die Gutschriften verwenden, um über ihrem IOPS-Maximum bis auf ihr Burst-IOPS-Level für einen festgelegten „Burst-Zeitraum“ zu IOPS-Burst-Wert aufzusteigen. Ein Volume kann für bis zu 60 Sekunden einen Burst ausführen, wenn das Cluster die Kapazität für die Burst-Volumes hat. Ein Volume kann für jede Sekunde, in der das Volume unter seinem maximalen IOPS-Limit ausgeführt wird, eine Sekunde Burst Credit (bis zu einem Maximum von 60 Sekunden) angesammelt werden.

  Die IOPS-Burst-IOPS-Werte sind auf zwei Arten begrenzt:

  - Ein Volume kann für einige Sekunden einen Spitzenwert über dem maximalen IOPS erzielen, der der Anzahl der Burst Credits entspricht, die es beim Volume gesammelt hat.
  - Wenn ein Volume über die Einstellung für maximale IOPS platzt, ist es durch die Einstellung für Burst IOPS eingeschränkt. Daher überschreitet der IOPS-Burst niemals die Burst-IOPS-Einstellung für das Volume.
- **Effektive max. Bandbreite** - die maximale Bandbreite wird berechnet, indem die Anzahl der IOPS (basierend auf der QoS-Kurve) mit der I/O-Größe multipliziert wird.

  Beispiel: QoS-Parametereinstellungen für 100 Min IOPS, 1000 Max IOPS und 1500 Burst IOPS wirken sich auf die Performance-Qualität aus:

  - Workloads können ein Maximum von 1000 IOPS erreichen und halten, bis sich der Zustand von Workload-Engpässen für IOPS im Cluster bemerkbar macht. Die IOPS werden dann inkrementell reduziert, bis sich die IOPS auf allen Volumes innerhalb der designierten QoS-Bereiche befinden und die Konflikte für die Performance sinken.
  - Die Performance auf allen Volumes wird über den Mindestwert von 100 IOPS erreicht. Die Werte sinken nicht unter die Einstellung für Min IOPS, könnten aber bei Entlastung der Workloads über 100 IOPS bleiben.
  - Die Performance beträgt in einem kontinuierlichen Zeitraum niemals mehr als 1000 IOPS oder weniger als 100 IOPS. Die Performance von 1500 IOPS (Burst IOPS) ist zulässig, aber nur für die Volumes, die Burst Credits aufgesammelt haben, wenn sie unter dem IOPS-Maximum laufen und nur für kurze Zeit zulässig sind. Burst-Werte werden niemals aufrechterhalten.

QoS-Wertbegrenzungen

Hier sind die möglichen Mindest- und Höchstwerte für QoS.

Parameter	Mindestwert	Standard	4 4 KB	5 8 KB	6 16 KB	262 KB
IOPS-Minimum	50	50	15,000	9,375*	5556*	385*
IOPS-Maximum	100	15,000	200,000**	125,000	74,074	5128
IOPS-Burst	100	15,000	200,000**	125,000	74.074	5128

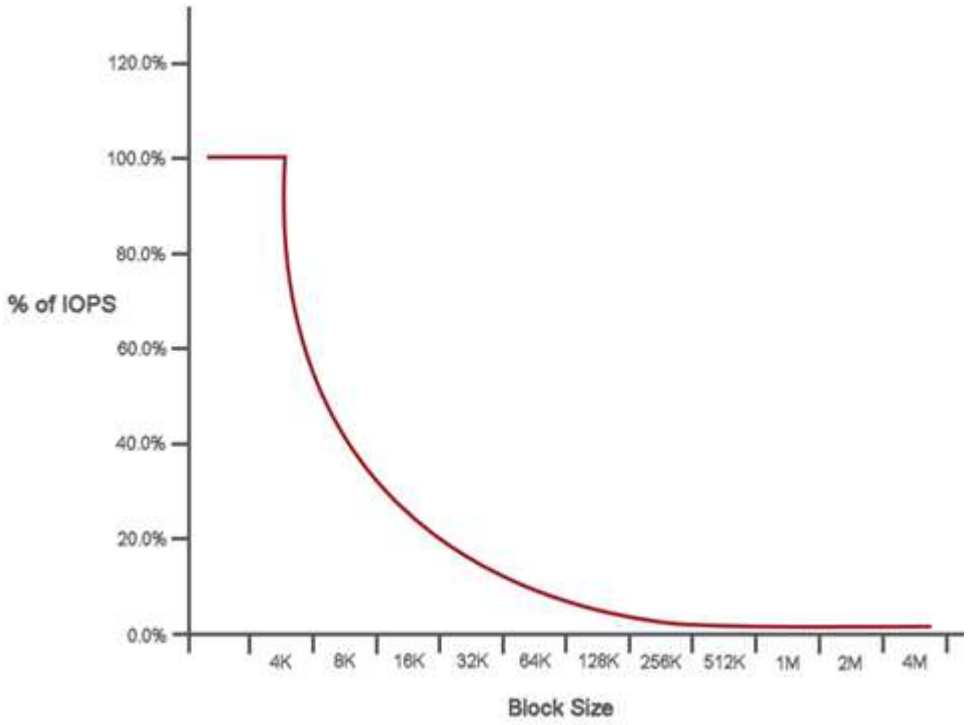
*Diese Schätzungen sind ungefähr. **Maximale IOPS und Burst IOPS können auf 200,000 gesetzt werden. Diese Einstellung ist jedoch nur erlaubt, die Performance eines Volumes effektiv zu nutzen. Die tatsächliche maximale Performance eines Volumes wird durch die Auslastung des Clusters und die Performance pro Node begrenzt.

QoS-Performance

Die QoS-Performance-Kurve zeigt die Beziehung zwischen Blockgröße und dem Prozentsatz der IOPS.

Die Blockgröße und die Bandbreite haben direkte Auswirkungen auf die Anzahl der IOPS, die eine Applikation erreichen kann. Element Software berücksichtigt die Blockgröße, die durch die Normalisierung der Blockgrößen auf 4 kb erhält. Je nach Workload kann das System die Blockgrößen erhöhen. Mit zunehmender Blockgröße erhöht das System die Bandbreite auf ein Niveau, das für die Verarbeitung größerer Blockgrößen erforderlich ist. Mit einer höheren Bandbreite verringert sich auch die Anzahl an IOPS, die das System erreichen kann.

Die QoS-Performance-Kurve zeigt die Beziehung zwischen zunehmenden Blockgrößen und dem sinkenden Prozentsatz an IOPS:



Wenn Blockgröße beispielsweise 4 kb und eine Bandbreite 4000 kbit/s beträgt, betragen die IOPS 1000. Bei einer Blockgröße von bis zu 8.000 USD erhöht sich die Bandbreite auf 5000 kBit/s und der IOPS-Wert sinkt auf 625. Unter Berücksichtigung der Blockgröße übernimmt das System dafür, dass Workloads mit niedrigerer Priorität, bei denen größere Blockgrößen zum Beispiel Backups und Hypervisor-Aktivitäten verwendet werden, nicht zu viele der Performance in Anspruch nehmen, die durch Datenverkehr mit höherer Priorität durch kleinere Blöcke benötigt wird.

QoS-Richtlinien (QoS

Mit einer QoS-Richtlinie können Sie standardisierte Quality-of-Service-Einstellungen erstellen und speichern, die auf viele Volumes angewendet werden können.

QoS-Richtlinien eignen sich am besten für Serviceumgebungen, beispielsweise mit Datenbank-, Applikations- oder Infrastrukturservern, die selten neu gestartet werden und den konstanten Zugriff auf den Storage benötigen. Einzelne Volume-QoS eignet sich am besten für lichtstarke VMs, z. B. virtuelle Desktops oder spezielle VMs mit Kiosk-Typ. Diese können täglich neu gestartet, eingeschaltet oder mehrfach ausgeschaltet werden.

QoS- und QoS-Richtlinien sollten nicht gemeinsam eingesetzt werden. Wenn Sie QoS-Richtlinien verwenden, verwenden Sie keine benutzerdefinierte QoS für ein Volume. Durch benutzerdefinierte QoS werden die QoS-Richtlinienwerte für Volume-QoS-Einstellungen überschrieben und angepasst.

Der ausgewählte Cluster muss zur Verwendung von QoS-Richtlinien Element 10.0 oder höher sein. Anderenfalls sind QoS-Richtlinienfunktionen nicht verfügbar.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"

Anforderungen

Netzwerkbetrieb

Das Netzwerk-Setup für ein SolidFire System besteht aus Switch- und Port-Anforderungen. Die Umsetzung davon hängt von Ihrem System ab.

Finden Sie weitere Informationen

- "Switch-Konfiguration für Cluster mit Element Software"
- "Anforderungen an Netzwerk-Ports"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Switch-Konfiguration für Cluster mit Element Software

Das NetApp Element Softwaresystem verfügt über bestimmte Switch-Anforderungen und Best Practices für eine optimale Storage-Performance.

Storage-Nodes benötigen je nach spezifischer Node-Hardware 10- oder 25-GbE-Ethernet-Switches für die Kommunikation von iSCSI-Storage-Services und zwischen Nodes innerhalb eines Clusters. 1GbE-Switches können für diese Arten von Datenverkehr verwendet werden:

- Management des Clusters und der Nodes
- Clusterinternen Managementdatenverkehr zwischen den Nodes
- Datenverkehr zwischen den Cluster-Knoten und der virtuellen Verwaltungsknoten

Best Practice: bei der Konfiguration von Ethernet-Switches für Cluster-Datenverkehr sollten Sie die folgenden Best Practices umsetzen:

- Für den Datenverkehr außerhalb des Storage-Systems im Cluster können Sie ein Paar 1-GbE-Switches implementieren, um Hochverfügbarkeit und Lastverteilung bereitzustellen.
- Auf den Storage-Netzwerk-Switches stellen Sie Switches paarweise bereit und konfigurieren und verwenden Jumbo Frames (eine MTU-Größe von 9216 Byte). So wird eine erfolgreiche Installation gewährleistet und Fehler im Speichernetzwerk aufgrund von fragmentierten Paketen vermieden.

Für die Elementbereitstellung sind mindestens zwei Netzwerksegmente erforderlich, eines für jeden der folgenden Verkehrstypen:

- Vereinfachtes
- Storage/Daten

Je nach den NetApp H-Series Storage-Node-Modellen und der geplanten Verkabelungskonfiguration können Sie diese Netzwerke mithilfe separater Switches physisch trennen oder sie über VLANs logisch trennen. Bei den meisten Implementierungen müssen diese Netzwerke jedoch durch VLANs logisch voneinander getrennt werden.

Storage-Nodes müssen vor, während und nach der Implementierung kommunizieren können.

Wenn Sie getrennte Managementnetzwerke für Storage-Nodes implementieren, stellen Sie sicher, dass diese Managementnetzwerke Netzwerkrouten zwischen ihnen haben. Diese Netzwerke müssen über Gateways verfügen, und es muss eine Route zwischen den Gateways vorhanden sein. Stellen Sie sicher, dass jedem neuen Node ein Gateway zugewiesen ist, um die Kommunikation zwischen den Nodes und Managementnetzwerken zu erleichtern.

Für NetApp Element ist Folgendes erforderlich:

- Alle mit NetApp H-Series Storage-Nodes verbundenen Switch-Ports müssen als Spanning Tree Edge Ports konfiguriert sein.
  - Bei Cisco Switches, je nach Switch-Modell, Softwareversion und Porttyp, können Sie dies mit einem der folgenden Befehle ausführen:
    - `spanning-tree port type edge`
    - `spanning-tree port type edge trunk`
    - `spanning-tree portfast`
    - `spanning-tree portfast trunk`
  - Auf Mellanox-Switches kann dies mit dem durchgeführt werden `spanning-tree port type edge` Befehl.
- Die Switches, die Storage-Datenverkehr verarbeiten, müssen Geschwindigkeiten von mindestens 10 GbE pro Port unterstützen (bis zu 25 GbE pro Port wird unterstützt).
- Die Switches, die Managementdatenverkehr verarbeiten, müssen Geschwindigkeiten von mindestens 1 GbE pro Port unterstützen.
- Sie müssen Jumbo Frames an den Switch-Ports konfigurieren, die Storage Traffic verarbeiten. Für eine erfolgreiche Installation müssen Hosts 9000-Byte-Pakete lückenlos versenden können.
- Die Netzwerklatenz zwischen allen Storage-Nodes sollte 2 ms nicht überschreiten.

Einige Nodes bieten zusätzliche Out-of-Band-Managementfunktionen über einen dedizierten Management-Port. NetApp H300S, H500S und H700S Nodes ermöglichen auch IPMI-Zugriff über Port A Als Best Practice wird empfohlen, das Remote-Management durch die Konfiguration von Out-of-Band-Management für alle Nodes in Ihrer Umgebung zu vereinfachen.

Finden Sie weitere Informationen

- "Netzwerk- und Switch-Anforderungen des NetApp HCI"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Anforderungen an Netzwerk-Ports

Möglicherweise müssen Sie die folgenden TCP- und UDP-Ports über die Edge-Firewall Ihres Rechenzentrums zulassen, damit Sie das System Remote verwalten und Clients außerhalb Ihres Rechenzentrums die Verbindung zu Ressourcen ermöglichen können. Einige dieser Ports sind je nach Nutzung des Systems möglicherweise nicht erforderlich.

Alle Ports sind TCP, sofern nicht anders angegeben, und alle TCP-Ports müssen die Dreiwege-Handshake-

Kommunikation zwischen dem NetApp-Supportserver, dem Verwaltungsknoten und den Knoten unterstützen, auf denen die Element-Software ausgeführt wird. Beispielsweise kommuniziert der Host auf einem Management-Knoten über TCP-Port 443 mit dem Host auf einem Speicher-Cluster-MVIP-Ziel, und der Ziel-Host kommuniziert über einen beliebigen Port zurück zum Quellhost.

Aktivieren Sie ICMP zwischen dem Managementknoten, Knoten mit Element Software und Cluster MVIP.

Die folgenden Abkürzungen werden in der Tabelle verwendet:

- MIP: Management-IP-Adresse, eine Adresse pro Node
- SIP: Speicher-IP-Adresse, eine Adresse pro Knoten
- MVIP: Management der virtuellen IP-Adresse
- SVIP: Virtuelle Speicher-IP-Adresse

Quelle	Ziel	Port	Beschreibung
ISCSI-Clients	Storage Cluster MVIP	443	(Optional) UI- und API-Zugriff
ISCSI-Clients	Storage Cluster SVIP	3260	ISCSI-Kommunikation des Clients
ISCSI-Clients	Speicherknoten SIP	3260	ISCSI-Kommunikation des Clients
Management-Node	`sfsupport.solidfire.com`	22	Reverse-SSH-Tunnel für den Support-Zugriff
Management-Node	MIP-Speicher-Node	22	SSH-Zugriff für die Unterstützung
Management-Node	DNS-Server	53 TCP/UDP	DNS-Suche
Management-Node	MIP-Speicher-Node	442	UI- und API-Zugriff auf Upgrades von Storage-Node und Element Software
Management-Node	Storage Cluster MVIP	442	UI- und API-Zugriff auf Upgrades von Storage-Node und Element Software
Management-Node	`monitoring.solidfire.com`	443	Berichterstellung für den Storage-Cluster an Active IQ
Management-Node	Storage Cluster MVIP	443	UI- und API-Zugriff auf Upgrades von Storage-Node und Element Software
Management-Node	repo.netapp.com	443	Zugriff auf Komponenten, die für die Installation/Aktualisierung einer On-Premises-Implementierung erforderlich sind

Quelle	Ziel	Port	Beschreibung
Management-Node	BMC/IPMI für Storage-Node	623 UDP	RMCP-Anschluss Dies ist erforderlich, um IPMI-fähige Systeme zu verwalten.
Management-Node	Witness Node	9442	Konfigurations-API-Service pro Node
Management-Node	VCenter Server	9443	VCenter Plug-in-Registrierung: Der Port kann nach Abschluss der Registrierung geschlossen werden.
SNMP-Server	Storage Cluster MVIP	161 UDP	SNMP-Abfrage
SNMP-Server	MIP-Speicher-Node	161 UDP	SNMP-Abfrage
BMC/IPMI für Storage-Node	Management-Node	623 UDP	RMCP-Anschluss Dies ist erforderlich, um IPMI-fähige Systeme zu verwalten.
MIP-Speicher-Node	DNS-Server	53 TCP/UDP	DNS-Suche
MIP-Speicher-Node	Management-Node	80	Upgrades für Element Software
MIP-Speicher-Node	S3/Swift-Endpunkt	80	(Optional) HTTP-Kommunikation mit S3/Swift-Endpunkt für Backup und Recovery
MIP-Speicher-Node	NTP-Server	123 UDP	NTP
MIP-Speicher-Node	Management-Node	162 UDP	(Optional) SNMP-Traps
MIP-Speicher-Node	SNMP-Server	162 UDP	(Optional) SNMP-Traps
MIP-Speicher-Node	LDAP-Server	389 TCP/UDP	(Optional) LDAP-Suche
MIP-Speicher-Node	Management-Node	443	Elementspeicher-Upgrades
MIP-Speicher-Node	Remote Storage Cluster MVIP	443	Kommunikation über die Verbindung des Remote-Replikationsclusters
MIP-Speicher-Node	MIP für Remote-Storage-Node	443	Kommunikation über die Verbindung des Remote-Replikationsclusters
MIP-Speicher-Node	S3/Swift-Endpunkt	443	(Optional) HTTPS-Kommunikation an S3/Swift-Endpunkt für Backup und Recovery

Quelle	Ziel	Port	Beschreibung
MIP-Speicher-Node	Management-Node	514 TCP/UDP 10514 TCP/UDP	Syslog-Weiterleitung
MIP-Speicher-Node	Syslog-Server	514 TCP/UDP 10514 TCP/UDP	Syslog-Weiterleitung
MIP-Speicher-Node	LDAPS Server	636 TCP/UDP	LDAPS-Suche
MIP-Speicher-Node	MIP für Remote-Storage-Node	2181	Cluster-übergreifende Kommunikation für Remote-Replizierung
Speicherknoten SIP	Remote-Speicherknoten SIP	2181	Cluster-übergreifende Kommunikation für Remote-Replizierung
Speicherknoten SIP	Speicherknoten SIP	3260	ISCSI miteinander verbinden
Speicherknoten SIP	Remote-Speicherknoten SIP	4000 bis 4020	Remote-Replizierung: Node-to-Node-Datentransfer
System Administrator-PC	Management-Node	442	HTTPS-UI-Zugriff auf den Management-Node
System Administrator-PC	MIP-Speicher-Node	442	HTTPS-UI- und API-Zugriff auf Storage-Node
System Administrator-PC	Management-Node	443	HTTPS-UI- und API-Zugriff auf den Management-Node
System Administrator-PC	Storage Cluster MVIP	443	HTTPS-UI- und API-Zugriff auf das Storage-Cluster
System Administrator-PC	Storage Node Baseboard Management Controller (BMC)/Intelligent Platform Management Interface (IPMI) H410 und H600 Serien	443	HTTPS-UI- und API-Zugriff auf die Remote-Steuerung des Nodes

Quelle	Ziel	Port	Beschreibung
System Administrator-PC	MIP-Speicher-Node	443	Erstellung von HTTPS-Storage-Clustern, UI-Zugriff nach der Implementierung auf das Storage-Cluster
System Administrator-PC	Storage Node BMC/IPMI H410 und H600 Series	623 UDP	Remote Management Control Protocol-Port: Dies ist erforderlich, um IPMI-fähige Systeme zu verwalten.
System Administrator-PC	Witness Node	8080	Witness Node pro Node Web-UI
VCenter Server	Storage Cluster MVIP	443	VCenter-Plug-in-API-Zugriff
VCenter Server	Remote-Plug-in	8333	Remote vCenter Plug-in Service
VCenter Server	Management-Node	8443	(Optional) vCenter Plug-in QoSSIOC-Service.
VCenter Server	Storage Cluster MVIP	8444	Zugriff auf vCenter VASA Provider (nur VVols)
VCenter Server	Management-Node	9443	VCenter Plug-in-Registrierung: Der Port kann nach Abschluss der Registrierung geschlossen werden.

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Probieren Sie es aus

Ressourcen und Tools für den Einstieg in die Element Software

- "Lab on Demand for Private Cloud Storage Flexibility with Element (Anmeldung erforderlich)": Dieses Lab präsentiert Konzepte wie uneingeschränktes Scale-out, garantierte Workload-Performance und Automatisierung der Storage-Infrastruktur für Storage-Systeme mit Element Software.
- "Storage-Funktionen mit Element Demo-Node testen": Element Demo Node ist eine virtuelle VMware-Maschinenversion der Element Software, die eine einfache Möglichkeit bietet, viele der wichtigsten Speicherfunktionen von NetApp HCI und SolidFire-Produkten zu demonstrieren.

Storage-Funktionen mit Element Demo-Node testen

"Element Demo-Node" Ist eine VMware Virtual Machine (VM)-Version der Element Software, die eine einfache Möglichkeit bietet, viele der wichtigsten Storage-Funktionen von NetApp HCI und SolidFire Produkten zu demonstrieren. Der Demo-Node ermöglicht Entwicklern, Code mit der Element API zu schreiben, ohne dass physische Hardware erforderlich ist. Es wird als OVA-Datei zur einfachen VMware-Bereitstellung verpackt.

Unterstützte Funktionen:

Element Demo Node ist nur zur Verwendung als Demo- und Entwicklungstool gedacht. Beachten Sie die folgenden Funktionseinschränkungen, bevor Sie den Demo-Node verwenden:

- Element Demo Node unterstützt kein Clustering. Sie funktioniert nur als Single-Node-Cluster.
- Bei Element-Upgrades wird keine Unterstützung geboten. Eine neuere Version von Element sollte mit einer neuen Demo-Node-VM getestet werden.
- Er ist nicht für die Demonstration der Storage-Performance gedacht. Die für den Demo-Node beobachtete Performance ist in keiner Weise indikativ für die Performance der physischen Cluster.
- Demo-Nodes können nicht zu NetApp HCI- oder SolidFire-Clustern hinzugefügt werden.
- VRF-VLANs werden nicht unterstützt (standardmäßig getaggte VLANs werden unterstützt).
- Multi-Drive Slice Service (MDSS) wird nicht unterstützt.
- Element Demo-Node wird nur durch VMFS-Datastores unterstützt. VVols werden nicht unterstützt.
- Hardwarebasierte Konfigurations- und Überwachungsfunktionen funktionieren nicht mit dem Demo-Node.
- Es unterstützt maximal 10 Snapshots pro Volume.
- Er unterstützt maximal 20 Konten pro Node/Cluster.
- Es unterstützt maximal 100 Volumes pro Account.
- Pro Account werden maximal 200 VVols unterstützt.
- Er unterstützt eine maximale Volume-Größe von 100 gib.
- Er unterstützt ein dauerhaftes Cluster-Limit von 3000 IOPS.

Es gelten alle anderen Einschränkungen für die Element Software. Weitere Informationen finden Sie in den Versionshinweisen zu Element Software.

VM-Anforderungen erfüllt

- 240 GB Gesamtkapazität (Größe und Anzahl der virtuellen Laufwerke für die VM können nicht geändert werden. Jeder zusätzliche Storage, der über den Hypervisor bereitgestellt wird, wird vom Gastbetriebssystem ignoriert.)
- 60-GB-Root-Festplatte
- Thick Provisioning/Eager Zeroed (ein 30-GB-Metadatenlaufwerk oder drei 50-GB-Blocklaufwerke) oder Thin Provisioning/Eager Null (**empfohlen**) (ein 30-GB-Metadatenlaufwerk oder drei 50-GB-Blocklaufwerke)
- Zwei vCPU (vollständig reserviert)
- 16 GB RAM (voll reserviert)
- Einzelner HBA für alle Festplatten, LSI Logic parallel
- Zwei vNICs, beide vmxnet3 (ein Management, ein Storage)

Host-Anforderungen erfüllt

- ESXI 6.0 oder 6.5 für Element Demo Node 11.7 VM
- ESXi 6.5 für Element Demo Node 12.0 und 12.2 VMs
- ESXi 6.7 und 7.0 für Element Demo Node 12.3 und 12.5 VMs
- Multi-Core 64-Bit Intel® Architektur

Laden Sie Den Element Demo-Node Herunter

Die Element Demo-Knoten-Software ist ein Satz von VMware-Dateien, die in einer .ova-Datei verpackt wurden.

Installieren Sie Element Demo Node auf VMware ESXi

Beim Installieren des Element Demo Node auf VMware ESXi werden die folgenden Aufgaben ausgeführt:

- Konfigurieren Sie die Netzwerkschnittstellen
- Registrieren des Demo-Knotens auf einem ESXi-Server
- Starten Sie den Demo-Knoten auf einem ESXi-Server

Konfigurieren Sie die Netzwerkschnittstellen

Für den Element Demo-Node sind zwei separate Netzwerke virtueller Maschinen erforderlich. Eine ist für Storage-Traffic und die andere für Management-Traffic. Sie sollten das Speichernetzwerk so konfigurieren, dass Jumbo Frames unterstützt werden.

Registrieren des Demo-Knotens auf einem ESXi-Server

Um Element Demo Node auf einem ESXi-Server zu registrieren, sollten Sie den Demo-Knoten .ova-Datei mit dem vSphere-Client bereitstellen.

Schritte

1. Melden Sie sich beim vSphere-Client an, und wählen Sie den ESXi-Host aus dem Bereich Inventar aus.
2. Wählen Sie **Datei** > **OVF-Vorlage bereitstellen**.

Der Assistent OVF-Vorlage bereitstellen wird gestartet.

3. Navigieren Sie auf der Seite **Vorlage auswählen** zur OVA-Datei, die Sie heruntergeladen haben, und wählen Sie **Öffnen**.
4. Wählen Sie **Weiter**.
5. Geben Sie auf der Seite **Name und Standort** einen Namen und einen Speicherort für die bereitgestellte Vorlage an, und wählen Sie dann **Weiter** aus.
6. Navigieren Sie auf der Seite **Select a Resource** zu dem Ort, an dem Sie die Vorlage ausführen möchten, und wählen Sie **Next**.
7. Überprüfen Sie die Details, und wählen Sie **Weiter**.
8. Wählen Sie auf der Seite „Speicher auswählen“ die Speicherort für die Dateien der virtuellen Maschine aus und wählen Sie dann **Weiter** aus.
9. Ordnen Sie auf der Seite **Netzwerke auswählen** das in der OVA-Datei verwendete Netzwerk den beiden separaten virtuellen Maschinennetzwerken in Ihrem Bestand zu und wählen Sie **Weiter**.
10. Überprüfen Sie auf der Seite **Ready to Complete** die Details zu der virtuellen Maschine, die Sie erstellen, und wählen Sie dann **Finish**.

Die Implementierung der Demo-Nodes kann einige Minuten in Anspruch nehmen.

Starten Sie den Demo-Knoten auf einem ESXi-Server

Starten Sie die Demo-Node-VM, um auf Element über die VMware ESXi Konsole zuzugreifen.

Schritte

1. Wählen Sie im vSphere Client die VM des Demo-Nodes aus, die Sie erstellt haben.
2. Wählen Sie die Registerkarte **Zusammenfassung**, um die Details zu dieser VM anzuzeigen.
3. Wählen Sie zum Starten der VM **Power On** aus.
4. Wählen Sie **Webkonsole Starten**.
5. Konfigurieren Sie den Demo-Knoten über die TUI. Weitere Informationen finden Sie unter "Konfigurieren Sie einen Storage-Node".

Support-Hilfe

Element Demo Node ist für freiwillige Helfer verfügbar. Stellen Sie Ihre Fragen zur Unterstützung auf der "Element Demo Node Forum".

Weitere Informationen

"Download-Seite für Element Demo-Node (Anmeldung erforderlich)"

Installation und Wartung von Hardware

H410S und H610S Hardware-Informationen

Storage-Nodes der H-Series installieren

Bevor Sie mit Ihrem All-Flash-Storage-System beginnen, sollten Sie die Storage Nodes richtig installieren und einrichten.

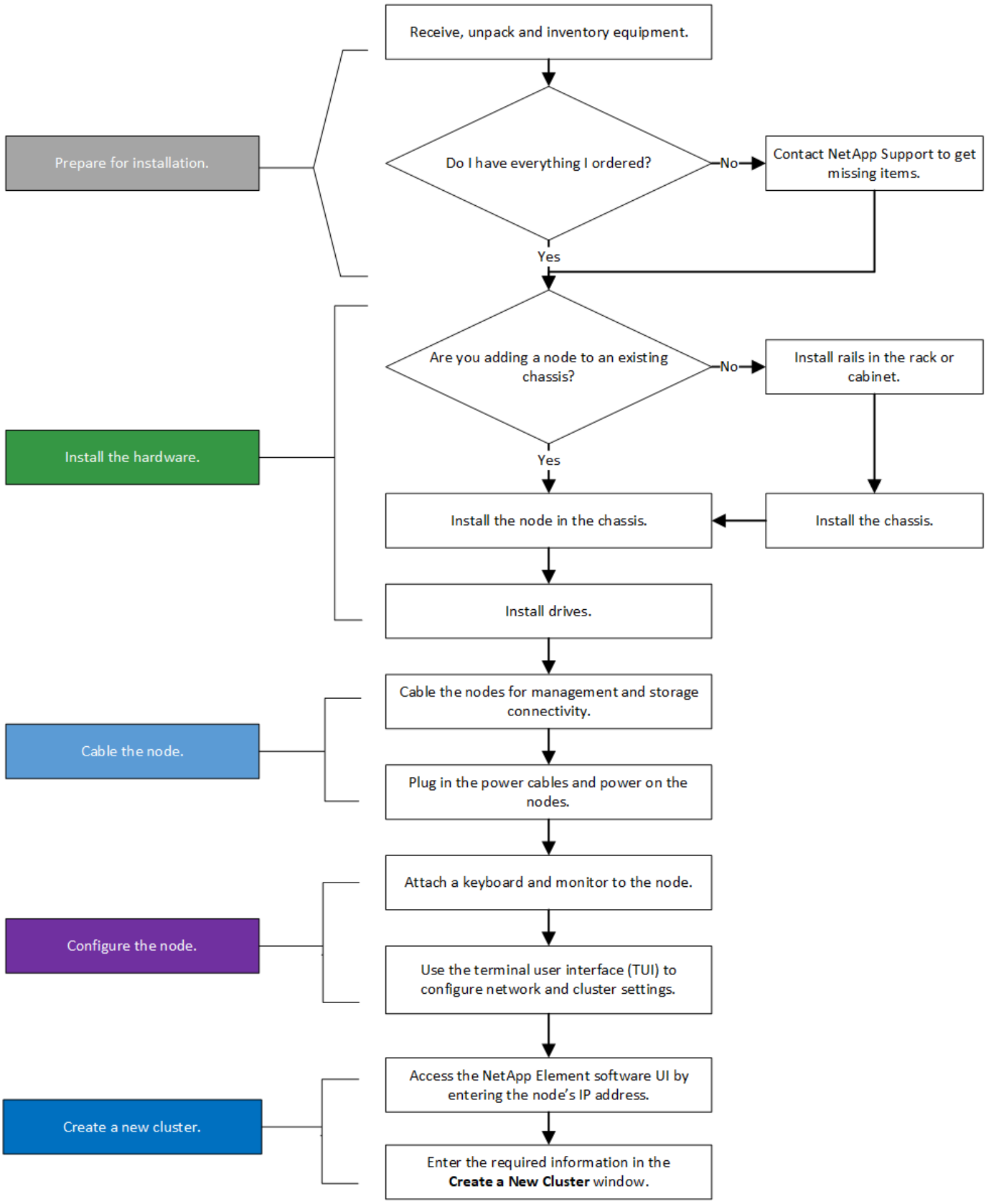
Siehe "Poster" Für eine visuelle Darstellung der Anweisungen.

- Workflow-Diagramme
- Installation vorbereiten
- Installieren Sie die Schienen
- Installieren und verkabeln Sie die Nodes
- Konfigurieren Sie die Nodes
- Erstellen eines Clusters

Workflow-Diagramme

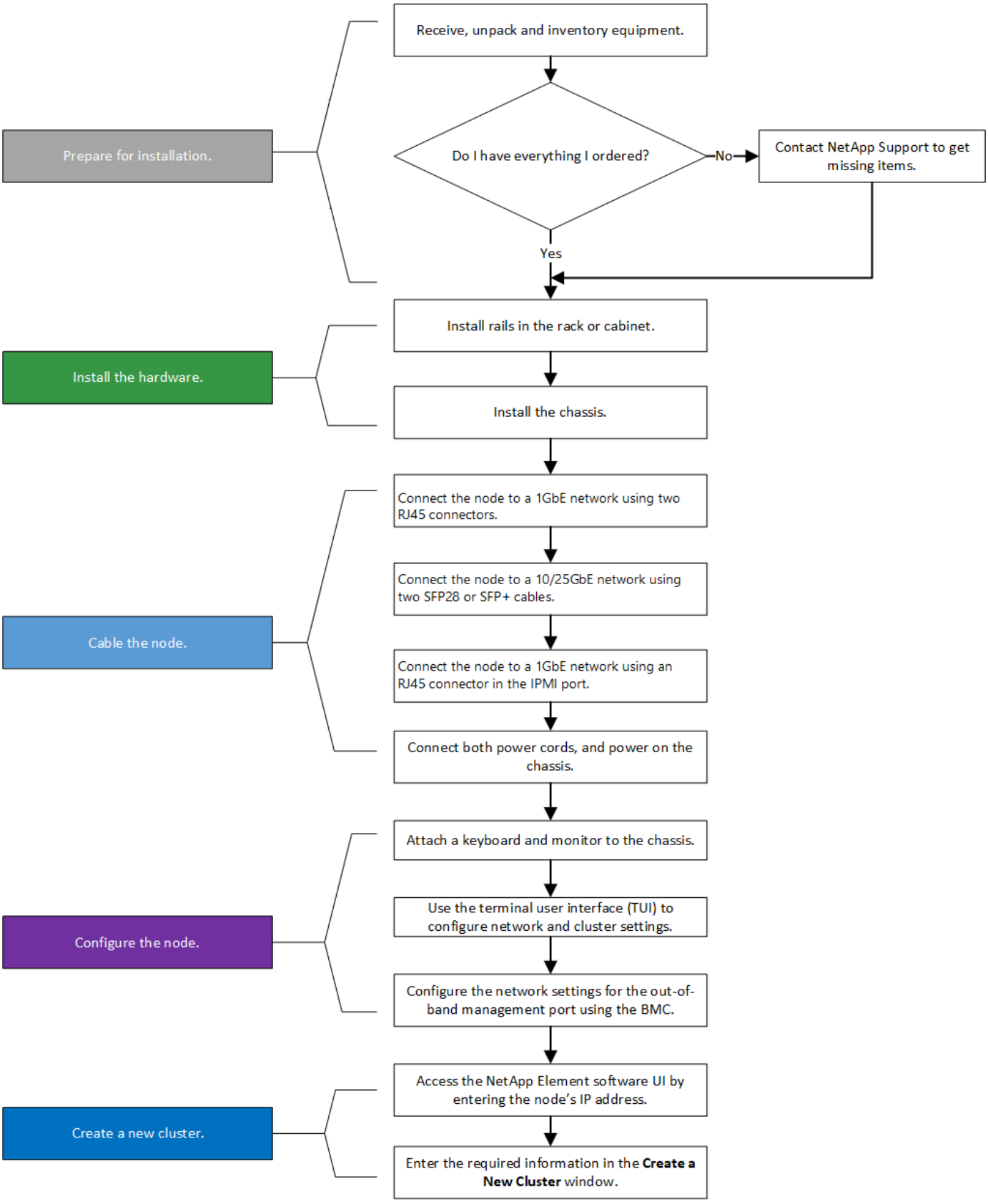
Die Workflow-Diagramme hier bieten einen allgemeinen Überblick über die Installationsschritte. Die Schritte variieren je nach Modell der H-Serie leicht.

H410S



H610S

Die Begriffe „Node“ und „Chassis“ werden bei H610S synonym verwendet, da Node und Chassis keine separaten Komponenten sind wie bei einem 2-HE-Chassis mit vier Nodes.



Installation vorbereiten

Überprüfen Sie vor der Installation die gelieferten Hardware und wenden Sie sich an den NetApp Support, wenn Teile fehlen.

Stellen Sie sicher, dass Sie an Ihrem Installationsstandort die folgenden Elemente installiert haben:

- Rack-Platz für das System.

Node-Typ	Rack-Fläche
H410S Nodes	Zwei Höheneinheiten (2 HE)
H610S Nodes	Eine Höheneinheit (1 HE)

- SFP28/SFP+ Direct-Attach-Kabel oder Transceiver
- CAT5e oder höhere Kabel mit RJ45-Stecker
- Ein Schalter für Tastatur, Video, Maus (KVM), um das System zu konfigurieren
- USB-Stick (optional)

Die Hardware, die an Sie geliefert wird, hängt davon ab, was Sie bestellen. Eine neue 2-HE-Bestellung mit vier Nodes umfasst das Chassis, die Blende, den Schienen-Kit, die Laufwerke, die Storage-Nodes, Und Stromkabel (zwei pro Chassis). Wenn Sie H610S Storage-Nodes bestellen, werden die Laufwerke im Chassis installiert.

Achten Sie beim Einbau der Hardware darauf, dass Sie das gesamte Verpackungsmaterial und die Verpackung aus dem Gerät entfernen. Dadurch wird verhindert, dass die Knoten überhitzt und heruntergefahren werden.

Installieren Sie die Schienen

Die Hardwarebestellung, die Ihnen zugestellt wurde, enthält eine Reihe von Gleitschienen. Sie benötigen einen Schraubendreher, um die Schieneninstallation abzuschließen. Die Installationsschritte variieren für jedes Node-Modell entsprechend.

Installieren Sie die Hardware von der Unterseite des Racks bis zur Oberseite, um zu verhindern, dass das Gerät umkippeln kann. Wenn Ihr Rack Stabilisatoren beinhaltet, müssen Sie diese vor der Installation der Hardware installieren.

- H410S
- H610S

H410S

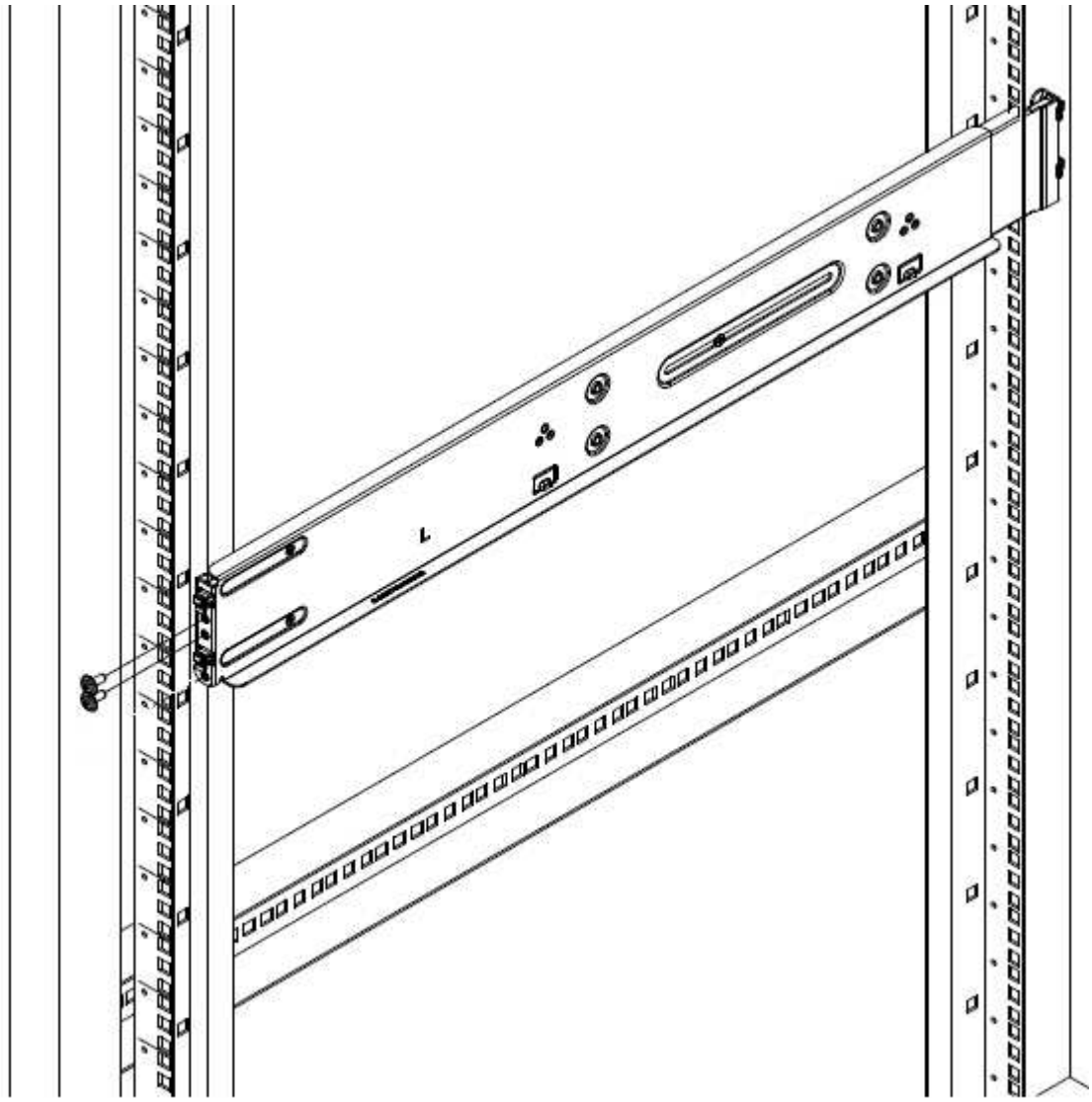
H410S Nodes sind in einem 2-HE-Chassis mit vier Nodes der H-Series installiert, das mit zwei Adaptersätzen ausgeliefert wird. Wenn Sie das Gehäuse in einem Rack mit runden Löchern einsetzen möchten, verwenden Sie die Adapter für ein Rack mit runden Löchern. Die Schienen für H410S Nodes passen ein Rack zwischen 29 Zoll und 33.5 Zoll Tiefe. Wenn die Schiene vollständig zusammengeschraubt ist, ist sie 28 Zoll lang, und die vorderen und hinteren Abschnitte der Schiene werden zusammen mit nur einer Schraube gehalten.

Wenn Sie das Gehäuse auf einer vollständig versetzten Schiene installieren, können die vorderen und hinteren Abschnitte der Schiene voneinander getrennt sein.

Schritte

1. Richten Sie die Vorderseite der Schiene an den Löchern an der vorderen Stange des Racks aus.

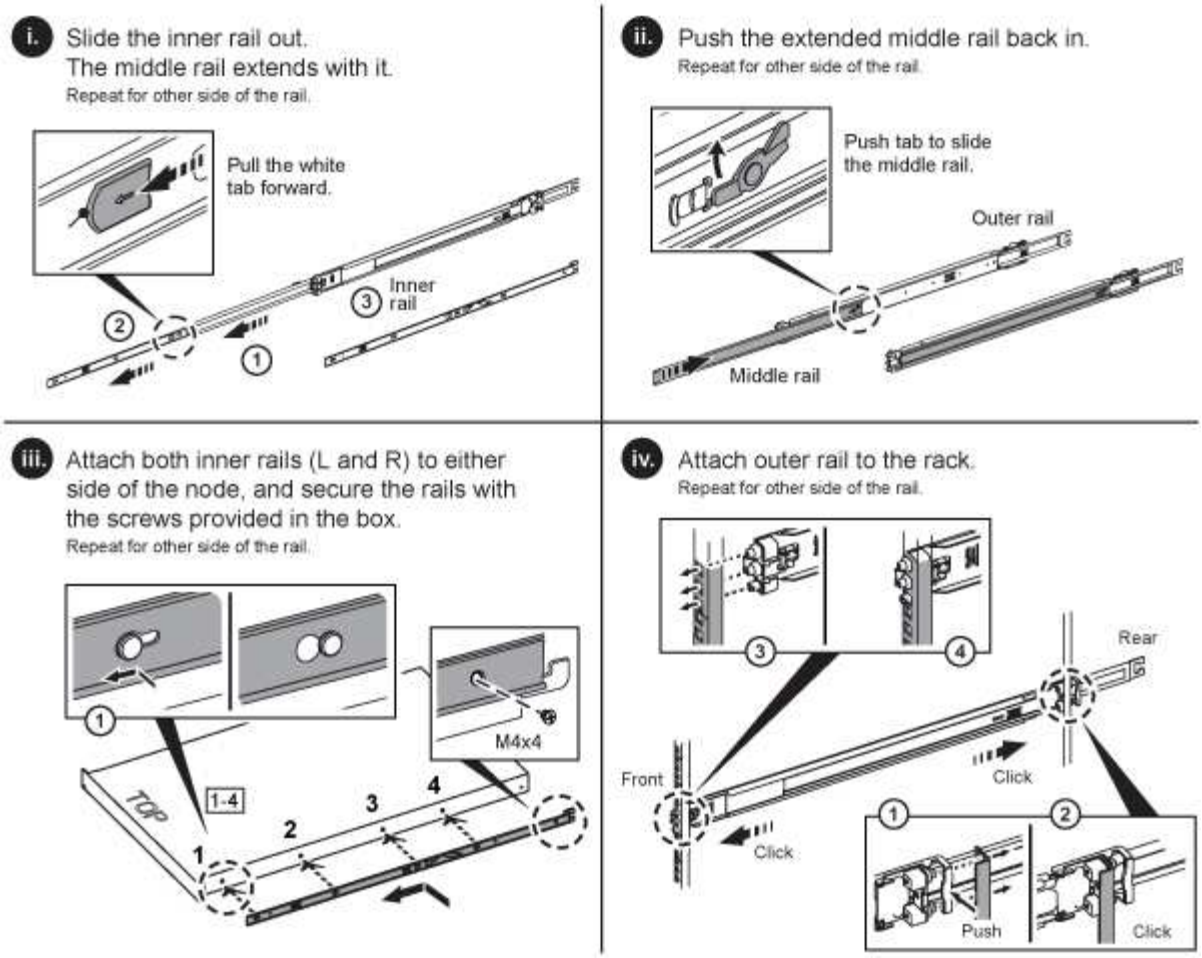
2. Schieben Sie die Haken an der Vorderseite der Schiene in die Löcher an der vorderen Stange des Racks und dann nach unten, bis die federbelasteten Stangen in die Rack-Löcher einrasten.
3. Befestigen Sie die Schiene mit Schrauben am Rack. Hier sehen Sie eine Abbildung der linken Schiene, die an der Vorderseite des Racks befestigt ist:



4. Ziehen Sie den hinteren Teil der Schiene auf die hintere Stange des Racks.
5. Richten Sie die Haken an der Rückseite der Schiene an den entsprechenden Löchern am hinteren Pfosten aus, um sicherzustellen, dass sich Vorder- und Rückseite der Schiene auf der gleichen Ebene befinden.
6. Montieren Sie die Rückseite der Schiene am Rack und befestigen Sie die Schiene mit Schrauben.
7. Führen Sie alle oben genannten Schritte für die andere Seite des Racks aus.

H610S

Folgende Abbildung zeigt die Installation von Schienen für einen H610S Storage-Node:



Auf dem H610S befinden sich linke und rechte Schienen. Positionieren Sie die Schraubenbohrung nach unten, so dass die H610S-Daumenschraube das Gehäuse an der Schiene befestigen kann.

Installieren und verkabeln Sie die Nodes

Der H410S Storage-Node wird in einem 2-HE-Chassis mit vier Nodes installiert. Installieren Sie bei H610S das Chassis/Node direkt auf den Schienen im Rack.

Entfernen Sie das gesamte Verpackungsmaterial und die Verpackung vom Gerät. So wird verhindert, dass die Nodes überhitzt und heruntergefahren werden.

- H410S
- H610S

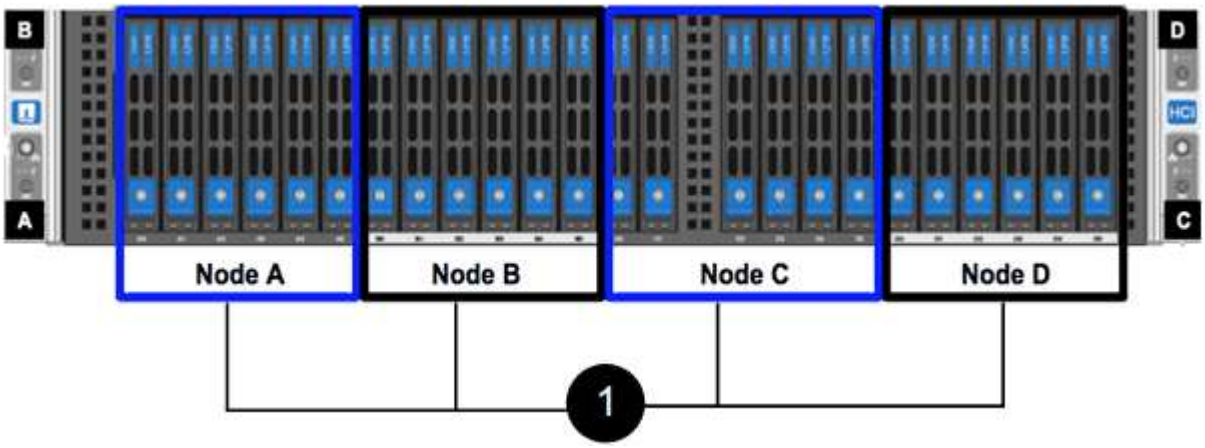
H410S

Schritte

1. Installieren Sie die H410S Nodes im Chassis. Dies ist ein Beispiel aus der Rückansicht eines Chassis mit vier installierten Nodes:

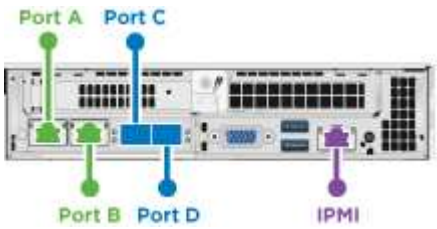
Gehen Sie beim Anheben der Hardware und beim Einbauen im Rack vorsichtig vor. Ein leeres 2-HE-Chassis mit vier Nodes wiegt 24.7 kg (54.45 lb) und ein Node wiegt 8.0 lb (3.6 kg).

2. Installieren Sie die Laufwerke.



3. Die Nodes verkabeln.

Wenn die Luftströmungsöffnungen an der Rückseite des Gehäuses durch Kabel oder Etiketten blockiert sind, kann dies zu vorzeitigen Komponentenausfällen aufgrund einer Überhitzung führen.



- Verbinden Sie für die Managementkonnektivität zwei CAT5e- oder höhere Kabel mit den Ports A und B.
- Verbinden Sie zwei SFP28/SFP+-Kabel oder Transceiver in den Ports C und D für die Speicherkonnektivität.
- (Optional, empfohlen) Verbinden Sie ein CAT5e-Kabel mit dem IPMI-Port für Out-of-Band-Management-Konnektivität.

4. Schließen Sie das Netzkabel an die beiden Netzteile pro Chassis an und stecken Sie sie in eine 240-V-PDU oder eine Steckdose.
5. Schalten Sie die Nodes ein.

Das Booten des Node dauert etwa sechs Minuten.

H610S

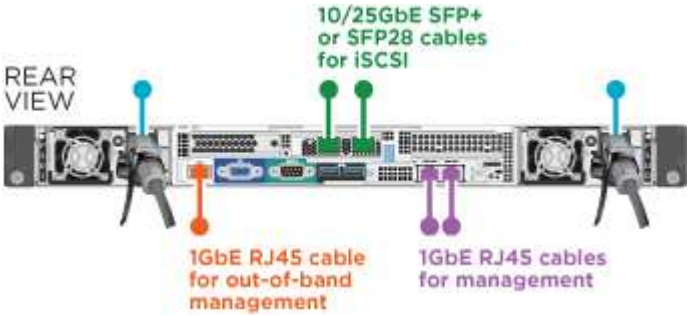
Schritte

1. Installieren Sie das H610S-Chassis. Hier sehen Sie eine Abbildung zur Installation des Node/Chassis im Rack:

> Gehen Sie beim Anheben der Hardware und beim Einbauen im Rack vorsichtig vor. Ein H610S Chassis wiegt 18.4 kg (40.5 lb).

2. Die Nodes verkabeln.

> Wenn die Luftströmungsöffnungen an der Rückseite des Gehäuses durch Kabel oder Etiketten blockiert sind, kann dies zu vorzeitigen Komponentenausfällen aufgrund einer Überhitzung führen.



   - Verbinden Sie den Node mit einem 10/25-GbE-Netzwerk mit zwei SFP28- oder SFP+-Kabeln.
   - Verbinden Sie den Node über zwei RJ45-Anschlüsse mit einem 1-GbE-Netzwerk.
   - Verbinden Sie den Node über einen RJ-45-Anschluss im IPMI-Port mit einem 1-GbE-Netzwerk.
   - Verbinden Sie die beiden Stromkabel mit dem Node.

3. Schalten Sie die Nodes ein.

> Es dauert etwa fünf Minuten und 30 Sekunden, bis der Node gebootet wird.

Konfigurieren Sie die Nodes

Nachdem Sie die Hardware im Rack untergebracht und verkabeln, können Sie Ihre neue Speicherressource konfigurieren.

Schritte

1. Schließen Sie eine Tastatur und einen Monitor an den Knoten an.
2. Konfigurieren Sie in der angezeigten Terminal User Interface (TUI) über die Bildschirmnavigation die Netzwerk- und Clustereinstellungen für den Knoten.

   Sie sollten die IP-Adresse des Knotens von der TUI erhalten. Dies ist erforderlich, wenn Sie einem Cluster den Node hinzufügen. Nachdem Sie die Einstellungen gespeichert haben, befindet sich der Node in einem ausstehenden Status und kann einem Cluster hinzugefügt werden. Weitere Informationen finden Sie im Abschnitt <INSERT Link to Setup >.

3. Konfigurieren Sie die Out-of-Band-Verwaltung mit dem Baseboard Management Controller (BMC). Diese Schritte gelten **nur für H610S** Nodes.
   a. Verwenden Sie einen Webbrowser, und navigieren Sie zur standardmäßigen BMC-IP-Adresse: 192.168.0.120
   b. Melden Sie sich mit **root** als Benutzername und **calvin** als Passwort an.
   c. Navigieren Sie im Bildschirm Knotenverwaltung zu **Einstellungen** > **Netzwerkeinstellungen** und konfigurieren Sie die Netzwerkparameter für den Out-of-Band-Management-Port.

Siehe "Dieser KB-Artikel (Anmeldung erforderlich)".

Erstellen eines Clusters

Nachdem Sie der Installation den Speicherknoten hinzugefügt und die neue Speicherressource konfiguriert haben, können Sie ein neues Storage-Cluster erstellen

Schritte

1. Greifen Sie von einem Client auf demselben Netzwerk wie der neu konfigurierte Node auf die NetApp Element Software-UI zu, indem Sie die IP-Adresse des Node eingeben.
2. Geben Sie die erforderlichen Informationen im Fenster **Erstellen eines neuen Clusters** ein. Siehe "Setup-Übersicht" Finden Sie weitere Informationen.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

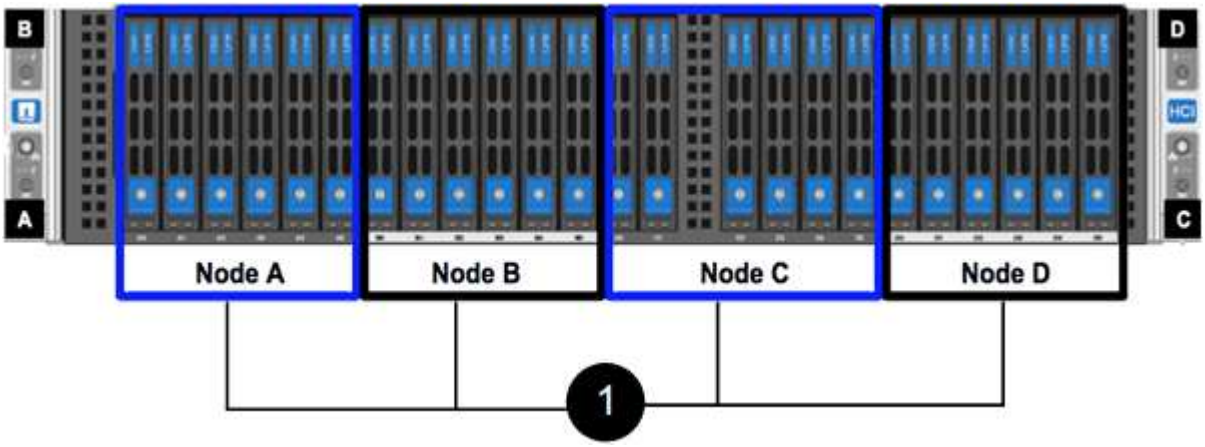
Einen H410S Node austauschen

Sie sollten einen Storage-Node ersetzen, wenn ein CPU-Fehler, Probleme mit der Radian-Karte oder andere Probleme mit der Hauptplatine auftreten oder sich nicht einschalten. Die Anweisungen gelten für H410S Storage-Nodes.

Warnmeldungen in der NetApp Element-Software-UI melden Sie bei Ausfall eines Speicherknoten. Verwenden Sie die Element-UI, um die Seriennummer (Service-Tag) des ausgefallenen Knotens zu erhalten. Sie benötigen diese Informationen, um den fehlgeschlagenen Node im Cluster zu finden.

Hier sehen Sie die Rückseite eines 2-HE-Chassis mit vier Nodes und vier Storage-Nodes:

Hier ist die Vorderansicht eines Chassis mit vier Nodes mit H410S Nodes, in dem die entsprechenden Schächte für jeden Node angezeigt werden:



Was Sie benötigen

- Sie haben überprüft, ob Ihr Storage-Node fehlerhaft ist und ersetzt werden muss.
- Sie haben einen Ersatz-Speicherknoten erhalten.
- Sie haben ein elektrostatisches Entladungsband (ESD) oder einen anderen antistatischen Schutz.
- Sie haben jedes Kabel gekennzeichnet, das mit dem Speicher-Node verbunden ist.

Hier finden Sie eine grobe Übersicht über die Schritte:

- Bereiten Sie den Austausch des Node vor
- Ersetzen Sie den Node im Chassis
- Fügen Sie den Node dem Cluster hinzu

Bereiten Sie den Austausch des Node vor

Sie sollten den fehlerhaften Storage-Node in der NetApp Element-Software-UI ordnungsgemäß aus dem Cluster entfernen, bevor Sie den Ersatz-Node installieren. Dies ist möglich, ohne dass es zu einer Serviceunterbrechung kommt. Sie sollten die Seriennummer des fehlerhaften Storage Node von der Element UI erhalten und mit der Seriennummer auf dem Aufkleber auf der Rückseite des Node übereinstimmen.

Schritte

1. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke**.
2. Entfernen Sie die Laufwerke vom Node mithilfe einer der folgenden Methoden:

Option	Schritte
Um einzelne Laufwerke zu entfernen	a. Klicken Sie auf **Aktionen** für das Laufwerk, das Sie entfernen möchten. b. Klicken Sie Auf **Entfernen**.
Um mehrere Laufwerke zu entfernen	a. Wählen Sie alle Laufwerke aus, die Sie entfernen möchten, und klicken Sie auf **Massenaktionen**. b. Klicken Sie Auf **Entfernen**.

3. Wählen Sie **Cluster** > **Knoten**.
4. Notieren Sie sich die Seriennummer (Service-Tag) des fehlerhaften Knotens. Sie sollten sie mit der Seriennummer auf dem Aufkleber auf der Rückseite des Node übereinstimmen.
5. Nachdem Sie die Seriennummer notieren, entfernen Sie den Node wie folgt aus dem Cluster:
   a. Wählen Sie für den Knoten, den Sie entfernen möchten, die Schaltfläche **Aktionen**.
   b. Wählen Sie **Entfernen**.

Ersetzen Sie den Node im Chassis

Nachdem Sie den fehlerhaften Node mithilfe der NetApp Element Software-UI aus dem Cluster entfernt haben, können Sie den Node physisch vom Chassis entfernen. Sie sollten den Ersatz-Node im selben Steckplatz im Chassis installieren, aus dem Sie den ausgefallenen Node entfernt haben.

Schritte

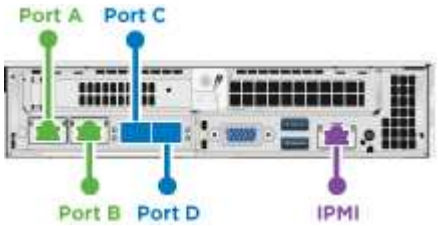
1. Tragen Sie vor dem Fortfahren einen antistatischen Schutz.
2. Packen Sie den neuen Storage-Node aus, und stellen Sie ihn auf eine Ebene Fläche in der Nähe des Chassis ein.

   Bewahren Sie das Verpackungsmaterial auf, wenn Sie den fehlerhaften Node an NetApp zurücksenden.

3. Beschriften Sie jedes Kabel, das an der Rückseite des Storage Node eingesetzt wird, den Sie entfernen möchten.

   Nach der Installation des neuen Speicherknoten sollten die Kabel in die ursprünglichen Anschlüsse eingesetzt werden.

   Dies ist ein Bild, das die Rückseite eines Storage-Nodes anzeigt:

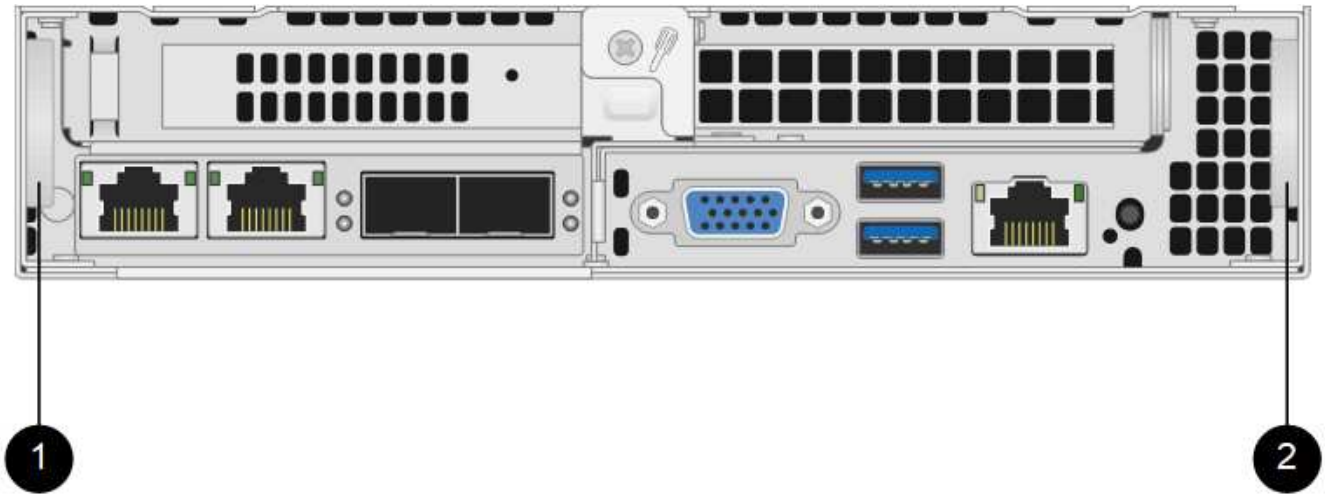


Port	Details
Port A	1/10-GbE-RJ45-Port

Port	Details
Port B	1/10-GbE-RJ45-Port
Port C	10 GbE SFP+ oder SFP28 Port
Port D	10 GbE SFP+ oder SFP28 Port
IPMI	1/10-GbE-RJ45-Port

4. Trennen Sie alle Kabel vom Storage-Node.
5. Ziehen Sie den Nockengriff auf der rechten Seite des Knotens nach unten, und ziehen Sie den Knoten mit beiden Nockengriffen heraus.

   Der Nockengriff, den Sie nach unten ziehen, hat einen Pfeil darauf, um die Richtung anzuzeigen, in der er sich bewegt. Der andere Nockengriff bewegt sich nicht und ist dort, um den Knoten herausziehen zu helfen.



Element	Beschreibung
1	CAM-Griff zum Herausziehen des Knotens
2	CAM-Griff, den Sie nach unten ziehen, bevor Sie den Knoten herausziehen.

Unterstützen Sie den Node mit beiden Händen, wenn Sie ihn aus dem Chassis ziehen.

6. Legen Sie den Knoten auf eine Ebene Fläche.

   Sie müssen den Node verpacken und ihn an NetApp zurücksenden.

7. Installieren Sie den Ersatzknoten im gleichen Steckplatz im Chassis.

Stellen Sie sicher, dass Sie beim Einschieben des Node in das Chassis keine übermäßige Kraft verwenden.

8. Verschieben Sie die Laufwerke vom entfernten Node und fügen Sie sie in den neuen Node ein.
9. Schließen Sie die Kabel wieder an die Anschlüsse an, von denen Sie sie ursprünglich getrennt haben.

   Die Etiketten, die Sie beim Abstecken auf den Kabeln angebracht haben, helfen Ihnen dabei.

   a. Wenn die Luftströmungsöffnungen an der Rückseite des Gehäuses durch Kabel oder Etiketten blockiert sind, kann dies zu vorzeitigen Komponentenausfällen aufgrund einer Überhitzung führen.
   b. Zwingen Sie die Kabel nicht zu den Ports. Kabel, Ports oder beides können beschädigt werden.

   Stellen Sie sicher, dass der Ersatz-Node auf die gleiche Weise wie die anderen Nodes im Chassis verkabelt ist.

10. Drücken Sie die Taste an der Vorderseite des Knotens, um ihn wieder einschalten zu können.

Fügen Sie den Node dem Cluster hinzu

Wenn Sie dem Cluster einen Node hinzufügen oder neue Laufwerke in einem vorhandenen Node installieren, werden die Laufwerke automatisch nach Verfügbarkeit registriert. Sie müssen die Laufwerke zum Cluster entweder über die Element-UI oder -API hinzufügen, bevor sie am Cluster teilnehmen können.

Die Softwareversion auf jedem Node in einem Cluster sollte kompatibel sein. Wenn Sie einem Cluster einen Node hinzufügen, wird im Cluster bei Bedarf die Cluster-Version der Element Software auf dem neuen Node installiert.

Schritte

1. Wählen Sie **Cluster** > **Knoten**.
2. Wählen Sie **Ausstehend** aus, um die Liste der ausstehenden Knoten anzuzeigen.
3. Führen Sie einen der folgenden Schritte aus:
   - Um einzelne Knoten hinzuzufügen, wählen Sie das Symbol **Aktionen** für den Knoten, den Sie hinzufügen möchten.
   - Um mehrere Knoten hinzuzufügen, aktivieren Sie das Kontrollkästchen der Knoten, die hinzugefügt werden sollen, und dann **Massenaktionen**.

   Wenn der Node, den Sie hinzufügen, eine andere Version der Element Software als die Version des Clusters hat, aktualisiert der Cluster den Node asynchron an die Version der auf dem Cluster-Master ausgeführten Element-Software. Nach der Aktualisierung des Node wird er sich automatisch dem Cluster hinzugefügt. Während dieses asynchronen Prozesses liegt der Node in einem `pendingActive` Bundesland.

4. Wählen Sie **Hinzufügen**.

   Der Node wird in der Liste der aktiven Nodes angezeigt.

5. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke**.

6. Wählen Sie **verfügbar**, um die Liste der verfügbaren Laufwerke anzuzeigen.
7. Führen Sie einen der folgenden Schritte aus:
   - Um einzelne Laufwerke hinzuzufügen, wählen Sie das Symbol **Aktionen** für das Laufwerk, das Sie hinzufügen möchten, und wählen Sie dann **Hinzufügen**.
   - Um mehrere Laufwerke hinzuzufügen, aktivieren Sie die Kontrollkästchen der Laufwerke, die hinzugefügt werden sollen, wählen Sie **Massenaktionen** und dann **Hinzufügen** aus.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Austausch eines H610S Nodes

Möglicherweise müssen Sie das Gehäuse austauschen, wenn der Lüfter, die CPU (Central Processing Unit) oder ein Duales Inline-Speichermodul (DIMM) ausfällt oder Überhitzungsprobleme oder Probleme mit dem Bootvorgang beheben. Die blinkende gelbe LED an der Vorderseite des Chassis zeigt an, dass ein Chassis möglicherweise ausgetauscht werden muss. Wenden Sie sich zunächst an den NetApp Support, bevor Sie fortfahren.

Siehe "KB-Artikel" Weitere Informationen zu Installationsanforderungen für H610S Nodes Neue und Ersatz-H610S Storage-Nodes weisen möglicherweise zusätzliche Installationsanforderungen auf Grundlage der vorhandenen Element Softwareversion des Storage-Clusters auf. Weitere Informationen erhalten Sie von Ihrem NetApp Support.

Die Begriffe „Node“ und „Chassis“ werden bei H610S gemeinsam verwendet, bei dem es sich um ein 1-HE-Chassis handelt.

Best Practices zum Hinzufügen und Entfernen von Laufwerken

Beim Hinzufügen von Laufwerken zum Cluster sollten Sie folgende Best Practices beachten:

- Fügen Sie alle Blocklaufwerke hinzu, und stellen Sie sicher, dass die Blocksynchronisierung abgeschlossen ist, bevor Sie die Slice-Laufwerke hinzufügen.
- Fügen Sie für Element Software ab 10.x alle Blocklaufwerke gleichzeitig ein. Stellen Sie sicher, dass Sie dies nicht für mehr als drei Knoten gleichzeitig tun.
- Fügen Sie bei der Element Software 9.x und früher drei Laufwerke gleichzeitig hinzu, um sie vollständig zu synchronisieren, bevor Sie die nächste Gruppe von drei hinzufügen.
- Entfernen Sie das Slice-Laufwerk, und stellen Sie sicher, dass die Schichtsynchronisierung abgeschlossen ist, bevor Sie die Blocklaufwerke entfernen.
- Entfernen Sie alle Blocklaufwerke gleichzeitig aus einem einzelnen Node. Vergewissern Sie sich, dass die Blocksynchronisierung abgeschlossen ist, bevor Sie zum nächsten Node fahren.

Was Sie benötigen

- Sie haben den NetApp Support kontaktiert. Wenn Sie einen Ersatz bestellen, sollten Sie beim NetApp Support einen Case eröffnen.

- Sie haben den Ersatzknoten erhalten.
- Sie haben ein elektrostatisches Entladungsband (ESD) oder einen anderen antistatischen Schutz.
- Wenn Sie den RTFI-Prozess (Return to Factory Image) durchführen müssen, haben Sie den USB-Schlüssel erhalten. NetApp Support hilft Ihnen bei der Entscheidung, ob der RTFI-Prozess ausgeführt werden muss.
- Sie verfügen über eine Tastatur und einen Monitor.
- Sie haben den ausgefallenen Node ordnungsgemäß aus dem Cluster entfernt.
- Wenn ein DIMM ausgefallen ist, haben Sie die Laufwerke entfernt, bevor Sie den Node aus dem Cluster entfernen.

Über diese Aufgabe

Alarme in der Element UI melden Sie, wenn ein Host ausfällt. Sie müssen die Seriennummer des ausgefallenen Hosts vom VMware vSphere Web Client mit der Seriennummer auf dem Aufkleber auf der Rückseite des Node übereinstimmen.

Schritte

1. Suchen Sie die Service-Tag-Nummer an der Vorderseite des ausgefallenen Gehäuses.

2. Vergewissern Sie sich, dass die Seriennummer auf der Service-Tag-Nummer der NetApp Support-Fallnummer bei der Bestellung des Ersatzgehäuses entspricht.
3. Schließen Sie die Tastatur und den Monitor an die Rückseite des defekten Gehäuses an.
4. Überprüfen Sie die Seriennummer des ausgefallenen Nodes mit NetApp Support.
5. Schalten Sie das Chassis aus.
6. Beschriften Sie die Laufwerke vorn und die Kabel auf der Rückseite mit ihren Positionen, damit Sie sie nach dem Austausch an denselben Stellen wiederaufnehmen können. Die Anordnung der Laufwerke im Gehäuse ist in der folgenden Abbildung dargestellt:

7. Entfernen Sie die Kabel.
8. Entfernen Sie das Gehäuse, indem Sie die Rändelschrauben an den BefestigungsOhren lösen. Sie sollten das fehlerhafte Chassis verpacken und an NetApp zurücksenden.
9. Setzen Sie das Ersatzgehäuse ein.
10. Entfernen Sie die Laufwerke sorgfältig aus dem ausgefallenen Chassis und setzen Sie sie in das Ersatzgehäuse ein.

> Sie sollten die Laufwerke in die gleichen Steckplätze einsetzen, bevor Sie sie entfernt haben.

11. Entfernen Sie die Netzteile aus dem ausgefallenen Gehäuse und setzen Sie sie in das Ersatzgehäuse ein.
12. Stecken Sie die Netzteilkabel und die Netzwerkkabel in die ursprünglichen Anschlüsse.
13. SFP-Transceiver (Small Form-Factor Pluggable) können möglicherweise in die 10-GbE-Ports des Ersatz-Nodes eingesetzt werden. Sie sollten sie entfernen, bevor Sie die 10-GbE-Ports verkabeln.

> Wenn der Switch die Kabel nicht erkennt, lesen Sie die Dokumentation des Switch-Anbieters.

14. Schalten Sie das Gehäuse ein, indem Sie den Netzschalter an der Vorderseite drücken. Es dauert etwa fünf Minuten und 30 Sekunden, bis der Node gebootet wird.
15. Führen Sie die Konfigurationsschritte durch.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Ersetzen Sie Laufwerke

Wenn ein Laufwerk defekt ist oder der Verschleiß des Laufwerks unter einen Schwellenwert fällt, sollten Sie dieses austauschen. Alarme in der Element Software-UI benachrichtigen Sie, wenn ein Laufwerk ausgefallen ist oder ausfällt. Sie können ein ausgefallenes Laufwerk im laufenden Betrieb austauschen.

Über diese Aufgabe

Dieses Verfahren dient zum Austausch von Laufwerken in H410S und H610S Storage-Nodes. Durch das Entfernen eines Laufwerks kann das Laufwerk offline geschaltet werden. Alle Daten auf dem Laufwerk werden entfernt und auf andere Laufwerke im Cluster migriert. Die Datenmigration auf andere aktive Laufwerke im System kann abhängig von Kapazitätsauslastung und aktiver I/O im Cluster einige Minuten bis eine Stunde dauern. Beim Entfernen und Austauschen von Laufwerken sollten Sie folgende Best Practices beachten:

- Halten Sie das Laufwerk in der ESD-Tasche, bis Sie bereit sind, es zu installieren.
- Öffnen Sie die ESD-Tasche von Hand oder schneiden Sie die Oberseite mit einer Schere ab.

- Tragen Sie stets ein ESD-Handgelenkband, das an einer unbemalten Oberfläche auf Ihrem Chassis geerdet ist.
- Beim Entfernen, Installieren oder Tragen eines Laufwerks immer beide Hände verwenden.
- Niemals ein Laufwerk in das Chassis zwingen.
- Verwenden Sie beim Transport von Laufwerken stets die genehmigte Verpackung.
- Legen Sie keine Laufwerke aufeinander ab.

Best Practices zum Hinzufügen und Entfernen von Laufwerken

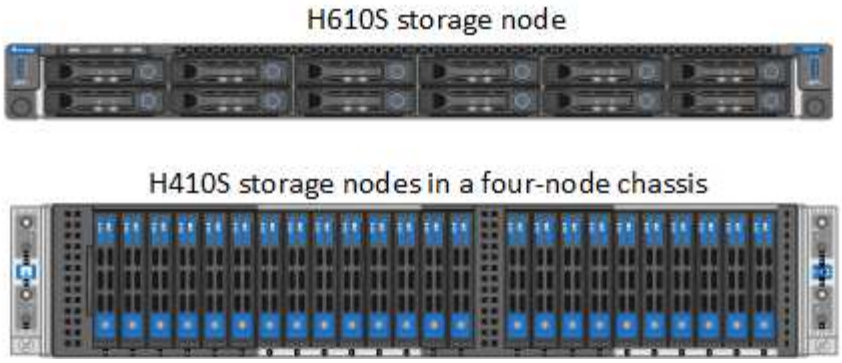
- Fügen Sie alle Blocklaufwerke hinzu, und stellen Sie sicher, dass die Blocksynchronisierung abgeschlossen ist, bevor Sie die Slice-Laufwerke hinzufügen.
- Fügen Sie für Element Software ab 10.x alle Blocklaufwerke gleichzeitig ein. Stellen Sie sicher, dass Sie dies nicht für mehr als drei Knoten gleichzeitig tun.
- Fügen Sie bei der Element Software 9.x und früher drei Laufwerke gleichzeitig hinzu, um sie vollständig zu synchronisieren, bevor Sie die nächste Gruppe von drei hinzufügen.
- Entfernen Sie das Slice-Laufwerk, und stellen Sie sicher, dass die Schichtsynchronisierung abgeschlossen ist, bevor Sie die Blocklaufwerke entfernen.
- Entfernen Sie alle Blocklaufwerke gleichzeitig aus einem einzelnen Node. Vergewissern Sie sich, dass die Blocksynchronisierung abgeschlossen ist, bevor Sie zum nächsten Node fahren.

Schritte

1. Entfernen Sie das Laufwerk mithilfe der NetApp Element Software-UI aus dem Cluster:
   a. Wählen Sie in der Element UI die Option **Cluster > Laufwerke** aus.
   b. Wählen Sie **fehlgeschlagen** aus, um die Liste der ausgefallenen Laufwerke anzuzeigen.
   c. Notieren Sie sich die Steckplatznummer des ausgefallenen Laufwerks. Sie benötigen diese Informationen, um das ausgefallene Laufwerk im Chassis zu finden.
   d. Wählen Sie **Aktionen** für das Laufwerk, das Sie entfernen möchten.
   e. Wählen Sie **Entfernen**.

   > Falls nicht genügend Kapazität zum Entfernen aktiver Laufwerke vor dem Entfernen eines Node vorhanden ist, wird beim Bestätigen des Entfernens des Laufwerks eine Fehlermeldung angezeigt. Nachdem Sie den Fehler behoben haben, können Sie das Laufwerk nun physisch aus dem Gehäuse entfernen.

2. Setzen Sie das Laufwerk aus dem Gehäuse wieder ein:
   a. Packen Sie das Ersatzlaufwerk aus und legen Sie es auf eine flache, statische Oberfläche in der Nähe des Racks. Speichern Sie das Verpackungsmaterial für, wenn Sie das ausgefallene Laufwerk an NetApp zurücksenden. Hier ist die Vorderansicht der H610S und H410S Storage-Nodes mit den Laufwerken:



b. (**H410S nur**) folgende Schritte durchführen:

   i. Identifizieren Sie den Knoten, indem Sie die Seriennummer (Service-Tag) mit der Nummer, die Sie in der Element-UI angegeben haben, übereinstimmen. Die Seriennummer befindet sich auf einem Aufkleber auf der Rückseite jedes Node. Nachdem Sie den Node identifiziert haben, können Sie die Steckplatzinformationen verwenden, um den Steckplatz zu identifizieren, in dem sich das ausgefallene Laufwerk befindet. Laufwerke sind alphabetisch von A bis D und von 0 bis 5 angeordnet.

   ii. Entfernen Sie die Blende.

   iii. Drücken Sie die Entriegelungstaste am ausgefallenen Laufwerk:

   Wenn Sie die Entriegelungstaste drücken, öffnen sich der Nockengriff an den Antriebsfedern teilweise und der Antrieb löst sich von der Mittelplatine aus.

   i. Öffnen Sie den Nockengriff, und schieben Sie das Laufwerk vorsichtig mit beiden Händen heraus.

   ii. Platzieren Sie das Laufwerk auf einer antistatischen, Ebenen Fläche.

   iii. Setzen Sie das Ersatzlaufwerk mit beiden Händen vollständig in den Steckplatz ein.

   iv. Drücken Sie den Nockengriff nach unten, bis er einrastet.

   v. Bringen Sie die Blende wieder an.

   vi. Benachrichtigen Sie den NetApp Support über den Austausch von Laufwerken. Der NetApp Support enthält Anweisungen zum Zurücksenden des ausgefallenen Laufwerks.

c. (**H610S nur**) folgende Schritte durchführen:

   i. Ordnen Sie die Steckplatznummer des ausgefallenen Laufwerks von der Element-UI mit der

Nummer auf dem Chassis an. Die LED am ausgefallenen Laufwerk leuchtet gelb.

ii. Entfernen Sie die Blende.

iii. Drücken Sie die Entriegelungstaste, und entfernen Sie das ausgefallene Laufwerk wie in der folgenden Abbildung gezeigt:

Stellen Sie sicher, dass der Griff des Fachs vollständig geöffnet ist, bevor Sie versuchen, das Laufwerk aus dem Gehäuse zu schieben.

i. Schieben Sie das Laufwerk heraus, und legen Sie es auf eine statisch freie, Ebene Fläche.

ii. Drücken Sie die Entriegelungstaste am Ersatzlaufwerk, bevor Sie es in den Laufwerkschacht einsetzen. Die Feder des Griffs der Laufwerksfachleiste ist geöffnet.

iii. Setzen Sie das Ersatzlaufwerk ohne übermäßige Kraft ein. Wenn das Laufwerk vollständig eingesetzt ist, hören Sie einen Klick.

iv. Schließen Sie den Griff des Laufwerksfachs vorsichtig.

v. Bringen Sie die Blende wieder an.

vi. Benachrichtigen Sie den NetApp Support über den Austausch von Laufwerken. Der NetApp Support enthält Anweisungen zum Zurücksenden des ausgefallenen Laufwerks.

3. Fügen Sie das Laufwerk über die Element-UI zurück zum Cluster hinzu.

Wenn Sie ein neues Laufwerk in einem bestehenden Knoten installieren, registriert sich das Laufwerk automatisch als **verfügbar** in der Element UI. Sie sollten das Laufwerk zum Cluster hinzufügen, bevor es am Cluster teilnehmen kann.

a. Wählen Sie in der Element UI die Option **Cluster > Laufwerke** aus.

b. Wählen Sie **verfügbar**, um die Liste der verfügbaren Laufwerke anzuzeigen.

c. Wählen Sie das Aktionen-Symbol für das Laufwerk aus, das Sie hinzufügen möchten, und wählen Sie **Hinzufügen**.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Ersetzen Sie ein Netzteil

Jedes Chassis besitzt zwei Netzteile für Redundanz bei der Stromversorgung. Wenn ein Netzteil defekt ist, sollten Sie es so schnell wie möglich austauschen, um sicherzustellen, dass das Gehäuse über eine redundante Stromquelle verfügt.

Was Sie benötigen

- Sie haben festgestellt, dass das Netzteil defekt ist.
- Sie haben ein Ersatznetzteil.
- Sie haben überprüft, dass das zweite Netzteil in Betrieb ist.

- Sie haben ein elektrostatisches Entladungsband (ESD) oder andere antistatische Vorsichtsmaßnahmen getroffen.

Über diese Aufgabe

Das Ersatzverfahren gilt für die folgenden Node-Modelle:

- Zwei Höheneinheiten (2 HE) mit vier Nodes NetApp HCI-Chassis
- Eine Rack-Einheit (1 HE) H610S Storage-Chassis

> Bei H610S werden die Begriffe „Node“ und „Chassis“ austauschbar, da Node und Chassis keine separaten Komponenten sind, anders als bei einem 2-HE-Chassis mit vier Nodes.

Alarme in der Element-UI liefern Informationen über das ausgefallene Netzteil, was sich auf PS1 oder PS2 bezieht. In einem NetApp HCI 2-HE-Chassis mit vier Nodes bezeichnet PS1 die Einheit in der oberen Zeile des Gehäuses und PS2 die Einheit in der unteren Zeile des Gehäuses. Sie können das fehlerhafte Netzteil austauschen, während das Gehäuse eingeschaltet und funktionsfähig ist, solange das redundante Netzteil funktioniert.

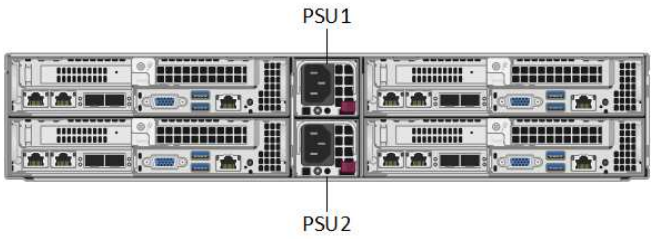
> Wenn Sie beide PSUs an einem Node ersetzen, müssen die Netzteile die gleiche Teilenummer und Nennleistung haben. Nicht übereinstimmende Netzteile können das System beschädigen.

Schritte

1. Suchen Sie das defekte Netzteil im Gehäuse. Die LED auf dem defekten Gerät zeigt gelb an.

   > Die Netzteile befinden sich je nach Gehäusetyp unterschiedlich.

   Die Positionen der Netzteile finden Sie in den folgenden Bildern:

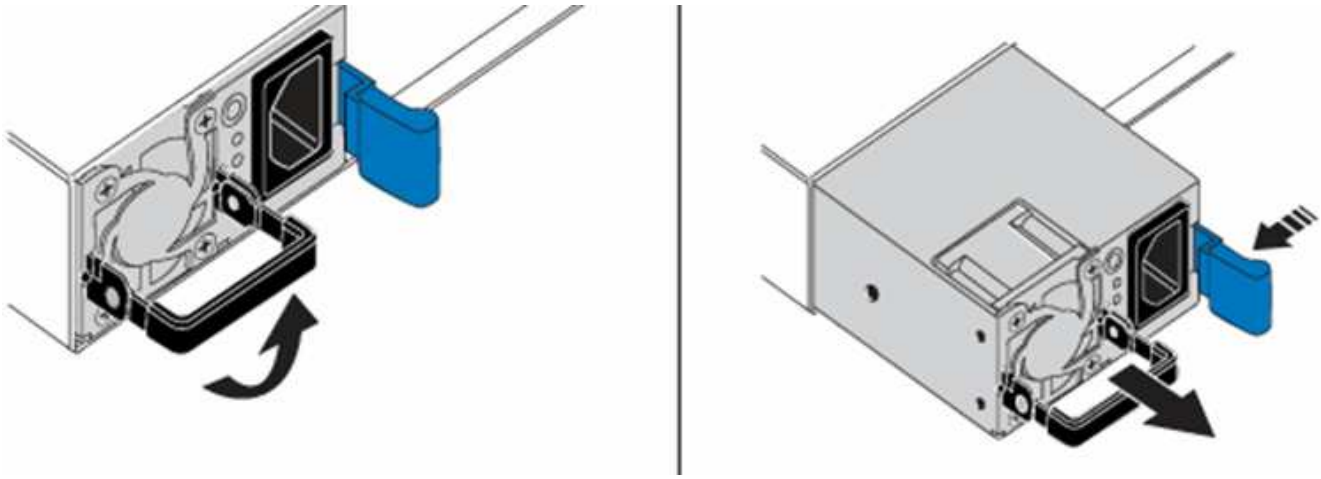
Modell	Position der Netzteile
2-HE-NetApp HCI-Storage-Chassis mit vier Nodes	 Die Nodes in Ihrem Chassis können je nach Node-Typ (Storage oder Computing) unterschiedlich aussehen.
H610S Chassis	

2. Identifizieren Sie den richtigen Knoten mithilfe des blauen Ausziehtags- oder der Seriennummer. Auf dem blauen Pulldown-Tag werden die Seriennummer (S/N) und das Laufwerklayout aufgeführt. Bestätigen Sie

die zu wartenden Seriennummer des Node.

- Wenn Sie beide Netzteile austauschen, fahren Sie mit Schritt 3 fort.
- Wenn Sie nur ein Netzteil ersetzen, fahren Sie mit Schritt 4 fort.

3. Vergewissern Sie sich, dass der Node heruntergefahren oder bereit ist, heruntergefahren wurde, um den Service zu nutzen. Beachten Sie Folgendes:
   - Ein Node, der heruntergefahren wurde, zeigt keine blauen ein/aus-LEDs an den Laufwerken oder dem Netzschalter an.
   - Ein Node, der noch nicht heruntergefahren wurde, zeigt blaue LEDs an den Laufwerken und den Netzschalter an.
   - Ein Node, der heruntergefahren wurde und für den Service bereit ist, zeigt eine blinkende PSU-LED an, die blinkt (grün) und aus (keine Farbe).
   - Ein Node, der noch nicht heruntergefahren wurde, zeigt die grünen LEDs an den Netzteilen an.
4. Ziehen Sie das Netzkabel vom Netzteil oder von beiden Netzkabeln ab, wenn Sie beide Geräte austauschen.
5. Heben Sie den Nockengriff an, und drücken Sie die blaue Verriegelung, um das Netzteil herauszuschieben.



Die Abbildung ist ein Beispiel. Die Positionen der Netzteile im Gehäuse und die Farbe der Entriegelungstaste variieren je nach Gehäusetyp.

Stellen Sie sicher, dass Sie beide Hände verwenden, um das Gewicht des Netzteils zu unterstützen.

Wiederholen Sie die Schritte 3, 4 und 5, wenn Sie ein zweites Netzteil ersetzen.

6. Suchen Sie das Etikett an der Netzteileinheit, die Sie aus dem Gehäuse entfernt haben. Das Etikett enthält Angaben zum Hersteller und zur Ausgangsleistung.

Ersetzen Sie das Netzteil nicht, wenn die Wattleistung des Netzteils Ihrer RMA nicht mit der Leistung des entfernten Netzteils übereinstimmt. Wenden Sie sich an den NetApp Support, um die nächsten Schritte zu erfahren.

7. Richten Sie die Kanten des Netzteils mit beiden Händen an der Öffnung im Gehäuse aus. Schieben Sie das Gerät vorsichtig mit dem Nockengriff in das Gehäuse, bis es einrastet, und bringen Sie den

Nockengriff in die aufrechte Position zurück.

8. Schließen Sie ein oder beide Netzkabel an.
9. Wenn Sie beide Netzteile ausgetauscht haben, fahren Sie mit der Vorderseite des Node fort und drücken Sie den Netzschalter, um die Nodes einschalten zu können. Nach dem Einschalten leuchtet die Betriebsschalter-LED durchgehend blau. Die blauen LEDs für die Laufwerke und die Identifikationstaste beginnen zu blinken.
10. Senden Sie das fehlerhafte Gerät an NetApp zurück. Befolgen Sie die Anweisungen im Lieferumfang, die Sie erhalten haben.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Hardwareinformationen zur SF-Series

Ein Chassis austauschen

Möglicherweise müssen Sie das Gehäuse austauschen, wenn der Lüfter, die CPU (Central Processing Unit) oder ein Duales Inline-Speichermodul (DIMM) ausfällt oder Überhitzungsprobleme oder Probleme mit dem Bootvorgang beheben. Cluster-Fehler in der Benutzeroberfläche der NetApp Element Software (UI) und die blinkende gelbe LED an der Vorderseite des Gehäuses zeigen, dass ein Gehäusetausch erforderlich ist. Wenden Sie sich zunächst an den NetApp Support, bevor Sie fortfahren.

Was Sie benötigen

- Sie haben den NetApp Support kontaktiert.

  Wenn Sie einen Ersatz bestellen, müssen Sie beim NetApp Support einen Case eröffnen.

- Sie haben das Ersatzgehäuse erhalten.
- Sie haben ein elektrostatisches Entladungsband (ESD) oder einen anderen antistatischen Schutz.
- Wenn Sie den RTFI-Prozess (Return to Factory Image) durchführen müssen, haben Sie den USB-Schlüssel erhalten.

  NetApp Support hilft Ihnen bei der Entscheidung, ob RTFI erforderlich ist. Siehe "Diesen KB-Artikel (Anmeldung erforderlich)".

- Sie verfügen über eine Tastatur und einen Monitor.

Über diese Aufgabe

Die Anweisungen in diesem Dokument gelten, wenn Sie ein 1-HE-Chassis (One-Rack Unit) mit einem der folgenden Nodes haben:

- SF2405
- SF4805
- SF9605

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

Je nach Ihrer Element Softwareversion werden die folgenden Nodes nicht unterstützt:

- Ab Element 12.8, SF4805, SF9605, SF19210 und SF38410 Storage-Nodes
- Ab Element 12.7, SF2405 und SF9608 Storage-Nodes und FC-Nodes FC0025 und SF-FCN-01
- Ab Element 12.0, SF3010, SF6010 und SF9010 Storage-Nodes

Schritte

1. Suchen Sie die Service-Tag-Nummer des ausgefallenen Chassis und stellen Sie sicher, dass die Seriennummer der Nummer auf dem Fall entspricht, den Sie bei der Bestellung des Ersatzes geöffnet haben.

   Sie können die Service-Tag-Nummer von der Vorderseite des Gehäuses aus finden.

   Die folgende Abbildung zeigt ein Beispiel für die Service-Tag-Nummer:

   Die obige Abbildung ist ein Beispiel. Die genaue Position der Service-Tag-Nummer kann je nach Hardware-Modell variieren.

2. Schließen Sie die Tastatur und den Monitor an die Rückseite des defekten Gehäuses an.
3. Überprüfen Sie die Chassis-Informationen mithilfe des NetApp Supports.
4. Schalten Sie das Chassis aus.
5. Beschriften Sie die Laufwerke an der Vorderseite des Chassis und die Kabel auf der Rückseite.

   Fibre Channel-Knoten haben keine Laufwerke in der Vorderseite.

6. Entfernen Sie die Netzteile und Kabel.
7. Entfernen Sie die Antriebe vorsichtig, und legen Sie sie auf eine antistatische, Ebene Oberfläche.

   Wenn Sie über einen Fibre Channel-Knoten verfügen, können Sie diesen Schritt überspringen.

8. Entfernen Sie das Gehäuse, indem Sie auf die Verriegelung drücken oder die Rändelschraube je nach Hardware-Modell herausdrehen.

   Sie sollten das fehlerhafte Chassis verpacken und an NetApp zurücksenden.

9. **Optional**: Entfernen Sie die Schienen und installieren Sie die neuen Schienen, die im Lieferumfang Ihres Ersatzgehäuses enthalten sind.

   Sie können die vorhandenen Schienen wiederverwenden. Wenn Sie die vorhandenen Schienen erneut verwenden, können Sie diesen Schritt überspringen.

10. Schieben Sie das Ersatzgehäuse auf die Schienen.
11. Legen Sie bei Storage-Nodes die Laufwerke des ausgefallenen Chassis in das Ersatzgehäuse ein.

    Sie sollten die Laufwerke in die gleichen Steckplätze einsetzen wie im ausgefallenen Chassis.

12. Installieren Sie die Netzteile.
13. Stecken Sie die Netzkabel sowie die 1-GbE- und 10-GbE-Kabel in die ursprünglichen Ports ein.

    SFP-Transceiver (Small Form Factor Pluggable) können möglicherweise in die 10-GbE-Ports des Ersatzgehäuses eingesetzt werden. Sie sollten sie entfernen, bevor Sie die 10-GbE-Ports verkabeln.

14. Wenn Sie festgestellt haben, dass Sie den RTFI-Prozess auf dem Knoten nicht ausführen müssen, starten Sie den Knoten und warten Sie, bis die Terminal-Benutzeroberfläche (TUI) angezeigt wird. Fahren Sie mit Schritt 16 fort, und lassen Sie den Knoten beim Hinzufügen über die UI ein erneutes Image erstellen.
15. **Optional**: Falls der NetApp Support eine erneute Abbildung des Knotens mit einem USB-Schlüssel empfiehlt, führen Sie die folgenden Teilschritte durch:
    a. Schalten Sie das Chassis ein. Es startet mit dem RTFI-Schlüsselbild.
    b. Geben Sie bei der ersten Eingabeaufforderung **Y** ein, um den Speicherknoten abzugbildern.
    c. Geben Sie an der zweiten Eingabeaufforderung **N** für die Hardware-Zustandsprüfung ein.

       Wenn das RTFI-Skript ein Problem mit einer Hardwarekomponente erkennt, wird ein Fehler in der Konsole angezeigt. Wenn ein Fehler auftritt, wenden Sie sich an den NetApp Support. Nach Abschluss des RTFI-Prozesses wird der Node heruntergefahren.

    d. Entfernen Sie den USB-Schlüssel aus dem USB-Steckplatz.
    e. Starten Sie den neu abgebauten Knoten, und warten Sie, bis die TUI angezeigt wird.
16. Konfigurieren Sie Netzwerk- und Clusterinformationen über die TUI.

    Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

17. Fügen Sie den neuen Node mithilfe der Cluster-TUI zum Cluster hinzu.

18. Packen Sie das ausgefallene Chassis zusammen und stellen Sie es wieder her.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Ersetzen von Laufwerken für SF-Series Storage-Nodes

Sie können ein ausgefallenes Solid State-Laufwerk gegen ein Ersatzlaufwerk austauschen.

Was Sie benötigen

- Sie haben ein Ersatzlaufwerk.
- Sie haben ein elektrostatisches Entladungsband (ESD) oder andere antistatische Vorsichtsmaßnahmen getroffen.
- Sie haben den NetApp Support kontaktiert, um zu überprüfen, ob die SSD ersetzt werden muss, und um die ordnungsgemäße Behebung des Problems zu gewährleisten.

  Wenn Sie den NetApp Support anrufen, benötigen Sie die Service-Tag-Nummer oder die Seriennummer. Der Support wird mit Ihnen zusammenarbeiten, um eine Ersatzlaufwerk gemäß Ihrer Service-Level-Vereinbarung zu erhalten.

Über diese Aufgabe

Die Anweisungen gelten für die folgenden SolidFire Storage-Node-Modelle:

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

Je nach Ihrer Element Softwareversion werden die folgenden Nodes nicht unterstützt:

- Ab Element 12.8, SF4805, SF9605, SF19210 und SF38410 Storage-Nodes
- Ab Element 12.7, SF2405 und SF9608 Storage Nodes
- Ab Element 12.0, SF3010, SF6010 und SF9010 Storage-Nodes

Die folgende Abbildung zeigt die Platzierung der Laufwerke in einem SF9605 Chassis:

Die obige Abbildung ist ein Beispiel. SF9608 verfügt über ein anderes Laufwerkslayout, das nur acht Laufwerke enthält, die von links nach rechts mit einer Durchfahrt von acht nummeriert sind.

In Steckplatz 0 ist das Metadatenlaufwerk für den Node gespeichert. Wenn Sie das Laufwerk in Steckplatz 0 ersetzen, müssen Sie den Aufkleber im Lieferumfang des Ersatzlaufwerks anbringen, damit Sie es separat vom Rest identifizieren können.

Beachten Sie bei der Handhabung von Laufwerken die folgenden Best Practices:

- Vermeiden Sie elektrostatische Entladungen, indem Sie das Laufwerk in der ESD-Tasche halten, bis Sie bereit sind, es zu installieren.
- Setzen Sie kein Metallwerkzeug oder Messer in den ESD-Beutel.
- Öffnen Sie die ESD-Tasche von Hand oder schneiden Sie die Oberseite mit einer Schere ab.
- Bewahren Sie den ESD-Beutel und alle Verpackungsmaterialien auf, falls Sie später ein Laufwerk zurückschicken müssen.
- Tragen Sie stets ein ESD-Handgelenkband, das an einer unbemalten Oberfläche auf Ihrem Chassis geerdet ist.
- Beim Entfernen, Installieren oder Tragen eines Laufwerks immer beide Hände verwenden.
- Niemals ein Laufwerk in das Chassis zwingen.
- Legen Sie keine Laufwerke aufeinander ab.
- Verwenden Sie beim Transport von Laufwerken stets die genehmigte Verpackung.

Hier finden Sie eine grobe Übersicht über die Schritte:

- Entfernen Sie das Laufwerk aus dem Cluster
- Setzen Sie das Laufwerk aus dem Gehäuse wieder ein
- Fügen Sie das Laufwerk dem Cluster hinzu

Entfernen Sie das Laufwerk aus dem Cluster

Das SolidFire-System setzt ein Laufwerk in den Status „ausgefallen“, wenn die Selbstdiagnose des Laufwerks den Node angibt, an dem es ausgefallen ist, oder ob die Kommunikation mit dem Laufwerk fünf oder anderthalb Minuten lang unterbrochen wird. Das System zeigt eine Liste der ausgefallenen Laufwerke an. Entfernen Sie ein ausgefallenes Laufwerk aus der Liste ausgefallener Laufwerke in der NetApp Element Software.

Schritte

1. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke**.
2. Wählen Sie **fehlgeschlagen** aus, um die Liste der ausgefallenen Laufwerke anzuzeigen.
3. Notieren Sie sich die Steckplatznummer des ausgefallenen Laufwerks.

   Sie benötigen diese Informationen, um das ausgefallene Laufwerk im Chassis zu finden.

4. Entfernen Sie das ausgefallene Laufwerk mit einer der folgenden Methoden:

Option	Schritte
Um einzelne Laufwerke zu entfernen	a. Wählen Sie **Aktionen** für das Laufwerk, das Sie entfernen möchten. b. Wählen Sie **Entfernen**.
Um mehrere Laufwerke zu entfernen	a. Wählen Sie alle Laufwerke aus, die Sie entfernen möchten, und wählen Sie **Massenaktionen**. b. Wählen Sie **Entfernen**.

Setzen Sie das Laufwerk aus dem Gehäuse wieder ein

Nachdem Sie ein ausgefallenes Laufwerk in der Element UI aus der Liste ausgefallener Laufwerke entfernt haben, sind Sie bereit, das ausgefallene Laufwerk physisch aus dem Chassis zu ersetzen.

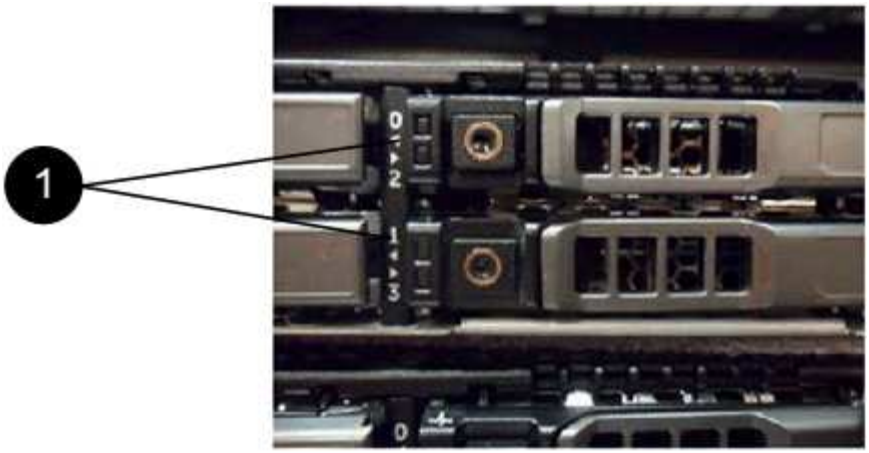
Schritte

1. Packen Sie das Ersatzlaufwerk aus und legen Sie es auf eine flache, statische Oberfläche in der Nähe des Racks.

   Speichern Sie das Verpackungsmaterial für, wenn Sie das ausgefallene Laufwerk an NetApp zurücksenden.

2. Ordnen Sie die Steckplatznummer des ausgefallenen Laufwerks von der Element-UI mit der Nummer auf dem Chassis an.

   Die folgende Abbildung zeigt die Nummerierung der Laufwerksschächte an:



Element	Beschreibung
1	Laufwerkssteckplatznummern

3. Drücken Sie den roten Kreis auf dem Laufwerk, das Sie entfernen möchten, um das Laufwerk zu lösen.

   Die Verriegelung öffnet sich.

4. Schieben Sie das Laufwerk aus dem Gehäuse heraus und legen Sie es auf einer statischen, Ebenen

Fläche ab.

5. Drücken Sie den roten Kreis auf dem Ersatzlaufwerk, bevor Sie ihn in den Steckplatz schieben.
6. Setzen Sie das Ersatzlaufwerk ein, und drücken Sie den roten Kreis, um die Verriegelung zu schließen.
7. Benachrichtigen Sie den NetApp Support über den Austausch von Laufwerken.

   Der NetApp Support enthält Anweisungen zum Zurücksenden des ausgefallenen Laufwerks.

Fügen Sie das Laufwerk dem Cluster hinzu

Nachdem Sie ein neues Laufwerk im Gehäuse installiert haben, wird es als verfügbar registriert. Sie sollten das Laufwerk über die Element-UI zum Cluster hinzufügen, bevor es am Cluster teilnehmen kann.

Schritte

1. Klicken Sie in der Element-UI auf **Cluster** > **Laufwerke**.
2. Klicken Sie auf **verfügbar**, um die Liste der verfügbaren Laufwerke anzuzeigen.
3. Wählen Sie eine der folgenden Optionen zum Hinzufügen von Laufwerken:

Option	Schritte
Um einzelne Laufwerke hinzuzufügen	a. Wählen Sie die Schaltfläche **Aktionen** für das Laufwerk, das Sie hinzufügen möchten. b. Wählen Sie **Hinzufügen**.
Um mehrere Laufwerke hinzuzufügen	a. Aktivieren Sie die Kontrollkästchen der Laufwerke, die hinzugefügt werden sollen, und wählen Sie dann **Massenaktionen** aus. b. Wählen Sie **Hinzufügen**.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Ersetzen Sie ein Netzteil

Jedes SolidFire-Gehäuse besitzt zwei Netzteile für Redundanz. Wenn eine Netzteileinheit ausfällt, sollten Sie sie so schnell wie möglich austauschen, um sicherzustellen, dass das Gehäuse über eine redundante Stromquelle verfügt.

Was Sie benötigen

- Sie haben festgestellt, dass das Netzteil ausgetauscht werden muss.
- Sie haben ein Ersatznetzteil.
- Sie haben überprüft, dass das zweite Netzteil in Betrieb ist.
- Sie haben ein elektrostatisches Entladungsband (ESD) oder andere antistatische Vorsichtsmaßnahmen getroffen.

Über diese Aufgabe

Die Anleitung gilt, wenn Sie ein 1-HE-Chassis (One-Rack Unit) mit einem der folgenden Nodes haben:

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

Je nach Version der Element Software werden die folgenden Nodes nicht unterstützt:

- Ab Element 12.8, SF4805, SF9605, SF19210 und SF38410 Storage-Nodes
- Ab Element 12.7, SF2405 und SF9608 Storage-Nodes und FC0025 und SF-FCN-01 FC-Nodes.
- Ab Element 12.0, SF3010, SF6010 und SF9010 Storage-Nodes

Schritte

1. Ziehen Sie das Netzkabel vom Netzteil ab, das Sie austauschen.
2. Drücken Sie die Entriegelungstaste, um das Netzteil aus dem Gehäuse zu schieben.

   Stellen Sie sicher, dass Sie beide Hände verwenden, um das Gewicht des Netzteils zu unterstützen.

3. Richten Sie die Kanten des Ersatznetzteils mit beiden Händen an der Öffnung im Gehäuse aus, und drücken Sie das Gerät vorsichtig in das Gehäuse.

   Verwenden Sie keine übermäßige Kraft, wenn Sie das Netzteil in das Gehäuse schieben, um Schäden an der Hardware zu vermeiden.

4. Schließen Sie das Netzkabel an.
5. Senden Sie die ausgefallene Einheit an NetApp zurück. Befolgen Sie die Anweisungen in dem Lieferumfang, die Sie erhalten haben.

   Hilfe beim Ersatzverfahren erhalten Sie vom NetApp Support.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Kehren Sie zur Factory Image Information zurück

Konfigurieren Sie die Rückkehr zum Werkbild

NetApp SolidFire Storage-Systeme schreiben mithilfe des RTFI-Prozesses (Return to Factory Image) ein Software-Image auf einen neuen Knoten oder stellen einen Knoten auf seinen ursprünglichen Zustand auf den Werkseinstellungen wieder her. Mit dem RTFI-Prozess werden alle vorhandenen Daten und Konfigurationen (falls vorhanden) sicher gelöscht und ein nicht konfiguriertes NetApp Element-Software-Image installiert. Der RTFI-Prozess ist für alle SolidFire-Knoten verfügbar.

SolidFire-Systeme nutzen bei allen Element Software-Installationen einen RTFI-Prozess. Hierzu zählen interne manuelle Installationen von Entwicklern, automatische Installationen durch automatisierte Framework-Tests, Feldinstallationen von Service Engineers und Kunden sowie Installationen verschiedener Integratoren und Partner. Der gleiche RTFI-Prozess wird auf allen SolidFire Knoten verwendet, unabhängig vom verwendeten Chassis oder Node-Typ, um Probleme automatisch zu beheben.

Dieses Handbuch richtet sich an Integratoren, die Storage-Probleme installieren, konfigurieren, verwenden oder Fehler beheben.

- Linux: Sie haben einige Hintergrundinformationen zu Linux-Systemen.
- Networking: Sie kennen sich mit Servernetzwerken und Netzwerk-Storage aus, einschließlich IP-Adressen, Netmasken und Gateways.

> Der RTFI-Prozess ist datenzerstörend und löscht sicher alle Daten und Konfigurationsdetails vom Knoten und installiert ein neues Betriebssystem. Vergewissern Sie sich, dass der für den RTFI-Prozess verwendete Node nicht im Rahmen eines Clusters aktiv ist.

Implementieren und Installieren des ISO-Image (RTFI International Organization for Standardization) und Durchführen des RTFI-Prozesses:

- RTFI-Bereitstellungs- und Installationsoptionen
- Führen Sie den RTFI-Prozess aus
- Menü RTFI-Optionen

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

RTFI-Bereitstellungs- und Installationsoptionen

Der RTFI-Prozess (Return to Factory Image) verwendet ein bootfähiges, installierbares Medium mit einem vollständig eigenständigen, minimalistischen Linux-Betriebssystem, um Element-Software auf einem Knoten bereitzustellen. Sie können das RTFI ISO-Image für Ihre Element Software-Version von der herunterladen "NetApp Support Website".

Nachdem Sie das RTFI ISO-Image heruntergeladen haben, können Sie es gemäß einer der folgenden gängigen Methoden bereitstellen:

- **Physikalischer USB-Schlüssel**: Sie können eine bootfähige Element-Software ISO auf einen USB-Schlüssel schreiben. Weitere Anweisungen finden Sie im Knowledge Base-Artikel "So erstellen Sie einen

RTFI-Schlüssel zum Neuabbild eines SolidFire-Speicherknoten". Stecken Sie den USB-Schlüssel mit der ISO in den Knoten und starten Sie über den USB-Schlüssel.

- **Virtuelles Medium mit dem Baseboard Management Controller (BMC) Management Port**: Sie können den BMC verwenden, um sich dynamisch an das ISO auf Ihrem Client-System anzubinden. Die ISO wird dem Host-Betriebssystem als virtuelles Laufwerk (CD oder DVD) zur Verfügung gestellt. Weitere Informationen finden Sie im Knowledge Base-Artikel "Wie RTFI ein Knoten über BMC".
- **Netzwerkstart mit einer Preboot Execution Environment (PXE), Trivial File Transfer Protocol (TFTP) oder FTP**: Anstatt ein ISO-Image manuell zu entpacken, können Sie es verwenden `autofs` Automatisches Extrahieren eines Bildes, wenn der RTFI-Prozess es anfordert. Dieser Implementierungsmechanismus erfordert bei der Ersteinrichtung eine größere Zahl, ermöglicht aber eine korrekte Automatisierung und Skalierbarkeit der Installation.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Das RTFI-Verfahren

Sie können den RTFI-Prozess (Return to Factory Image) starten, indem Sie mit dem Knoten durch Textkonsolenaufforderungen interagieren, die vor dem Systemstart angezeigt werden.

Der RTFI-Prozess ist datenzerstörend und löscht sicher alle Daten und Konfigurationsdetails vom Knoten und installiert ein neues Betriebssystem. Vergewissern Sie sich, dass der für den RTFI-Prozess verwendete Node nicht im Rahmen eines Clusters aktiv ist.

Der RTFI Prozess führt die folgenden grundlegenden Operationen durch:

1. Startet die Installation nach der Bestätigung durch den Benutzer und validiert das Bild.
2. Entsperrt alle Laufwerke auf einem Knoten.
3. Überprüft und blinkt die Firmware.
4. Prüft die Hardware.
5. Testet Hardware.
6. Secure löscht alle ausgewählten Laufwerke.
7. Partitioniert das Root-Laufwerk und erstellt Dateisysteme.
8. Kann das Bild einhängen und entpackt werden.
9. Konfiguriert den Host-Namen, die Netzwerkumgebung (Dynamic Host Configuration Protocol), die Standard-Clusterkonfiguration und den GRUB-Bootloader.
10. Beendet alle Services, sammelt Protokolle und startet neu.

Informationen zum Konfigurieren des Knotens nach erfolgreichem Abschluss des RTFI-Prozesses finden Sie im "Dokumentation für Ihre Element Softwareversion". Nachdem ein Knoten den RTFI-Prozess erfolgreich abgeschlossen hat, wechselt er standardmäßig in den Status *available* (nicht konfiguriert).

Führen Sie den RTFI-Prozess aus

Gehen Sie folgendermaßen vor, um die Element Software auf dem SolidFire-Knoten wiederherzustellen.

Informationen zum Erstellen eines USB-Schlüssels oder zur Verwendung des BMC für den RTFI-Prozess finden Sie unter RTFI-Bereitstellungs- und Installationsoptionen.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie die folgenden Anforderungen erfüllen:

- Sie haben Zugriff auf eine Konsole für den SolidFire-Node.
- Der Knoten, auf dem Sie den RTFI-Prozess ausführen, wird eingeschaltet und mit einem Netzwerk verbunden.
- Der Knoten, auf dem Sie den RTFI-Prozess ausführen, ist nicht Teil eines aktiven Clusters.
- Sie haben Zugriff auf startfähige Installationsmedien, die das Image der entsprechenden Element Software-Version für Ihre Konfiguration enthalten.

Sollten Sie Bedenken haben, wenden Sie sich an den NetApp Support, bevor Sie den RTFI-Prozess durchführen.

Schritte

1. Schließen Sie einen Monitor und eine Tastatur an die Rückseite des Knotens an, oder stellen Sie eine Verbindung zur BMC IP-Benutzeroberfläche her, und öffnen Sie die **iKVM/HTML5**-Konsole über die Registerkarte **Remote Control** in der Benutzeroberfläche.
2. Stecken Sie einen USB-Schlüssel mit einem entsprechenden Bild in einen der beiden USB-Steckplätze auf der Rückseite des Knotens ein.
3. Schalten Sie den Knoten ein oder setzen Sie ihn zurück. Wählen Sie während des Startvorgangs Boot Device aus, indem Sie **F11**:

> Sie müssen **F11** mehrmals in schneller Folge auswählen, da der Bildschirm des Startgeräts schnell vorbei geht.

4. Markieren Sie im Menü Start Device Selection die USB-Option.

   Die angezeigten Optionen hängen von der verwendeten USB-Marke ab.

   > Wenn keine USB-Geräte aufgeführt sind, gehen Sie zum BIOS, überprüfen Sie, ob der USB in der Startreihenfolge aufgeführt ist, und versuchen Sie es erneut.
   >
   > Wenn das Problem dadurch nicht behoben wird, gehen Sie zum BIOS, navigieren Sie zur Registerkarte **Speichern und Beenden**, wählen Sie **Wiederherstellen auf optimierten Standardwerten**, übernehmen und speichern Sie die Einstellungen und starten Sie neu.

5. Eine Liste der Bilder auf dem hervorgehobenen USB-Gerät wird angezeigt. Wählen Sie die gewünschte Version aus, und wählen Sie ENTER, um den RTFI-Prozess zu starten.

   Der Name der RTFI-Bildelement-Software und die Versionsnummer werden angezeigt.

6. An der ersten Eingabeaufforderung werden Sie benachrichtigt, dass beim Prozess alle Daten vom Node entfernt werden und dass die Daten nach dem Beginn des Prozesses nicht wiederhergestellt werden können. Geben Sie **Ja** ein, um zu beginnen.

   > Nach dem Start des Prozesses werden alle Daten- und Konfigurationsdetails dauerhaft vom Node gelöscht. Wenn Sie nicht fortfahren möchten, werden Sie an den weitergeleitet Menü RTFI-Optionen.

   > Wenn Sie die Konsole während des RTFI-Prozesses ansehen möchten, können Sie die Tasten **alt+F8** drücken, um auf die ausführliche Modus-Konsole umzuschalten. Drücken Sie **alt+F7**, um zur primären GUI zurückzukehren.

7. Geben Sie **No** ein, wenn Sie dazu aufgefordert werden, umfassende Hardware-Tests durchzuführen, es sei denn, Sie haben einen Grund zum Verdacht eines Hardwarefehlers oder werden zur Durchführung der Tests durch NetApp Support weitergeleitet.

   Eine Meldung gibt an, dass der RTFI-Prozess abgeschlossen ist und das System ausgeschaltet wird.

8. Entfernen Sie gegebenenfalls alle bootfähigen Installationsmedien, nachdem der Node heruntergefahren wurde.

   Der Node ist jetzt eingeschaltet und konfiguriert. Siehe "Bei der Element Software wird die Storage-Dokumentation eingerichtet" Um den Speicher-Node zu konfigurieren.

   Wenn während des RTFI-Prozesses eine Fehlermeldung aufgetreten ist, lesen Sie den Abschnitt Menü RTFI-Optionen.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Menü RTFI-Optionen

Das folgende Optionsmenü wird angezeigt, wenn der RTFI-Prozess nicht erfolgreich ist oder Sie sich für den Vorgang entscheiden, nicht bei der ersten RTFI-

Prozessaufforderung fortzufahren.

Wenden Sie sich an den NetApp Support, bevor Sie eine der folgenden Befehlsoptionen verwenden.

Option	Beschreibung
Neu Booten	Beendet den RTFI-Prozess und startet den Knoten im aktuellen Status neu. Eine Bereinigung wird nicht durchgeführt.
Power Off	Normal schaltet den Node im aktuellen Status aus. Eine Bereinigung wird nicht durchgeführt.
Beenden	Beendet den RTFI-Prozess und öffnet eine Eingabeaufforderung.
UploadLogs	Erfasst alle Protokolle des Systems und lädt ein einziges konsolidiertes Protokollarchiv auf eine angegebene URL hoch.

Protokolle hochladen

Sammeln Sie alle Protokolle auf dem System, und laden Sie sie gemäß dem folgenden Verfahren auf eine angegebene URL hoch.

Schritte

1. Geben Sie in der Menüaufforderung RTFI-Optionen **UploadLogs** ein.
2. Geben Sie die Informationen für das Remote-Verzeichnis ein:

   a. Geben Sie eine URL ein, die das Protokoll enthält. Beispiel: `ftp://,scp://,http://,orhttps://.`

   b. (Optional) Fügen Sie einen integrierten Benutzernamen und ein Kennwort hinzu. Beispiel: `scp://user:password@URLaddress.com`.

   Eine vollständige Palette von Syntaxoptionen finden Sie im "Curl" Benutzerhandbuch.

   Die Protokolldatei wird hochgeladen und als a in das angegebene Verzeichnis gespeichert `.tbz2` Archivierung:

Den Stütztunnel verwenden

Falls Sie technischen Support für Ihr NetApp HCI System oder SolidFire All-Flash-Storage-System benötigen, können Sie sich per Fernzugriff mit Ihrem System verbinden. Um eine Sitzung zu starten und Remote-Zugriff zu erhalten, kann der NetApp Support eine Reverse Secure Shell-(SSH)-Verbindung zu Ihrer Umgebung öffnen.

Sie können einen TCP-Port für eine SSH-Reverse-Tunnel-Verbindung mit NetApp Support öffnen. Über diese Verbindung kann sich NetApp Support beim Management Node einloggen.

Bevor Sie beginnen

- Für Managementservices ab Version 2.18 ist die Möglichkeit für den Remote-Zugriff auf dem Management-Node standardmäßig deaktiviert. Informationen zum Aktivieren der Fernzugriffsfunktionen finden Sie unter "Verwalten der SSH-Funktionalität auf dem Management-Node".
- Wenn sich der Managementknoten hinter einem Proxyserver befindet, sind die folgenden TCP-Ports in der Datei sshd.config erforderlich:

TCP-Port	Beschreibung	Verbindungsrichtung
443	API-Aufrufe/HTTPS zur Umkehrung der Port-Weiterleitung über offenen Support-Tunnel zur Web-UI	Management-Node zu Storage-Nodes
22	SSH-Login-Zugriff	Management-Node zu Storage-Nodes oder von Storage-Nodes zum Management-Node

Schritte

- Melden Sie sich bei Ihrem Management-Knoten an und öffnen Sie eine Terminalsitzung.
- Geben Sie an einer Eingabeaufforderung Folgendes ein:

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

- Um den Remote Support-Tunnel zu schließen, geben Sie Folgendes ein:

```
rst --killall
```

- (Optional) Deaktivieren "Remote-Zugriffsfunktion" Ein weiteres Jahr in der

> SSH bleibt auf dem Management-Node aktiviert, wenn Sie ihn nicht deaktivieren. Die SSH-fähige Konfiguration bleibt auf dem Management-Node durch Updates und Upgrades bestehen, bis sie manuell deaktiviert ist.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Storage-Nodes

Die unterstützten Firmware-Versionen für H-Series und SolidFire Storage Nodes

- H610S
- H410S
- SF38410, SF19210, SF9605 UND SF4805

H610S

Modellnummer (Familienanteil): H610S **volle Modellnummer:** H610S-1, H610S-1-NE, H610S-2, H610S-2-NE, H610S-4, H610S-4-NE UND H610S-2F

Komponenten-Firmware, die von einem Storage Firmware Bundle verwaltet wird

Während des Zeitrahmens von 11.x war die NetApp Element-Software die einzige Möglichkeit, Firmware freizugeben. Ab Element 12.0 wurde das Konzept eines **Storage Firmware Bundle** eingeführt und Firmware-Updates wurden nun durch ein unabhängig veröffentlichtes Speicher-Firmware-Bundle oder Speicher-Firmware-Bundle ermöglicht, das im Rahmen einer Element 12.x-Version enthalten ist.

Ein Bindestrich (**-**) in der folgenden Tabelle zeigt an, dass die jeweilige Hardware-Komponente IN diesem gegebenen Freigabefahrzeug NICHT unterstützt wurde.

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Modul Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Modul Smart (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Modul Micron (Gen 1)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Modul Micron (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.182.0	12024-10-17	3B14	4.01.07	122	14.25.1020	16.32.1010	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.5	2.17	CXV8202Q	CXV8501Q	EDA5602Q	EA59000Q	0109	0109	0108	GDC5A02Q	11093A10	110B3A10
Speicher-Firmware-Paket 2.175.0	06/15/2023	3B11	3.94.07	122	14.25.1020	16.32.1010	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.5	2.17	CXV8202Q	CXV8501Q	EDA5602Q	EA59000Q	0109	0109	0108	GDC5602Q	11092A10	110B2A10

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Modul Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Modul Smart (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Modul Micron (Gen 1)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Modul Micron (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.164.0	10/20/2022	3B11	3.94.07	122	14.25.1020	16.32.1010	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.3	2.16	CXV8202Q	CXV8501Q	EDA5602Q	EA59000Q	0109	0109	0108	GDC5602Q	11092A10	110B2A10

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.164.0 bis NetApp Element 12.7	10/20/2022	3B11	3.94.07	122	14.25.1020	16.32.1010	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.3	2.16	CXV8202Q	CXV8501Q	EDA5602Q	EA59000Q	0109	0109	0108	GDC5602Q	11092A10	110B2A10

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Modul Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Modul Smart (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Modul Micron (Gen 1)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Modul Micron (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.150.4	06/08/2022	3B11	3.94.07	122	14.25.1020	-	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.3	2.16	CXV8202Q	CXV8501Q	EDA5602Q	EA59000Q	0109	0109	0108	GDC5502Q	11092A10	110B2A10

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.150.4 bis NetApp Element 12.5	06/08/2022	3B11	3.94.07	122	14.25.1020	-	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.3	2.16	CXV8202Q	CXV8501Q	EDA5602Q	EA59000Q	0109	0109	0108	GDC5502Q	11092A10	110B2A10

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Modul Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Modul Smart (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Modul Micron (Gen 1)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Modul Micron (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.146.2	02/22/2022	3B11	3.94.07	122	14.25.1020	-	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.3	2.16	CXV8202Q	CXV8501Q	EDA5602Q	EA59000Q	0109	0109	0108	GDC5502Q	11092A10	110B2A10

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM EnergySource (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.9.4bis NetApp Element 12.3	09/16/2021	3B06	3.91.07	122	14.25.1020	-	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.1	2.16	CXV8202Q	CXV8501Q	EDA5402Q	EDA5700Q	0109	0109	0108	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.9.4 bis NetApp Element 12.3.1.165	12/06/2021	3B06	3.91.07	122	14.25.1020	-	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.1	2.16	CXV8202Q	CXV8501Q	EDA5402Q	EDA5700Q	0109	0109	0108	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Modul Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Modul Smart (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Modul Micron (Gen 1)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Modul Micron (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.99.2	12/06/2021	3B06	3.91.07	122	14.25.1020	-	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.1	2.16	CXV8202Q	CXV8501Q	EDA5402Q	EDA5700Q	0109	0109	0108	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM EnergySource (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.9.1 bis NetApp Element 12.3.1.103	09/16/2021	3B06	3.86.07	122	14.25.1020	-	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.1	2.16	CXV82020 2Q	CXV85010 1Q	EDA5402 2Q	EDA5700 0Q	0109	0109	0108	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.99 bis NetApp Element 12.3	04/15/2021	3B06	3.86.07	122	14.25.1020	-	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.1	2.16	CXV8202Q	CXV8501Q	EDA5402Q	EDA5700Q	0109	0109	0108	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.76.8	02/03/2021	3B06	3.86.07	122	14.25.1020	-	3.1	2.16	26,2C	1.30	25,3C	1.40	-	-	-	CXV82022Q	CXV85011Q	EDA54022Q	EDA57000Q	0109	0109	0108	-	-	-
Speicher-Firmware-Paket 2.27.1	09/29/2020	3B03	3.84.07	122	14.02.1002	-	3.1	2.16	26,2C	1.30	25,3C	1.40	-	-	-	CXV82022Q	CXV85011Q	EA53002Q	EA56000Q	0108	0108	0108	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM EnergySource (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.76.8bis NetApp Element 12.2.1	06/02/2021	3B06	3.86.07	122	14.25.1020	-	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.1	2.16	CXV8202Q	CXV8501Q	EDA5402Q	EDA5700Q	0109	0109	0108	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.21 bis NetApp Element 12.2	09/29/2020	3B03	3.84.07	122	14.22.1002	-	3.1	2.16	26,2C	1.30	25,3C	1.40	-	-	-	CXV8202Q	CXV8501Q	EA5302Q	EA5600Q	0108	0108	0108	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM EnergySource (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 2.76.8bis NetApp Element 12.0.1	06/02/2021	3B06	3.86.07	122	14.25.1020	-	3.1	2.16	26,2C	1.30	25,3C	1.40	1.10	3.1	2.16	CXV8202Q	CXV8501Q	EDA5402Q	EDA5700Q	0109	0109	0108	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM EnergySource (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energieequelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
Speicher-Firmware-Paket 1.2.17 bis NetApp Element 12.0	03/20/2020	3B03	3.78.07	122	14.22.1002	-	3.1	2.16	26,2C	1.30	25,3C	1.40	-	-	-	CXV8202Q	CXV8501Q	EDA5202Q	EA5200Q	0108	0108	0108	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
NetApp Element 11.8	03/11/2020	3B03	3.78.07	122	14.22.1002	-	3.1	2.16	26,2C	1.30	25,3C	1.40	-	-	-	CXV8202Q	CXV8501Q	EDA5202Q	EA5200Q	0108	0108	0107	-	-	-
NetApp Element 11.7	11/21/2019	3A10	3.76.07	117	14.22.1002	-	2.C	2.07	26,2C	1.30	25,3C	1.40	-	-	-	CXV8202Q	CXV8501Q	EDA5202Q	EA5200Q	0108	0108	0107	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
NetApp Element 11.5.1	02/20/2020	3A08	3.76.07	117	14.22.1002	-	2.C	2.07	26,2C	1.30	25,3C	1.40	-	-	-	CXV8202Q	CXV8501Q	EDA5202Q	EA52000Q	0108	0108	0107	-	-	-
NetApp Element 11.5	09/26/2019	3A08	3.76.07	117	14.22.1002	-	2.C	2.07	26,2C	1.30	-	-	-	-	-	CXV8202Q	CXV8501Q	EDA5202Q	EA52000Q	-	-	0107	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
NetApp Element 11.3.2	02/19/2020	3A08	3.76.07	117	14.22.1002	-	2.C	2.07	26,2C	1.30	25,3C	1.40	-	-	-	CXV8202Q	CXV8501Q	EDA5202Q	EA5200Q	0108	0108	-	-	-	-
NetApp Element 11.3.1	08/19/2019	3A08	3.76.07	117	14.22.1002	-	2.C	2.07	26,2C	1.30	-	-	-	-	-	CXV8202Q	CXV8501Q	EDA5202Q	EA5200Q	-	-	-	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 2)	Cache NVDIMM NVDIMM Energi equelle (PGEM) Agigatech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (N-SED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (N-SED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (N-SED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (N-SED)
NetApp Element 11.1.1	02/19/2020	3A06	3.70.07	117	14.22.10 02	-	2.C	2.07	26,2C	1.30	25,3C	1.40	-	-	-	CXV820 2Q	CXV850 1Q	EDA520 2Q	EA5200 Q	0108	0108	-	-	-	-
NetApp Element 11.1	04/25/2019	3A06	3.70.07	117	14.22.10 02	-	2.C	2.07	26,2C	1.30	-	-	-	-	-	CXV820 2Q	CXV850 1Q	EDA520 2Q	EA5200 Q	-	-	-	-	-	-

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	CPLD	10/25-GbE-NIC CX4	10/25-GbE-NIC CX5	Cache NVDIMM NVDIMM Module Smart (Gen 1)	Cache NVDIMM NVDIMM Energy Source (BPM) Smart (Gen 1)	Cache NVDIMM NVDIMM Module Smart (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (BPM) Smart (Gen 2)	Cache NVDIMM NVDIMM Module Micron (Gen 1)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Aging atech (Gen 1)	Cache NVDIMM NVDIMM Module Micron (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Aging atech (Gen 2)	Cache NVDIMM NVDIMM Energie equelle (PGEM) Aging atech (Gen 3)	Laufwerk Samsung PM963 (SED)	Laufwerk Samsung PM963 (NSED)	Laufwerk Samsung PM983 (SED)	Laufwerk Samsung PM983 (NSED)	Antrieb Kioxia CD5 (SED)	Antrieb Kioxia CD5 (NSED)	Laufwerk CD5 (FIPS)	Laufwerk Samsung PM9A3 (SED)	Laufwerk SK Hynix PE8010 (SED)	Laufwerk SK Hynix PE8010 (NSED)
NetApp Element 11.0.2	02/19/2020	3A06	3.70.07	117	14.22.1002	-	2.C	2.07	26,2C	1.30	25,3C	1.40	-	-	-	CXV8202Q	CXV8501Q	EDA5202Q	EA5200Q	0108	0108	-	-	-	-
NetApp Element 11	11/29/2018	3A06	3.70.07	117	14.22.1002	-	2.C	2.07	26,2C	1.30	-	-	-	-	-	CXV8202Q	CXV8501Q	EDA5202Q	EA5200Q	-	-	-	-	-	-

Die Komponenten-Firmware wird nicht von einem Storage Firmware-Bundle gemanagt

Die folgende Firmware wird nicht von einem Storage Firmware Bundle verwaltet:

Komponente	Aktuelle Version
1/10-/25-GbE-NIC	3.2d 0x80000b4b

Komponente	Aktuelle Version
Startgerät	M161225i

H410S

Modellnummer (Familienanteil): H410S **volle Modellnummern:** H410S-0, H410S-1, H410S-1-NE und H410S-2

Komponenten-Firmware, die von einem Storage Firmware Bundle verwaltet wird

Komponenten-Firmware, die von einem Storage Firmware Bundle verwaltet wird.

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	10/25-GbE-NIC SMCI Mellanox	Cache-NVDIMM RMS200	Cache-NVDIMM RMS300	Laufwerk Samsung PM863 (SED)	Laufwerk Samsung PM863 (N-SED)	Laufwerk Toshiba Hawk-4 (SED)	Laufwerk Toshiba Hawk-4 (N-SED)	Laufwerk Samsung PM883 (SED)
Speicher-Firmware-Paket 2.182.0	1 2024-10-17	NAT3.6	07.02.00	14.25.1020	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Speicher-Firmware-Paket 2.175.0	06/15/2023	NAT3.4	07.02.00	14.25.1020	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Speicher-Firmware-Paket 2.164.0 bis NetApp Element 12.7	10/20/2022	NAT3.4	6.98.00	14.25.1020	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Speicher-Firmware-Paket 2.164.0	10/20/2022	NAT3.4	6.98.00	14.25.1020	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	10/25-GbE-NIC SMCI Mellanox	Cache-NVDIMM RMS200	Cache-NVDIMM RMS300	Laufwerk Samsung PM863 (SED)	Laufwerk Samsung PM863 (N-SED)	Laufwerk Toshiba Hawk-4 (SED)	Laufwerk Toshiba Hawk-4 (N-SED)	Laufwerk Samsung PM883 (SED)
Speicher-Firmware-Paket 2.164.0 bis NetApp Element 12.7	10/20/2022	NAT3.4	6.98.00	14.25.1020	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Speicher-Firmware-Paket 2.150.4 bis NetApp Element 12.5	06/08/2022	NAT3.4	6.98.00	14.25.1020	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Speicher-Firmware-Paket 2.99 bis NetApp Element 12.3	04/15/2021	NA2.1	6.84.00	14.25.1020	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
Speicher-Firmware-Paket 2.76.8 bis NetApp Element 12.2.1	06/02/2021	NA2.1	6.84.00	14.25.1020	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	10/25-GbE-NIC SMCI Mellanox	Cache-NVDIMM RMS200	Cache-NVDIMM RMS300	Laufwerk Samsung PM863 (SED)	Laufwerk Samsung PM863 (N-SED)	Laufwerk Toshiba Hawk-4 (SED)	Laufwerk Toshiba Hawk-4 (N-SED)	Laufwerk Samsung PM883 (SED)
Speicher-Firmware-Paket 1.2.17 bis NetApp Element 12.0	03/20/2020	NA2.1	3.25	14.21.1000	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
NetApp Element 11.8.2	02/22/2022	NA2.1	3.25	14.21.1000	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
NetApp Element 11.8.1	06/02/2021	NA2.1	3.25	14.21.1000	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
NetApp Element 11.8	03/11/2020	NA2.1	3.25	14.21.1000	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
NetApp Element 11.7	11/21/2019	NA2.1	3.25	14.21.1000	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
NetApp Element 11.5.1	02/19/2020	NA2.1	3.25	14.21.1000	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
NetApp Element 11.5	09/26/2019	NA2.1	3.25	14.21.1000	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
NetApp Element 11.3.2	02/19/2020	NA2.1	3.25	14.21.1000	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
NetApp Element 11.3.1	08/19/2019	NA2.1	3.25	14.21.1000	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
NetApp Element 11.1.1	02/19/2020	NA2.1	3.25	14.17.2020	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
NetApp Element 11.1	04/25/2019	NA2.1	3.25	14.17.2020	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q

Fahrzeug Lösen	Freigabedatum	BIOS	BMC	10/25-GbE-NIC SMCI Mellanox	Cache-NVDIMM RMS200	Cache-NVDIMM RMS300	Laufwerk Samsung PM863 (SED)	Laufwerk Samsung PM863 (N-SED)	Laufwerk Toshiba Hawk-4 (SED)	Laufwerk Toshiba Hawk-4 (N-SED)	Laufwerk Samsung PM883 (SED)
NetApp Element 11.0.2	02/19/2020	NA2.1	3.25	14.17.2020	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
NetApp Element 11.0	11/29/2018	NA2.1	3.25	14.17.2020	Ae3b8cc	-	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q

Die Komponenten-Firmware wird nicht von einem Storage Firmware-Bundle gemanagt

Die folgende Firmware wird nicht von einem Storage Firmware Bundle verwaltet:

Komponente	Aktuelle Version
CPLD	01.A1.06
SAS-Adapter	16.00.01.00
Mikrocontroller-Einheit (MCU)	1.18
SIOM 1/10-GbE-NIC	1.93
Stromversorgung	1.3
Boot-Gerät SSDSCKJB240G7	N2010121
Boot-Gerät MTFDDAV240TCB1AR	DOMU037

SF38410, SF19210, SF9605 und SF4805

Volle Modellnummern: SF38410, SF19210, SF9605 und SF4805

Komponenten-Firmware, die von einem Storage Firmware Bundle verwaltet wird

Während des Zeitrahmens von 11.x war die NetApp Element-Software die einzige Möglichkeit, Firmware freizugeben. Ab Element 12.0 wurde das Konzept eines **Storage Firmware Bundle** eingeführt und Firmware-Updates wurden nun durch ein unabhängig veröffentlichtes Speicher-Firmware-Bundle oder Speicher-Firmware-Bundle ermöglicht, das im Rahmen einer Element 12.x-Version enthalten ist.

Ein Bindestrich (**-**) in der folgenden Tabelle zeigt an, dass die jeweilige Hardware-Komponente IN diesem gegebenen Freigabefahrzeug NICHT unterstützt wurde.

Fahrzeug Lösen	Freigabedatum	NIC	CACHE NVDIMM RMS200 (RMS200)	CACHE NVDIMM RMS200 (RMS300)	Laufwerk Samsung PM863 (SED)	Laufwerk Samsung PM863 (N-SED)	Laufwerk Toshiba Hawk-4 (SED)	Laufwerk Toshiba Hawk-4 (N-SED)	Laufwerk Samsung PM883 (SED)
Speicher-Firmware-Paket 2.164.0	10/20/2022	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Speicher-Firmware-Paket 2.164.0 bis NetApp Element 12.7	10/20/2022	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Speicher-Firmware-Paket 2.150.4	06/08/2022	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Speicher-Firmware-Paket 2.150.4 bis NetApp Element 12.5	06/08/2022	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Speicher-Firmware-Paket 2.146.2	02/22/2022	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Speicher-Firmware-Paket 2.99.4 bis NetApp Element 12.3	09/16/2021	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
Speicher-Firmware-Paket 2.99.4 bis NetApp Element 12.3.1.165	12/06/2021	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q

Fahrzeug Lösen	Freigabedatum	NIC	CACHE NVDIMM RMS200 (RMS200)	CACHE NVDIMM RMS200 (RMS300)	Laufwerk Samsung PM863 (SED)	Laufwerk Samsung PM863 (N-SED)	Laufwerk Toshiba Hawk-4 (SED)	Laufwerk Toshiba Hawk-4 (N-SED)	Laufwerk Samsung PM883 (SED)
Speicher-Firmware-Paket 2.99.2	08/03/2021	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
Speicher-Firmware-Paket 2.99.1 bis NetApp Element 12.3.1.103	09/16/2021	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
Speicher-Firmware-Paket 2.99 bis NetApp Element 12.3	04/15/2021	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
Speicher-Firmware-Paket 2.76.8	02/03/2021	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
Speicher-Firmware-Paket 2.27.1	09/29/2020	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q
Speicher-Firmware-Paket 2.76.8 bis NetApp Element 12.2.1	06/02/2021	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
Speicher-Firmware-Paket 2.21 bis NetApp Element 12.2	09/29/2020	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q

Fahrzeug Lösen	Freigabedatum	NIC	CACHE NVDIMM RMS200 (RMS200)	CACHE NVDIMM RMS200 (RMS300)	Laufwerk Samsung PM863 (SED)	Laufwerk Samsung PM863 (N-SED)	Laufwerk Toshiba Hawk-4 (SED)	Laufwerk Toshiba Hawk-4 (N-SED)	Laufwerk Samsung PM883 (SED)
Speicher-Firmware-Paket 2.76.8 bis NetApp Element 12.0.1	06/02/2021	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
Speicher-Firmware-Paket 1.2.17 bis NetApp Element 12.0	03/20/2020	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q
NetApp Element 11.8.2	02/22/2022	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q
NetApp Element 11.8.1	06/02/2021	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q
NetApp Element 11.8	03/11/2020	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q
NetApp Element 11.7	11/21/2019	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q
NetApp Element 11.5.1	02/19/2020	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q
NetApp Element 11.5	09/26/2019	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q
NetApp Element 11.3.2	02/19/2020	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q
NetApp Element 11.3.1	08/19/2019	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q

Fahrzeug Lösen	Freigabedatum	NIC	CACHE NVDIMM RMS200 (RMS200)	CACHE NVDIMM RMS200 (RMS300)	Laufwerk Samsung PM863 (SED)	Laufwerk Samsung PM863 (N-SED)	Laufwerk Toshiba Hawk-4 (SED)	Laufwerk Toshiba Hawk-4 (N-SED)	Laufwerk Samsung PM883 (SED)
NetApp Element 11.1.1	02/19/2020	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q
NetApp Element 11.1	04/25/2019	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q
NetApp Element 11.0.2	02/19/2020	7.10.18	Ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q
NetApp Element 11	11/29/2018	7.10.18	Ae3b8cc	-	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7104Q

Die Komponenten-Firmware wird nicht von einem Storage Firmware-Bundle gemanagt

Die folgende Firmware wird nicht von einem Storage Firmware Bundle verwaltet:

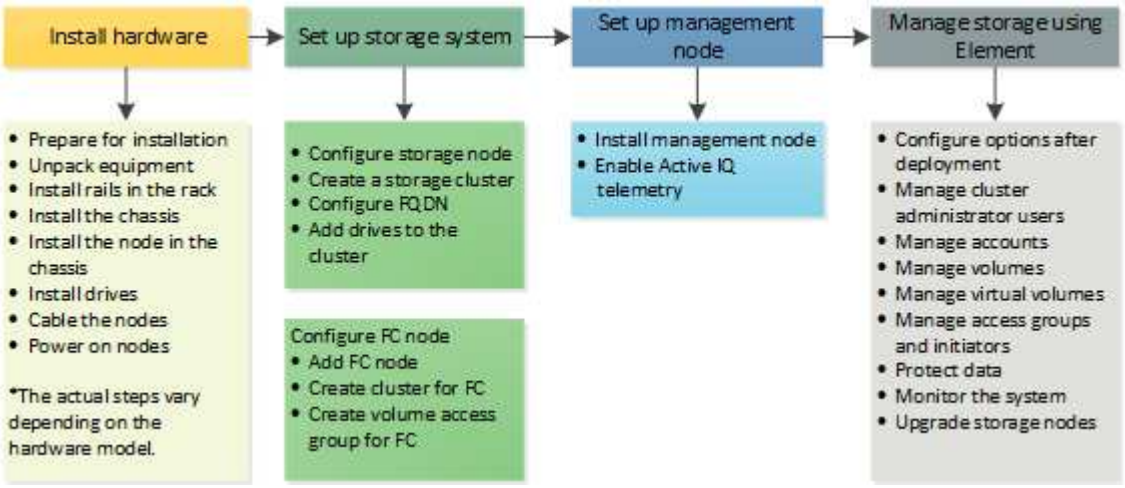
Komponente	Aktuelle Version
BIOS	2.8.0
IDRAC	2.75.75.75
Identitätsmodul	N41WC 1.02
SAS-Adapter	16.00.01.00
Stromversorgung	1.3
Boot-Gerät	M161225i

Storage einrichten

Erfahren Sie mehr über die Einrichtung von Speichersystemen.

An diesem Punkt sollten Sie die Hardware installiert haben. Die Hardware beinhaltet auch die Element Software.

Als Nächstes müssen Sie das Storage-System für Ihre Umgebung einrichten. Sie können ein Cluster mit Storage-Nodes oder Fibre Channel Nodes einrichten und es über Element Software managen, nachdem Sie Nodes in einer Höheneinheit installiert und verkabeln und dann wieder einschalten.



Schritte zur Einrichtung von Speicher

1. Wählen Sie eine der folgenden Optionen:
   - "Richten Sie ein Cluster mit Storage Nodes ein"

     Sie können ein Cluster mit Storage-Nodes einrichten und mithilfe von Element Software managen, nachdem Sie Nodes in einer Höheneinheit installiert und verkabeln und dann wieder einschalten. Anschließend können Sie zusätzliche Komponenten in Ihrem Speichersystem installieren und konfigurieren.

   - "Richten Sie das Cluster mit Fibre Channel Nodes ein"

     Sie können einen Cluster mit Fibre-Channel-Knoten einrichten und ihn mithilfe der Element-Software verwalten, nachdem Sie die Knoten in einer Rack-Einheit installiert und verkabelt und eingeschaltet haben. Anschließend können Sie weitere Komponenten in Ihrem Speichersystem installieren und konfigurieren.

2. "Ermitteln der zu installierenden SolidFire-Komponenten"
3. "Einrichten eines Management-Node und Aktivieren der Active IQ Telemetrie"

Weitere Informationen

- "Erfahren Sie mehr über die nächsten Schritte zur Storage-Nutzung"
- "Dokumentation von SolidFire und Element Software"

Richten Sie ein Cluster mit Storage-Nodes ein

Konfigurieren Sie einen Storage-Node

Sie müssen einzelne Nodes konfigurieren, bevor Sie sie einem Cluster hinzufügen können. Nachdem Sie einen Knoten in einer Rack-Einheit installiert und verkabeln und einschalten, können Sie die Knotennetzwerkeinstellungen über die UI pro Node oder die Node Terminal User Interface (TUI) konfigurieren. Stellen Sie sicher, dass Sie über die erforderlichen Netzwerkkonfigurationsinformationen für den Node verfügen, bevor Sie fortfahren.

Es gibt zwei Optionen für die Konfiguration von Speicher-Nodes:

- UI pro Node: Verwenden Sie die Benutzeroberfläche pro Knoten. (`https://<node_management_IP>:442`) um die Knotennetzwerkeinstellungen zu konfigurieren.
- TUI: Verwenden Sie die Node Terminal User Interface (TUI), um den Knoten zu konfigurieren.

Sie können einem Cluster keinen Node mit DHCP-zugewiesenen IP-Adressen hinzufügen. Über die DHCP-IP-Adresse können Sie den Node zunächst in der UI, der TUI oder der API pro Node konfigurieren. Während dieser Erstkonfiguration können Sie statische IP-Adressinformationen hinzufügen, damit Sie den Node zu einem Cluster hinzufügen können.

Nach der Erstkonfiguration können Sie mit der Management-IP-Adresse des Node auf den Node zugreifen. Anschließend können Sie die Node-Einstellungen ändern, zu einem Cluster hinzufügen oder einen Cluster mit dem Node erstellen. Zudem können Sie mithilfe von Element Software-API-Methoden einen neuen Node konfigurieren.

> Ab Element Version 11.0 können Nodes mit IPv4, IPv6 oder beiden Adressen für ihr Managementnetzwerk konfiguriert werden. Dies gilt sowohl für Storage-Nodes als auch für Management-Nodes, mit Ausnahme von Management-Node 11.3 und höher, der IPv6 nicht unterstützt. Wenn Sie ein Cluster erstellen, kann für das MVIP nur eine einzelne IPv4- oder IPv6-Adresse verwendet werden, und der entsprechende Adresstyp muss auf allen Knoten konfiguriert werden.

Konfigurieren Sie einen Storage-Node über die UI pro Node

Sie können Nodes über die Benutzeroberfläche pro Node konfigurieren.

Über diese Aufgabe

- Sie können den Node so konfigurieren, dass er eine IPv4- oder eine IPv6-Adresse hat.
- Sie benötigen die in der TUI angezeigte DHCP-Adresse, um auf einen Knoten zugreifen zu können. Sie können einem Cluster keine DHCP-Adressen verwenden, um einen Node hinzuzufügen.

> Sie sollten die Management-Schnittstellen (Bond1G) und Storage-Schnittstellen (Bond10G) für separate Subnetze konfigurieren. Bond1G- und Bond10G-Schnittstellen für dasselbe Subnetz verursachen Routing-Probleme, wenn Storage Traffic über die Bond1G-Schnittstelle gesendet wird. Wenn Sie dasselbe Subnetz für Management und Storage-Verkehr verwenden müssen, konfigurieren Sie den Management-Traffic manuell, um die Bond10G-Schnittstelle zu verwenden. Dies können Sie für jeden Knoten mithilfe der **Cluster-Einstellungen**-Seite der Pro-Node-Benutzeroberfläche tun.

Schritte

1. Geben Sie in einem Browser-Fenster die DHCP-IP-Adresse eines Node ein.

   Sie müssen die Erweiterung hinzufügen. `:442` um auf den Knoten zuzugreifen; zum Beispiel `https://172.25.103.6:442`Die

   Die Registerkarte **Network Settings** wird mit dem Abschnitt **Bond1G** geöffnet.

2. Geben Sie die 1G-Verwaltungsnetzwerkeinstellungen ein.
3. Klicken Sie Auf **Änderungen Übernehmen**.
4. Klicken Sie auf **Bond10G**, um die Einstellungen des 10G-Speichernetzwerks anzuzeigen.
5. Geben Sie die Einstellungen für das 10G-Speichernetzwerk ein.
6. Klicken Sie Auf **Änderungen Übernehmen**.
7. Klicken Sie Auf **Cluster-Einstellungen**.
8. Geben Sie den Hostnamen für das 10G-Netzwerk ein.
9. Geben Sie den Cluster-Namen ein.

   Dieser Name muss der Konfiguration für alle Nodes hinzugefügt werden, bevor ein Cluster erstellt werden kann. Alle Nodes in einem Cluster müssen identische Cluster-Namen aufweisen. Bei Cluster-Namen wird die Groß-/Kleinschreibung berücksichtigt.

10. Klicken Sie Auf **Änderungen Übernehmen**.

Konfigurieren Sie über die TUI einen Storage-Node

Über die Terminal User Interface (TUI) können Sie die Erstkonfiguration neuer Knoten vornehmen.

Sie sollten die Bond1G (Management)- und Bond10G (Storage)-Schnittstellen für separate Subnetze konfigurieren. Bond1G- und Bond10G-Schnittstellen für dasselbe Subnetz verursachen Routing-Probleme, wenn Storage Traffic über die Bond1G-Schnittstelle gesendet wird. Wenn Sie dasselbe Subnetz für Management und Storage-Verkehr verwenden müssen, konfigurieren Sie den Management-Traffic manuell, um die Bond10G-Schnittstelle zu verwenden. Dies können Sie für jeden Knoten mithilfe der Seite **Cluster** > **Knoten** der Element-Benutzeroberfläche tun.

Schritte

1. Schließen Sie eine Tastatur und einen Monitor an den Knoten an, und schalten Sie den Knoten ein.

   Das NetApp Storage Main Menu der TUI erscheint auf dem tty1 Terminal.

   Wenn der Knoten den Konfigurationsserver nicht erreichen kann, zeigt die TUI eine Fehlermeldung an. Überprüfen Sie die Verbindung des Konfigurationsservers oder die Netzwerkverbindung, um den Fehler zu beheben.

2. Wählen Sie **Netzwerk** > **Netzwerkkonfiguration**.

   Um durch das Menü zu navigieren, drücken Sie die nach-oben- oder nach-unten-Taste. Um zu einer anderen Schaltfläche oder zu den Feldern von den Schaltflächen zu wechseln, drücken Sie **Tab**. Um zwischen Feldern zu navigieren, verwenden Sie die nach-oben- oder nach-unten-Pfeiltasten.

3. Wählen Sie **Bond1G (Management)** oder **Bond10G (Storage)** aus, um die 1G- und 10G-Netzwerkeinstellungen für den Node zu konfigurieren.
4. Drücken Sie für die Felder „Bond Mode“ und „Status“ die Taste **Tab**, um die Schaltfläche „Hilfe“ auszuwählen und die verfügbaren Optionen zu ermitteln.

   Alle Nodes in einem Cluster müssen identische Cluster-Namen aufweisen. Bei Cluster-Namen wird die Groß-/Kleinschreibung berücksichtigt. Wenn im Netzwerk ein DHCP-Server mit verfügbaren IP-Adressen ausgeführt wird, wird im Feld Adresse die 1-GbE-Adresse angezeigt.

5. Drücken Sie **Tab**, um die **OK**-Taste auszuwählen und die Änderungen zu speichern.

   Der Node wird in einen ausstehenden Status versetzt, und er kann einem vorhandenen oder einem neuen Cluster hinzugefügt werden.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Erstellen eines Storage-Clusters

Sie können ein Storage-Cluster erstellen, nachdem Sie alle einzelnen Nodes konfiguriert haben. Wenn Sie ein Cluster erstellen, wird automatisch ein Cluster-Administrator-Benutzerkonto für Sie erstellt. Der Clusteradministrator verfügt über die Berechtigung zum Verwalten aller Clusterattribute und kann andere Cluster-Administratorkonten erstellen.

Was Sie benötigen

- Sie haben den Management-Node installiert.
- Sie haben alle einzelnen Nodes konfiguriert.

Über diese Aufgabe

Während der Konfiguration eines neuen Node werden jedem Node 1-GB- oder 10-GB-Management-IP-Adressen (MIP) zugewiesen. Sie müssen eine der bei der Konfiguration erstellten Node-IP-Adressen verwenden, um die Seite Neues Cluster erstellen zu öffnen. Die verwendete IP-Adresse hängt vom Netzwerk ab, das Sie für das Cluster-Management ausgewählt haben.

Wenn Sie Cluster-weit aktivieren möchten "Softwareverschlüsselung für Daten im Ruhezustand" Bei SolidFire All-Flash-Storage-Clustern müssen Sie dies während der Cluster-Erstellung tun. Ab Element 12.5 müssen Sie während der Cluster-Erstellung in der UI „Cluster erstellen“ die Softwareverschlüsselung im Ruhezustand aktivieren. Für Element 12.3.x und früher müssen Sie den Cluster mithilfe der erstellen "CreateCluster erstellen" API-Methode und ändern Sie den enableSoftwareVerschlüsselungAtRest-Parameter in `true`. Nachdem die Softwareverschlüsselung im Ruhezustand auf dem Cluster aktiviert wurde, kann sie nicht deaktiviert werden. Das können Sie "Aktivieren und deaktivieren Sie" Hardwarebasierte Verschlüsselung für Daten im Ruhezustand nach der Cluster-Erstellung

Beim Erstellen eines neuen Clusters müssen folgende Aspekte berücksichtigt werden:

- Wenn Sie Storage-Nodes in einem gemeinsam genutzten Chassis nutzen, sollte möglicherweise der Entwurf für eine Ausfallsicherung auf Chassis-Ebene mithilfe der Schutz-Domänen-Funktion in Betracht gezogen werden.
- Wenn ein freigegebenes Gehäuse nicht verwendet wird, können Sie ein benutzerdefiniertes Schutz-Domain-Layout definieren.

Schritte

1. Geben Sie in einem Browser-Fenster ein `https://MIP:443`, Wobei MIP die Management-Node-IP-Adresse ist.
2. Geben Sie unter Erstellen eines neuen Clusters die folgenden Informationen ein:
   - Management-VIP: Routingfähige virtuelle IP im 1-GbE- oder 10-GbE-Netzwerk für Netzwerk-Management-Aufgaben.

     Sie können ein neues Cluster mit einer IPv4- oder IPv6-Adresse erstellen.

   - ISCSI (Storage) VIP: Virtuelle IP im 10-GbE-Netzwerk für Storage und iSCSI-Erkennung.

     Sie können den MVIP-, SVIP- oder Cluster-Namen nicht ändern, nachdem Sie den Cluster erstellt haben.

   - Benutzername: Der primäre Clusteradministrator-Benutzername für authentifizierten Zugriff auf das Cluster. Sie müssen den Benutzernamen für die zukünftige Referenz speichern.

     Sie können Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern für den Benutzernamen und das Passwort verwenden.

   - Passwort: Passwort für authentifizierten Zugriff auf das Cluster. Sie müssen das Kennwort für die spätere Referenz speichern. Standardmäßig ist die zwei-Wege-Datensicherung aktiviert. Sie können diese Einstellung nicht ändern.
3. Lesen Sie die Endbenutzer-Lizenzvereinbarung und wählen Sie **Ich stimme zu**.
4. **Optional**: Stellen Sie in der Liste Knoten sicher, dass die Kontrollkästchen für Knoten, die nicht im Cluster enthalten sein sollen, nicht ausgewählt sind.
5. Wählen Sie **Cluster Erstellen**.

   Das System kann je nach Anzahl der Nodes im Cluster mehrere Minuten dauern, bis der Cluster erstellt wurde. In einem ordnungsgemäß konfigurierten Netzwerk sollte ein kleines Cluster mit fünf Nodes weniger als eine Minute dauern. Nach dem Erstellen des Clusters wird das Fenster Erstellen eines neuen Clusters an die MVIP-URL-Adresse für den Cluster umgeleitet und die Element-UI angezeigt.

Finden Sie weitere Informationen

- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Greifen Sie auf die Benutzeroberfläche der Element Software zu

Sie können über die Management Virtual IP (MVIP)-Adresse des primären Cluster-Knotens auf die Element-UI zugreifen.

Sie müssen sicherstellen, dass Popup-Blocker und NoScript-Einstellungen in Ihrem Browser deaktiviert sind.

Je nach Konfiguration während der Cluster-Erstellung können Sie über IPv4- und IPv6-Adressen auf die UI zugreifen.

Schritte

1. Folgenden Optionen wählbar:
   - IPv6: Geben Sie ein `https://[IPv6_MVIP_address]`. Beispiel:

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

   - IPv4: Geben Sie ein `https://[IPv4 MVIP address]`. Beispiel:

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

2. Geben Sie für DNS den Hostnamen ein.
3. Klicken Sie durch alle Authentifizierungszertifikatmeldungen.

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Fügen Sie Laufwerke zu einem Cluster hinzu

Wenn Sie dem Cluster einen Node hinzufügen oder neue Laufwerke in einem vorhandenen Node installieren, werden die Laufwerke automatisch nach Verfügbarkeit registriert. Sie müssen die Laufwerke zum Cluster entweder über die Element-UI oder -API hinzufügen, bevor sie am Cluster teilnehmen können.

Laufwerke werden in der Liste Verfügbare Laufwerke nicht angezeigt, wenn folgende Bedingungen vorliegen:

- Laufwerke befinden sich im Status „aktiv“, „Entfernen“, „Löschen“ oder „Fehlgeschlagen“.
- Der Knoten, von dem das Laufwerk Teil ist, befindet sich im Status „Ausstehend“.

Schritte

1. Wählen Sie in der Element-Benutzeroberfläche **Cluster** > **Laufwerke** aus.
2. Klicken Sie auf **verfügbar**, um die Liste der verfügbaren Laufwerke anzuzeigen.
3. Führen Sie einen der folgenden Schritte aus:
   - Um einzelne Laufwerke hinzuzufügen, klicken Sie auf das **Aktionen** -Symbol für das Laufwerk, das Sie hinzufügen möchten, und klicken Sie auf **Hinzufügen**.

- Um mehrere Laufwerke hinzuzufügen, aktivieren Sie die Kontrollkästchen der Laufwerke, die hinzugefügt werden sollen, klicken Sie auf **Massenaktionen** und klicken Sie auf **Hinzufügen**.

```
== 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^]
```

Richten Sie ein Cluster mit Fibre Channel Nodes ein

Konfigurieren Sie einen Fibre Channel-Node

Mit Fibre Channel Nodes können Sie das Cluster mit einer Fibre Channel-Netzwerkstruktur verbinden. Fibre Channel Nodes werden paarweise hinzugefügt und im aktiv/aktiv-Modus betrieben (alle Nodes verarbeiten aktiv den Datenverkehr für das Cluster). Cluster, die Element Softwareversion 9.0 und höher ausführen, unterstützen bis zu vier Nodes. Cluster mit früheren Versionen unterstützen maximal zwei Nodes.

Sie müssen sicherstellen, dass die folgenden Bedingungen erfüllt sind, bevor Sie einen Fibre Channel-Node konfigurieren:

- Mindestens zwei Fibre Channel Nodes sind mit Fibre Channel Switches verbunden.
- Alle SolidFire Fibre Channel-Ports sollten mit Ihrem Fibre Channel Fabric verbunden sein. Die vier SolidFire-Bond10G-Netzwerkverbindungen sollten an eine LACP-Bond-Gruppe auf Switch-Ebene angeschlossen werden. Dies ermöglicht die beste Gesamt-Performance der Fibre Channel-Systeme.
- Prüfen und Validieren aller Best Practices für Fibre Channel Cluster in diesem NetApp Knowledge Base Artikel

  "Best Practice für SolidFire FC Cluster"

Für Fibre Channel Nodes und Storage Nodes sind die Schritte für Netzwerk- und Cluster-Konfiguration identisch.

Wenn Sie einen neuen Cluster mit Fibre Channel Nodes und SolidFire Storage Nodes erstellen, sind die WWPN-Adressen (Worldwide Port Name) für die Nodes in der Element UI verfügbar. Sie können die WWPN-Adressen verwenden, um den Fibre Channel-Switch zu Zone.

WWPNs sind im System registriert, wenn Sie ein neues Cluster mit Nodes erstellen. In der Element UI finden Sie die WWPN-Adressen in der Spalte WWPN der Registerkarte FC-Ports, auf die Sie über die Registerkarte Cluster zugreifen.

Weitere Informationen

Fügen Sie einem Cluster Fibre Channel Nodes hinzu

Erstellen Sie ein neues Cluster mit Fibre Channel Nodes

Erstellen Sie ein neues Cluster mit Fibre Channel Nodes

Sie können ein neues Cluster erstellen, nachdem Sie die einzelnen Fibre Channel Nodes konfiguriert haben. Wenn Sie ein Cluster erstellen, wird automatisch ein Cluster-Administrator-Benutzerkonto für Sie erstellt. Der Clusteradministrator verfügt über die Berechtigung zum Verwalten aller Clusterattribute und kann andere Cluster-Administratorkonten erstellen.

Während der Konfiguration eines neuen Node werden jedem Node 1-GB- oder 10-GB-Management-IP-Adressen (MIP) zugewiesen. Sie müssen eine der bei der Konfiguration erstellten Node-IP-Adressen verwenden, um die Seite Neues Cluster erstellen zu öffnen. Die verwendete IP-Adresse hängt vom Netzwerk ab, das Sie für das Cluster-Management ausgewählt haben.

Was Sie benötigen

Sie haben die einzelnen Fibre Channel Nodes konfiguriert.

Schritte

1. Geben Sie in einem Browserfenster eine Knoten-MIP-Adresse ein.
2. Geben Sie unter Erstellen eines neuen Clusters die folgenden Informationen ein:
   - Management-VIP: Routingfähige virtuelle IP im 1-GbE- oder 10-GbE-Netzwerk für Netzwerk-Management-Aufgaben.
   - ISCSI (Storage) VIP: Virtuelle IP im 10-GbE-Netzwerk für Storage und iSCSI-Erkennung.

     Sie können SVIP nicht ändern, nachdem Sie das Cluster erstellt haben.

   - Benutzername: Der primäre Clusteradministrator-Benutzername für authentifizierten Zugriff auf das Cluster. Sie müssen den Benutzernamen für die zukünftige Referenz speichern.

     Sie können Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern für den Benutzernamen verwenden.

   - Passwort: Passwort für authentifizierten Zugriff auf das Cluster. Sie müssen den Benutzernamen für die zukünftige Referenz speichern. Standardmäßig ist die zwei-Wege-Datensicherung aktiviert. Sie können diese Einstellung nicht ändern.
3. Lesen Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Ich stimme zu**.
4. **Optional**: Stellen Sie in der Liste Knoten sicher, dass die Kontrollkästchen für Knoten, die nicht im Cluster enthalten sein sollen, nicht ausgewählt sind.
5. Klicken Sie Auf **Cluster Erstellen**.

   Das System kann je nach Anzahl der Nodes im Cluster mehrere Minuten dauern, bis der Cluster erstellt wurde. In einem ordnungsgemäß konfigurierten Netzwerk sollte ein kleines Cluster mit fünf Nodes weniger als eine Minute dauern. Nach dem Erstellen des Clusters wird das Fenster Erstellen eines neuen Clusters an die MVIP-URL-Adresse für den Cluster umgeleitet und die Web-UI angezeigt.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Fügen Sie einem Cluster Fibre Channel Nodes hinzu

Sie können einem Cluster Fibre Channel Nodes hinzufügen, wenn mehr Storage benötigt wird, oder während der Cluster-Erstellung. Fibre Channel-Knoten erfordern die Erstkonfiguration, wenn sie zum ersten Mal eingeschaltet sind. Nachdem der Node konfiguriert wurde, wird er in der Liste der ausstehenden Nodes angezeigt und Sie können ihn einem Cluster hinzufügen.

Die Softwareversion auf jedem Fibre Channel-Knoten in einem Cluster muss kompatibel sein. Wenn Sie einem Cluster einen Fibre Channel Node hinzufügen, installiert das Cluster nach Bedarf die Cluster-Version des Elements auf dem neuen Node.

Schritte

1. Wählen Sie **Cluster** > **Knoten**.
2. Klicken Sie auf **Ausstehend**, um die Liste der ausstehenden Knoten anzuzeigen.
3. Führen Sie einen der folgenden Schritte aus:
   - Um einzelne Knoten hinzuzufügen, klicken Sie auf das Symbol **Aktionen** für den Knoten, den Sie hinzufügen möchten.
   - Um mehrere Knoten hinzuzufügen, aktivieren Sie das Kontrollkästchen der Knoten, die hinzugefügt werden sollen, und dann **Massenaktionen**.

   > Wenn der Node, den Sie hinzufügen, eine andere Version des Elements als die im Cluster ausgeführte Version hat, aktualisiert der Cluster den Node asynchron an die Version des Elements, das auf dem Cluster-Master ausgeführt wird. Nach der Aktualisierung des Node wird er sich automatisch dem Cluster hinzugefügt. Während dieses asynchronen Prozesses befindet sich der Knoten im hängenden Zustand aktiv.

4. Klicken Sie Auf **Hinzufügen**.

   Der Node wird in der Liste der aktiven Nodes angezeigt.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Einrichten von Zonen für Fibre Channel-Nodes

Wenn Sie einen neuen Cluster mit Fibre Channel-Nodes und SolidFire-Storage-Nodes erstellen, sind die WWPN-Adressen (Worldwide Port Name) für die Nodes in der Web-Benutzeroberfläche verfügbar. Sie können die WWPN-Adressen verwenden, um den Fibre Channel-Switch zu Zone.

WWPNs sind im System registriert, wenn Sie ein neues Cluster mit Nodes erstellen. In der Element UI finden Sie die WWPN-Adressen in der Spalte WWPN der Registerkarte FC-Ports, auf die Sie über die Registerkarte Cluster zugreifen.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Erstellen einer Volume-Zugriffsgruppe für Fibre Channel-Clients

Volume-Zugriffsgruppen ermöglichen die Kommunikation zwischen Fibre Channel Clients und Volumes auf einem SolidFire Storage-System. Das Zuordnen von Fibre Channel-Client-Initiatoren (WWPN) zu den Volumes einer Volume-Zugriffsgruppe ermöglicht den sicheren Daten-I/O zwischen einem Fibre Channel-Netzwerk und einem SolidFire Volume.

Sie können auch iSCSI-Initiatoren zu einer Volume-Zugriffsgruppe hinzufügen. Dadurch können die Initiatoren auf dieselben Volumes in der Volume-Zugriffsgruppe zugreifen.

Schritte

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie Auf **Zugriffsgruppe Erstellen**.
3. Geben Sie im Feld **Name** einen Namen für die Zugriffsgruppe des Volumes ein.
4. Wählen Sie die Fibre Channel-Initiatoren aus der Liste **Unbound Fibre Channel Initiatoren** aus, und fügen Sie sie hinzu.

   Sie können Initiatoren zu einem späteren Zeitpunkt hinzufügen oder löschen.

5. **Optional:** Wählen und fügen Sie einen iSCSI-Initiator aus der Liste **Initiatoren** hinzu.
6. So hängen Sie Volumes an die Zugriffsgruppe an:
   a. Wählen Sie ein Volume aus der Liste **Volumes** aus.
   b. Klicken Sie Auf **Volumen Anhängen**.
7. Klicken Sie Auf **Zugriffsgruppe Erstellen**.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Ermitteln der zu installierenden SolidFire-Komponenten

Vielleicht möchten Sie je nach Konfiguration und Bereitstellung prüfen, welche SolidFire Komponenten wie Management-Node, Active IQ und NetApp Monitoring Agent (NMA) installiert werden sollten.

In der folgenden Tabelle sind die zusätzlichen Komponenten aufgeführt und gibt an, ob diese installiert werden sollen.

Komponente	Standalone SolidFire Storage-Cluster	NetApp HCI Cluster
Management-Node	Empfehlenswert	Standardmäßig installiert, erforderlich
Active IQ	Empfohlen*	Empfohlen*
NetApp Monitoring Agent	Nicht unterstützt	Empfehlenswert

*Active IQ ist für kapazitätslizenzierte SolidFire Storage Cluster erforderlich.

Schritte

1. Ermitteln Sie, welche Komponenten installiert werden sollen.
2. Führen Sie die Installation gemäß der durch "Installieren Sie den Management-Node" Verfahren.

> Verwenden Sie zum Einrichten von Active IQ den `--telemetry_active` Parameter im Setup-Skript, um die Datenerfassung für die Analyse durch Active IQ zu ermöglichen.

3. Informationen zu NetApp Monitoring Agent finden Sie hier "Verfahren".

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Richten Sie einen Management-Node ein

Sie können den NetApp Element Software-Management-Node (mNode) installieren, um Upgrades durchzuführen und Systemservices bereitzustellen, Cluster-Ressourcen und -Einstellungen zu managen, Systemtests und Dienstprogramme auszuführen und den NetApp Support-Zugriff zur Fehlerbehebung zu aktivieren.

1. Siehe "Installieren Sie den Management-Node" Dokumentation.

> Verwenden Sie zum Einrichten von Active IQ den `--telemetry_active` Parameter im Setup-Skript, um die Datenerfassung für die Analyse durch Active IQ zu ermöglichen.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Konfigurieren Sie vollständig qualifizierten Domänennamen Web UI-Zugriff

Mit SolidFire All-Flash-Speicher mit NetApp Element Software 12.2 oder höher können Sie unter Verwendung des vollständig qualifizierten Domain-Namens (FQDN) auf Webschnittstellen des Speicherclusters zugreifen. Wenn Sie den FQDN für den Zugriff auf Webbenutzerschnittstellen wie die Element-Web-UI, die Benutzeroberfläche per Node oder die Management-Node-Benutzeroberfläche verwenden möchten, müssen Sie zuerst eine Speichercluster-Einstellung hinzufügen, um den vom Cluster verwendeten FQDN zu identifizieren.

Durch diesen Prozess kann das Cluster eine Anmeldesitzung ordnungsgemäß umleiten und die Integration in externe Services wie Schlüsselmanager und Identitätsanbieter für die Multi-Faktor-Authentifizierung verbessern.

Was Sie benötigen

- Diese Funktion erfordert Element 12.2 oder höher.
- Für die Konfiguration dieser Funktion mit NetApp Hybrid Cloud Control REST-APIs sind Management-Services 2.15 oder höher erforderlich.
- Für die Konfiguration dieser Funktion mit der NetApp Hybrid Cloud Control UI sind Management-Services ab 2.19 erforderlich.
- Zur Verwendung VON REST-APIs müssen Sie einen Management-Node mit Version 11.5 oder höher bereitgestellt haben.
- Sie benötigen vollqualifizierte Domain-Namen für den Management-Node und jeden Storage-Cluster, die korrekt zur Management Node-IP-Adresse und den einzelnen Storage-Cluster-IP-Adressen auflösen.

Über NetApp Hybrid Cloud Control und DIE REST-API können Sie den FQDN-Webbenutzerzugriff konfigurieren oder entfernen. Sie können auch Fehler bei falsch konfigurierten FQDNs beheben.

- Konfigurieren Sie den FQDN-Web-UI-Zugriff mit NetApp Hybrid Cloud Control
- Konfigurieren Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API
- Entfernen Sie FQDN Web-UI-Zugriff mit NetApp Hybrid Cloud Control
- Entfernen Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API
- Fehlerbehebung

Konfigurieren Sie den FQDN-Web-UI-Zugriff mit NetApp Hybrid Cloud Control

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie das Menüsymbol oben rechts auf der Seite aus.

4. Wählen Sie **Konfigurieren**.
5. Wählen Sie im Fenster **vollqualifizierte Domänennamen** die Option **Einrichtung** aus.
6. Geben Sie im daraufhin angezeigten Fenster die FQDNs für den Managementknoten und jeden Speichercluster ein.
7. Wählen Sie **Speichern**.

   Im Fensterbereich **Fully Qualified Domain Names** werden alle Speichercluster mit dem zugehörigen MVIP und FQDN aufgelistet.

   Nur verbundene Speichercluster mit dem FQDN-Satz werden im Fensterbereich **vollqualifizierte Domänennamen** aufgeführt.

Konfigurieren Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API

Schritte

1. Stellen Sie sicher, dass die Element-Speicherknoten und der mNode für die Netzwerkumgebung richtig konfiguriert sind, damit FQDNs in der Umgebung aufgelöst werden können. Um DNS einzustellen, wechseln Sie zur Benutzeroberfläche für Speicherknoten pro Knoten und zum Managementknoten und wählen Sie dann **Netzwerkeinstellungen** > **Managementnetzwerk** aus.
   a. UI pro Node für Storage-Nodes: `https://<storage_node_management_IP>:442`
   b. UI pro Node für den Management-Node: `https://<management_node_IP>:442`
2. Ändern Sie die Storage-Cluster-Einstellungen mithilfe der Element API.
   a. Greifen Sie auf die Element API zu, und erstellen Sie mithilfe der die folgende Clusterschnittstelle "CreateClusterSchnittstellenPräferenz" API-Methode, Einfügen des Clusters MVIP FQDN für den Vorzugswert:
      - Name: `mvip_fqdn`
      - Wert: `Fully Qualified Domain Name for the Cluster MVIP`

        In diesem Beispiel ist FQDN=storagecluster.my.org:

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

3. Ändern Sie die Management-Node-Einstellungen mit der REST-API auf dem Management-Node:
   a. Rufen Sie die REST-API-UI für den Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode/2/`

      Beispiel:

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

   a. Klicken Sie auf **authorize** oder ein Schloss-Symbol und geben Sie den Cluster-Benutzernamen und das Passwort ein.

b. Geben Sie die Client-ID als ein `mnode-client`.

c. Klicken Sie auf **autorisieren**, um die Sitzung zu starten und dann das Fenster zu schließen.

d. Wählen Sie in der Liste Server die Option aus `mnode2`.

e. Klicken Sie auf **GET /settings**.

f. Klicken Sie auf **Probieren Sie es aus**.

g. Klicken Sie Auf **Ausführen**.

h. Notieren Sie alle Proxyeinstellungen, die im Antwortkörper gemeldet wurden.

i. Klicken Sie auf **PUT/settings**.

j. Klicken Sie auf **Probieren Sie es aus**.

k. Geben Sie im Bereich Text anfordern den Management-Node FQDN als Wert für das ein `mnode_fqdn` Parameter.

l. Geben Sie alle Proxy-Einstellungswerte ein, die Sie zuvor in den verbleibenden Parametern im Anforderungskörper aufgezeichnet haben. Wenn Sie die Proxyparameter leer lassen oder nicht in den Text der Anforderung aufnehmen, werden die vorhandenen Proxyeinstellungen entfernt.

m. Klicken Sie Auf **Ausführen**.

Entfernen Sie FQDN Web-UI-Zugriff mit NetApp Hybrid Cloud Control

Mit diesem Verfahren können Sie den FQDN-Webzugriff für den Managementknoten und die Speichercluster entfernen.

Schritte

1. Wählen Sie im Fenster **vollqualifizierte Domänennamen** die Option **Bearbeiten** aus.
2. Löschen Sie im resultierenden Fenster den Inhalt im Textfeld **FQDN**.
3. Wählen Sie **Speichern**.

   Das Fenster wird geschlossen, und der FQDN wird nicht mehr im Bereich **Fully Qualified Domain Names** aufgeführt.

Entfernen Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API

Schritte

1. Ändern Sie die Storage-Cluster-Einstellungen mithilfe der Element API.

   a. Greifen Sie auf die Element API zu und löschen Sie mithilfe der die folgende Clusterschnittstelle `DeleteClusterInterfacePreference` API-Methode:

      - Name: `mvip_fqdn`

        Beispiel:

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

2. Ändern Sie die Management-Node-Einstellungen mit der REST-API auf dem Management-Node:

a. Rufen Sie die REST-API-UI für den Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode/2/`. Beispiel:

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

b. Wählen Sie **authorize** oder ein Schloss-Symbol aus und geben Sie den Benutzernamen und das Kennwort des Element Clusters ein.

c. Geben Sie die Client-ID als ein `mnode-client`.

d. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

e. Schließen Sie das Fenster.

f. Wählen Sie **PUT /settings**.

g. Wählen Sie **Probieren Sie es aus**.

h. Geben Sie im Bereich des Anforderungskörpers keinen Wert für das ein `mnode_fqdn` Parameter. Geben Sie außerdem an, ob der Proxy verwendet werden soll (`true` Oder `false`) Für die `use_proxy` Parameter.

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

i. Wählen Sie **Ausführen**.

Fehlerbehebung

Wenn FQDNs falsch konfiguriert sind, können Sie Probleme beim Zugriff auf den Managementknoten, einen Speichercluster oder beide haben. Verwenden Sie die folgenden Informationen, um die Fehlerbehebung zu unterstützen.

Problem	Ursache	Auflösung
• Beim Versuch, entweder mit dem FQDN auf den Management-Node oder den Speicher-Cluster zuzugreifen, wird ein Browserfehler angezeigt. • Sie können sich mit einer IP-Adresse nicht entweder beim Management-Node oder beim Storage-Cluster einloggen.	Der FQDN des Managementknoten und der FQDN des Speicherclusters sind beide falsch konfiguriert.	Verwenden Sie die REST-API-Anweisungen auf dieser Seite, um die FQDN-Einstellungen des Management-Nodes und Speicherclusters zu entfernen und erneut zu konfigurieren.

Problem	Ursache	Auflösung
• Beim Versuch, auf den Speicher-Cluster-FQDN zuzugreifen, wird ein Browserfehler angezeigt. • Sie können sich mit einer IP-Adresse nicht entweder beim Management-Node oder beim Storage-Cluster einloggen.	Der FQDN des Managementknoten ist richtig konfiguriert, der Speichercluster-FQDN ist jedoch falsch konfiguriert.	Mithilfe der REST-API-Anweisungen auf dieser Seite können Sie die FQDN-Einstellungen des Speicherclusters entfernen und erneut konfigurieren
• Beim Versuch, auf den Verwaltungsknoten FQDN zuzugreifen, wird ein Browserfehler angezeigt. • Sie können sich mit einer IP-Adresse beim Management-Node und Storage-Cluster einloggen.	Der FQDN des Managementknoten ist falsch konfiguriert, der Speichercluster-FQDN ist jedoch korrekt konfiguriert.	Melden Sie sich bei NetApp Hybrid Cloud Control an, um die FQDN-Einstellungen des Managementknoten in der UI zu korrigieren, oder VERWENDEN Sie die REST-API-Anweisungen auf dieser Seite, um die Einstellungen zu korrigieren.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Was kommt als Nächstes

Nachdem Sie Element Software eingerichtet haben, managen Sie Storage, indem Sie einige der folgenden Optionen ausführen:

- "Greifen Sie auf die Benutzeroberfläche der Element Software zu"
- "Konfigurieren Sie nach der Bereitstellung die SolidFire Systemoptionen"
- "Konten verwalten"
- "Management des Systems"
- "Management von Volumes und virtuellen Volumes"
- "Sichern Sie Ihre Daten"
- "Fehler im System beheben"

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"
- "NetApp Element Plug-in für vCenter Server"

Storage-Management mit Element Software

Storage-Management mit Element Software

Mit Element Software können Sie SolidFire Storage einrichten, Cluster-Kapazität und -Performance überwachen und Storage-Aktivitäten in einer mandantenfähigen Infrastruktur managen.

Element ist das Storage-Betriebssystem, das Herzstück eines SolidFire Clusters ist. Element Software wird auf allen Nodes im Cluster unabhängig ausgeführt. Es ermöglicht den Nodes des Clusters, Ressourcen zu kombinieren und externen Clients als einzelnes Storage-System zur Verfügung zu stellen. Element Software ist für die gesamte Clusterkoordination, den Umfang und das Management des Systems verantwortlich.

Die Softwareschnittstelle basiert auf der Element API.

- "Greifen Sie auf die Benutzeroberfläche der Element Software zu"
- "Konfigurieren Sie nach der Bereitstellung die SolidFire Systemoptionen"
- "Aktualisieren von Komponenten des Storage-Systems"
- "Verwenden Sie grundlegende Optionen in der UI für Element Software"
- "Konten verwalten"
- "Management des Systems"
- "Management von Volumes und virtuellen Volumes"
- "Sichern Sie Ihre Daten"
- "Fehler im System beheben"

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Greifen Sie auf die Benutzeroberfläche der Element Software zu

Sie können über die Management Virtual IP (MVIP)-Adresse des primären Cluster-Knotens auf die Element-UI zugreifen.

Sie müssen sicherstellen, dass Popup-Blocker und NoScript-Einstellungen in Ihrem Browser deaktiviert sind.

Je nach Konfiguration während der Cluster-Erstellung können Sie über IPv4- und IPv6-Adressen auf die UI zugreifen.

1. Folgenden Optionen wählbar:
    - IPv6: Geben Sie https://[IPv6 MVIP-Adresse ein, z. B.:

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

- IPv4: Geben Sie https://[IPv4 MVIP-Adresse ein, z. B.:

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

2. Geben Sie für DNS den Hostnamen ein.
3. Klicken Sie durch alle Authentifizierungszertifikatmeldungen.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Konfigurieren Sie nach der Bereitstellung die SolidFire Systemoptionen

Konfigurieren Sie nach der Bereitstellung die SolidFire Systemoptionen

Nach der Einrichtung des SolidFire Systems sollten Sie möglicherweise einige optionale Aufgaben ausführen.

Wenn Sie die Anmeldedaten im System ändern, sollten Sie die Auswirkungen auf andere Komponenten kennen.

Darüber hinaus können Einstellungen für Multi-Faktor-Authentifizierung, externes Verschlüsselungsmanagement und die Sicherheit von Federal Information Processing Standards (FIPS) konfiguriert werden. Sie sollten sich auch die Aktualisierung von Kennwörtern ansehen, wenn nötig.

Weitere Informationen

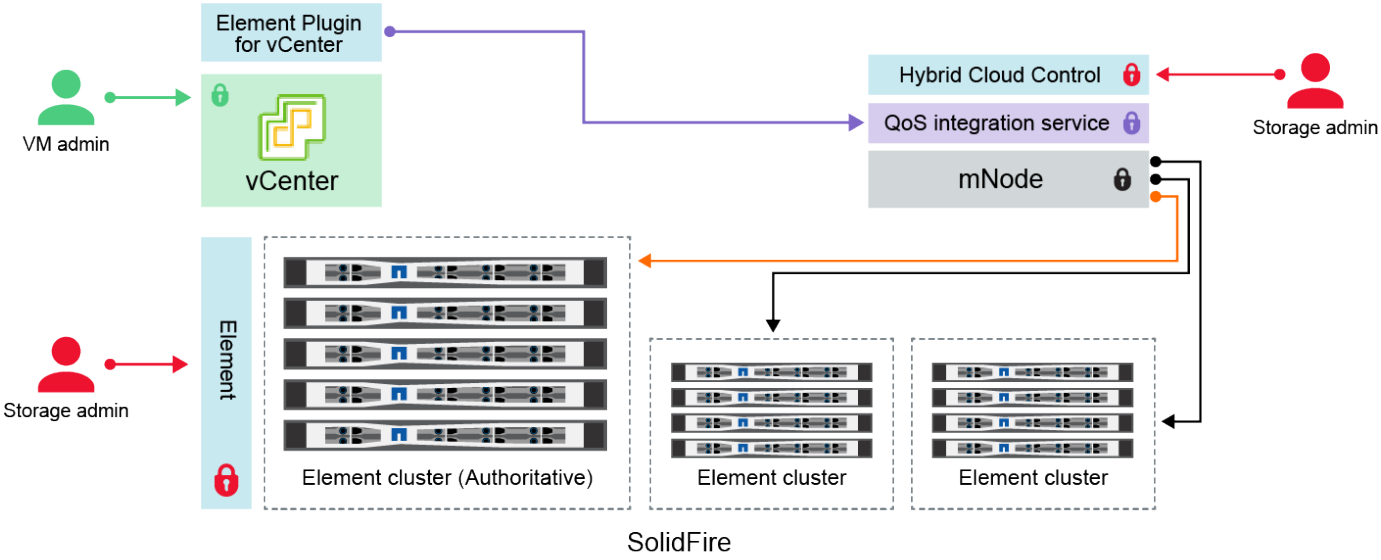
- "Anmeldedaten in NetApp HCI und NetApp SolidFire ändern"
- "Ändern Sie das Standard-SSL-Zertifikat der Element Software"
- "Ändern Sie das IPMI-Passwort für Knoten"
- "Multi-Faktor-Authentifizierung aktivieren"
- "Erste Schritte mit externem Verschlüsselungsmanagement"
- "Erstellen eines Clusters, das FIPS-Laufwerke unterstützt"

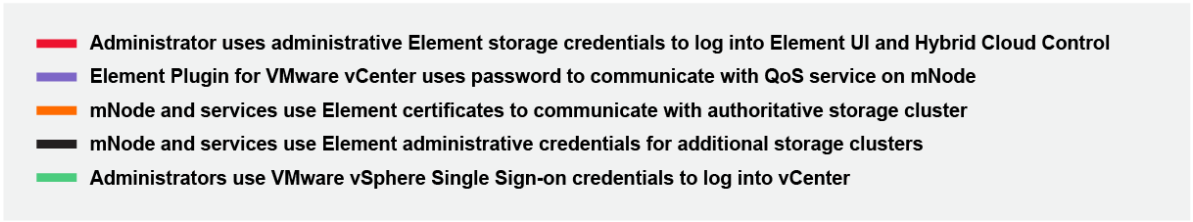
Anmeldedaten in NetApp HCI und NetApp SolidFire ändern

Abhängig von den Sicherheitsrichtlinien im Unternehmen, die NetApp HCI oder NetApp SolidFire implementiert haben, gehört das Ändern von Anmeldedaten oder Passwörtern in der Regel zu den Sicherheitspraktiken. Bevor Sie Passwörter ändern, sollten Sie sich der Auswirkungen auf andere Softwarekomponenten in der Bereitstellung bewusst sein.

Wenn Sie die Anmeldedaten für eine Komponente einer NetApp HCI- oder NetApp SolidFire-Implementierung ändern, enthält die folgende Tabelle Anweisungen zu den Auswirkungen auf andere Komponenten.

Interaktionen von NetApp SolidFire-Komponenten:





Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
Anmeldedaten für Element	**Gilt für**: NetApp HCI und SolidFire Administratoren verwenden diese Anmeldedaten zur Anmeldung bei: • Element Benutzeroberfläche auf dem Element Storage-Cluster • Hybrid Cloud Control auf dem Management-Node (mNode) Wenn Hybrid Cloud Control mehrere Storage-Cluster managt, akzeptiert es nur die Admin-Anmeldeinformationen für die Storage-Cluster, bekannt als das *autorisierende Cluster*, für das der mNode ursprünglich eingerichtet wurde. Bei Storage-Clustern, die später zu Hybrid Cloud Control hinzugefügt werden, speichert der mNode die Anmeldedaten des Administrators sicher. Wenn Anmeldeinformationen für nachträglich hinzugefügte Speicher-Cluster geändert werden, müssen die Anmeldeinformationen auch im mnode mit der mNode-API aktualisiert werden.	• "Aktualisieren der Passwörter für den Storage-Cluster-Administrator." • Aktualisieren Sie die Anmeldedaten des Storage-Cluster-Administrators im mNode mithilfe des "Modifizierter clusteradmin API".
VSphere Single Sign On – Zugangsdaten	**Gilt nur für**: NetApp HCI Administratoren verwenden diese Zugangsdaten, um sich beim VMware vSphere Client anzumelden. Wenn vCenter Teil der Installation von NetApp HCI ist, werden in der NetApp Deployment Engine die folgenden Anmeldedaten konfiguriert: • username@vsphere.local mit dem angegebenen Passwort, und • administrator@vsphere.local mit dem angegebenen Passwort. Wenn ein vorhandenes vCenter für die Implementierung von NetApp HCI verwendet wird, werden die Anmeldeinformationen für vSphere Single Sign-On von DEN IT-VMware-Administratoren gemanagt.	"Aktualisieren der vCenter- und ESXi-Anmeldedaten".

Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
Baseboard Management Controller (BMC) Zugangsdaten	**Gilt nur für**: NetApp HCI Administratoren melden sich mithilfe dieser Anmeldedaten beim BMC der NetApp Computing-Nodes in einer NetApp HCI-Implementierung an. Das BMC bietet grundlegende Hardware-Überwachung und Funktionen der virtuellen Konsole. BMC-Anmeldeinformationen (auch als „*IPMI*“ bezeichnet) für jeden NetApp Computing-Node werden in NetApp HCI-Implementierungen sicher auf dem mNode gespeichert. NetApp Hybrid Cloud Control verwendet BMC-Anmeldeinformationen in einem Service-Konto, um während eines Upgrades der Computing-Node-Firmware mit dem BMC in den Computing-Nodes zu kommunizieren. Wenn die BMC-Anmeldedaten geändert werden, müssen auch die Anmeldeinformationen für die jeweiligen Computing-Nodes auf dem mnode aktualisiert werden, damit alle Hybrid Cloud Control-Funktionen erhalten bleiben.	• "Konfigurieren Sie IPMI für jeden Node in NetApp HCI". • Für H410C, H610C und H615C Nodes "Ändern Sie das Standard-IPMI-Passwort". • Für H410S und H610S Nodes "Ändern Sie das IPM-Standardpasswort". • "Ändern Sie BMC-Anmeldeinformationen auf dem Management-Node".
ESXi Anmeldedaten	**Gilt nur für**: NetApp HCI Administratoren können sich über SSH oder die lokale DCUI mit einem lokalen Root-Konto bei ESXi Hosts anmelden. In NetApp HCI-Implementierungen ist der Benutzername „root“, und das Passwort wurde bei der Erstinstallation dieses Computing-Node in der NetApp Deployment Engine angegeben. ESXi Root-Anmeldedaten für jeden NetApp Computing-Node werden in NetApp HCI-Implementierungen sicher auf dem mnode gespeichert. NetApp Hybrid Cloud Control verwendet die Zugangsdaten in der Kapazität eines Service-Kontos, um direkt während Upgrades der Firmware des Computing-Nodes und Zustandsprüfungen mit ESXi Hosts zu kommunizieren. Wenn die ESXi-Root-Anmeldedaten von einem VMware-Administrator geändert werden, müssen die Anmeldeinformationen für die jeweiligen Computing-Nodes auf dem mnode aktualisiert werden, damit die Hybrid Cloud Control-Funktionalität erhalten bleibt.	"Anmeldedaten für vCenter- und ESXi-Hosts aktualisieren".

Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
Passwort für die QoS-Integration	**Gilt für**: NetApp HCI und optional in SolidFire Nicht für interaktive Anmeldungen durch Administratoren verwendet. Die QoS-Integration zwischen VMware vSphere und Element Software wird durch folgende aktiviert: • Element Plug-in für vCenter Server und • QoS-Service auf dem mNode. Für die Authentifizierung verwendet der QoS-Service ein Passwort, das ausschließlich in diesem Zusammenhang verwendet wird. Das QoS-Passwort wird bei der Erstinstallation des Element Plug-in für vCenter Server angegeben oder während der NetApp HCI-Implementierung automatisch generiert. Keine Auswirkung auf andere Komponenten.	"Aktualisieren Sie die QoSSIOC-Anmeldeinformationen im NetApp Element-Plug-in für vCenter Server". Das SIOC-Passwort des NetApp Element-Plug-ins für vCenter-Server wird auch als *QoSSIOC-Passwort* bezeichnet. Lesen Sie den Element Plug-in for vCenter Server KB Artikel.
Anmeldedaten für vCenter Service Appliance	**Gilt für**: NetApp HCI nur bei Einrichtung über die NetApp Deployment Engine Administratoren können sich bei den virtuellen Maschinen der vCenter Server Appliance anmelden. In NetApp HCI-Implementierungen ist der Benutzername „root“, und das Passwort wurde bei der Erstinstallation dieses Computing-Node in der NetApp Deployment Engine angegeben. Je nach der bereitgestellten VMware vSphere Version können sich auch bestimmte Administratoren in der vSphere Single Sign-On-Domäne bei der Appliance anmelden. Keine Auswirkung auf andere Komponenten.	Es sind keine Änderungen erforderlich.
Anmeldedaten für NetApp Management-Node-Admin	**Gilt für**: NetApp HCI und optional in SolidFire Zur erweiterten Konfiguration und Fehlerbehebung können sich Administratoren bei Virtual Machines des NetApp Management Node anmelden. Je nach implementierter Management-Node-Version ist die Anmeldung über SSH nicht standardmäßig aktiviert. In NetApp HCI-Implementierungen wurden Benutzername und Passwort vom Benutzer während der Erstinstallation dieses Computing-Node in der NetApp Deployment Engine angegeben. Keine Auswirkung auf andere Komponenten.	Es sind keine Änderungen erforderlich.

Weitere Informationen

- "Ändern Sie das Standard-SSL-Zertifikat der Element Software"
- "Ändern Sie das IPMI-Passwort für Knoten"
- "Multi-Faktor-Authentifizierung aktivieren"
- "Erste Schritte mit externem Verschlüsselungsmanagement"
- "Erstellen eines Clusters, das FIPS-Laufwerke unterstützt"

Ändern Sie das Standard-SSL-Zertifikat der Element Software

Sie können mithilfe der NetApp Element API das Standard-SSL-Zertifikat und den privaten Schlüssel des Storage-Node im Cluster ändern.

Beim Erstellen eines NetApp Element-Software-Clusters erstellt das Cluster ein einzigartiges SSL-Zertifikat (Secure Sockets Layer) mit einem privaten Schlüssel, das für die gesamte HTTPS-Kommunikation über die Element-UI, die UI pro Node oder die APIs verwendet wird. Die Element Software unterstützt selbstsignierte Zertifikate sowie Zertifikate, die von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt und verifiziert werden.

Sie können die folgenden API-Methoden verwenden, um mehr Informationen über das Standard-SSL-Zertifikat zu erhalten und Änderungen vorzunehmen.

- **GetSSLZertifikat**

  Sie können das verwenden "GetSSLCertificate-Methode" So rufen Sie Informationen zum derzeit installierten SSL-Zertifikat ab, einschließlich aller Zertifikatdetails.

- **SetSSLZertifikat**

  Sie können das verwenden "SetSSLCertificate-Methode" Zum Festlegen der Cluster- und Node-SSL-Zertifikate auf das von Ihnen zur Verfügung gestellt Zertifikat und den privaten Schlüssel. Das System überprüft das Zertifikat und den privaten Schlüssel, um zu verhindern, dass ein ungültiges Zertifikat angewendet wird.

- **RemoveSSLZertifikat**

  Der "RemoveSSLCertificate-Methode" Entfernt das derzeit installierte SSL-Zertifikat und den privaten Schlüssel. Das Cluster generiert dann ein neues selbstsigniertes Zertifikat und einen privaten Schlüssel.

> Das Cluster-SSL-Zertifikat wird automatisch auf alle neuen Nodes angewendet, die dem Cluster hinzugefügt wurden. Jeder Node, der aus dem Cluster entfernt wurde, wird auf ein selbstsigniertes Zertifikat zurückgesetzt und alle benutzerdefinierten Zertifikate und Schlüsselinformationen werden vom Node entfernt.

Weitere Informationen

- "Ändern Sie das Standard-SSL-Zertifikat für den Management-Node"
- "Welche Anforderungen gelten für das Festlegen benutzerdefinierter SSL-Zertifikate in der Element Software?"
- "Dokumentation von SolidFire und Element Software"

- "NetApp Element Plug-in für vCenter Server"

Ändern Sie das Standard-IPMI-Passwort für Nodes

Sie können das Standard-Administratorpasswort für die Intelligent Platform Management Interface (IPMI) ändern, sobald Sie Remote-IPMI-Zugriff auf den Node haben. Sie möchten dies möglicherweise tun, wenn Installationsupdates vorhanden sind.

Weitere Informationen zur Konfiguration des IPM-Zugriffs für Knoten finden Sie unter "Konfigurieren Sie IPMI für jeden Node".

Sie können das IPM-Passwort für diese Knoten ändern:

- H410S Nodes
- H610S Nodes

Ändern Sie das Standard-IPMI-Passwort für H410S-Nodes

Sie sollten das Standardpasswort für das IPMI-Administratorkonto auf jedem Speicherknoten ändern, sobald Sie den IPMI-Netzwerkport konfigurieren.

Was Sie benötigen

Sie sollten die IPMI-IP-Adresse für jeden Storage-Node konfiguriert haben.

Schritte

1. Öffnen Sie einen Webbrowser auf einem Computer, der das IPMI-Netzwerk erreichen kann, und navigieren Sie zu der IPMI-IP-Adresse für den Knoten.
2. Geben Sie den Benutzernamen ein `ADMIN` Und Passwort `ADMIN` In der Eingabeaufforderung für die Anmeldung.
3. Klicken Sie beim Anmelden auf die Registerkarte **Konfiguration**.
4. Klicken Sie Auf **Benutzer**.
5. Wählen Sie die aus `ADMIN` Benutzer und klicken Sie auf **Benutzer ändern**.
6. Aktivieren Sie das Kontrollkästchen **Passwort ändern**.
7. Geben Sie ein neues Passwort in die Felder **Passwort** und **Passwort bestätigen** ein.
8. Klicken Sie auf **Ändern** und dann auf **OK**.
9. Wiederholen Sie dieses Verfahren für alle anderen H410S-Nodes mit Standard-IPMI-Kennwörtern.

Ändern Sie das Standard-IPMI-Passwort für H610S-Nodes

Sie sollten das Standardpasswort für das IPMI-Administratorkonto auf jedem Speicherknoten ändern, sobald Sie den IPMI-Netzwerkport konfigurieren.

Was Sie benötigen

Sie sollten die IPMI-IP-Adresse für jeden Storage-Node konfiguriert haben.

Schritte

1. Öffnen Sie einen Webbrowser auf einem Computer, der das IPMI-Netzwerk erreichen kann, und navigieren Sie zu der IPMI-IP-Adresse für den Knoten.

2. Geben Sie den Benutzernamen ein `root` Und Passwort `calvin` In der Eingabeaufforderung für die Anmeldung.
3. Wenn Sie sich anmelden, klicken Sie oben links auf der Seite auf das Symbol für die Menünavigation, um das Fach für die Seitenleiste zu öffnen.
4. Klicken Sie Auf **Einstellungen**.
5. Klicken Sie Auf **Benutzerverwaltung**.
6. Wählen Sie den **Administrator**-Benutzer aus der Liste aus.
7. Aktivieren Sie das Kontrollkästchen **Passwort ändern**.
8. Geben Sie ein neues, starkes Passwort in die Felder **Passwort** und **Passwort bestätigen** ein.
9. Klicken Sie unten auf der Seite auf **Speichern**.
10. Wiederholen Sie dieses Verfahren für alle anderen H610S-Nodes mit Standard-IPMI-Kennwörtern.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Verwenden Sie grundlegende Optionen in der UI für Element Software

Verwenden Sie grundlegende Optionen in der UI für Element Software

Über die NetApp Element Software-Webbenutzeroberfläche (Element UI) können Sie allgemeine Aufgaben auf Ihrem SolidFire-System überwachen und ausführen.

Zu den grundlegenden Optionen gehören die Anzeige von API-Befehlen, die durch UI-Aktivitäten aktiviert sind, und die Angabe von Feedback.

- "Zeigt die API-Aktivität an"
- "Symbole in der Element-Schnittstelle"
- "Feedback mitteilen"

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

API-Aktivität

Zeigt die API-Aktivität an

Das Element System nutzt die NetApp Element API als Grundlage für seine Funktionen. Mit der Element UI können Sie verschiedene Arten von API-Aktivitäten in Echtzeit auf dem System anzeigen, während Sie die Schnittstelle verwenden. Mit dem API-Protokoll können Sie vom Benutzer initiierte und Hintergrund-System-API-Aktivitäten sowie API-

Aufrufe auf der Seite anzeigen, die Sie derzeit anzeigen.

Mithilfe des API-Protokolls können Sie ermitteln, welche API-Methoden für bestimmte Aufgaben verwendet werden. Außerdem erfahren Sie, wie Sie die API-Methoden und -Objekte zum Erstellen benutzerdefinierter Anwendungen verwenden.

Weitere Informationen zu den einzelnen Methoden finden Sie unter "Element Software-API-Referenz"Die

1. Klicken Sie in der Element UI-Navigationsleiste auf **API-Protokoll**.
2. So ändern Sie den Typ der API-Aktivität, die im Fenster API-Protokoll angezeigt wird:
   a. Wählen Sie **Requests**, um API-Request-Traffic anzuzeigen.
   b. Wählen Sie **Antworten**, um den API-Antwortdatenverkehr anzuzeigen.
   c. Filtern Sie die Typen von API-Traffic, indem Sie eine der folgenden Optionen auswählen:
      - **Benutzer initiiert**: API-Verkehr durch Ihre Aktivitäten während dieser Web-UI-Sitzung.
      - **Hintergrundabfrage**: API-Traffic, der durch Systemaktivität im Hintergrund erzeugt wird.
      - **Aktuelle Seite**: API Traffic generiert durch Aufgaben auf der Seite, die Sie gerade sehen.

Weitere Informationen

- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Aktualisierungsrate der Schnittstelle, die von einer Clusterlast beeinflusst wird

Abhängig von den API-Reaktionszeiten kann das Cluster möglicherweise das Datenaktualisierungsintervall für bestimmte Teile der NetApp Element Softwareseite automatisch anpassen, die Sie anzeigen.

Das Aktualisierungsintervall wird auf die Standardeinstellung zurückgesetzt, wenn Sie die Seite in Ihrem Browser neu laden. Sie können das aktuelle Aktualisierungsintervall anzeigen, indem Sie oben rechts auf der Seite auf den Cluster-Namen klicken. Beachten Sie, dass das Intervall steuert, wie oft API-Anforderungen erstellt werden, nicht wie schnell die Daten vom Server zurückkommen.

Wenn ein Cluster stark beansprucht ist, können API-Anforderungen von der Element UI in die Warteschlange gestellt werden. Wenn die Systemantwort erheblich verzögert wird, z. B. eine langsame Netzwerkverbindung in Verbindung mit einem überlasteten Cluster, werden Sie möglicherweise von der Element UI abgemeldet, wenn das System nicht schnell genug auf API-Anfragen in der Warteschlange reagiert. Wenn Sie zum Abmeldebildschirm umgeleitet werden, können Sie sich erneut anmelden, nachdem Sie eine erste Browser-Authentifizierungsaufforderung abgesagt haben. Wenn Sie zur Übersichtsseite zurückkehren, werden Sie möglicherweise nach Cluster-Anmeldedaten gefragt, wenn diese nicht vom Browser gespeichert werden.

Symbole in der Element-Schnittstelle

Die NetApp Element-Softwareoberfläche zeigt Symbole an, die Aktionen darstellen, die Sie für Systemressourcen ergreifen können.

Folgende Tabelle enthält eine Kurzübersicht:

Symbol	Beschreibung
	Aktionen
	Backup auf
	Klon oder Kopie
	Löschen oder löschen
	Bearbeiten
	Filtern
	Paar
	Aktualisierung
	Wiederherstellen
	Wiederherstellen von
	Rollback
	Snapshot

Feedback mitteilen

Sie können die Webbenutzeroberfläche der Element Software verbessern und alle UI-Probleme beheben, indem Sie das Feedback-Formular verwenden, das über die gesamte Benutzeroberfläche zugänglich ist.

1. Klicken Sie auf einer beliebigen Seite in der Element UI auf die Schaltfläche **Feedback**.
2. Geben Sie relevante Informationen in die Felder Zusammenfassung und Beschreibung ein.

3. Fügen Sie hilfreiche Screenshots an.
4. Geben Sie einen Namen und eine E-Mail-Adresse ein.
5. Aktivieren Sie das Kontrollkästchen, um Daten zu Ihrer aktuellen Umgebung einzuschließen.
6. Klicken Sie Auf **Absenden**.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Konten verwalten

Konten verwalten

In SolidFire Storage-Systemen können Mandanten Konten verwenden, um Clients eine Verbindung zu Volumes in einem Cluster zu ermöglichen. Wenn Sie ein Volume erstellen, wird es einem bestimmten Konto zugewiesen. Sie können auch Cluster-Administratorkonten für ein SolidFire Storage-System verwalten.

- "Arbeiten Sie mit Konten, die CHAP verwenden"
- "Verwalten von Benutzerkonten für Cluster-Administratoren"

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Arbeiten Sie mit Konten, die CHAP verwenden

In SolidFire Storage-Systemen können Mandanten Konten verwenden, um Clients eine Verbindung zu Volumes in einem Cluster zu ermöglichen. Ein Konto enthält die CHAP-Authentifizierung (Challenge-Handshake Authentication Protocol), die für den Zugriff auf die ihm zugewiesenen Volumes erforderlich ist. Wenn Sie ein Volume erstellen, wird es einem bestimmten Konto zugewiesen.

Einem Konto können bis zu zweitausend Volumes zugewiesen sein, ein Volume kann jedoch nur zu einem Konto gehören.

CHAP-Algorithmen

Ab Element 12.7 werden sichere FIPS-kompatible CHAP-Algorithmen SHA1, SHA-256 und SHA3-256 unterstützt. Wenn ein Host-iSCSI-Initiator eine iSCSI-Sitzung mit einem Element-iSCSI-Ziel erstellt, fordert er eine Liste von CHAP-Algorithmen zur Verwendung an. Das Element iSCSI-Ziel wählt den ersten Algorithmus aus, der es aus der vom Host-iSCSI-Initiator angeforderten Liste unterstützt. Um zu überprüfen, ob das Element iSCSI-Ziel den sichersten Algorithmus wählt, müssen Sie den Host-iSCSI-Initiator so konfigurieren, dass eine Liste von Algorithmen gesendet wird, die von der sichersten geordnet sind, z. B. SHA3-256, um die Sicherheit am wenigsten zu gewährleisten. SHA1 oder MD5. Wenn SHA-Algorithmen nicht vom Host-iSCSI-Initiator angefordert werden, wählt das Element iSCSI-Ziel MD5 aus, vorausgesetzt, die vorgeschlagene

Algorithmusliste vom Host enthält MD5. Möglicherweise müssen Sie die Host-iSCSI-Initiator-Konfiguration aktualisieren, um die Unterstützung für die sicheren Algorithmen zu aktivieren.

Wenn Sie während eines Upgrades für Element 12.7 oder höher die Host-iSCSI-Initiatorkonfiguration bereits aktualisiert haben, um eine Sitzungsanfrage mit einer Liste zu senden, die SHA-Algorithmen enthält, werden beim Neustart der Speicherknoten die neuen sicheren Algorithmen aktiviert und neue oder erneut verbundene iSCSI-Sitzungen unter Verwendung des sichersten Protokolls eingerichtet. Alle bestehenden iSCSI-Sitzungen wechseln während des Upgrades von MD5 auf SHA. Wenn Sie die Host-iSCSI-Initiator-Konfiguration nicht aktualisieren, um SHA anzufordern, werden die vorhandenen iSCSI-Sitzungen weiterhin MD5 verwenden. Nach der Aktualisierung der CHAP-Algorithmen des Host-iSCSI-Initiators sollten die iSCSI-Sitzungen auf der Grundlage von Wartungsaktivitäten schrittweise von MD5 auf SHA umstellen, was zu einer erneuten Verbindung der iSCSI-Sitzung führt.

Der Standard-Host-iSCSI-Initiator in Red hat Enterprise Linux (RHEL) 8.3 verfügt beispielsweise über die `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` Die Einstellung hat kommentiert, was zu einem iSCSI-Initiator nur mit MD5 führt. Wenn Sie diese Einstellung auf dem Host kommentieren und den iSCSI-Initiator neu starten, werden iSCSI-Sitzungen von diesem Host ausgelöst, um SHA3-256 zu verwenden.

Bei Bedarf können Sie das verwenden "ListISSessions" API-Methode zum Anzeigen der CHAP-Algorithmen, die für jede Sitzung verwendet werden.

Erstellen Sie ein Konto

Sie können ein Konto erstellen, um den Zugriff auf Volumes zu ermöglichen.

Jeder Kontoname im System muss eindeutig sein.

1. Wählen Sie **Management** > **Konten**.
2. Klicken Sie Auf **Konto Erstellen**.
3. Geben Sie einen **Benutzername** ein.
4. Geben Sie im Abschnitt **CHAP-Einstellungen** die folgenden Informationen ein:

   Lassen Sie die Felder für Anmeldeinformationen leer, um ein Kennwort automatisch zu generieren.

   - **Initiatorschlüssel** für CHAP-Knoten-Session-Authentifizierung.
   - **Target Secret** für CHAP-Knoten-Session-Authentifizierung.
5. Klicken Sie Auf **Konto Erstellen**.

Kontodetails anzeigen

Sie können Leistungsaktivitäten für einzelne Konten in einem grafischen Format anzeigen.

Die Diagramminformationen liefern I/O- und Durchsatzinformationen für das Konto. Die Aktivitätslevel der durchschnittlichen und Spitzenwerte werden in Schritten von 10 Sekunden angezeigt. Diese Statistiken enthalten Aktivitäten für alle Volumes, die dem Konto zugewiesen sind.

1. Wählen Sie **Management** > **Konten**.
2. Klicken Sie auf das Symbol Aktionen für ein Konto.
3. Klicken Sie Auf **Details Anzeigen**.

Hier sind einige Details:

- **Status**: Der Status des Kontos. Mögliche Werte:
  - Aktiv: Ein aktives Konto.
  - Gesperrt: Ein gesperrtes Konto.
  - Entfernt: Ein Konto, das gelöscht und gelöscht wurde.
- **Aktive Volumes**: Die Anzahl der aktiven Volumes, die dem Konto zugewiesen sind.
- **Komprimierung**: Die Komprimierungs-Effizienzbewertung für die dem Konto zugewiesenen Volumes.
- **Deduplizierung**: Die Deduplizierungs-Effizienzbewertung für die Volumes, die dem Account zugewiesen sind.
- **Thin Provisioning**: Die Thin Provisioning-Effizienzbewertung für die dem Konto zugewiesenen Volumes.
- **Gesamteffizienz**: Die Gesamteffizienz-Punktzahl für die dem Account zugewiesenen Volumes.

Bearbeiten Sie ein Konto

Sie können ein Konto bearbeiten, um den Status zu ändern, die CHAP-Schlüssel zu ändern oder den Kontonamen zu ändern.

Das Ändern von CHAP-Einstellungen in einem Konto oder das Entfernen von Initiatoren oder Volumes aus einer Zugriffsgruppe kann dazu führen, dass Initiatoren unerwartet den Zugriff auf Volumes verlieren. Um zu überprüfen, ob der Volume-Zugriff nicht unerwartet verloren geht, loggen Sie sich immer iSCSI-Sitzungen aus, die von einer Konto- oder Zugriffsgruppenänderung betroffen sind, und überprüfen Sie, ob die Initiatoren nach Abschluss der Änderungen an den Initiatoreinstellungen und den Cluster-Einstellungen eine Verbindung zu Volumes herstellen können.

> Persistente Volumes, die mit Managementservices verknüpft sind, werden einem neuen Konto zugewiesen, das während der Installation oder Aktualisierung erstellt wird. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie das zugehörige Konto nicht.

1. Wählen Sie **Management** > **Konten**.
2. Klicken Sie auf das Symbol Aktionen für ein Konto.
3. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
4. **Optional:** Bearbeiten Sie den **Benutzername**.
5. **Optional:** Klicken Sie auf die Dropdown-Liste **Status** und wählen Sie einen anderen Status aus.

   > Wenn Sie den Status auf **gesperrt** ändern, werden alle iSCSI-Verbindungen zum Konto beendet, und das Konto kann nicht mehr aufgerufen werden. Volumes, die mit dem Konto verbunden sind, werden gepflegt. Die Volumes können jedoch nicht über iSCSI erkannt werden.

6. **Optional:** Bearbeiten Sie unter **CHAP-Einstellungen** die Anmeldeinformationen **Initiator Secret** und **Target Secret** für die Knotensitzauthentifizierung.

   > Wenn Sie die **CHAP-Einstellungen**-Anmeldeinformationen nicht ändern, bleiben diese unverändert. Wenn Sie die Felder für die Anmeldeinformationen leer lassen, generiert das System neue Passwörter.

7. Klicken Sie Auf **Änderungen Speichern**.

Löschen Sie ein Konto

Sie können ein Konto löschen, wenn es nicht mehr benötigt wird.

Löschen und löschen Sie alle Volumes, die mit dem Konto verknüpft sind, bevor Sie das Konto löschen.

> Persistente Volumes, die mit Managementservices verknüpft sind, werden einem neuen Konto zugewiesen, das während der Installation oder Aktualisierung erstellt wird. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie das zugehörige Konto nicht.

1. Wählen Sie **Management** > **Konten**.
2. Klicken Sie auf das Aktionen-Symbol für das Konto, das Sie löschen möchten.
3. Wählen Sie im Menü Ergebnis die Option **Löschen** aus.
4. Bestätigen Sie die Aktion.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Verwalten von Benutzerkonten für Cluster-Administratoren

Sie können Cluster-Administratorkonten für ein SolidFire-Speichersystem verwalten, indem Sie Cluster-Administratorkonten erstellen, löschen und bearbeiten, das Kennwort für den Cluster-Administrator ändern und LDAP-Einstellungen konfigurieren, um den Systemzugriff für Benutzer zu verwalten.

Kontotypen für Storage-Cluster-Administratoren

In einem Storage-Cluster mit NetApp Element Software können zwei Arten von Administratorkonten vorhanden sein: Das primäre Cluster-Administratorkonto und ein Cluster-Administratorkonto.

- **Primary Cluster Administrator Account**

  Dieses Administratorkonto wird erstellt, wenn das Cluster erstellt wird. Dieses Konto ist das primäre administrative Konto mit der höchsten Zugriffsebene auf das Cluster. Dieses Konto ist analog zu einem Root-Benutzer in einem Linux-System. Sie können das Kennwort für dieses Administratorkonto ändern.

- **Cluster-Administratorkonto**

  Sie können einem Cluster-Administratorkonto einen begrenzten administrativen Zugriff gewähren, um bestimmte Aufgaben in einem Cluster auszuführen. Die jedem Cluster-Administratorkonto zugewiesenen Zugangsdaten werden zur Authentifizierung von API- und Element-UI-Anforderungen innerhalb des Storage-Systems verwendet.

> Ein lokales (nicht-LDAP)-Cluster-Administratorkonto ist erforderlich, um über die UI pro Node auf aktive Knoten in einem Cluster zuzugreifen. Kontoanmeldeinformationen sind für den Zugriff auf einen Node, der noch nicht Teil eines Clusters ist, nicht erforderlich.

Zeigen Sie Details zum Cluster-Administrator an

1. So erstellen Sie ein Cluster-weites (nicht-LDAP)-Cluster-Administratorkonto:
   a. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
2. Auf der Seite Cluster-Administratoren auf der Registerkarte Benutzer können Sie die folgenden Informationen anzeigen:

   - **ID**: Dem Cluster Administrator Konto zugewiesene sequentielle Nummer.
   - **Benutzername**: Der Name, der dem Cluster Administrator-Konto bei der Erstellung gegeben wurde.
   - **Zugriff**: Die dem Benutzerkonto zugewiesenen Benutzerberechtigungen. Mögliche Werte:
     - Lesen
     - Berichterstellung
     - Knoten
     - Laufwerke
     - Volumes
     - Konten
     - Clusteradministratoren
     - Verwalter
     - SupportAdmin

     Alle Berechtigungen sind für den Zugriffstyp des Administrators verfügbar.

     Über die API sind Zugriffstypen verfügbar, die in der Element UI nicht verfügbar sind.

+

   - **Typ**: Der Typ des Clusteradministrators. Mögliche Werte:
     - Cluster
     - Ldap
   - **Attributes**: Wenn das Cluster-Administratorkonto mit der Element API erstellt wurde, zeigt diese Spalte alle Name-Wert-Paare an, die mit dieser Methode festgelegt wurden.

     Sehen"NetApp Element Software-API-Referenz" .

Erstellen eines Cluster-Administratorkontos

Sie können neue Cluster-Administratorkonten mit Berechtigungen erstellen, um den Zugriff auf bestimmte Bereiche des Storage-Systems zu ermöglichen oder einzuschränken. Wenn Sie Berechtigungen für ein Cluster-Administratorkonto festlegen, gewährt das System schreibgeschützte Rechte für alle Berechtigungen, die Sie dem Cluster-Administrator nicht zuweisen.

Wenn Sie ein LDAP-Cluster-Administratorkonto erstellen möchten, stellen Sie sicher, dass LDAP auf dem Cluster konfiguriert ist, bevor Sie beginnen.

"Aktivieren Sie die LDAP-Authentifizierung über die Benutzeroberfläche von Element"

Sie können später Berechtigungen für Cluster-Administratorkonten für Berichterstellung, Nodes, Laufwerke,

Volumes, Konten, Und Cluster-Level-Zugriff. Wenn Sie eine Berechtigung aktivieren, weist das System Schreibzugriff für diese Ebene zu. Das System gewährt dem Administrator-Benutzer schreibgeschützten Zugriff für die Ebenen, die Sie nicht auswählen.

Sie können auch ein vom Systemadministrator erstelltes Cluster-Administratorkonto später entfernen. Sie können das primäre Cluster-Administratorkonto, das beim Erstellen des Clusters erstellt wurde, nicht entfernen.

1. So erstellen Sie ein Cluster-weites (nicht-LDAP)-Cluster-Administratorkonto:
   a. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
   b. Klicken Sie Auf **Cluster-Admin Erstellen**.
   c. Wählen Sie den Benutzertyp **Cluster** aus.
   d. Geben Sie einen Benutzernamen und ein Kennwort für das Konto ein und bestätigen Sie das Passwort.
   e. Wählen Sie Benutzerberechtigungen aus, die auf das Konto angewendet werden sollen.
   f. Aktivieren Sie das Kontrollkästchen, um der Endnutzer-Lizenzvereinbarung zuzustimmen.
   g. Klicken Sie Auf **Cluster-Admin Erstellen**.
2. So erstellen Sie ein Cluster-Administratorkonto im LDAP-Verzeichnis:
   a. Klicken Sie auf **Cluster** > **LDAP**.
   b. Stellen Sie sicher, dass die LDAP-Authentifizierung aktiviert ist.
   c. Klicken Sie auf **Benutzerauthentifizierung testen** und kopieren Sie den Distinguished Name, der für den Benutzer oder eine der Gruppen angezeigt wird, deren Mitglied der Benutzer ist, damit Sie ihn später einfügen können.
   d. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
   e. Klicken Sie Auf **Cluster-Admin Erstellen**.
   f. Wählen Sie den LDAP-Benutzertyp aus.
   g. Befolgen Sie im Feld Distinguished Name das Beispiel im Textfeld, um einen vollständigen Distinguished Name für den Benutzer oder die Gruppe einzugeben. Alternativ können Sie ihn aus dem Distinguished Name einfügen, den Sie früher kopiert haben.

      Wenn der Distinguished Name Teil einer Gruppe ist, hat jeder Benutzer, der Mitglied dieser Gruppe auf dem LDAP-Server ist, Berechtigungen für dieses Administratorkonto.

   Um LDAP Cluster Admin-Benutzer oder -Gruppen hinzuzufügen, lautet das allgemeine Format des Benutzernamens „`LDAP:<Full Distinguished Name>`“.

   a. Wählen Sie Benutzerberechtigungen aus, die auf das Konto angewendet werden sollen.
   b. Aktivieren Sie das Kontrollkästchen, um der Endnutzer-Lizenzvereinbarung zuzustimmen.
   c. Klicken Sie Auf **Cluster-Admin Erstellen**.

Berechtigungen für Cluster-Administratoren bearbeiten

Sie können die Berechtigungen für Cluster-Administratorkonten für Berichterstellung, Nodes, Laufwerke, Volumes, Konten, Und Cluster-Level-Zugriff. Wenn Sie eine Berechtigung aktivieren, weist das System Schreibzugriff für diese Ebene zu. Das System gewährt dem Administrator-Benutzer schreibgeschützten Zugriff für die Ebenen, die Sie nicht auswählen.

1. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
2. Klicken Sie auf das Symbol Aktionen für den Cluster-Administrator, den Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.
4. Wählen Sie Benutzerberechtigungen aus, die auf das Konto angewendet werden sollen.
5. Klicken Sie Auf **Änderungen Speichern**.

Ändern Sie Passwörter für Cluster-Administratorkonten

Mithilfe der Element-UI können Sie die Kennwörter für den Cluster-Administrator ändern.

1. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
2. Klicken Sie auf das Symbol Aktionen für den Cluster-Administrator, den Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.
4. Geben Sie im Feld Passwort ändern ein neues Passwort ein und bestätigen Sie es.
5. Klicken Sie Auf **Änderungen Speichern**.

Verwandte Informationen

- "Informieren Sie sich über die für Element APIs verfügbaren Zugriffstypen"
- "Aktivieren Sie die LDAP-Authentifizierung über die Benutzeroberfläche von Element"
- "Deaktivieren Sie LDAP"
- "NetApp Element Plug-in für vCenter Server"

LDAP verwalten

Sie können das Lightweight Directory Access Protocol (LDAP) einrichten, um eine sichere, Verzeichnisbasierte Anmeldefunktion für den SolidFire-Speicher zu ermöglichen. Sie können LDAP auf Clusterebene konfigurieren und LDAP-Benutzer und -Gruppen autorisieren.

Zum Verwalten von LDAP wird die LDAP-Authentifizierung auf einem SolidFire-Cluster unter Verwendung einer vorhandenen Microsoft Active Directory-Umgebung eingerichtet und die Konfiguration getestet.

Sie können IPv4- und IPv6-Adressen verwenden.

Die Aktivierung von LDAP umfasst die folgenden grundlegenden Schritte, die im Detail beschrieben werden:

1. * Vorkonfigurationsschritte für LDAP-Unterstützung durchführen*. Stellen Sie sicher, dass Sie über alle erforderlichen Details zur Konfiguration der LDAP-Authentifizierung verfügen.
2. **LDAP-Authentifizierung aktivieren**. Verwenden Sie entweder die Element-UI oder die Element-API.
3. **Validierung der LDAP-Konfiguration**. Überprüfen Sie optional, ob der Cluster mit den richtigen Werten konfiguriert ist, indem Sie die GetLdapConfiguration API-Methode ausführen oder die LCAP-Konfiguration über die Element-UI prüfen.
4. **Testen Sie die LDAP-Authentifizierung** (mit dem `readonly` Benutzer). Überprüfen Sie, ob die LDAP-Konfiguration korrekt ist, indem Sie die TestLdapAuthentication API-Methode oder die Element-UI ausführen. Verwenden Sie für diesen ersten Test den Benutzernamen “sAMAccountName” des `readonly` Benutzer: Dadurch wird überprüft, ob Ihr Cluster für die LDAP-Authentifizierung richtig konfiguriert ist, und

es wird auch überprüft, dass die `readonly` Anmeldedaten und Zugriff sind korrekt. Wenn dieser Schritt fehlschlägt, wiederholen Sie die Schritte 1 bis 3.

5. **Testen Sie die LDAP-Authentifizierung** (mit einem Benutzerkonto, das Sie hinzufügen möchten). Wiederholen Sie setp 4 mit einem Benutzerkonto, das Sie als Element Cluster-Administrator hinzufügen möchten. Kopieren Sie die `distinguished` Name (DN) oder der Benutzer (oder die Gruppe). Dieser DN wird in Schritt 6 verwendet.
6. **Fügen Sie den LDAP-Cluster-Admin** hinzu (kopieren Sie den DN aus dem Test-LDAP-Authentifizierungsschritt und fügen Sie ihn ein). Erstellen Sie mit der Element UI oder der AddLdapClusterAdmin API-Methode einen neuen Cluster-Admin-Benutzer mit der entsprechenden Zugriffsebene. Fügen Sie für den Benutzernamen den vollständigen DN ein, den Sie in Schritt 5 kopiert haben. Dadurch wird sichergestellt, dass der DN korrekt formatiert ist.
7. **Testen Sie den Cluster-Administratorzugriff**. Loggen Sie sich mit dem neu erstellten LDAP-Cluster-Admin-Benutzer beim Cluster ein. Wenn Sie eine LDAP-Gruppe hinzugefügt haben, können Sie sich als jeder Benutzer dieser Gruppe anmelden.

Führen Sie die Schritte zur Vorkonfiguration für die LDAP-Unterstützung durch

Bevor Sie die LDAP-Unterstützung in Element aktivieren, sollten Sie einen Windows Active Directory-Server einrichten und weitere Vorkonfigurationsaufgaben durchführen.

Schritte

1. Richten Sie einen Windows Active Directory-Server ein.
2. **Optional:** LDAPS-Support aktivieren.
3. Erstellen von Benutzern und Gruppen
4. Erstellen Sie ein schreibgeschütztes Dienstkonto (z. B. „`sfReadonly`“), das für das Durchsuchen des LDAP-Verzeichnisses verwendet werden soll.

Aktivieren Sie die LDAP-Authentifizierung über die Benutzeroberfläche von Element

Sie können die Integration des Speichersystems mit einem vorhandenen LDAP-Server konfigurieren. Dies ermöglicht LDAP-Administratoren ein zentrales Management des Speichersystemzugriffs für Benutzer.

Sie können LDAP entweder mit der Element-Benutzeroberfläche oder der Element-API konfigurieren. In diesem Verfahren wird beschrieben, wie LDAP über die Element-UI konfiguriert wird.

Dieses Beispiel zeigt, wie die LDAP-Authentifizierung auf SolidFire konfiguriert und verwendet wird `SearchAndBind` Als Authentifizierungstyp. Das Beispiel verwendet einen einzelnen Windows Server 2012 R2 Active Directory Server.

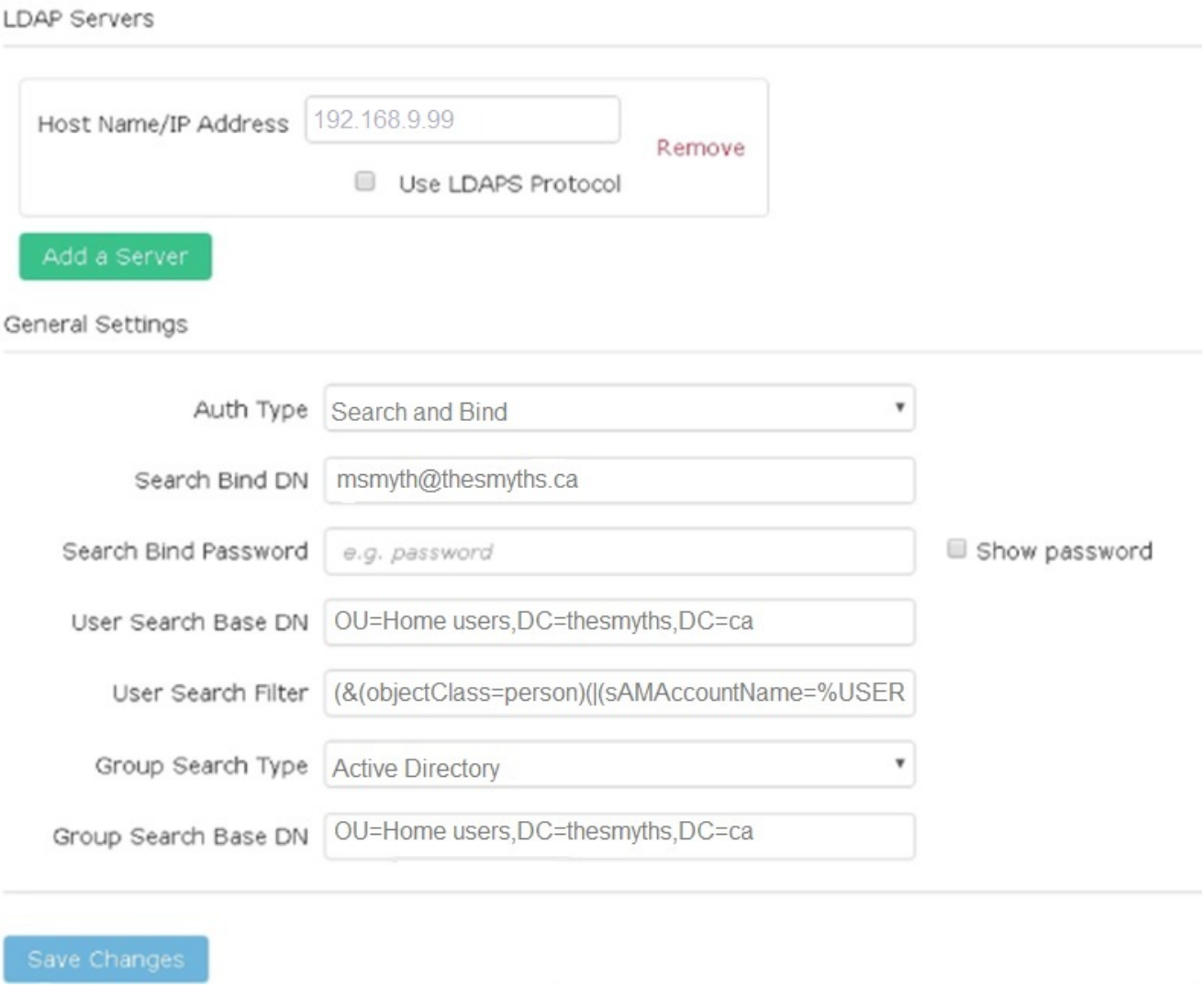
Schritte

1. Klicken Sie auf **Cluster** > **LDAP**.
2. Klicken Sie auf **Ja**, um die LDAP-Authentifizierung zu aktivieren.
3. Klicken Sie auf **Server hinzufügen**.
4. Geben Sie die * Hostname/IP-Adresse* ein.

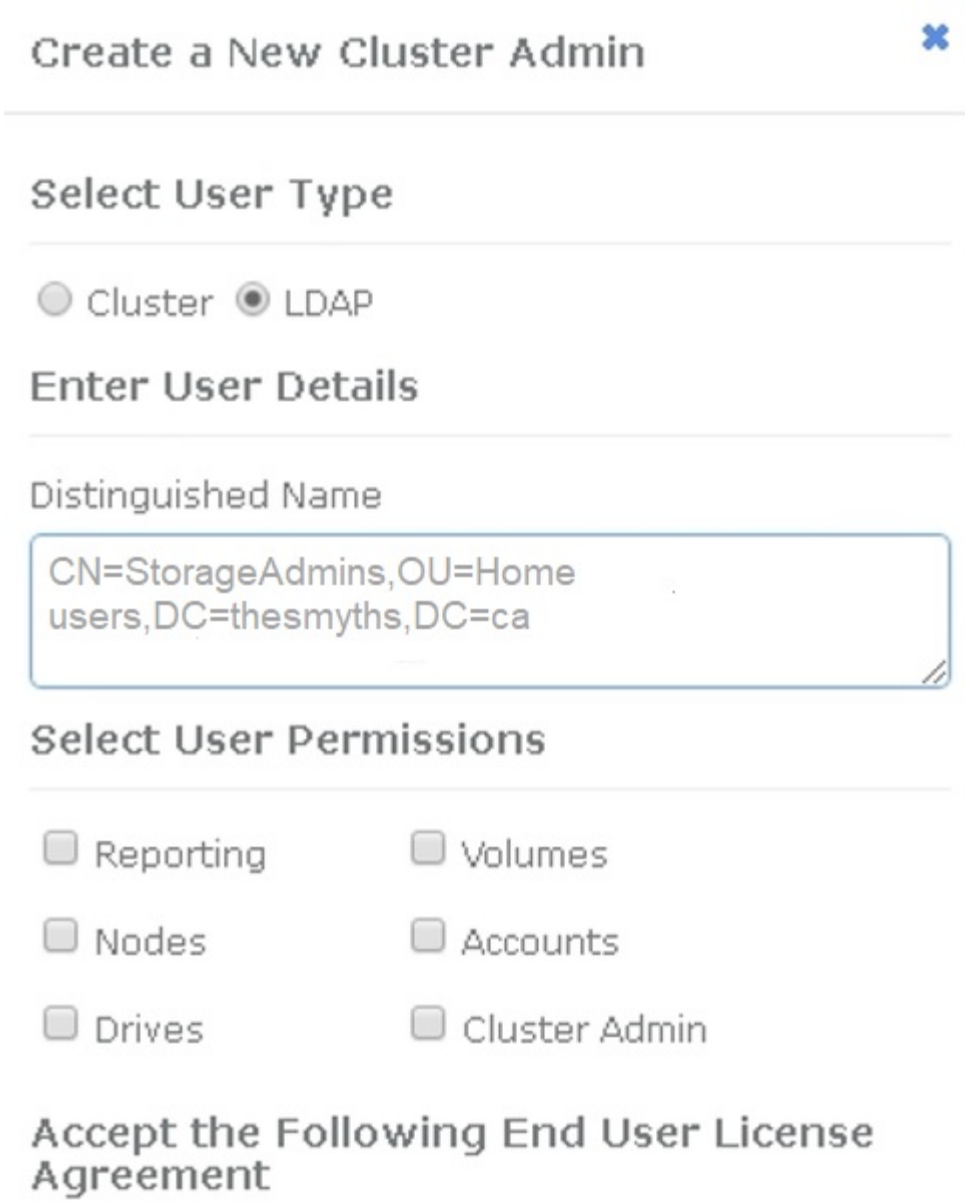
   Es kann auch eine optionale benutzerdefinierte Portnummer eingegeben werden.

   Wenn Sie beispielsweise eine benutzerdefinierte Portnummer hinzufügen möchten, geben Sie <Host Name oder ip-Adresse>:<Port number> ein

5. **Optional:** Wählen Sie **LDAPS-Protokoll verwenden**.
6. Geben Sie die erforderlichen Informationen unter **Allgemeine Einstellungen** ein.



7. Klicken Sie auf **LDAP aktivieren**.
8. Klicken Sie auf **Benutzerauthentifizierung testen**, wenn Sie den Serverzugriff für einen Benutzer testen möchten.
9. Kopieren Sie den Distinguished Name und Benutzergruppeninformationen, die später beim Erstellen von Cluster-Administratoren angezeigt werden.
10. Klicken Sie auf **Änderungen speichern**, um neue Einstellungen zu speichern.
11. Um einen Benutzer in dieser Gruppe zu erstellen, damit sich jeder anmelden kann, führen Sie Folgendes aus:
    a. Klicken Sie Auf **Benutzer** > **Ansicht**.



b. Klicken Sie für den neuen Benutzer auf **LDAP** für den Benutzertyp, und fügen Sie die Gruppe ein, die Sie in das Feld Distinguished Name kopiert haben.
c. Wählen Sie die Berechtigungen aus, normalerweise alle Berechtigungen.
d. Scrollen Sie nach unten zur Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Ich akzeptiere**.
e. Klicken Sie Auf **Cluster-Admin Erstellen**.

   Jetzt haben Sie einen Benutzer mit dem Wert einer Active Directory-Gruppe.

Um dies zu testen, melden Sie sich von der Element UI ab und melden Sie sich als Benutzer in dieser Gruppe an.

Aktivieren Sie die LDAP-Authentifizierung mit der Element API

Sie können die Integration des Speichersystems mit einem vorhandenen LDAP-Server konfigurieren. Dies ermöglicht LDAP-Administratoren ein zentrales Management des Speichersystemzugriffs für Benutzer.

Sie können LDAP entweder mit der Element-Benutzeroberfläche oder der Element-API konfigurieren. In

diesem Verfahren wird beschrieben, wie LDAP mithilfe der Element-API konfiguriert wird.

Um die LDAP-Authentifizierung auf einem SolidFire-Cluster zu nutzen, aktivieren Sie zuerst die LDAP-Authentifizierung auf dem Cluster mithilfe der `EnableLdapAuthentication` API-Methode.

Schritte

1. Aktivieren Sie die LDAP-Authentifizierung zuerst auf dem Cluster mithilfe des `EnableLdapAuthentication` API-Methode.
2. Geben Sie die erforderlichen Informationen ein.

```
{
     "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. Ändern Sie die Werte der folgenden Parameter:

Verwendete Parameter	Beschreibung
AuthType: SearchAndBind	Gibt an, dass der Cluster das Readonly-Dienstkonto verwendet, um zuerst nach dem authentifizierten Benutzer zu suchen und diesen Benutzer anschließend zu binden, wenn er gefunden und authentifiziert wurde.
GroupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Gibt den Speicherort in der LDAP-Struktur an, der mit der Suche nach Gruppen beginnt. In diesem Beispiel haben wir die Wurzel unseres Baumes verwendet. Wenn Ihr LDAP-Baum sehr groß ist, sollten Sie diesen auf eine granularere Unterstruktur setzen, um die Suchzeiten zu verkürzen.

Verwendete Parameter	Beschreibung
UserSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Gibt den Speicherort in der LDAP-Struktur an, der mit der Suche nach Benutzern beginnt. In diesem Beispiel haben wir die Wurzel unseres Baumes verwendet. Wenn Ihr LDAP-Baum sehr groß ist, sollten Sie diesen auf eine granularere Unterstruktur setzen, um die Suchzeiten zu verkürzen.
GroupSearchType: ActiveDirectory	Verwendet den Windows Active Directory-Server als LDAP-Server.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Um den userPrincipalName (E-Mail-Adresse für die Anmeldung) zu verwenden, können Sie den Suchfilter folgendermaßen ändern:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
Oder, um sowohl userPrincipalName als auch sAMAccountName zu suchen, können Sie den folgenden BenutzerSearchFilter verwenden:
 	
`"(&(objectClass=person)(`
	(SAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))“ ----

Nutzt den sAMAccountName als unseren Benutzernamen für die Anmeldung beim SolidFire-Cluster. Diese Einstellungen weisen LDAP darauf hin, nach dem bei der Anmeldung im sAMAccountName angegebenen Benutzernamen zu suchen und die Suche auch auf Einträge zu beschränken, die “Person” als Wert im objectClass-Attribut haben.	SuchhinBindDN
Dies ist der Distinguished Name of Readonly user, der für die Suche nach dem LDAP-Verzeichnis verwendet wird. Für Active Directory ist es in der Regel am einfachsten, den userPrincipalName (E-Mail-Adressformat) für den Benutzer zu verwenden.	SucheBindPasswort

Um dies zu testen, melden Sie sich von der Element UI ab und melden Sie sich als Benutzer in dieser Gruppe an.

LDAP-Details anzeigen

Zeigen Sie LDAP-Informationen auf der LDAP-Seite auf der Registerkarte Cluster an.

Sie müssen LDAP aktivieren, um diese LDAP-Konfigurationseinstellungen anzuzeigen.

1. Um LDAP-Details mit der Element UI anzuzeigen, klicken Sie auf **Cluster** > **LDAP**.
   - **Hostname/IP-Adresse**: Adresse eines LDAP- oder LDAPS-Verzeichnisservers.
   - **Auth Typ**: Die Benutzerauthentifizierungsmethode. Mögliche Werte:
     - Direct Bind
     - Suche Und Bindung
   - **Suche Bind DN**: Ein vollständig qualifizierter DN zur Anmeldung bei, um eine LDAP-Suche für den Benutzer durchzuführen (benötigt Bindeebene-Zugriff auf das LDAP-Verzeichnis).
   - **Suche Bind Password**: Passwort zur Authentifizierung des Zugriffs auf den LDAP-Server.
   - **Basis-DN der Benutzersuche**: Der Basis-DN des Baums, der zum Starten der Benutzersuche verwendet wird. Das System sucht die Unterstruktur vom angegebenen Speicherort aus.
   - **User Search Filter**: Geben Sie unter Verwendung Ihres Domainnamens Folgendes ein:

     ```
     (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
     ```

   - **Gruppenkuchsart**: Suchart, die den verwendeten Standardfilter für die Gruppensuche steuert. Mögliche Werte:
     - Active Directory: Verschachtelte Mitgliedschaft aller LDAP-Gruppen eines Benutzers.
     - Keine Gruppen: Keine Gruppenunterstützung.
     - Mitglied-DN: Gruppen im Mitgliedsstil (Einzelebene).
   - **Gruppensuche Basis-DN**: Der Basis-DN des Baumes, der zum Starten der Gruppensuche verwendet wird. Das System sucht die Unterstruktur vom angegebenen Speicherort aus.
   - **Benutzerauthentifizierung testen**: Nachdem LDAP konfiguriert ist, testen Sie den Benutzernamen und die Passwort-Authentifizierung für den LDAP-Server. Geben Sie ein Konto ein, das bereits vorhanden ist, um dies zu testen. Der Distinguished Name und Benutzergruppeninformationen werden angezeigt, die Sie beim Erstellen von Cluster-Administratoren kopieren können.

Testen Sie die LDAP-Konfiguration

Nach der Konfiguration von LDAP sollten Sie es entweder mit der Element-UI oder der Element-API testen `TestLdapAuthentication` Methode.

Schritte

1. So testen Sie die LDAP-Konfiguration mit der Element UI:
   a. Klicken Sie auf **Cluster** > **LDAP**.
   b. Klicken Sie auf **LDAP-Authentifizierung testen**.
   c. Lösen Sie Probleme, indem Sie die Informationen in der folgenden Tabelle verwenden:

Fehlermeldung	Beschreibung
`xLDAPUserNotFound`	• Der zu testenden Benutzer wurde im konfigurierten nicht gefunden `userSearchBaseDN` Unterbaum. • Der `userSearchFilter` Ist falsch konfiguriert.
`xLDAPBindFailed (Error: Invalid credentials)`	• Der getestete Benutzername ist ein gültiger LDAP-Benutzer, aber das angegebene Passwort ist falsch. • Der getestete Benutzername ist ein gültiger LDAP-Benutzer, das Konto ist jedoch derzeit deaktiviert.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	Der LDAP-Server-URI ist falsch.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	Der schreibgeschützte Benutzername oder das Kennwort ist falsch konfiguriert.
`xLDAPSearchFailed (Error: No such object)`	Der `userSearchBaseDN` Ist kein gültiger Speicherort innerhalb der LDAP-Struktur.
`xLDAPSearchFailed (Error: Referral)`	• Der `userSearchBaseDN` Ist kein gültiger Speicherort innerhalb der LDAP-Struktur. • Der `userSearchBaseDN` Und `groupSearchBaseDN` Befinden sich in einer geschachtelten Organisationseinheit. Dies kann zu Berechtigungsproblemen führen. Die Problemumgehung besteht darin, die Organisationseinheit in die Benutzer- und Gruppenbasis-DN-Einträge einzubeziehen (z. B.: `ou=storage, cn=company, cn=com`)

2. So testen Sie die LDAP-Konfiguration mit der Element API:
   a. Rufen Sie die TestLdapAuthentication-Methode auf.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

b. Überprüfen Sie die Ergebnisse. Wenn der API-Aufruf erfolgreich ist, enthalten die Ergebnisse den Distinguished Name des angegebenen Benutzers sowie eine Liste der Gruppen, in denen der Benutzer Mitglied ist.

```
{
"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"
     }
}
```

Deaktivieren Sie LDAP

Sie können die LDAP-Integration über die Element-UI deaktivieren.

Bevor Sie beginnen, sollten Sie alle Konfigurationseinstellungen beachten, da die Deaktivierung von LDAP alle Einstellungen löscht.

Schritte

1. Klicken Sie auf **Cluster** > **LDAP**.
2. Klicken Sie Auf **Nein**.
3. Klicken Sie auf **LDAP deaktivieren**.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Management des Systems

Management des Systems

Sie können Ihr System in der Element UI verwalten. Dies ermöglicht die Multi-Faktor-Authentifizierung, das Managen von Cluster-Einstellungen, unterstützt FIPS (Federal Information Processing Standards) und nutzt externes Verschlüsselungsmanagement.

- "Multi-Faktor-Authentifizierung aktivieren"
- "Konfigurieren Sie Cluster-Einstellungen"
- "Erstellen eines Clusters, das FIPS-Laufwerke unterstützt"
- "Erste Schritte mit externem Verschlüsselungsmanagement"

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Multi-Faktor-Authentifizierung aktivieren

Richten Sie die Multi-Faktor-Authentifizierung ein

Multi-Faktor-Authentifizierung (MFA) verwendet zum Verwalten von Benutzersitzungen einen Drittanbieter-Identitätsanbieter (IdP) über die Security Assertion Markup Language (SAML). MFA ermöglicht Administratoren, zusätzliche Authentifizierungsfaktoren wie Passwort und Textnachricht, Kennwort und E-Mail-Nachricht nach Bedarf zu konfigurieren.

Sie können diese grundlegenden Schritte über die Element API verwenden, um Ihr Cluster zur Multi-Faktor-Authentifizierung einzurichten.

Einzelheiten zu jeder API-Methode finden Sie in der "Element-API-Referenz"Die

1. Erstellen Sie eine neue IdP-Konfiguration (Identity Provider) eines Drittanbieters für das Cluster, indem Sie die folgende API-Methode aufrufen und die IdP-Metadaten im JSON-Format übergeben: `CreateIdpConfiguration`

   IDP-Metadaten werden im Klartextformat aus dem Drittanbieter-IdP abgerufen. Diese Metadaten müssen validiert werden, um sicherzustellen, dass sie korrekt in JSON formatiert sind. Es stehen zahlreiche JSON-Formatierer-Anwendungen zur Verfügung, die Sie verwenden können, z. B.:https://freeformatter.com/json-escape.html.

2. Abrufen der Cluster-Metadaten über sMetadataUrl, um Daten in die IdP eines Drittanbieters zu kopieren, indem Sie die folgende API-Methode aufrufen: `ListIdpConfigurations`

   SpMetadataUrl ist eine URL, mit der die Metadaten des Dienstanbieters für das IdP aus dem Cluster abgerufen werden, um eine Vertrauensbeziehung aufzubauen.

3. Konfigurieren Sie die SAML-Behauptungen auf dem IdP eines Drittanbieters so, dass das Attribut „ `NameID`“ verwendet wird, dass ein Benutzer für die Prüfprotokollierung eindeutig identifiziert wird und dass Single Logout ordnungsgemäß funktioniert.
4. Erstellen Sie ein oder mehrere Cluster-Administrator-Benutzerkonten, die von einem Drittanbieter-IdP zur

Autorisierung authentifiziert wurden, indem Sie die folgende API-Methode aufrufen:`AddIdpClusterAdmin`

> Der Benutzername für den IdP-Clusteradministrator muss mit dem SAML-Attribut Name/Wert-Mapping für den gewünschten Effekt übereinstimmen, wie in den folgenden Beispielen dargestellt:

- Email=bob@company.com — wobei das IdP so konfiguriert ist, dass es eine E-Mail-Adresse in den SAML-Attributen gibt.
- Group=Cluster-Administrator - wobei das IdP so konfiguriert ist, dass es eine Gruppeneigenschaft freigibt, in der alle Benutzer Zugriff haben sollen. Beachten Sie, dass die Paarung des SAML-Attributs Name/Wert zwischen Groß- und Kleinschreibung und Sicherheit beachtet wird.

5. MFA für das Cluster aktivieren, indem Sie die folgende API-Methode aufrufen: `EnableIdpAuthentication`

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Zusätzliche Informationen für Multi-Faktor-Authentifizierung

Beachten Sie die folgenden Einschränkungen bei der Multi-Faktor-Authentifizierung.

- Um nicht mehr gültige IdP-Zertifikate zu aktualisieren, müssen Sie einen nicht-IdP-Admin-Benutzer verwenden, um die folgende API-Methode aufrufen zu können: `UpdateIdpConfiguration`
- MFA ist nicht kompatibel mit Zertifikaten, die weniger als 2048 Bit lang sind. Standardmäßig wird auf dem Cluster ein 2048-Bit-SSL-Zertifikat erstellt. Sie sollten beim Aufruf der API-Methode vermeiden, ein kleineres Zertifikat einzurichten: `SetSSLCertificate`

> Wenn das Cluster ein Zertifikat verwendet, das vor dem Upgrade weniger als 2048-Bit enthält, muss das Cluster-Zertifikat nach dem Upgrade auf Element 12.0 oder höher mit einem Zertifikat von mindestens 2048 Bit aktualisiert werden.

- IDP Admin-Benutzer können nicht dazu verwendet werden, API-Aufrufe direkt (beispielsweise über SDKs oder Postman) zu tätigen oder andere Integrationen (z. B. OpenStack Cinder oder vCenter Plug-in) zu verwenden. Fügen Sie entweder LDAP-Cluster-Administratorbenutzer oder lokale Cluster-Admin-Benutzer hinzu, wenn Sie Benutzer mit diesen Fähigkeiten erstellen müssen.

Weitere Informationen

- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Konfigurieren Sie Cluster-Einstellungen

Aktivieren und deaktivieren Sie die Verschlüsselung für ein Cluster im Ruhezustand

Mit SolidFire Clustern können Sie alle auf Cluster-Laufwerken gespeicherten Daten im

Ruhezustand verschlüsseln. Sie können den Cluster-weiten Schutz von Self-Encrypting Drives (SED) mit beiden aktivieren "Hardware- oder softwarebasierte Verschlüsselung im Ruhezustand".

Die Hardware-Verschlüsselung im Ruhezustand wird über die Element UI oder API aktiviert. Die Aktivierung der Hardware-Verschlüsselung im Ruhezustand hat keine Auswirkungen auf die Performance und Effizienz des Clusters. Die Softwareverschlüsselung im Ruhezustand ist nur mit der Element API möglich.

Die hardwarebasierte Verschlüsselung für Daten im Ruhezustand ist bei der Cluster-Erstellung standardmäßig nicht aktiviert und kann von der Element UI aktiviert und deaktiviert werden.

> Bei SolidFire All-Flash-Storage-Clustern muss die Softwareverschlüsselung im Ruhezustand während der Cluster-Erstellung aktiviert sein und nach dem Erstellen des Clusters nicht deaktiviert werden können.

Was Sie benötigen

- Sie verfügen über Cluster-Administratorrechte zum Aktivieren oder Ändern von Verschlüsselungseinstellungen.
- Bei der hardwarebasierten Verschlüsselung im Ruhezustand haben Sie vor der Änderung von Verschlüsselungseinstellungen sichergestellt, dass sich das Cluster in einem ordnungsgemäßen Zustand befindet.
- Wenn Sie die Verschlüsselung deaktivieren, müssen zwei Knoten an einem Cluster teilnehmen, um auf den Schlüssel zuzugreifen, um die Verschlüsselung auf einem Laufwerk zu deaktivieren.

Überprüfen Sie den Status der Verschlüsselung im Ruhezustand

Mithilfe der können Sie den aktuellen Status der Verschlüsselung im Ruhezustand und/oder Softwareverschlüsselung im Ruhezustand auf dem Cluster anzeigen "GetClusterInfo" Methode. Sie können das verwenden "GetSoftwareVerschlüsselungAtRestInfo" Methode zum Abrufen von Informationen, die das Cluster verwendet, um Daten im Ruhezustand zu verschlüsseln.

> Das UI-Dashboard der Element Software unter `https://<MVIP>/` Derzeit wird für hardwarebasierte Verschlüsselung nur die Verschlüsselung im Ruhezustand angezeigt.

Optionen

- Hardwarebasierte Verschlüsselung für Daten im Ruhezustand
- Softwarebasierte Verschlüsselung im Ruhezustand aktivieren
- Deaktivieren Sie die hardwarebasierte Verschlüsselung für Daten im Ruhezustand

Hardwarebasierte Verschlüsselung für Daten im Ruhezustand

> Um die Verschlüsselung im Ruhezustand über eine externe Verschlüsselungsmanagementkonfiguration zu aktivieren, müssen Sie die Verschlüsselung im Ruhezustand über die aktivieren "API". Wenn Sie die Verwendung der Schaltfläche der vorhandenen Element-Benutzeroberfläche aktivieren, wird die Nutzung intern generierter Schlüssel wiederhergestellt.

1. Wählen Sie in der Element-UI die Option **Cluster** > **Einstellungen**.
2. Wählen Sie **Verschlüsselung im Ruhezustand aktivieren**.

Softwarebasierte Verschlüsselung im Ruhezustand aktivieren

Die Softwareverschlüsselung für Daten im Ruhezustand kann nicht deaktiviert werden, nachdem sie auf dem Cluster aktiviert ist.

1. Führen Sie während der Cluster-Erstellung den aus "Cluster-Methode erstellen" Mit `enableSoftwareEncryptionAtRest` Auf einstellen `true`.

Deaktivieren Sie die hardwarebasierte Verschlüsselung für Daten im Ruhezustand

1. Wählen Sie in der Element-UI die Option **Cluster** > **Einstellungen**.
2. Wählen Sie **Verschlüsselung im Ruhezustand deaktivieren**.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Legen Sie den Schwellenwert für den vollen Cluster fest

Sie können die Ebene ändern, auf der das System eine Warnung zur Blockclusterfülle generiert, indem Sie die folgenden Schritte durchführen. Darüber hinaus können Sie die ModifyClusterFullThreshold API-Methode verwenden, um den Level zu ändern, auf dem das System eine Block- oder Metadaten-Warnung erzeugt.

Was Sie benötigen

Sie müssen über Administratorrechte für den Cluster verfügen.

Schritte

1. Klicken Sie Auf **Cluster** > **Einstellungen**.
2. Geben Sie im Abschnitt „Cluster Full Settings“ einen Prozentsatz in **Warnung anheben ein, wenn die Kapazität von _ % verbleibt, bevor Helix nach einem Node-Ausfall nicht wieder herstellen konnte**.
3. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

"Wie werden die BlockSpace Schwellenwerte für Element berechnet"

Aktivieren und Deaktivieren des Volume Load Balancing

Ab Element 12.8 können Sie mithilfe von Volume Load Balancing Volumes auf Basis der tatsächlichen IOPS durch jedes Volume verteilen, anstatt der in der QoS-Richtlinie konfigurierten Mindestwerte. Sie können den Volume Load Balancing, der standardmäßig deaktiviert ist, mithilfe der Element UI oder API aktivieren und deaktivieren.

Schritte

1. Wählen Sie **Cluster** > **Einstellungen**.
2. Ändern Sie im Abschnitt Cluster Specific den Status für Volume Load Balancing:

Aktivieren Sie Volume Load Balancing

Wählen Sie **Enable Load Balancing on Actual IOPS**, und bestätigen Sie Ihre Auswahl.

Volume-Lastausgleich Deaktivieren:

Wählen Sie **Load Balancing für tatsächliche IOPS deaktivieren**, und bestätigen Sie Ihre Auswahl.

3. Wählen Sie optional **Reporting** > **Übersicht**, um die Statusänderung für Balance auf ist-IOPS zu bestätigen. Möglicherweise müssen Sie die Informationen zum Clusterzustand nach unten scrollen, um den Status anzuzeigen.

Weitere Informationen

- "Aktivieren Sie Volume Load Balancing mithilfe der API"
- "Deaktivieren Sie den Volume Load Balancing mithilfe der API"
- "Erstellung und Management von QoS-Richtlinien für Volumes"

Aktivieren und deaktivieren Sie den Zugriff auf den Support

Sie können den Support-Zugriff für die Fehlerbehebung vorübergehend für den Zugriff von NetApp Support-Mitarbeitern auf Storage Nodes über SSH aktivieren.

Um den Support-Zugriff zu ändern, müssen Sie über Berechtigungen für Cluster-Administratoren verfügen.

1. Klicken Sie Auf **Cluster** > **Einstellungen**.
2. Geben Sie im Abschnitt Support-Zugriff aktivieren/deaktivieren die Dauer (in Stunden) ein, die Sie dem Support Zugriff gewähren möchten.
3. Klicken Sie Auf **Support-Zugriff Aktivieren**.
4. **Optional:** um den Support-Zugriff zu deaktivieren, klicken Sie auf **Support-Zugriff deaktivieren**.

Banner für Nutzungsbedingungen verwalten

Sie können ein Banner aktivieren, bearbeiten oder konfigurieren, das eine Nachricht für den Benutzer enthält.

Optionen

Aktivieren Sie das Banner für Nutzungsbedingungen
Bearbeiten Sie den Banner für Nutzungsbedingungen
Deaktivieren Sie den Banner für die Nutzungsbedingungen

Aktivieren Sie das Banner für Nutzungsbedingungen

Sie können ein Banner für Nutzungsbedingungen aktivieren, das angezeigt wird, wenn sich ein Benutzer bei der Element-Benutzeroberfläche anmeldet. Wenn der Benutzer auf das Banner klickt, wird ein Textfeld mit der für den Cluster konfigurierten Meldung angezeigt. Das Banner kann jederzeit abgewiesen werden.

Sie müssen über Berechtigungen für Cluster-Administratoren verfügen, um die Nutzungsbestimmungen aktivieren zu können.

1. Klicken Sie auf **Benutzer** > **Nutzungsbedingungen**.

2. Geben Sie im Formular **Nutzungsbedingungen** den Text ein, der für das Dialogfeld Nutzungsbedingungen angezeigt werden soll.

   Überschreiten Sie maximal 4096 Zeichen.

3. Klicken Sie Auf **Aktivieren**.

Bearbeiten Sie den Banner für Nutzungsbedingungen

Sie können den Text bearbeiten, den ein Benutzer sieht, wenn er das Anmeldebanner „Nutzungsbedingungen“ ausgewählt hat.

Was Sie benötigen

- Um die Nutzungsbedingungen zu konfigurieren, müssen Sie über Berechtigungen für Cluster-Administratoren verfügen.
- Stellen Sie sicher, dass die Funktion „Nutzungsbedingungen“ aktiviert ist.

Schritte

1. Klicken Sie auf **Benutzer** > **Nutzungsbedingungen**.
2. Bearbeiten Sie im Dialogfeld **Nutzungsbedingungen** den Text, der angezeigt werden soll.

   Überschreiten Sie maximal 4096 Zeichen.

3. Klicken Sie Auf **Änderungen Speichern**.

Deaktivieren Sie den Banner für die Nutzungsbedingungen

Sie können den Banner „Nutzungsbedingungen“ deaktivieren. Bei deaktiviertem Banner wird der Benutzer nicht mehr aufgefordert, die Nutzungsbedingungen bei Verwendung der Element-UI zu akzeptieren.

Was Sie benötigen

- Um die Nutzungsbedingungen zu konfigurieren, müssen Sie über Berechtigungen für Cluster-Administratoren verfügen.
- Stellen Sie sicher, dass die Nutzungsbedingungen aktiviert sind.

Schritte

1. Klicken Sie auf **Benutzer** > **Nutzungsbedingungen**.
2. Klicken Sie Auf **Deaktivieren**.

Legen Sie das Network Time Protocol fest

Konfigurieren Sie die Network Time Protocol-Server für das abzufragenden Cluster

Sie können jeden Node in einem Cluster anweisen, einen NTP-Server (Network Time Protocol) nach Updates abzufragen. Das Cluster kontaktiert nur konfigurierte Server und fordert von ihnen NTP-Informationen an.

Mit NTP werden Uhren über ein Netzwerk synchronisiert. Die Verbindung zu einem internen oder externen NTP-Server sollte Teil der ersten Cluster-Einrichtung sein.

Konfigurieren Sie NTP auf dem Cluster, um auf einen lokalen NTP-Server zu verweisen. Sie können die IP-Adresse oder den FQDN-Hostnamen verwenden. Der NTP-Standardserver zum Erstellungszeitpunkt des Clusters ist auf us.pool.ntp.org eingestellt. Es kann jedoch nicht immer eine Verbindung zu diesem Standort hergestellt werden, abhängig vom physischen Standort des SolidFire Clusters.

Die Verwendung des FQDN hängt davon ab, ob die DNS-Einstellungen des einzelnen Speicherknoten vorhanden und betriebsbereit sind. Konfigurieren Sie dazu die DNS-Server auf jedem Speicherknoten und stellen Sie sicher, dass die Ports geöffnet sind, indem Sie die Seite Netzwerkport-Anforderungen überprüfen.

Sie können bis zu fünf verschiedene NTP-Server eingeben.

Sie können IPv4- und IPv6-Adressen verwenden.

Was Sie benötigen

Um diese Einstellung zu konfigurieren, müssen Sie über Berechtigungen für Cluster-Administratoren verfügen.

Schritte

1. Konfigurieren Sie eine Liste der IPs und/oder FQDNs in den Servereinstellungen.
2. Stellen Sie sicher, dass DNS auf den Knoten ordnungsgemäß eingestellt ist.
3. Klicken Sie Auf **Cluster** > **Einstellungen**.
4. Wählen Sie unter Network Time Protocol Settings **No** die standardmäßige NTP-Konfiguration.
5. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

- "Konfigurieren Sie das Cluster, um NTP-Broadcasts abzuhören"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Konfigurieren Sie das Cluster, um NTP-Broadcasts abzuhören

Mithilfe des Broadcast-Modus können Sie jeden Node in einem Cluster anweisen, um auf dem Netzwerk nach NTP (Network Time Protocol)-Broadcast-Meldungen von einem bestimmten Server abzuhören.

Mit NTP werden Uhren über ein Netzwerk synchronisiert. Die Verbindung zu einem internen oder externen NTP-Server sollte Teil der ersten Cluster-Einrichtung sein.

Was Sie benötigen

- Um diese Einstellung zu konfigurieren, müssen Sie über Berechtigungen für Cluster-Administratoren verfügen.
- Sie müssen einen NTP-Server im Netzwerk als Broadcast-Server konfigurieren.

Schritte

1. Klicken Sie Auf **Cluster** > **Einstellungen**.
2. Geben Sie den NTP-Server oder die Server, die den Broadcast-Modus in die Serverliste verwenden, ein.
3. Wählen Sie unter Network Time Protocol Settings **Ja** aus, um einen Broadcast-Client zu verwenden.
4. Um den Broadcast-Client einzustellen, geben Sie im Feld **Server** den NTP-Server ein, den Sie im

Broadcast-Modus konfiguriert haben.

5. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

- "Konfigurieren Sie die Network Time Protocol-Server für das abzufragenden Cluster"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

SNMP managen

Erfahren Sie mehr über SNMP

Sie können Simple Network Management Protocol (SNMP) in Ihrem Cluster konfigurieren.

Sie können einen SNMP-Anforderer auswählen, die zu verwendende SNMP-Version auswählen, den Benutzer des SNMP-Benutzerbasierten Sicherheitsmodells (USM) identifizieren und Traps zur Überwachung des SolidFire-Clusters konfigurieren. Sie können auch die Basisdateien des Managements für Informationen anzeigen und auf sie zugreifen.

Sie können IPv4- und IPv6-Adressen verwenden.

SNMP-Details

Auf der SNMP-Seite der Registerkarte Cluster können Sie die folgenden Informationen anzeigen:

- **SNMP MIBs**

  Die MIB-Dateien, die für Sie zum Anzeigen oder Herunterladen zur Verfügung stehen.

- **Allgemeine SNMP-Einstellungen**

  Sie können SNMP aktivieren oder deaktivieren. Nachdem Sie SNMP aktiviert haben, können Sie wählen, welche Version verwendet werden soll. Wenn Sie Version 2 verwenden, können Sie Anfragesteller hinzufügen, und wenn Sie Version 3 verwenden, können Sie USM-Benutzer einrichten.

- **SNMP-Trap-Einstellungen**

  Sie können ermitteln, welche Traps erfasst werden sollen. Sie können den Host, Port und die Community-Zeichenfolge für jeden Trap-Empfänger festlegen.

Konfigurieren eines SNMP-Anforderers

Wenn die SNMP-Version 2 aktiviert ist, können Sie einen Anforderer aktivieren oder deaktivieren und die Anfragesteller so konfigurieren, dass autorisierte SNMP-Anforderungen empfangen werden.

1. Klicken Sie auf Menü:Cluster[SNMP].
2. Klicken Sie unter **Allgemeine SNMP-Einstellungen** auf **Ja**, um SNMP zu aktivieren.

3. Wählen Sie aus der Liste **Version Version 2**.
4. Geben Sie im Abschnitt * Requitors* die Informationen **Community String** und **Network** ein.

> Standardmäßig ist die Community-Zeichenfolge öffentlich, und das Netzwerk ist localhost. Sie können diese Standardeinstellungen ändern.

5. **Optional:** um einen weiteren Anforderer hinzuzufügen, klicken Sie auf **Antragsteller hinzufügen** und geben die Informationen **Community String** und **Network** ein.
6. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

- Konfigurieren Sie SNMP-Traps
- Zeigen Sie verwaltete Objektdaten mithilfe von Management-Informationen-Basisdateien an

Konfigurieren eines SNMP-USM-Benutzers

Wenn Sie SNMP-Version 3 aktivieren, müssen Sie einen USM-Benutzer so konfigurieren, dass er autorisierte SNMP-Anforderungen erhält.

1. Klicken Sie auf **Cluster** > **SNMP**.
2. Klicken Sie unter **Allgemeine SNMP-Einstellungen** auf **Ja**, um SNMP zu aktivieren.
3. Wählen Sie aus der Liste **Version** die Option **Version 3** aus.
4. Geben Sie im Abschnitt **USM-Benutzer** den Namen, das Passwort und die Passphrase ein.
5. **Optional:** um einen anderen USM-Benutzer hinzuzufügen, klicken Sie auf **USM-Benutzer hinzufügen** und geben den Namen, das Passwort und die Passphrase ein.
6. Klicken Sie Auf **Änderungen Speichern**.

Konfigurieren Sie SNMP-Traps

Systemadministratoren können SNMP-Traps verwenden, die auch als Benachrichtigungen bezeichnet werden, um den Zustand des SolidFire Clusters zu überwachen.

Wenn SNMP-Traps aktiviert sind, generiert das SolidFire-Cluster Traps im Zusammenhang mit Ereignisprotokolleinträgen und Systemwarnungen. Um SNMP-Benachrichtigungen zu erhalten, müssen Sie die Traps auswählen, die erzeugt werden sollen, und die Empfänger der Trap-Informationen identifizieren. Standardmäßig werden keine Traps generiert.

1. Klicken Sie auf **Cluster** > **SNMP**.
2. Wählen Sie im Abschnitt **SNMP Trap Settings** einen oder mehrere Traps aus, die vom System generiert werden sollen:
   - Cluster-Fehler-Traps
   - Cluster-Gelöste Fehler-Traps
   - Cluster-Event-Köder
3. Geben Sie im Abschnitt **Trap-Empfänger** die Informationen zu Host, Port und Community-Zeichenfolge für einen Empfänger ein.

4. **Optional**: Um einen anderen Trap-Empfänger hinzuzufügen, klicken Sie auf **Trap-Empfänger hinzufügen** und geben Sie Host-, Port- und Community-String-Informationen ein.
5. Klicken Sie Auf **Änderungen Speichern**.

Zeigen Sie verwaltete Objektdaten mithilfe von Management-Informationen-Basisdateien an

Sie können die Management Information Base (MIB)-Dateien anzeigen und herunterladen, die zum Definieren der verwalteten Objekte verwendet werden. Die SNMP-Funktion unterstützt schreibgeschützten Zugriff auf die Objekte, die in der SolidFire-Storage-ecluster-MIB definiert sind.

Die statistischen Daten in der MIB zeigen die Systemaktivität für die folgenden:

- Cluster-Statistiken
- Volume-Statistiken
- Volumes nach Kontostatistiken
- Node-Statistiken
- Andere Daten wie Berichte, Fehler und Systemereignisse

Das System unterstützt auch den Zugriff auf die MIB-Datei, die die OIDS (OIDS) für SF-Series-Produkte enthält.

Schritte

1. Klicken Sie auf **Cluster** > **SNMP**.
2. Klicken Sie unter **SNMP MIBs** auf die MIB-Datei, die Sie herunterladen möchten.
3. Öffnen oder speichern Sie die MIB-Datei in dem sich daraus ergebenden Downloadfenster.

Verwalten Sie Laufwerke

Jeder Node enthält mindestens ein physisches Laufwerk, für das ein Teil der Daten für das Cluster gespeichert wird. Das Cluster verwendet die Kapazität und Performance des Laufwerks, nachdem das Laufwerk erfolgreich zu einem Cluster hinzugefügt wurde. Sie können die Element UI zum Managen von Laufwerken verwenden.

Laufwerke für Details

Auf der Seite Laufwerke auf der Registerkarte Cluster finden Sie eine Liste der aktiven Laufwerke im Cluster. Sie können die Seite filtern, indem Sie auf den Registerkarten „aktiv“, „verfügbar“, „Entfernen“, „Löschen“ und „Fehlgeschlagen“ auswählen.

Beim ersten Initialisieren eines Clusters ist die Liste der aktiven Laufwerke leer. Sie können Laufwerke hinzufügen, die einem Cluster nicht zugewiesen sind und auf der Registerkarte verfügbar aufgeführt sind, nachdem ein neues SolidFire Cluster erstellt wurde.

Die folgenden Elemente werden in der Liste der aktiven Laufwerke angezeigt.

- **Fahrausweis**

  Die dem Laufwerk zugewiesene sequenzielle Nummer.

- **Knoten-ID**

  Die Node-Nummer, die beim Hinzufügen des Node zum Cluster zugewiesen ist.

- **Knotenname**

  Der Name des Knotens, der das Laufwerk beherbergt.

- **Slot**

  Die Steckplatznummer, in der sich das Laufwerk befindet.

- * Kapazität*

  Die Größe des Laufwerks, in GB.

- **Seriell**

  Die Seriennummer des Laufwerks.

- **Tragen Sie Rest**

  Die Verschleißanzeige.

  Das Storage-System meldet den ungefähren Verschleiß der einzelnen Solid State Drives (SSDs) zum Schreiben und Löschen von Daten. Ein Laufwerk, das 5 Prozent seiner entworfenen Schreib- und Löschzyklen verbraucht hat, meldet 95 Prozent verbleibende Abnutzung. Die Informationen zum Laufwerksverschleiß werden vom System nicht automatisch aktualisiert. Sie können die Seite aktualisieren oder schließen und neu laden, um die Informationen zu aktualisieren.

- **Typ**

  Der Laufwerkstyp. Der Typ kann entweder Block- oder Metadaten sein.

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Managen von Nodes

Managen von Nodes

Sie können SolidFire Storage und Fibre Channel Nodes über die Seite Nodes auf der Registerkarte Cluster verwalten.

Wenn ein neu hinzugefügter Node mehr als 50 % der gesamten Cluster-Kapazität beträgt, wird einige der Kapazitäten dieses Node unbrauchbar („ungenutzt“) gemacht, sodass die Kapazitätsregel eingehalten wird. Dies bleibt der Fall, bis mehr Storage hinzugefügt wird. Wenn ein sehr großer Node hinzugefügt wird, der auch die Kapazitätsregel nicht befolgt, kann der zuvor isolierte Node nicht mehr ungenutzt bleiben, während der neu hinzugefügte Node ungenutzt ist. Um dies zu vermeiden, sollte immer paarweise Kapazität hinzugefügt werden. Wenn ein Node ungenutzt wird, ist ein geeigneter Cluster-Fehler zu werfen.

Weitere Informationen

Fügen Sie einem Cluster einen Node hinzu

Fügen Sie einem Cluster einen Node hinzu

Sie können einem Cluster Nodes hinzufügen, wenn mehr Storage benötigt wird oder nach der Cluster-Erstellung. Nodes müssen die Erstkonfiguration erfordern, wenn sie zum ersten Mal eingeschaltet sind. Nachdem der Node konfiguriert wurde, wird er in der Liste der ausstehenden Nodes angezeigt und Sie können ihn einem Cluster hinzufügen.

Die Softwareversion auf jedem Node in einem Cluster muss kompatibel sein. Wenn Sie einem Cluster einen Node hinzufügen, installiert das Cluster nach Bedarf die Cluster-Version der NetApp Element Software auf dem neuen Node.

Sie können einem vorhandenen Cluster Nodes mit kleineren oder größeren Kapazitäten hinzufügen. Sie können einem Cluster größere Node-Kapazitäten hinzufügen, um eine Kapazitätssteigerung zu ermöglichen. Größere Nodes, die zu einem Cluster mit kleineren Nodes hinzugefügt werden, müssen paarweise hinzugefügt werden. So kann Double Helix die Daten im Fall eines Ausfall eines der größeren Nodes ausreichend Speicherplatz verschieben. Einem größeren Node-Cluster können kleinere Node-Kapazitäten hinzugefügt werden, um die Performance zu verbessern.

> Wenn ein neu hinzugefügter Node mehr als 50 % der gesamten Cluster-Kapazität beträgt, wird einige der Kapazitäten dieses Node unbrauchbar („ungenutzt“) gemacht, sodass die Kapazitätsregel eingehalten wird. Dies bleibt der Fall, bis mehr Storage hinzugefügt wird. Wenn ein sehr großer Node hinzugefügt wird, der auch die Kapazitätsregel nicht befolgt, kann der zuvor isolierte Node nicht mehr ungenutzt bleiben, während der neu hinzugefügte Node ungenutzt ist. Um dies zu vermeiden, sollte immer paarweise Kapazität hinzugefügt werden. Wenn ein Node gestrandet wird, wird der stranddecacity-Cluster-Fehler geworfen.

"NetApp Video: Skalieren nach eigenen Regeln: Erweitern eines SolidFire-Clusters"

Sie können NetApp HCI Appliances Nodes hinzufügen.

Schritte

1. Wählen Sie **Cluster** > **Knoten**.
2. Klicken Sie auf **Ausstehend**, um die Liste der ausstehenden Knoten anzuzeigen.

   Wenn der Vorgang zum Hinzufügen von Nodes abgeschlossen ist, werden diese in der Liste der aktiven Nodes angezeigt. Bis dahin werden die ausstehenden Knoten in der Liste „Ausstehend aktiv“ angezeigt.

   SolidFire installiert die Element Softwareversion des Clusters auf den ausstehenden Nodes, wenn Sie sie einem Cluster hinzufügen. Dies kann einige Minuten dauern.

3. Führen Sie einen der folgenden Schritte aus:
   - Um einzelne Knoten hinzuzufügen, klicken Sie auf das Symbol **Aktionen** für den Knoten, den Sie hinzufügen möchten.
   - Um mehrere Knoten hinzuzufügen, aktivieren Sie das Kontrollkästchen der Knoten, die hinzugefügt werden sollen, und dann **Massenaktionen**. **Hinweis:** Wenn der Knoten, den Sie hinzufügen, eine andere Version der Element-Software hat als die Version, die auf dem Cluster ausgeführt wird, aktualisiert der Cluster den Knoten asynchron auf die Version der Element-Software, die auf dem Cluster-Master ausgeführt wird. Nach der Aktualisierung des Node wird er sich automatisch dem

Cluster hinzugefügt. Während dieses asynchronen Prozesses befindet sich der Knoten im hängenden Zustand aktiv.

4. Klicken Sie Auf **Hinzufügen**.

   Der Node wird in der Liste der aktiven Nodes angezeigt.

Weitere Informationen

Node-Versionierung und -Kompatibilität

Node-Versionierung und -Kompatibilität

Die Node-Kompatibilität basiert auf der auf einem Node installierten Version der Element Software. Bei Element Software-basierten Storage-Clustern wird automatisch ein Node zur Element Softwareversion im Cluster Image erstellt, wenn der Node und das Cluster nicht kompatible Versionen aufweisen.

In der folgenden Liste werden die Signifikanzstufen der Softwareversion, aus der die Versionsnummer der Element Software bestand, beschrieben:

- **Major**

  Die erste Zahl bezeichnet eine Software-Version. Ein Node mit einer Hauptkomponentennummer kann keinem Cluster mit Nodes einer anderen Major-Patch-Nummer hinzugefügt werden. Bei Nodes mit gemischten Hauptversionen kann kein Cluster erstellt werden.

- **Klein**

  Die zweite Zahl bezeichnet kleinere Software-Funktionen oder Verbesserungen an vorhandenen Softwarefunktionen, die zu einer größeren Version hinzugefügt wurden. Diese Komponente wird innerhalb einer Hauptversionskomponente erhöht, um anzugeben, dass diese inkrementelle Version nicht mit anderen inkrementellen Versionen von Element Software mit einer anderen kleineren Komponente kompatibel ist. Beispielsweise ist 11.0 nicht mit 11.1 kompatibel und 11.1 nicht mit 11.2 kompatibel.

- **Mikro**

  Die dritte Zahl bezeichnet einen kompatiblen Patch (inkrementelle Freigabe) für die Element-Softwareversion, die von den Hauptkomponenten dargestellt wird. Beispielsweise ist 11.0.1 kompatibel mit 11.0.2, und 11.0.2 ist kompatibel mit 11.0.3.

Major- und Minor-Versionsnummern müssen für Kompatibilität übereinstimmen. Micronummern müssen nicht übereinstimmen, um Kompatibilität zu gewährleisten.

Kapazität des Clusters in einer gemischten Node-Umgebung

Sie können verschiedene Node-Typen in einem Cluster kombinieren. SF-Series 2405, 3010, 4805, 6010, 9605 9010, 19210, 38410 und H-Series können gleichzeitig in einem Cluster eingesetzt werden.

Die H-Series besteht aus H610S-1, H610S-2, H610S-4 und H410S Nodes. Diese Nodes sind sowohl 10 GbE als auch 25 GbE fähig.

Am besten dürfen nicht verschlüsselte und verschlüsselte Nodes miteinander kombiniert werden. In einem Cluster mit gemischten Nodes kann kein Node mehr als 33 % der gesamten Cluster-Kapazität enthalten. Beispielsweise ist in einem Cluster mit vier SF-Series 4805 Nodes der größte Node, der allein hinzugefügt werden kann, eine SF-Series 9605. Der Cluster-Kapazitätsschwellenwert wird anhand des potenziellen Verlusts des größten Node in dieser Situation berechnet.

Je nach Element Softwareversion werden die folgenden SF-Series Storage-Nodes nicht unterstützt:

Beginnt mit…	Storage-Node nicht unterstützt…
Element 12.8	• SF4805 • SF9605 • SF19210 • SF38410
Element 12.7	• SF2405 • SF9608
Element 12.0	• SF3010 • SF6010 • SF9010

Wenn Sie versuchen, einen dieser Knoten auf eine nicht unterstützte Elementversion zu aktualisieren, wird eine Fehlermeldung angezeigt, die besagt, dass der Knoten nicht von Element 12.x unterstützt wird

Zeigen Sie Node-Details an

Sie können Details für einzelne Nodes wie Service-Tags, Laufwerkdetails und Grafiken für die Nutzung und Laufwerksstatistiken anzeigen. Die Seite Nodes der Registerkarte Cluster enthält die Spalte Version, in der Sie die Softwareversion jedes Node anzeigen können.

Schritte

1. Klicken Sie Auf **Cluster** > **Knoten**.
2. Um die Details für einen bestimmten Knoten anzuzeigen, klicken Sie auf das Symbol **Aktionen** für einen Knoten.
3. Klicken Sie Auf **Details Anzeigen**.
4. Überprüfen Sie die Node-Details:
   - **Knoten-ID**: Die vom System generierte ID für den Knoten.
   - **Knotenname**: Der Hostname des Knotens.
   - **Knotenrolle**: Die Rolle, die der Knoten im Cluster hat. Mögliche Werte:
     - Cluster Master: Der Knoten, der clusterweite administrative Aufgaben ausführt und MVIP und SVIP enthält.
     - Ensemble Node: Ein Knoten, der am Cluster teilnimmt. Je nach Clustergröße gibt es entweder 3 oder 5 Ensemble-Knoten.

        - Fibre Channel: Ein Node im Cluster.
    - **Node Typ**: Der Modelltyp des Knotens.
    - **Aktive Laufwerke**: Die Anzahl der aktiven Laufwerke im Knoten.
    - **Knotenauslastung**: Der Prozentsatz der Knotenauslastung basierend auf nodeHeat. Der angezeigte Wert ist recentPrimaryTotalHeat als Prozentsatz. Verfügbar ab Element 12.8.
    - **Management IP**: Die Management-IP-Adresse (MIP), die dem Knoten für 1GbE- oder 10GbE-Netzwerkadministratoraufgaben zugewiesen wurde.
    - **Cluster IP**: Die Cluster IP (CIP) Adresse, die dem Knoten zugewiesen wurde, der für die Kommunikation zwischen Knoten im selben Cluster verwendet wurde.
    - **Speicher-IP**: Die Speicher-IP (SIP)-Adresse, die dem Knoten zugewiesen ist, der für die iSCSI-Netzwerkerkennung und den gesamten Datenverkehr im Datennetz verwendet wird.
    - **Management VLAN ID**: Die virtuelle ID für das Management Local Area Network.
    - **Storage VLAN ID**: Die virtuelle ID für das Storage Local Area Network.
    - **Version**: Die Version der Software, die auf jedem Knoten ausgeführt wird.
    - **Replication Port**: Der Port, der auf Knoten für die Remote-Replikation verwendet wird.
    - **Service-Tag**: Die dem Knoten zugewiesene eindeutige Service-Tag-Nummer.
    - **Benutzerdefinierte Schutzdomäne**: Die benutzerdefinierte Schutzdomäne, die dem Knoten zugewiesen ist.

Zeigen Sie Details zu Fibre Channel-Ports an

Sie können Details zu Fibre Channel-Ports, z. B. deren Status, ihr Name und ihre Port-Adresse, auf der Seite FC-Ports anzeigen.

Zeigen Sie Informationen zu den Fibre Channel-Ports an, die mit dem Cluster verbunden sind.

Schritte

1. Klicken Sie auf **Cluster** > **FC-Ports**.
2. Um Informationen auf dieser Seite zu filtern, klicken Sie auf **Filter**.
3. Überprüfen Sie die Details:
    - **Knoten-ID**: Der Knoten, der die Sitzung für die Verbindung hostet.
    - **Knotenname**: Vom System generierter Knotenname.
    - **Steckplatz**: Steckplatznummer, wo sich der Fibre Channel-Port befindet.
    - **HBA-Port**: Physischer Port am Fibre Channel Host Bus Adapter (HBA).
    - **WWNN**: Der World Wide Node Name.
    - **WWPN**: Der weltweite Zielname des Ports.
    - **Switch WWN**: Der weltweite Name des Fibre Channel Switch.
    - **Port State**: Aktueller Zustand des Ports.
    - **NPort-ID**: Die Node-Port-ID auf der Fibre Channel Fabric.
    - **Geschwindigkeit**: Die ausgehandelte Fibre Channel-Geschwindigkeit. Folgende Werte sind möglich:
        - 4 Gbit/s

- 8 Gbit/s
- 16 Gbit/s

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Managen Sie virtuelle Netzwerke

Managen Sie virtuelle Netzwerke

Durch das virtuelle Netzwerk im SolidFire Storage kann der Datenverkehr zwischen mehreren Clients, die sich in separaten logischen Netzwerken befinden, mit einem Cluster verbunden werden. Die Verbindungen zum Cluster werden im Netzwerk-Stack durch VLAN-Tagging getrennt.

Weitere Informationen

- Fügen Sie ein virtuelles Netzwerk hinzu
- Aktivieren Sie virtuelles Routing und Forwarding
- Bearbeiten eines virtuellen Netzwerks
- VRF-VLANs bearbeiten
- Löschen Sie ein virtuelles Netzwerk

Fügen Sie ein virtuelles Netzwerk hinzu

Sie können einer Cluster-Konfiguration ein neues virtuelles Netzwerk hinzufügen, um eine mandantenfähige Umgebungsverbindung zu einem Cluster zu ermöglichen, auf dem Element Software ausgeführt wird.

Was Sie benötigen

- Identifizieren Sie den Block der IP-Adressen, der den virtuellen Netzwerken auf den Clusterknoten zugewiesen wird.
- Geben Sie eine SVIP-Adresse (Storage-Netzwerk-IP) an, die als Endpunkt für den gesamten NetApp Element-Datenverkehr verwendet werden soll.

Für diese Konfiguration müssen Sie die folgenden Kriterien berücksichtigen:

- Bei VLANs, die nicht VRF-aktiviert sind, müssen sich Initiatoren in demselben Subnetz wie das SVIP befinden.
- VLANs, die VRF-aktiviert sind, müssen sich keine Initiatoren in demselben Subnetz wie die SVIP befinden und Routing wird unterstützt.
- Der Standard-SVIP erfordert keine Initiatoren, die sich im selben Subnetz wie der SVIP befinden, und Routing wird unterstützt.

Wenn ein virtuelles Netzwerk hinzugefügt wird, wird für jeden Node eine Schnittstelle erstellt und jeder benötigt eine virtuelle Netzwerk-IP-Adresse. Die Anzahl der IP-Adressen, die Sie beim Erstellen eines neuen virtuellen

Netzwerks angeben, muss der Anzahl der Nodes im Cluster entsprechen oder größer sein. Virtuelle Netzwerkadressen werden von einzelnen Nodes automatisch bereitgestellt und ihnen zugewiesen. Sie müssen den Nodes im Cluster keine virtuellen Netzwerkadressen manuell zuweisen.

Schritte

1. Klicken Sie Auf **Cluster** > **Netzwerk**.
2. Klicken Sie auf **VLAN erstellen**.
3. Geben Sie im Dialogfeld **Neues VLAN** Werte in die folgenden Felder ein:
   - **VLAN-Name**
   - **VLAN-Tag**
   - **SVIP**
   - **Netzmaske**
   - (Optional) **Beschreibung**
4. Geben Sie die **Starting IP**-Adresse für den IP-Adressbereich in **IP-Adressblöcken** ein.
5. Geben Sie die **Größe** des IP-Bereichs als Anzahl der IP-Adressen ein, die in den Block einbezogen werden sollen.
6. Klicken Sie auf **Einen Block hinzufügen**, um einen nicht kontinuierlichen Block von IP-Adressen für dieses VLAN hinzuzufügen.
7. Klicken Sie auf **VLAN erstellen**.

Details zum virtuellen Netzwerk anzeigen

Schritte

1. Klicken Sie Auf **Cluster** > **Netzwerk**.
2. Überprüfen Sie die Details.
   - **ID**: Eindeutige ID des VLAN-Netzwerks, das vom System zugewiesen wird.
   - **Name**: Eindeutiger vom Benutzer zugewiesener Name für das VLAN-Netzwerk.
   - **VLAN Tag**: VLAN-Tag, der beim Erstellen des virtuellen Netzwerks zugewiesen wurde.
   - **SVIP**: Speicher virtuelle IP-Adresse, die dem virtuellen Netzwerk zugewiesen ist.
   - **Netzmaske**: Netzmaske für dieses virtuelle Netzwerk.
   - **Gateway**: Eindeutige IP-Adresse eines virtuellen Netzwerk-Gateways. VRF muss aktiviert sein.
   - **VRF aktiviert**: Angabe, ob virtuelles Routing und Forwarding aktiviert ist oder nicht.
   - **Verwendete IPs**: Der Bereich der virtuellen Netzwerk-IP-Adressen, die für das virtuelle Netzwerk verwendet werden.

Aktivieren Sie virtuelles Routing und Forwarding

Sie können virtuelles Routing und Forwarding (VRF) aktivieren, wodurch mehrere Instanzen einer Routing-Tabelle in einem Router existieren und gleichzeitig arbeiten können. Diese Funktion ist nur für Speichernetzwerke verfügbar.

Sie können VRF nur zum Zeitpunkt der Erstellung eines VLANs aktivieren. Wenn Sie wieder zu nicht-VRF wechseln möchten, müssen Sie das VLAN löschen und neu erstellen.

1. Klicken Sie Auf **Cluster** > **Netzwerk**.
2. Um VRF auf einem neuen VLAN zu aktivieren, wählen Sie **VLAN erstellen**.
   a. Geben Sie relevante Informationen für das neue VRF/VLAN ein. Siehe Hinzufügen eines virtuellen Netzwerks.
   b. Aktivieren Sie das Kontrollkästchen **VRF aktivieren**.
   c. **Optional**: Geben Sie ein Gateway ein.
3. Klicken Sie auf **VLAN erstellen**.

Weitere Informationen

Fügen Sie ein virtuelles Netzwerk hinzu

Bearbeiten eines virtuellen Netzwerks

Sie können VLAN-Attribute wie VLAN-Name, Netzmaske und Größe der IP-Adressblöcke ändern. VLAN-Tag und SVIP können nicht für ein VLAN geändert werden. Das Gateway-Attribut ist kein gültiger Parameter für nicht-VRF-VLANs.

Wenn iSCSI-, Remote-Replikation- oder andere Netzwerksitzungen vorhanden sind, kann die Änderung fehlschlagen.

Beim Verwalten der Größe von VLAN-IP-Adressbereichen sollten Sie die folgenden Einschränkungen beachten:

- Sie können IP-Adressen nur aus dem ursprünglichen IP-Adressbereich entfernen, der zum Zeitpunkt der Erstellung des VLANs zugewiesen wurde.
- Sie können einen IP-Adressblock entfernen, der nach dem ursprünglichen IP-Adressbereich hinzugefügt wurde, aber Sie können einen IP-Adressenblock nicht durch Entfernen von IP-Adressen ändern.
- Wenn Sie versuchen, IP-Adressen entweder aus dem anfänglichen IP-Adressbereich oder in einem IP-Block zu entfernen, die von Nodes im Cluster verwendet werden, kann der Vorgang fehlschlagen.
- Sie können bestimmte nicht verwendete IP-Adressen nicht anderen Nodes im Cluster neu zuweisen.

Sie können einen IP-Adressblock hinzufügen, indem Sie wie folgt vorgehen:

1. Wählen Sie **Cluster** > **Netzwerk**.
2. Wählen Sie das Aktionen-Symbol für das zu bearbeitende VLAN aus.
3. Wählen Sie **Bearbeiten**.
4. Geben Sie im Dialogfeld **VLAN bearbeiten** die neuen Attribute für das VLAN ein.
5. Wählen Sie **Einen Block hinzufügen** aus, um einen nicht kontinuierlichen Block mit IP-Adressen für das virtuelle Netzwerk hinzuzufügen.
6. Wählen Sie **Änderungen Speichern**.

Link zur Fehlerbehebung in KB-Artikeln

Link zu den Knowledge Base-Artikeln, um Hilfe bei der Fehlerbehebung bei der Verwaltung Ihrer VLAN-IP-Adressbereiche zu erhalten.

- "Doppelte IP-Warnung nach Hinzufügen eines Speicherknoten in VLAN zu Element Cluster"

- "So legen Sie fest, welche VLAN-IP-Adressen verwendet werden und welchen Knoten diese IP-Adressen in Element zugewiesen sind"

VRF-VLANs bearbeiten

Sie können VRF-VLAN-Attribute wie VLAN-Name, Netmask, Gateway und IP-Adressblöcke ändern.

1. Klicken Sie Auf **Cluster** > **Netzwerk**.
2. Klicken Sie auf das Aktionen-Symbol für das zu bearbeitende VLAN.
3. Klicken Sie Auf **Bearbeiten**.
4. Geben Sie im Dialogfeld **VLAN bearbeiten** die neuen Attribute für das VRF-VLAN ein.
5. Klicken Sie Auf **Änderungen Speichern**.

Löschen Sie ein virtuelles Netzwerk

Sie können ein virtuelles Netzwerkobjekt entfernen. Sie müssen die Adressblöcke einem anderen virtuellen Netzwerk hinzufügen, bevor Sie ein virtuelles Netzwerk entfernen.

1. Klicken Sie Auf **Cluster** > **Netzwerk**.
2. Klicken Sie auf das Symbol Aktionen für das zu löschende VLAN.
3. Klicken Sie Auf **Löschen**.
4. Bestätigen Sie die Meldung.

Weitere Informationen

Bearbeiten eines virtuellen Netzwerks

Erstellen eines Clusters, das FIPS-Laufwerke unterstützt

Elementcluster für FIPS-Laufwerke vorbereiten

Für die Implementierung von Lösungen in vielen Kundenumgebungen wird die Sicherheit immer wichtiger. Federal Information Processing Standards (FIPS) sind Standards für die Sicherheit und Interoperabilität von Computern. Die nach FIPS 140-2 zertifizierte Verschlüsselung für Daten im Ruhezustand ist Bestandteil der Gesamtlösung.

Damit die Funktion von FIPS-Laufwerken aktiviert werden kann, sollten Nodes, bei denen einige FIPS-Laufwerke unterstützen und andere nicht, nicht kombiniert werden.

Ein Cluster gilt als FIPS-Laufwerke, die den folgenden Bedingungen entsprechen:

- Alle Laufwerke sind als FIPS-Laufwerke zertifiziert.
- Alle Nodes sind FIPS-Laufwerke.
- Die Verschlüsselung für Daten im Ruhezustand (OHR) ist aktiviert.
- Die FIPS-Laufwerksfunktion ist aktiviert. Alle Laufwerke und Nodes müssen FIPS-fähig sein und die Verschlüsselung im Ruhezustand muss aktiviert sein, um die FIPS-Laufwerksfunktion zu aktivieren.

Verschlüsselung für Daten im Ruhezustand aktivieren

Die Cluster-weite Verschlüsselung im Ruhezustand wird aktiviert und deaktiviert. Diese Funktion ist standardmäßig nicht aktiviert. Zur Unterstützung von FIPS-Laufwerken müssen Sie die Verschlüsselung im Ruhezustand aktivieren.

1. Klicken Sie in der NetApp Element Software-Benutzeroberfläche auf **Cluster** > **Einstellungen**.
2. Klicken Sie auf **Verschlüsselung im Ruhezustand aktivieren**.

Weitere Informationen

- Aktivieren und Deaktivieren der Verschlüsselung für ein Cluster
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Ermitteln, ob Nodes für die FIPS-Laufwerksfunktion bereit sind

Sie sollten überprüfen, ob alle Nodes im Storage Cluster zur Unterstützung von FIPS-Laufwerken bereit sind. Hierzu verwenden Sie die NetApp Element Software GetFipsReport API-Methode.

Der resultierende Bericht zeigt einen der folgenden Status an:

- Keine: Node unterstützt nicht die FIPS-Laufwerksfunktion.
- Partiell: Node ist FIPS-fähig, nicht alle Laufwerke sind FIPS-Laufwerke.
- Bereit: Node ist FIPS-fähig. Alle Laufwerke sind FIPS-Laufwerke oder es sind keine Laufwerke vorhanden.

Schritte

1. Prüfen Sie mithilfe der Element API, ob die Nodes und Laufwerke im Storage-Cluster FIPS-Laufwerke unterstützen:

   ```
   GetFipsReport
   ```

2. Überprüfen Sie die Ergebnisse, und notieren Sie alle Knoten, die keinen Status von „bereit“ aufweisen.
3. Prüfen Sie bei Knoten, die keinen Status bereit hatten, ob das Laufwerk die FIPS-Laufwerksfunktion unterstützt:
   - Geben Sie mithilfe der Element API Folgendes ein: `GetHardwareList`
   - Notieren Sie sich den Wert des **DriveEncrypting CapabilityType**. Ist der FIPS-2, unterstützt die Hardware die FIPS-Laufwerksfunktion.

     Weitere Informationen finden Sie hier `GetFipsReport` oder `ListDriveHardware` im "Element-API-Referenz"Die
4. Wenn das Laufwerk die FIPS-Laufwerksfunktion nicht unterstützt, ersetzen Sie die Hardware durch FIPS-Hardware (entweder Node oder Laufwerke).

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"

- "NetApp Element Plug-in für vCenter Server"

Aktivierung der FIPS-Laufwerksfunktion

Die Funktion für FIPS-Laufwerke kann über die NetApp Element Software aktiviert werden `EnableFeature` API-Methode.

Die Verschlüsselung im Ruhezustand muss auf dem Cluster aktiviert sein und alle Nodes und Laufwerke müssen FIPS-fähig sein, wie angegeben, wenn der GetFipsReport den Status bereit für alle Nodes anzeigt.

Schritt

1. Aktivieren Sie mithilfe der Element API FIPS auf allen Laufwerken, indem Sie Folgendes eingeben:

   ```
   EnableFeature params: FipsDrives
   ```

Weitere Informationen

- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Prüfen Sie den FIPS-Laufwerksstatus

Sie können mithilfe der NetApp Element Software prüfen, ob die FIPS-Laufwerksfunktion auf dem Cluster aktiviert ist `GetFeatureStatus` API-Methode, die angibt, ob der Status „FIPS Drives enabled“ wahr oder „false“ ist.

1. Überprüfen Sie mithilfe der Element API die FIPS-Laufwerksfunktion auf dem Cluster, indem Sie Folgendes eingeben:

   ```
   GetFeatureStatus
   ```

2. Überprüfen Sie die Ergebnisse der `GetFeatureStatus` API-Aufruf. Wenn der Wert für aktivierte FIPS-Laufwerke den Wert hat, ist die Funktion für FIPS-Laufwerke aktiviert.

   ```
   {"enabled": true,
   "feature": "FipsDrives"
   }
   ```

Weitere Informationen

- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Fehlerbehebung für die FIPS-Laufwerksfunktion

Über die NetApp Element Software-UI lassen sich Benachrichtigungen über Clusterfehler oder Fehler im System anzeigen, die sich auf die FIPS-Laufwerksfunktion beziehen.

1. Wählen Sie über die Element-UI die Option **Reporting** > **Alerts** aus.
2. Suchen Sie nach Clusterfehlern, einschließlich:
   - Übereinstimmende FIPS-Laufwerke
   - FIPS führt zu Compliance-Verstößen
3. Vorschläge zur Problembehebung finden Sie unter Informationen zu Cluster-Fehlercodes.

Weitere Informationen

- Cluster-Fehlercodes
- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Sichere Kommunikation herstellen

Aktivieren Sie FIPS 140-2 für HTTPS auf dem Cluster

Sie können die API-Methode EnableFeature verwenden, um den FIPS 140-2-Betriebsmodus für HTTPS-Kommunikation zu aktivieren.

NetApp Element ermöglicht die Aktivierung des Betriebsmodus Federal Information Processing Standards (FIPS) 140-2 auf dem Cluster. Wenn Sie diesen Modus aktivieren, wird das NetApp Cryptographic Security Module (NCSM) aktiviert und für die gesamte Kommunikation über HTTPS mit der NetApp Element UI und API auf FIPS 140-2 Level 1 zertifizierte Verschlüsselung genutzt.

> Nach Aktivierung des FIPS 140-2-Modus kann dieser nicht deaktiviert werden. Wenn FIPS 140-2-Modus aktiviert ist, wird jeder Node im Cluster neu gebootet und läuft über einen Selbsttest, ob das NCSM korrekt aktiviert ist und im FIPS 140-2-zertifizierten Modus betrieben wird. Dies führt zu einer Unterbrechung der Management- und Storage-Verbindungen auf dem Cluster. Sie sollten diesen Modus sorgfältig planen und nur aktivieren, wenn Ihre Umgebung die von ihm angebotenen Verschlüsselungsmechanismen benötigt.

Weitere Informationen finden Sie unter Element API Informationen.

Dies ist ein Beispiel für die API-Anforderung zur Aktivierung von FIPS:

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "fips"
    },
    "id": 1
}
```

Nach Aktivierung dieses Betriebsmodus werden alle HTTPS-Kommunikationen mit den nach FIPS 140-2 genehmigten Chiffren verwendet.

Weitere Informationen

- SSL-Chiffren
- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

SSL-Chiffren

SSL-Chiffren sind Verschlüsselungsalgorithmen, die von Hosts zur Einrichtung einer sicheren Kommunikation verwendet werden. Es gibt Standardchiffren, die Element Software unterstützt und nicht-Standardchiffren, wenn der FIPS 140-2-Modus aktiviert ist.

Die folgenden Listen enthalten die von der Element-Software unterstützten Standard-SSL-Chiffren (Secure Socket Layer) und die SSL-Chiffren, die unterstützt werden, wenn der FIPS 140-2-Modus aktiviert ist:

- **FIPS 140-2 deaktiviert**

  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 aktiviert**

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

Weitere Informationen

Aktivieren Sie FIPS 140-2 für HTTPS auf dem Cluster

Erste Schritte mit externem Verschlüsselungsmanagement

Erste Schritte mit externem Verschlüsselungsmanagement

EKM (External Key Management) bietet eine sichere Verwaltung des Authentifizierungsschlüssels (AK) in Verbindung mit einem externen EKS-Server (Off-Cluster). Die AKS werden verwendet, um Self-Encrypting Drives (SEDs) zu sperren und zu entsperren "Verschlüsselung für Daten im Ruhezustand" Ist auf dem Cluster aktiviert. Der EKS sorgt für die sichere Erzeugung und Lagerung der AKS. Der Cluster verwendet für die Kommunikation mit dem EKS das Key Management Interoperability Protocol (KMIP), ein OASIS-definiertes Standardprotokoll.

- "Externe Verwaltung einrichten"
- "Verschlüsselung der Software beim Rest-Master-Schlüssel"
- "Wiederherstellen von nicht zugänglichen oder ungültigen Authentifizierungsschlüsseln"
- "Befehle für externes Verschlüsselungsmanagement-API"

Weitere Informationen

- "CreateCluster API, die zur Aktivierung der Softwareverschlüsselung im Ruhezustand verwendet werden kann"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Externes Verschlüsselungsmanagement einrichten

Sie können diese Schritte ausführen und die aufgeführten Element-API-Methoden verwenden, um Ihre externe Verschlüsselungsmanagementfunktion einzurichten.

Was Sie benötigen

- Wenn Sie externes Verschlüsselungsmanagement in Kombination mit Softwareverschlüsselung im Ruhezustand einrichten, ist die Softwareverschlüsselung im Ruhezustand aktiviert "CreateCluster erstellen" Methode auf einem neuen Cluster, das keine Volumes enthält.

Schritte

1. Bauen Sie eine Vertrauensbeziehung mit dem externen Key Server (EKS) auf.
   a. Erstellen Sie ein öffentliches/privates Schlüsselpaar für das Element Cluster, das zur Schaffung einer Vertrauensbeziehung mit dem Schlüsselserver verwendet wird, indem Sie die folgende API-Methode aufrufen: "CreatePublicPrivateKeyPair"
   b. Holen Sie sich die Zertifikatsign-Anforderung (CSR), die die Zertifizierungsstelle unterzeichnen muss.

Der CSR ermöglicht dem Schlüsselserver zu überprüfen, ob das Element-Cluster, das auf die Schlüssel zugreift, als Element-Cluster authentifiziert ist. Rufen Sie die folgende API-Methode auf: "GetClientCertificateSignRequest"

c. Verwenden Sie die EKS/Zertifizierungsstelle, um den abgerufenen CSR zu unterzeichnen. Weitere Informationen finden Sie in der Dokumentation von Drittanbietern.

2. Erstellen Sie auf dem Cluster einen Server und Provider, um mit dem EKS zu kommunizieren. Ein Schlüsselanbieter legt fest, wo ein Schlüssel abgerufen werden soll, und ein Server definiert die spezifischen Attribute der EKS, die mit kommuniziert werden.

   a. Erstellen Sie einen Schlüsselanbieter, bei dem die Schlüsselserverdetails gespeichert werden, indem Sie die folgende API-Methode aufrufen: "CreateKeyProviderKmip"

   b. Erstellen Sie einen Schlüsselserver mit dem signierten Zertifikat und dem öffentlichen Schlüsselzertifikat der Zertifizierungsstelle, indem Sie die folgenden API-Methoden aufrufen:
   "CreateKeyServerkmip"
   "TestKeyServerkmip"

   Wenn der Test fehlschlägt, überprüfen Sie die Serverkonnektivität und -Konfiguration. Wiederholen Sie dann den Test.

   c. Fügen Sie den Schlüsselserver in den Container des Schlüsselanbieters hinzu, indem Sie die folgenden API-Methoden aufrufen:"AddKeyServerToProviderKmip"
   "TestKeyProviderKmip"

   Wenn der Test fehlschlägt, überprüfen Sie die Serverkonnektivität und -Konfiguration. Wiederholen Sie dann den Test.

3. Führen Sie als nächsten Schritt für die Verschlüsselung im Ruhezustand einen der folgenden Schritte aus:

   a. (Für Hardware-Verschlüsselung im Ruhezustand) aktivieren "Hardware-Verschlüsselung für Daten im Ruhezustand" Durch Angabe der ID des Schlüsselanbieters, der den Schlüsselserver enthält, der zum Speichern der Schlüssel verwendet wird, indem der angerufen wird "EnableVerschlüsselungAtZiel" API-Methode.

   > Sie müssen die Verschlüsselung im Ruhezustand über das aktivieren "API". Die Aktivierung der Verschlüsselung im Ruhezustand mithilfe der vorhandenen Element UI-Schaltfläche bewirkt, dass die Funktion mithilfe intern generierter Schlüssel zurückgesetzt wird.

   b. (Für Softwareverschlüsselung im Ruhezustand) in der Reihenfolge "Softwareverschlüsselung für Daten im Ruhezustand" Um den neu erstellten Schlüsselanbieter nutzen zu können, geben Sie die Schlüssel-Provider-ID an den weiter "RekeySoftwareVerschlüsselungAtRestMasterKey" API-Methode.

Weitere Informationen

- "Aktivieren und Deaktivieren der Verschlüsselung für ein Cluster"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Verschlüsselung der Software beim Rest-Master-Schlüssel

Mit der Element-API können Sie einen vorhandenen Schlüssel neu Schlüssel rekeykey. Durch diesen Prozess wird ein neuer Master-Ersatzschlüssel für Ihren externen

Verschlüsselungsmanagement-Server erstellt. Master-Schlüssel werden immer durch neue Master-Schlüssel ersetzt und nie dupliziert oder überschrieben.

Unter Umständen müssen Sie die Daten im Rahmen eines der folgenden Verfahren erneut keywichtigen:

- Erstellen Sie einen neuen Schlüssel im Rahmen einer Änderung vom internen Verschlüsselungsmanagement bis zum externen Verschlüsselungsmanagement.
- Erstellen Sie einen neuen Schlüssel als Reaktion auf oder als Schutz gegen sicherheitsrelevante Ereignisse.

> Dieser Prozess ist asynchron und gibt eine Antwort zurück, bevor der Rekeyvorgang abgeschlossen ist. Sie können das verwenden "GetAsyncResult" Methode zum Abfragen des Systems, um zu sehen, wann der Prozess abgeschlossen ist.

Was Sie benötigen

- Mithilfe des haben Sie die Softwareverschlüsselung im Ruhezustand aktiviert "CreateCluster erstellen" Methode in einem neuen Cluster, das keine Volumes enthält und keinen I/O enthält Verwenden Sie den Link:./API/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] Um zu bestätigen, dass der Staat ist `enabled` Bevor Sie fortfahren.
- Das ist schon "Sie haben eine Vertrauensbeziehung aufgebaut" Zwischen dem SolidFire-Cluster und einem externen Schlüsselserver (EKS). Führen Sie die aus "TestKeyProviderKmip" Methode, um zu überprüfen, ob eine Verbindung zum Schlüsselanbieter hergestellt wurde.

Schritte

1. Führen Sie die aus "ListKeyProvidersKmip" Befehl und Kopie der Schlüssel-Provider-ID (`keyProviderID`).
2. Führen Sie die aus "RekeySoftwareVerschlüsselungAtRestMasterKey" Mit dem `keyManagementType` Parameter als `external` Und `keyProviderID` Als ID-Nummer des Schlüsselanbieters aus dem vorherigen Schritt:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

3. Kopieren Sie die `asyncHandle` Wert aus dem `RekeySoftwareEncryptionAtRestMasterKey` Befehlsantwort.
4. Führen Sie die aus "GetAsyncResult" Befehl mit dem `asyncHandle` Wert aus dem vorherigen Schritt, um die Änderung der Konfiguration zu bestätigen. In der Befehlsantwort sollten Sie sehen, dass die ältere Master Key-Konfiguration mit neuen Schlüsselinformationen aktualisiert wurde. Kopieren Sie die neue Schlüssel-Provider-ID zur Verwendung in einem späteren Schritt.

```
{
   "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. Führen Sie die aus `GetSoftwareEncryptionatRestInfo` Befehl, um zu bestätigen, dass neue wichtige Details, einschließlich `keyProviderID`, Wurden aktualisiert.

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

Weitere Informationen

- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Wiederherstellen von nicht zugänglichen oder ungültigen Authentifizierungsschlüsseln

Gelegentlich kann es zu einem Fehler kommen, der Benutzereingriff erfordert. Im Fehlerfall wird ein Cluster-Fehler (auch als Cluster-Fehlercode bezeichnet) generiert. Die beiden wahrscheinlichsten Fälle werden hier beschrieben.

Das Cluster kann die Laufwerke nicht entsperren, da ein KmipServerFault-Clusterfehler vorliegt.

Dies kann auftreten, wenn das Cluster zum ersten Mal gebootet wird und der Schlüsselserver nicht zugänglich ist oder der erforderliche Schlüssel nicht verfügbar ist.

1. Befolgen Sie ggf. die Wiederherstellungsschritte in den Cluster-Fehlercodes.

Es kann ein SliceServiceUnHealthy Fehler gesetzt werden, weil die Metadaten-Laufwerke als fehlgeschlagen markiert und in den Status „verfügbar“ gesetzt wurden.

Schritte zum Löschen:

1. Fügen Sie die Laufwerke erneut hinzu.
2. Prüfen Sie nach 3 bis 4 Minuten, dass der `sliceServiceUnhealthy` Fehler wurde behoben.

Siehe "Cluster-Fehlercodes" Finden Sie weitere Informationen.

Befehle für externes Verschlüsselungsmanagement-API

Liste aller zur Verwaltung und Konfiguration von EKM verfügbaren APIs.

Wird zum Aufbau einer Vertrauensbeziehung zwischen dem Cluster und externen Servern im Kundenbesitz verwendet:

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

Wird zur Definition der spezifischen Details externer kundeneigener Server verwendet:

- CreateKeyServerkmip
- ModifyKeyServerkmip
- DeleteKeyServerkmip
- GetKeyServerkmip
- ListKeyServersKmip
- TestKeyServerkmip

Wird zur Erstellung und Verwaltung von Schlüsselanbietern verwendet, die externe Schlüsselserver verwalten:

- CreateKeyProviderKmip

- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareVerschlüsselungAtRestMasterKey
- TestKeyProviderKmip

Informationen zu den API-Methoden finden Sie unter "API-Referenzinformationen"Die

Management von Volumes und virtuellen Volumes

Erfahren Sie mehr über die Verwaltung von Volumen und virtuellen Volumen.

Sie können die Daten in einem Cluster verwalten, auf dem die Element Software ausgeführt wird, auf der Registerkarte Management in der Element UI. Verfügbare Cluster-Managementfunktionen umfassen die Erstellung und das Management von Daten-Volumes, Volume-Zugriffsgruppen, Initiatoren und QoS-Richtlinien (Quality of Service).

Arbeiten mit Volumes

Das SolidFire System stellt mithilfe von Volumes Storage bereit. Volumes sind Blockgeräte, auf die über das Netzwerk von iSCSI- oder Fibre Channel-Clients zugegriffen wird. Auf der Seite Volumes auf der Registerkarte Management können Sie Volumes auf einem Node erstellen, bearbeiten, klonen und löschen. Es lassen sich außerdem Statistiken zur Volume-Bandbreite und zur I/O-Auslastung anzeigen.

"Lernen Sie, wie Sie mit Volumen arbeiten."

Arbeiten mit virtuellen Volumes

Über die Element UI lassen sich Informationen anzeigen und Aufgaben für virtuelle Volumes und deren zugehörigen Storage-Container, Protokollendpunkte, Bindungen und Hosts ausführen.

Das Storage-System der NetApp Element Software ist mit deaktivierter Virtual Volumes (VVols)-Funktion ausgestattet. Sie müssen eine einmalige Aufgabe ausführen, vSphere VVol Funktionen manuell über die Element UI zu aktivieren.

Nachdem Sie die VVol Funktionen aktiviert haben, wird eine Registerkarte VVols in der Benutzeroberfläche angezeigt, die VVols-bezogene Monitoring-Optionen und begrenzte Managementoptionen bietet. Zudem fungiert eine Storage-seitige Softwarekomponente, bekannt als VASA Provider, als Storage Awareness-Service für vSphere. Die meisten VVols Befehle, beispielsweise die Erstellung von VVols, das Klonen und die Bearbeitung, werden von einem vCenter Server oder ESXi Host initiiert und vom VASA Provider zu Element APIs für das Element Software Storage-System übersetzt. Über die Element UI lassen sich Befehle zum Erstellen, Löschen und Managen von Storage-Containern und zum Löschen virtueller Volumes ausführen.

In vSphere sind die meisten für die Nutzung der Virtual Volumes-Funktion mit Element Software-Storage-Systemen erforderlichen Konfigurationen vorhanden. Informationen zum Registrieren von VASA Provider in vCenter finden Sie im Konfigurationsleitfaden zu VMware vSphere Virtual Volumes für SolidFire Storage_, zum Erstellen und Managen von VVol Datastores und zum Management von Storage auf Basis von Richtlinien.

Registrieren Sie bei Element 12.5 und früheren Versionen nicht mehr als einen NetApp Element VASA Provider in einer einzelnen vCenter Instanz. Wenn ein zweiter NetApp Element VASA Provider hinzugefügt wird, macht das alle VVOL Datastores unzugänglich.

VASA-Unterstützung für mehrere vCenters steht als Upgrade-Patch zur Verfügung, wenn Sie bereits einen VASA Provider bei vCenter registriert haben. Laden Sie die VASA39 .tar.gz-Datei von der herunter, um sie zu installieren "NetApp Software-Downloads" Ort und folgen Sie den Anweisungen im Manifest. Der NetApp Element VASA Provider verwendet ein NetApp Zertifikat. Bei diesem Patch wird das Zertifikat von vCenter nicht verändert, um mehrere vCenters für die Verwendung von VASA und VVols zu unterstützen. Ändern Sie das Zertifikat nicht. Benutzerdefinierte SSL-Zertifikate werden von VASA nicht unterstützt.

"Erfahren Sie mehr über die Arbeit mit virtuellen Volumen."

Arbeiten Sie mit Volume-Zugriffsgruppen und -Initiatoren

ISCSI-Initiatoren oder Fibre Channel-Initiatoren können auf die in den Volume-Zugriffsgruppen definierten Volumes zugreifen.

Sie können Zugriffsgruppen erstellen, indem Sie iSCSI-Initiator-IQNs oder Fibre Channel-WWPNs in einer Sammlung von Volumes zuordnen. Jeder IQN, den Sie einer Zugriffsgruppe hinzufügen, kann auf jedes Volume in der Gruppe zugreifen, ohne dass eine CHAP-Authentifizierung erforderlich ist.

Es gibt zwei Arten von CHAP-Authentifizierungsmethoden:

- CHAP-Authentifizierung auf Kontoebene: Sie können CHAP-Authentifizierung für das Konto zuweisen.
- CHAP-Authentifizierung auf Initiatorebene: Sie können bestimmten Initiatoren eindeutige CHAP-Ziele und Schlüssel zuweisen, ohne an ein einziges CHAP-Konto gebunden zu sein. Diese CHAP-Authentifizierung auf Initiatorebene ersetzt Anmeldeinformationen auf Kontoebene.

Optional können Sie mit CHAP pro Initiator die Initiatorautorisierung und die CHAP-Authentifizierung per Initiator erzwingen. Diese Optionen können pro Initiator definiert werden, und eine Zugriffsgruppe kann eine Kombination von Initiatoren mit verschiedenen Optionen enthalten.

Jeder WWPN, den Sie einer Zugriffsgruppe hinzufügen, ermöglicht den Fibre-Channel-Netzwerkzugriff auf die Volumes in der Zugriffsgruppe.

Volume-Zugriffsgruppen verfügen über die folgenden Grenzen:

- In einer Zugriffsgruppe sind maximal 64 IQNs oder WWPNs zulässig.
- Eine Zugriffsgruppe kann aus maximal 2000 Volumes bestehen.
- Ein IQN oder WWPN kann nur zu einer Zugriffsgruppe gehören.
- Ein einzelnes Volume kann zu maximal vier Zugriffsgruppen gehören.

"Erfahren Sie mehr über die Arbeit mit Volumenzugriffsgruppen und Initiatoren."

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Arbeiten mit Volumes

Management von Quality-of-Service-Richtlinien

Eine QoS-Richtlinie (Quality of Service) ermöglicht das Erstellen und Speichern einer standardisierten Quality of Service-Einstellung, die auf viele Volumes angewendet werden kann. Sie können QoS-Richtlinien auf der Seite QoS-Richtlinien auf der Registerkarte Management erstellen, bearbeiten und löschen.

> Wenn Sie QoS-Richtlinien verwenden, verwenden Sie keine benutzerdefinierte QoS für ein Volume. Durch benutzerdefinierte QoS werden die QoS-Richtlinienwerte für Volume-QoS-Einstellungen überschrieben und angepasst.

"NetApp Video: SolidFire Quality of Service-Richtlinien"

Siehe "Leistung und Servicequalität".

- Erstellen einer QoS-Richtlinie
- Bearbeiten einer QoS-Richtlinie
- Löschen einer QoS-Richtlinie

Erstellen einer QoS-Richtlinie

Sie können QoS-Richtlinien erstellen und sie bei der Erstellung von Volumes anwenden.

1. Wählen Sie **Management** > **QoS-Richtlinien**.
2. Klicken Sie auf **QoS-Richtlinie erstellen**.
3. Geben Sie den **Policy Name** ein.
4. Geben Sie die**Min IOPS**-, **Max IOPS**- und **Burst IOPS**-Werte ein.
5. Klicken Sie auf **QoS-Richtlinie erstellen**.

Bearbeiten einer QoS-Richtlinie

Sie können den Namen einer vorhandenen QoS-Richtlinie ändern oder die mit der Richtlinie verknüpften Werte bearbeiten. Die Änderung einer QoS-Richtlinie wirkt sich auf alle Volumes aus, die mit der Richtlinie verknüpft sind.

1. Wählen Sie **Management** > **QoS-Richtlinien**.
2. Klicken Sie auf das Symbol Aktionen für die QoS-Richtlinie, die Sie bearbeiten möchten.
3. Wählen Sie im Menü Ergebnis die Option**Bearbeiten** aus.
4. Ändern Sie im Dialogfeld **QoS-Richtlinie bearbeiten** die folgenden Eigenschaften nach Bedarf:
   - Name Der Richtlinie
   - IOPS-Minimum
   - IOPS-Maximum
   - IOPS-Burst
5. Klicken Sie Auf **Änderungen Speichern**.

Löschen einer QoS-Richtlinie

Die QoS-Richtlinie kann gelöscht werden, wenn sie nicht mehr benötigt wird. Wenn Sie eine QoS-Richtlinie löschen, behalten alle mit der Richtlinie verknüpften Volumes die QoS-Einstellungen bei, werden aber einer Richtlinie nicht zugeordnet.

> Wenn Sie versuchen, die Zuordnung eines Volumes zu einer QoS-Richtlinie aufzuheben, können Sie die QoS-Einstellungen für dieses Volume individuell ändern.

1. Wählen Sie **Management** > **QoS-Richtlinien**.
2. Klicken Sie auf das Symbol Aktionen für die QoS-Richtlinie, die Sie löschen möchten.
3. Wählen Sie im Menü Ergebnis die Option **Löschen** aus.
4. Bestätigen Sie die Aktion.

Weitere Informationen

- "Entfernen Sie die QoS-Richtlinienzuordnung eines Volumes"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Volumes managen

Das SolidFire System stellt mithilfe von Volumes Storage bereit. Volumes sind Blockgeräte, auf die über das Netzwerk von iSCSI- oder Fibre Channel-Clients zugegriffen wird.

Auf der Seite Volumes auf der Registerkarte Management können Sie Volumes auf einem Node erstellen, bearbeiten, klonen und löschen.

Erstellen eines Volumes

Sie können ein Volume erstellen und das Volume einem bestimmten Konto zuordnen. Jedes Volume muss einem Konto zugeordnet sein. Mit dieser Zuordnung kann das Konto über die iSCSI-Initiatoren mit den CHAP-Anmeldeinformationen auf das Volume zugreifen.

Sie können die QoS-Einstellungen für ein Volume während der Erstellung festlegen.

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie Auf **Volume Erstellen**.
3. Geben Sie im Dialogfeld **Neues Volume erstellen** den **Volume-Namen** ein.
4. Geben Sie die Gesamtgröße des Volumes ein.

   > Die standardmäßige Auswahl der Volume-Größe ist in GB. Sie können Volumes mithilfe der Größe in GB oder gib erstellen:

   - 1 GB = 1 000 000 000 Bytes
   - 1 gib = 1 073 741 824 Byte
5. Wählen Sie für das Volume eine **Blockgröße** aus.

6. Klicken Sie auf die Dropdown-Liste **Konto** und wählen Sie das Konto aus, das Zugriff auf das Volume haben soll.

   Wenn kein Konto vorhanden ist, klicken Sie auf den Link **Konto erstellen**, geben Sie einen neuen Kontonamen ein und klicken Sie auf **Erstellen**. Der Account wird erstellt und dem neuen Volume zugeordnet.

   Wenn mehr als 50 Konten vorhanden sind, wird die Liste nicht angezeigt. Beginnen Sie mit der Eingabe, und die automatische Vervollständigung zeigt mögliche Werte an, die Sie auswählen können.

7. Um die * Quality of Service* einzustellen, führen Sie einen der folgenden Schritte aus:
   a. Unter **Richtlinie** können Sie eine vorhandene QoS-Richtlinie auswählen, sofern verfügbar.
   b. Legen Sie unter **Benutzerdefinierte Einstellungen** benutzerdefinierte Mindest-, Maximum- und Burst-Werte für IOPS fest oder verwenden Sie die Standard-QoS-Werte.

      Volumes mit einem IOPS-Wert von max oder Burst über 20,000 IOPS erfordern möglicherweise eine hohe Warteschlangentiefe oder mehrere Sitzungen, um diesen IOPS-Level auf einem einzelnen Volume zu erreichen.

8. Klicken Sie Auf **Volume Erstellen**.

Zeigen Sie Volume-Details an

1. Wählen Sie **Management** > **Volumes**.
2. Überprüfen Sie die Details.
   - **ID**: Die vom System generierte ID für das Volume.
   - **Name**: Der Name, der dem Volume bei seiner Erstellung gegeben wurde.
   - **Konto**: Der Name des Kontos, der dem Volume zugewiesen ist.
   - **Access Groups**: Der Name der Volume Access Group oder der Gruppen, zu denen das Volume gehört.
   - **Zugriff**: Die Art des Zugriffs, die dem Volume bei der Erstellung zugewiesen wurde. Mögliche Werte:
     - Lese-/Schreibzugriff: Alle Lese- und Schreibvorgänge werden akzeptiert.
     - Schreibgeschützt: Alle Leseaktivitäten sind zulässig; Schreibvorgänge sind nicht zulässig.
     - Gesperrt: Nur Administratorzugriff zulässig.
     - ReplicationTarget: Als Ziel-Volume in einem replizierten Volume-Paar festgelegt.
   - **Verwendet**: Der Prozentsatz des genutzten Speicherplatzes im Volumen.
   - **Größe**: Die Gesamtgröße (in GB) des Volumens.
   - **Primary Node ID**: Der primäre Knoten für dieses Volume.
   - **Sekundäre Knoten-ID**: Die Liste der sekundären Knoten für dieses Volumen. Kann mehrere Werte während vorübergehender Zustände sein, wie die Änderung von sekundären Knoten, hat aber in der Regel einen einzigen Wert.
   - **QoS Throttle**: Ermittelt, ob das Volume aufgrund der hohen Last am primären Speicherknoten gedrosselt wird.
   - **QoS-Richtlinie**: Name und Link zur benutzerdefinierten QoS-Richtlinie.

- **Minimum IOPS**: Die Mindestzahl an IOPS für das Volume garantiert.
- **Maximale IOPS**: Die maximale Anzahl von IOPS für das Volume zulässig.
- **Burst IOPS**: Die maximale Anzahl an IOPS über einen kurzen Zeitraum für das Volume zulässig. Standard = 15,000.
- **Snapshots**: Die Anzahl der Snapshots, die für den Datenträger erstellt wurden.
- **Attributes**: Attribute, die dem Volumen über eine API-Methode als Schlüssel/Wert-Paar zugewiesen wurden.
- **512e**: Gibt an, ob 512e auf einem Volumen aktiviert ist. Mögliche Werte:
  - Ja.
  - Nein
- **Erstellt am**: Das Datum und die Uhrzeit, zu der der Band erstellt wurde.

Details zu einzelnen Volumes anzeigen

Sie können Performance-Statistiken für einzelne Volumes anzeigen.

1. Wählen Sie **Reporting** > **Volume Performance**.
2. Klicken Sie in der Liste Volume auf das Aktionen-Symbol für ein Volume.
3. Klicken Sie Auf **Details Anzeigen**.

   Unten auf der Seite wird ein Fach mit allgemeinen Informationen zum Volume angezeigt.

4. Um weitere Informationen zum Volumen anzuzeigen, klicken Sie auf **Weitere Details**.

   Das System zeigt detaillierte Informationen sowie Performance-Diagramme für das Volume an.

Aktive Volumes bearbeiten

Volume-Attribute wie QoS-Werte, Volume-Größe und die Maßeinheit, in der Byte-Werte berechnet werden, können geändert werden. Außerdem haben Sie die Möglichkeit, den Kontozugriff für die Replizierungsnutzung zu ändern oder den Zugriff auf das Volume zu beschränken.

Sie können die Größe eines Volume ändern, wenn unter den folgenden Bedingungen genügend Speicherplatz auf dem Cluster vorhanden ist:

- Normale Betriebsbedingungen.
- Volume-Fehler oder -Ausfälle werden gemeldet.
- Das Volume ist zu klonen.
- Das Volume wird neu synchronisiert.

Schritte

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie im Fenster **Active** auf das Aktionen-Symbol für das zu bearbeitende Volumen.
3. Klicken Sie Auf **Bearbeiten**.
4. **Optional:** Ändern Sie die Gesamtgröße des Volumens.
   - Sie können die Volume-Größe vergrößern, aber nicht verkleinern. Sie können die Größe eines

Volumes nur in einem einzigen Größenänderungs-Vorgang anpassen. Speicherbereinigung und Software-Upgrades unterbrechen die Größenänderung nicht.

- Wenn Sie die Volume-Größe für die Replikation anpassen, sollten Sie zuerst die Größe des Volumes erhöhen, das als Replikationsziel zugewiesen wurde. Anschließend können Sie die Größe des Quellvolumens anpassen. Das Zielvolume kann größer oder gleich groß sein wie das Quellvolume, kann aber nicht kleiner sein.

  Die standardmäßige Auswahl der Volume-Größe ist in GB. Sie können Volumes mithilfe der Größe in GB oder gib erstellen:

- 1 GB = 1 000 000 000 Bytes
- 1 gib = 1 073 741 824 Byte

5. **Optional:** Wählen Sie eine andere Zugriffsebene für ein Konto aus einer der folgenden Optionen:
   - Schreibgeschützt
   - Lese-/Schreibzugriff
   - Gesperrt
   - Replizierungsziel
6. **Optional:** Wählen Sie das Konto aus, das Zugriff auf das Volumen haben soll.

   Wenn das Konto nicht vorhanden ist, klicken Sie auf den Link **Konto erstellen**, geben Sie einen neuen Kontonamen ein und klicken Sie auf **Erstellen**. Der Account wird erstellt und dem Volume zugeordnet.

   Wenn mehr als 50 Konten vorhanden sind, wird die Liste nicht angezeigt. Beginnen Sie mit der Eingabe, und die automatische Vervollständigung zeigt mögliche Werte an, die Sie auswählen können.

7. **Optional:** um die Auswahl in **Quality of Service** zu ändern, führen Sie einen der folgenden Schritte aus:
   a. Unter **Richtlinie** können Sie eine vorhandene QoS-Richtlinie auswählen, sofern verfügbar.
   b. Legen Sie unter **Benutzerdefinierte Einstellungen** benutzerdefinierte Mindest-, Maximum- und Burst-Werte für IOPS fest oder verwenden Sie die Standard-QoS-Werte.

   Wenn Sie QoS-Richtlinien für ein Volume verwenden, können Sie durch benutzerdefinierte QoS festlegen, dass die QoS-Richtlinie, die mit dem Volume verbunden ist, entfernt wird. Durch benutzerdefinierte QoS werden die QoS-Richtlinienwerte für Volume-QoS-Einstellungen überschrieben und angepasst.

   Wenn Sie IOPS-Werte ändern, sollten Sie sich Dutzende oder Hunderte erhöhen. Eingabewerte erfordern gültige ganze Zahlen.

   Konfigurieren Sie Volumes mit einem extrem hohen Burst-Wert. So kann das System gelegentlich sequenzielle Workloads mit großen Blöcken schneller verarbeiten und zugleich die anhaltenden IOPS für ein Volume einschränken.

8. Klicken Sie Auf **Änderungen Speichern**.

Löschen Sie ein Volume

Ein oder mehrere Volumes können aus einem Element Storage-Cluster gelöscht werden.

Das System löscht kein gelöschtes Volume sofort; das Volume bleibt etwa acht Stunden lang verfügbar. Wenn Sie ein Volume wiederherstellen, bevor das System es bereinigt, wird das Volume wieder online geschaltet und die iSCSI-Verbindungen werden wiederhergestellt.

Wenn ein Volume, das zum Erstellen eines Snapshots verwendet wird, gelöscht wird, werden die zugehörigen Snapshots inaktiv. Wenn die gelöschten Quell-Volumes gelöscht werden, werden auch die zugehörigen inaktiven Snapshots aus dem System entfernt.

Persistente Volumes, die mit Managementservices verbunden sind, werden bei der Installation oder bei einem Upgrade einem neuen Konto erstellt und zugewiesen. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie die Volumes oder ihr zugehörigem Konto nicht.

Schritte

1. Wählen Sie **Management** > **Volumes**.
2. So löschen Sie ein einzelnes Volume:
   a. Klicken Sie auf das Symbol Aktionen für das zu löschende Volume.
   b. Klicken Sie im Menü Ergebnis auf **Löschen**.
   c. Bestätigen Sie die Aktion.

   Das System verschiebt das Volumen in den Bereich **gelöscht** auf der Seite **Bände**.
3. So löschen Sie mehrere Volumes:
   a. Aktivieren Sie in der Liste der Volumes das Kontrollkästchen neben den Volumes, die Sie löschen möchten.
   b. Klicken Sie Auf **Massenaktionen**.
   c. Klicken Sie im Menü Ergebnis auf **Löschen**.
   d. Bestätigen Sie die Aktion.

   Das System verschiebt die Volumes in den Bereich **gelöscht** auf der Seite **Volumes**.

Wiederherstellen eines gelöschten Volumes

Sie können ein Volume im System wiederherstellen, wenn es gelöscht, aber noch nicht gelöscht wurde. Etwa acht Stunden nach dem Löschen löscht das System ein Volume automatisch. Wenn das System das Volume gelöscht hat, können Sie es nicht wiederherstellen.

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie auf die Registerkarte **gelöscht**, um die Liste der gelöschten Volumes anzuzeigen.
3. Klicken Sie auf das Symbol Aktionen für das Volume, das Sie wiederherstellen möchten.
4. Klicken Sie im Menü Ergebnis auf **Wiederherstellen**.
5. Bestätigen Sie die Aktion.

   Das Volume wird in der Liste **Active** Volumes platziert und iSCSI-Verbindungen zum Volume werden wiederhergestellt.

Löschen Sie ein Volumen

Wenn ein Volume gelöscht wird, wird es dauerhaft aus dem System entfernt. Alle Daten auf dem Volume gehen verloren.

Das System löscht gelöschte Volumes automatisch acht Stunden nach dem Löschen. Wenn Sie jedoch ein Volumen vor der geplanten Zeit löschen möchten, können Sie dies tun.

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie auf die Schaltfläche **gelöscht**.
3. Führen Sie die Schritte zum Löschen eines einzelnen Volumes oder mehrerer Volumes durch.

Option	Schritte
Löschen Sie ein einzelnes Volumen	a. Klicken Sie auf das Aktionen-Symbol für das zu löschung gewünschte Volumen. b. Klicken Sie Auf **Löschen**. c. Bestätigen Sie die Aktion.
Löschen mehrerer Volumes	a. Wählen Sie die Volumes aus, die Sie löschen möchten. b. Klicken Sie Auf **Massenaktionen**. c. Wählen Sie im Menü Ergebnis die Option **Löschen** aus. d. Bestätigen Sie die Aktion.

Klonen Sie ein Volume

Sie können einen Klon eines einzelnen Volumes oder mehrerer Volumes erstellen, um eine zeitpunktgenaue Kopie der Daten zu erstellen. Wenn Sie ein Volume klonen, erstellt das System einen Snapshot des Volume und erstellt dann eine Kopie der Daten, auf die der Snapshot verweist. Dies ist ein asynchroner Prozess und die erforderliche Zeit hängt von der Größe des zum Klonen benötigten Volumes und der aktuellen Cluster-Last ab.

Das Cluster unterstützt bis zu zwei aktuell laufende Klonanforderungen pro Volume und bis zu acht aktive Volume-Klonvorgänge gleichzeitig. Anforderungen, die über diese Grenzen hinausgehen, werden zur späteren Verarbeitung in die Warteschlange gestellt.

Betriebssysteme unterscheiden sich in der Behandlung geklonter Volumes. VMware ESXi behandelt ein geklontes Volume als Volume-Kopie oder als Snapshot Volume. Das Volume ist ein verfügbares Gerät zur Erstellung eines neuen Datastores. Weitere Informationen zum Mounten von Klon-Volumes und zum Handling von Snapshot-LUNs finden Sie in der VMware-Dokumentation auf "Mounten einer VMFS-Datastore-Kopie" Und "Managen doppelter VMFS-Datenspeicher".

Bevor Sie ein geklontes Volume auf eine geringere Größe klonen, müssen Sie die Partitionen so vorbereiten, dass sie sich in das kleinere Volume integrieren.

Schritte

1. Wählen Sie **Management** > **Volumes**.

2. Um ein einzelnes Volume zu klonen, führen Sie folgende Schritte aus:
   a. Klicken Sie in der Liste der Volumes auf der Seite **Active** auf das Aktionen-Symbol für das zu klonenden Volume.
   b. Klicken Sie im Menü Ergebnis auf **Klonen**.
   c. Geben Sie im Fenster **Clone Volume** einen Volume-Namen für das neu geklonte Volume ein.
   d. Wählen Sie eine Größe und Messung für das Volumen aus, indem Sie die Spinbox **Volume Size** und die Liste verwenden.

      Die standardmäßige Auswahl der Volume-Größe ist in GB. Sie können Volumes mithilfe der Größe in GB oder gib erstellen:

      - 1 GB = 1 000 000 000 Bytes
      - 1 gib = 1 073 741 824 Byte

   e. Wählen Sie den Zugriffstyp für das neu geklonte Volume aus.
   f. Wählen Sie aus der Liste **Konto** ein Konto aus, das dem neu geklonten Volume zugeordnet werden soll.

      Sie können in diesem Schritt ein Konto erstellen, wenn Sie auf den Link **Konto erstellen** klicken, einen Kontonamen eingeben und auf **Erstellen** klicken. Das System fügt das Konto nach dem Erstellen automatisch der **Konto**-Liste hinzu.

3. So klonen Sie mehrere Volumes:
   a. Aktivieren Sie in der Liste der Volumes auf der Seite **Active** das Kontrollkästchen neben beliebigen Volumes, die Sie klonen möchten.
   b. Klicken Sie Auf **Massenaktionen**.
   c. Wählen Sie im Menü Ergebnis die Option **Klonen** aus.
   d. Geben Sie im Dialogfeld **mehrere Volumes klonen** ein Präfix für die geklonten Volumes im Feld **New Volume Name Prefix** ein.
   e. Wählen Sie aus der Liste **Konto** ein Konto aus, das mit den geklonten Volumes verknüpft werden soll.
   f. Wählen Sie den Zugriffstyp für die geklonten Volumes aus.
4. Klicken Sie Auf **Klonen Starten**.

   Wenn Sie die Volume-Größe eines Klons erhöhen, führt dies zu einem neuen Volume mit zusätzlichem freien Speicherplatz am Ende des Volumes. Je nachdem, wie Sie das Volume nutzen, müssen Sie unter Umständen Partitionen erweitern oder neue Partitionen im freien Speicherplatz erstellen, um es nutzen zu können.

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Weisen Sie LUNs Fibre Channel Volumes zu

Sie können die LUN-Zuweisung für ein Fibre Channel-Volume in einer Volume-

Zugriffsgruppe ändern. Sie können auch Fibre Channel-Volume-LUN-Zuweisungen erstellen, wenn Sie eine Volume-Zugriffsgruppe erstellen.

Das Zuweisen neuer Fibre Channel-LUNs ist eine erweiterte Funktion und kann unbekannte Auswirkungen auf den verbundenen Host haben. Beispielsweise wird die neue LUN-ID möglicherweise nicht automatisch auf dem Host erkannt, und der Host benötigt möglicherweise einen erneuten Scan, um die neue LUN-ID zu ermitteln.

1. Wählen Sie **Management** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol Aktionen für die Zugriffsgruppe, die Sie bearbeiten möchten.
3. Wählen Sie im Menü Ergebnis die Option**Bearbeiten** aus.
4. Klicken Sie unter **LUN-IDs zuweisen** im Dialogfeld **Volume-Zugriffsgruppe bearbeiten** auf den Pfeil in der Liste **LUN-Zuweisungen**.
5. Geben Sie für jedes Volume in der Liste, dem Sie eine LUN zuweisen möchten, einen neuen Wert in das entsprechende Feld **LUN** ein.
6. Klicken Sie Auf **Änderungen Speichern**.

Wenden Sie eine QoS-Richtlinie auf Volumes an

Sie können Massen eine vorhandene QoS-Richtlinie auf ein oder mehrere Volumes anwenden.

Die QoS-Richtlinie, die Sie als Massenware anwenden möchten, muss vorhanden sein.

1. Wählen Sie **Management** > **Volumes**.
2. Aktivieren Sie in der Liste der Volumes das Kontrollkästchen neben allen Volumes, auf die Sie die QoS-Richtlinie anwenden möchten.
3. Klicken Sie Auf **Massenaktionen**.
4. Klicken Sie im Menü Ergebnis auf **QoS Policy anwenden**.
5. Wählen Sie die QoS-Richtlinie aus der Dropdown-Liste aus.
6. Klicken Sie Auf **Anwenden**.

Weitere Informationen

Quality of Service-Richtlinien

Entfernen Sie die QoS-Richtlinienzuordnung eines Volumes

Sie können eine QoS-Richtlinienzuordnung aus einem Volume entfernen, indem Sie benutzerdefinierte QoS-Einstellungen auswählen.

Das Volume, das Sie ändern möchten, sollte einer QoS-Richtlinie zugewiesen werden.

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie auf das Symbol Aktionen für ein Volume, das eine QoS-Richtlinie enthält, die Sie ändern möchten.
3. Klicken Sie Auf **Bearbeiten**.

4. Klicken Sie im Ergebnismenü unter **Quality of Service** auf **Benutzerdefinierte Einstellungen**.
5. Ändern Sie **Min IOPS**, **Max IOPS** und **Burst IOPS** oder behalten Sie die Standardeinstellungen bei.
6. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

Löschen einer QoS-Richtlinie

Arbeiten mit virtuellen Volumes

Aktivierung virtueller Volumes

Sie müssen die Funktion von vSphere Virtual Volumes (VVols) manuell über die NetApp Element Software aktivieren. Im Element Software-System ist die VVols-Funktion standardmäßig deaktiviert und wird nicht automatisch im Rahmen einer neuen Installation oder eines neuen Upgrades aktiviert. Die Aktivierung der VVols-Funktion ist eine einmalige Konfigurationsaufgabe.

Was Sie benötigen

- Der Cluster muss Element 9.0 oder höher ausführen.
- Der Cluster muss mit einer ESXi 6.0 Umgebung oder höher verbunden sein, die mit VVols kompatibel ist.
- Wenn Sie Element 11.3 oder höher verwenden, muss der Cluster mit einer ESXi 6.0 Update 3 oder höher Umgebung verbunden sein.

> Durch die Aktivierung der Funktion von vSphere Virtual Volumes wird die Konfiguration der Element Software dauerhaft geändert. Die VVols Funktionalität sollten nur aktiviert werden, wenn das Cluster mit einer mit VMware ESXi VVols kompatiblen Umgebung verbunden ist. Sie können die VVols-Funktion deaktivieren und nur die Standardeinstellungen wiederherstellen, indem Sie das Cluster wieder zum Werkseinstellungen zurücksetzen, d. h. alle Daten im System werden gelöscht.

Schritte

1. Wählen Sie **Cluster** > **Einstellungen**.
2. Ermitteln Sie Cluster-spezifische Einstellungen für Virtual Volumes.
3. Klicken Sie Auf **Virtuelle Volumes Aktivieren**.
4. Klicken Sie auf **Ja**, um die Änderung der Konfiguration der virtuellen Volumes zu bestätigen.

   Die Registerkarte **VVols** wird in der Element-UI angezeigt.

   > Wenn die VVols Funktion aktiviert ist, startet das SolidFire Cluster den VASA Provider, öffnet Port 8444 für den VASA Traffic und erstellt Protokollendpunkte, die von vCenter und allen ESXi Hosts erkannt werden können.

5. Kopieren Sie die VASA Provider-URL aus den Virtual Volumes (VVols) Einstellungen unter **Cluster** > **Einstellungen**. Sie verwenden diese URL, um den VASA Provider in vCenter zu registrieren.
6. Erstellen Sie einen Speicher-Container in **VVols** > **Storage Container**.

Sie müssen mindestens einen Storage-Container erstellen, damit VMs in einem VVol Datastore bereitgestellt werden können.

7. Wählen Sie **VVols** > **Protokollendpunkte** aus.
8. Vergewissern Sie sich, dass für jeden Node im Cluster ein Protokollendpunkt erstellt wurde.

Weitere Konfigurationsaufgaben sind in vSphere erforderlich. Informationen zum Registrieren von VASA Provider in vCenter finden Sie im Konfigurationsleitfaden zu VMware vSphere Virtual Volumes für SolidFire Storage_, zum Erstellen und Managen von VVol Datastores und zum Management von Storage auf Basis von Richtlinien.

Weitere Informationen

"Konfigurationsleitfaden für VMware vSphere Virtual Volumes für SolidFire Storage"

Details zu virtuellen Volumes anzeigen

Sie können Informationen zu virtuellen Volumes für alle aktiven virtuellen Volumes auf dem Cluster in der Element UI prüfen. Sie können außerdem Performance-Aktivitäten für jedes virtuelle Volume anzeigen, einschließlich Eingaben, Ausgaben, Durchsatz, Latenz, Warteschlangentiefe und Volume-Informationen

Was Sie benötigen

- Die VVols Funktion sollte in der Element UI für den Cluster aktiviert sein.
- Sie sollten einen zugeordneten Speicher-Container erstellt haben.
- Sie sollten vSphere Cluster entsprechend der VVols Funktion der Element Software konfigurieren.
- Sie sollten mindestens eine VM in vSphere erstellt haben.

Schritte

1. Klicken Sie auf **VVols** > **Virtual Volumes**.

   Die Informationen für alle aktiven virtuellen Volumes werden angezeigt.

2. Klicken Sie auf das Symbol **Aktionen** für das virtuelle Volume, das Sie überprüfen möchten.
3. Wählen Sie im Menü Ergebnis die Option **Details anzeigen**.

Details

Die Seite Virtual Volumes auf der Registerkarte VVols bietet Informationen zu jedem aktiven virtuellen Volume des Clusters, z. B. Volume-ID, Snapshot ID, ID des übergeordneten virtuellen Volumes und die ID des virtuellen Volumes.

- **Volumen-ID**: Die ID des zugrunde liegenden Volumens.
- **Snapshot ID**: Die ID des zugrunde liegenden Volumen-Snapshots. Der Wert ist 0, wenn das virtuelle Volume keinen SolidFire-Snapshot darstellt.
- **Parent Virtual Volume ID**: Die virtuelle Volume-ID des übergeordneten virtuellen Volume. Wenn die ID null ist, ist das virtuelle Volume unabhängig und es besteht keine Verknüpfung zu einem übergeordneten Volume.

- **Virtual Volume ID**: Die UUID des virtuellen Volumes.
- **Name**: Der Name, der dem virtuellen Volume zugewiesen ist.
- **Storage Container**: Der Speicher-Container, der das virtuelle Volume besitzt.
- **Gast-OS-Typ**: Betriebssystem, das mit dem virtuellen Volume verknüpft ist.
- **Virtual Volume Typ**: Der virtuelle Volume-Typ: Konfiguration, Daten, Speicher, Swap, oder andere.
- **Zugriff**: Die Lese-Schreib-Berechtigungen, die dem virtuellen Volume zugewiesen sind.
- **Größe**: Die Größe des virtuellen Volumes in GB oder gib.
- **Snapshots**: Die Anzahl der damit verbundenen Snapshots. Klicken Sie auf die Nummer, um die Snapshot-Details zu verknüpfen.
- **Minimum IOPS**: Die minimale IOPS QoS Einstellung des virtuellen Volumes.
- **Maximale IOPS**: Die maximale IOPS-QoS-Einstellung des virtuellen Volumes.
- **Burst IOPS**: Die maximale Burst-QoS-Einstellung des virtuellen Volumes.
- **VMW_VmID**: Informationen in Feldern, die mit "VMW_" vorstehen, werden von VMware definiert.
- **Erstellungszeit**: Die Zeit, die die Erstellung des virtuellen Volumes abgeschlossen wurde.

Details für einzelne virtuelle Volumes

Die Seite Virtual Volumes auf der Registerkarte VVols bietet folgende Informationen zu virtuellen Volumes, wenn Sie ein einzelnes virtuelles Volume auswählen und dessen Details anzeigen.

- **VMW_XXX**: Informationen in Feldern, die mit "VMW_" konfrontiert sind, werden von VMware definiert.
- **Parent Virtual Volume ID**: Die virtuelle Volume-ID des übergeordneten virtuellen Volume. Wenn die ID null ist, ist das virtuelle Volume unabhängig und es besteht keine Verknüpfung zu einem übergeordneten Volume.
- **Virtual Volume ID**: Die UUID des virtuellen Volumes.
- **Virtual Volume Typ**: Der virtuelle Volume-Typ: Konfiguration, Daten, Speicher, Swap, oder andere.
- **Volumen-ID**: Die ID des zugrunde liegenden Volumens.
- **Zugriff**: Die Lese-Schreib-Berechtigungen, die dem virtuellen Volume zugewiesen sind.
- **Kontoname**: Name des Kontos, das den Datenträger enthält.
- **Zugriffsgruppen**: Zugeordnete Volume-Zugriffsgruppen.
- **Gesamtvolumen Größe**: Insgesamt bereitgestellte Kapazität in Bytes.
- **Non-Zero Blocks**: Gesamtzahl von 4KiB Blöcken mit Daten nach Abschluss des letzten Garbage Collection Vorgangs.
- **Zero Blocks**: Gesamtzahl der 4KiB-Blöcke ohne Daten nach Abschluss der letzten Runde der Müllentnahme.
- **Snapshots**: Die Anzahl der damit verbundenen Snapshots. Klicken Sie auf die Nummer, um die Snapshot-Details zu verknüpfen.
- **Minimum IOPS**: Die minimale IOPS QoS Einstellung des virtuellen Volumes.
- **Maximale IOPS**: Die maximale IOPS-QoS-Einstellung des virtuellen Volumes.
- **Burst IOPS**: Die maximale Burst-QoS-Einstellung des virtuellen Volumes.
- **Enable 512**: Da virtuelle Volumes immer 512-Byte-Blockgrößen-Emulation verwenden, ist der Wert immer ja.

- **Volumen gekoppelt**: Gibt an, ob ein Volumen gekoppelt ist.
- **Erstellungszeit**: Die Zeit, die die Erstellung des virtuellen Volumes abgeschlossen wurde.
- **Blocks Größe**: Größe der Blöcke auf dem Volumen.
- **Nicht ausgerichtete Schreibvorgänge**: Für 512e Volumen, die Anzahl der Schreibvorgänge, die sich nicht an einer grenze des 4k-Sektors befanden. Eine hohe Anzahl von nicht ausgerichteten Schreibvorgängen kann auf eine falsche Ausrichtung der Partition hindeuten.
- **Nicht ausgerichtete Lesevorgänge**: Für 512e Volumen, die Anzahl der Leseoperationen, die sich nicht an der grenze des 4k-Sektors befanden. Eine hohe Anzahl von nicht ausgerichteten Lesevorgängen kann auf eine falsche Ausrichtung der Partition hindeuten.
- **ScsiEUIDeviceID**: Weltweit eindeutige SCSI-Geräte-ID für das Volumen im 16-Byte-Format EUI-64.
- **ScsiNAADeviceID**: Weltweit eindeutige SCSI-Geräte-ID für das Volume im NAA IEEE-Registered Extended-Format.
- **Attribute**: Liste von Name-Wert-Paaren im JSON-Objektformat.

Löschen Sie ein virtuelles Volume

Obwohl virtuelle Volumes immer aus der VMware Management-Ebene gelöscht werden sollten, ist die Funktion zum Löschen virtueller Volumes in der Element-UI aktiviert. Sie sollten ein virtuelles Volume nur bei Bedarf aus der Element UI löschen, beispielsweise wenn vSphere virtuelle Volumes auf dem SolidFire Storage nicht bereinigt.

1. Wählen Sie **VVols** > **Virtual Volumes** aus.
2. Klicken Sie auf das Aktionen-Symbol für das virtuelle Volume, das Sie löschen möchten.
3. Wählen Sie im Menü Ergebnis die Option **Löschen** aus.

> Sie sollten ein virtuelles Volume von der VMware Management-Ebene löschen, um vor dem Löschen sicherzustellen, dass das virtuelle Volume ordnungsgemäß getrennt wird. Sie sollten ein virtuelles Volume nur bei Bedarf aus der Element UI löschen, beispielsweise wenn vSphere virtuelle Volumes auf dem SolidFire Storage nicht bereinigt. Wenn Sie ein virtuelles Volume aus der Element UI löschen, wird das Volume sofort gelöscht.

4. Bestätigen Sie die Aktion.
5. Aktualisieren Sie die Liste der virtuellen Volumes, um zu bestätigen, dass das virtuelle Volume entfernt wurde.
6. **Optional**: Wählen Sie **Reporting** > **Ereignisprotokoll**, um zu bestätigen, dass die Löschung erfolgreich war.

Management von Storage-Containern

Ein Storage-Container ist eine Darstellung von vSphere Datastores, die auf einem Cluster mit Element Software erstellt wurde.

Storage-Container werden erstellt und an NetApp Element Accounts gebunden. Ein auf Element Storage erstellter Storage-Container wird als vSphere Datastore in vCenter und ESXi angezeigt. Storage Container weisen keinem Speicherplatz auf Element Storage zu. Sie werden einfach dazu verwendet, virtuelle Volumes logisch zu verknüpfen.

Pro Cluster werden maximal vier Storage-Container unterstützt. Zur Aktivierung der VVols Funktion ist

mindestens ein Storage-Container erforderlich.

Erstellen eines Storage-Containers

Es können Storage Container in der Element UI erstellt und in vCenter ermittelt werden. Sie müssen mindestens einen Storage-Container erstellen, um mit der Bereitstellung der auf VVol basierenden Virtual Machines zu beginnen.

Aktivieren Sie vor Beginn die VVols Funktion in der Element UI für das Cluster.

Schritte

1. Wählen Sie **VVols** > **Storage Container** aus.
2. Klicken Sie auf die Schaltfläche **Storage Container erstellen**.
3. Geben Sie im Dialogfeld **Erstellen eines neuen Speicherbehälters** Informationen zum Speichercontainer ein:
   a. Geben Sie einen Namen für den Speichercontainer ein.
   b. Konfigurieren Sie Initiator- und Zielschlüssel für CHAP.

      Lassen Sie die Felder für CHAP-Einstellungen leer, um automatisch Schlüssel zu generieren.

   c. Klicken Sie auf die Schaltfläche **Storage Container erstellen**.
4. Überprüfen Sie, ob der neue Speichercontainer in der Liste auf der Unterregisterkarte **Storage Container** angezeigt wird.

   Da eine NetApp Element-Konto-ID automatisch erstellt und dem Storage-Container zugewiesen wird, muss kein Konto manuell erstellt werden.

Zeigen Sie Details zum Storage-Container an

Auf der Seite Storage Container auf der Registerkarte VVols können Sie Informationen für alle aktiven Storage-Container auf dem Cluster anzeigen.

- **Konto-ID**: Die ID des NetApp Element-Kontos, das mit dem Speichercontainer verknüpft ist.
- **Name**: Der Name des Speicherbehälters.
- **Status**: Der Status des Lagerbehälters. Mögliche Werte:
  - Aktiv: Der Speicherbehälter wird verwendet.
  - Gesperrt: Der Speicherbehälter ist gesperrt.
- **PE Typ**: Der Protokollendpunkttyp (SCSI ist das einzige verfügbare Protokoll für Element Software).
- **Speicher-Container-ID**: Die UUID des virtuellen Volume-Speichercontainers.
- **Active Virtual Volumes**: Die Anzahl der aktiven virtuellen Volumes, die mit dem Speicher-Container verbunden sind.

Zeigen Sie die Details zu einzelnen Storage-Containern an

Sie können die Storage-Container-Informationen für einen einzelnen Storage-Container anzeigen. Wählen Sie dazu auf der Seite Storage-Container auf der Registerkarte VVols die entsprechende Option aus.

- **Konto-ID**: Die ID des NetApp Element-Kontos, das mit dem Speichercontainer verknüpft ist.
- **Name**: Der Name des Speicherbehälters.
- **Status**: Der Status des Lagerbehälters. Mögliche Werte:
  - Aktiv: Der Speicherbehälter wird verwendet.
  - Gesperrt: Der Speicherbehälter ist gesperrt.
- **CHAP-Initiatorschlüssel**: Der eindeutige CHAP-Schlüssel für den Initiator.
- **CHAP Target Secret**: Der eindeutige CHAP-Schlüssel für das Ziel.
- **Speicher-Container-ID**: Die UUID des virtuellen Volume-Speichercontainers.
- **Protocol Endpoint Type**: Gibt den Protokollendpunkttyp an (SCSI ist das einzige verfügbare Protokoll).

Bearbeiten eines Speichercontainers

Sie können die CHAP-Authentifizierung für Speichercontainer in der Element-UI ändern.

1. Wählen Sie **VVols** > **Storage Container** aus.
2. Klicken Sie auf das Symbol **Aktionen** für den Speichercontainer, den Sie bearbeiten möchten.
3. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
4. Bearbeiten Sie unter CHAP-Einstellungen die Anmeldeinformationen für Initiatorschlüssel und Zielschlüssel, die für die Authentifizierung verwendet werden.

   Wenn Sie die Anmeldeinformationen für CHAP-Einstellungen nicht ändern, bleiben diese unverändert. Wenn Sie die Felder mit den Anmeldeinformationen leer lassen, generiert das System automatisch neue Geheimnisse.

5. Klicken Sie Auf **Änderungen Speichern**.

Löschen eines Speichercontainers

Sie können Storage Container von der Element UI löschen.

Was Sie benötigen

Stellen Sie sicher, dass alle Virtual Machines aus dem VVol Datastore entfernt wurden.

Schritte

1. Wählen Sie **VVols** > **Storage Container** aus.
2. Klicken Sie auf das Symbol **Aktionen** für den zu löschenden Speichercontainer.
3. Wählen Sie im Menü Ergebnis die Option **Löschen** aus.
4. Bestätigen Sie die Aktion.
5. Aktualisieren Sie die Liste der Speichercontainer auf der Unterregisterkarte **Speichercontainer**, um zu bestätigen, dass der Speichercontainer entfernt wurde.

Protokollendpunkte

Erfahren Sie mehr über Protokollendpunkte.

Protokollendpunkte sind Zugriffspunkte, die von einem Host zur Storage-Adresse in

einem Cluster verwendet werden, auf dem die NetApp Element Software ausgeführt wird. Protokollendpunkte können nicht von einem Benutzer gelöscht oder geändert werden, sind keinem Konto zugeordnet und können nicht einer Volume-Zugriffsgruppe hinzugefügt werden.

Ein Cluster, auf dem Element Software ausgeführt wird, erstellt automatisch einen Protokollendpunkt pro Storage-Node im Cluster. Ein Storage-Cluster mit sechs Nodes verfügt beispielsweise über sechs Protokollendpunkte, die jedem ESXi Host zugeordnet sind. Protokollendpunkte werden dynamisch von Element Software gemanagt und ohne Eingriffe erstellt, verschoben oder entfernt. Protokollendpunkte sind das Ziel für Multi-Pathing und fungieren als I/O-Proxy für subsidiäre LUNs. Jeder Protokollendpunkt nutzt eine verfügbare SCSI-Adresse, genau wie ein Standard-iSCSI-Ziel. Protokollendpunkte werden im vSphere Client als ein einzelnes Block-Storage-Gerät (512 Byte) angezeigt, dieses Storage-Gerät kann jedoch nicht formatiert oder als Storage verwendet werden.

ISCSI ist das einzige unterstützte Protokoll. Das Fibre Channel-Protokoll wird nicht unterstützt.

Details zu Protokollendpunkten

Die Seite Protokollendpunkte auf der Registerkarte VVols bieten Informationen zu Protokollendpunkten.

- * Primary Provider ID*

  Die ID des primären Protokollendpunktanbieters.

- **Sekundäre Provider-ID**

  Die ID des Endpunktanbieters für das sekundäre Protokoll.

- * Protokollendpunkt-ID*

  Die UUID des Protokollendpunkts.

- * Protokoll Endpunktzustand*

  Der Status des Protokollendpunkts. Folgende Werte sind möglich:

  - Aktiv: Der Protokollendpunkt wird verwendet.
  - Start: Der Protokollendpunkt wird gestartet.
  - Failover: Der Protokollendpunkt ist ein Failover aufgetreten.
  - Reserviert: Der Protokollendpunkt ist reserviert.

- * Anbieter Typ*

  Der Typ des Provider des Protokollendpunkts. Folgende Werte sind möglich:

  - Primär
  - Sekundär

- **SCSI NAA GERÄTE-ID**

  Die weltweit eindeutige SCSI-Gerätekennung für den Protokollendpunkt im NAA IEEE Registered Extended Format.

Bindungen

Lerne mehr über Bindungen

Um I/O-Vorgänge für ein virtuelles Volume durchzuführen, muss ein ESXi Host zuerst das virtuelle Volume binden.

Der SolidFire Cluster wählt einen optimalen Protokollendpunkt, erstellt eine Bindung, die den ESXi Host und das virtuelle Volume dem Protokollendpunkt zugeordnet und die Bindung an den ESXi Host zurückgibt. Nach der Bindung kann der ESXi Host I/O-Vorgänge mit dem gebundenen virtuellen Volume ausführen.

Details zu Bindungen

Die Seite Bindungen auf der Registerkarte VVols bietet verbindliche Informationen zu jedem virtuellen Volume.

Folgende Informationen werden angezeigt:

- **Host-ID**

  Die UUID für den ESXi-Host, der virtuelle Volumes hostet und dem Cluster bekannt ist.

- * Protokollendpunkt-ID*

  Protokollendpunkt-IDs, die jedem Node im SolidFire Cluster entsprechen.

- * Protokollendpunkt in Band-ID*

  Die SCSI-NAA-Geräte-ID des Protokollendpunkts.

- * Protokollendpunkt Typ*

  Der Endpunkt-Typ des Protokolls.

- **VVol Binding ID**

  Die bindende UUID des virtuellen Volumes.

- * VVol ID*

  Die Universally Unique Identifier (UUID) des virtuellen Volumes.

- **VVol Secondary ID**

  Die sekundäre ID des virtuellen Volumes als LUN-ID der zweiten SCSI-Ebene.

Host-Details

Die Seite Hosts auf der Registerkarte VVols bietet Informationen zu VMware ESXi Hosts, die virtuelle Volumes hosten.

Folgende Informationen werden angezeigt:

- **Host-ID**

Die UUID für den ESXi-Host, der virtuelle Volumes hostet und dem Cluster bekannt ist.

- **Host-Adresse**

  Die IP-Adresse oder der DNS-Name für den ESXi-Host.

- **Bindungen**

  Binding-IDs für alle virtuellen Volumes, die vom ESXi-Host gebunden sind.

- **ESX Cluster-ID**

  Die vSphere-Host-Cluster-ID oder vCenter-GUID.

- **Initiator-IQNs**

  Initiator-IQNs für den Host des virtuellen Volumes.

- **SolidFire-Protokoll Endpunkt-IDs**

  Die Protokollendpunkte, die derzeit für den ESXi Host sichtbar sind.

Arbeiten Sie mit Volume-Zugriffsgruppen und -Initiatoren

Erstellen einer Volume-Zugriffsgruppe

Sie können Volume-Zugriffsgruppen erstellen, indem Sie Initiatoren einer Sammlung von Volumes für den gesicherten Zugriff zuordnen. Sie können dann den Zugriff auf die Volumes in der Gruppe mit einem Schlüssel-CHAP-Initiator und Zielschlüssel gewähren.

Wenn Sie Initiator-basiertes CHAP verwenden, können Sie CHAP-Anmeldeinformationen für einen einzelnen Initiator in einer Volume-Zugriffsgruppe hinzufügen, wodurch mehr Sicherheit gewährleistet wird. Damit können Sie diese Option für bereits vorhandene Volume Access Groups anwenden.

Schritte

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie Auf **Zugriffsgruppe Erstellen**.
3. Geben Sie im Feld **Name** einen Namen für die Zugriffsgruppe des Volumes ein.
4. Sie haben folgende Möglichkeiten, um der Volume-Zugriffsgruppe einen Initiator hinzuzufügen:

Option	Beschreibung
Hinzufügen eines Fibre Channel-Initiators	a. Wählen Sie unter Initiatoren hinzufügen einen vorhandenen Fibre Channel-Initiator aus der Liste Unbound Fibre Channel Initiatoren aus. b. Klicken Sie auf **FC-Initiator hinzufügen**. Sie können während dieses Schritts einen Initiator erstellen, wenn Sie auf den Link **Initiator erstellen** klicken, einen Initiatornamen eingeben und auf **Erstellen** klicken. Das System fügt den Initiator automatisch der Liste Initiatoren hinzu, nachdem Sie ihn erstellt haben. Ein Beispiel für das Format: `5f:47:ac:c0:5c:74:d4:02`
Hinzufügen eines iSCSI-Initiators	Wählen Sie unter Initiatoren hinzufügen einen vorhandenen Initiator aus der Liste Initiatoren aus. **Hinweis:** Wenn Sie in diesem Schritt auf den Link **Initiator erstellen** klicken, einen Initiatornamen eingeben und auf **Erstellen** klicken, können Sie einen Initiator erstellen. Das System fügt den Initiator automatisch der Liste Initiatoren hinzu, nachdem Sie ihn erstellt haben. Ein Beispiel für das Format: `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b` Den Initiator-IQN für jedes Volume finden Sie, indem Sie im Menü Aktionen für das Volume auf der Liste **Verwaltung** > **Volumes** > **Active** die Option **Details anzeigen** wählen. Wenn Sie einen Initiator ändern, können Sie das requiredCHAP-Attribut auf „true“ umschalten, sodass Sie den Zielinitiatorschlüssel festlegen können. Weitere Informationen finden Sie unter API-Informationen zur ModifyInitiator API-Methode. "Storage-Management mit der Element API"

5. **Optional:** Fügen Sie weitere Initiatoren nach Bedarf hinzu.
6. Wählen Sie unter Volumes hinzufügen ein Volume aus der Liste **Volumes** aus.

   Der Datenträger wird in der Liste **angehängte Volumes** angezeigt.
7. **Optional:** Hinzufügen Sie weitere Volumen nach Bedarf.
8. Klicken Sie Auf **Zugriffsgruppe Erstellen**.

Weitere Informationen

Fügen Sie einer Zugriffsgruppe Volumes hinzu

Zeigen Sie die Details einzelner Zugriffsgruppen an

Sie können Details für eine einzelne Zugriffsgruppe, z. B. verbundene Volumes und Initiatoren, in einem grafischen Format anzeigen.

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol Aktionen für eine Zugriffsgruppe.
3. Klicken Sie Auf **Details Anzeigen**.

Details zu Volume-Zugriffsgruppen

Die Seite Zugriffsgruppen auf der Registerkarte Verwaltung enthält Informationen zu Volume Access Groups.

Folgende Informationen werden angezeigt:

- **ID**: Die vom System generierte ID für die Zugriffsgruppe.
- **Name**: Der Name, der der Zugriffsgruppe bei der Erstellung gegeben wurde.
- **Aktive Volumes**: Die Anzahl der aktiven Volumes in der Zugriffsgruppe.
- **Komprimierung**: Die Kompressionseffizienz für die Zugriffsgruppe.
- **Deduplizierung**: Die Deduplizierungs-Effizienzbewertung für die Zugriffsgruppe.
- **Thin Provisioning**: Die Thin Provisioning-Effizienzbewertung für die Zugriffsgruppe.
- **Gesamteffizienz**: Die Gesamteffizienz für die Access Group.
- **Initiatoren**: Die Anzahl der Initiatoren, die mit der Zugriffsgruppe verbunden sind.

Fügen Sie einer Zugriffsgruppe Volumes hinzu

Sie können Volumes zu einer Volume-Zugriffsgruppe hinzufügen. Jedes Volume kann mehr als einer Volume-Zugriffsgruppe angehören. Sie können die Gruppen sehen, zu denen jedes Volume gehört, auf der Seite **Active** Volumes.

Mit diesem Verfahren können Sie auch Volumes zu einer Zugriffsgruppe für Fibre Channel-Volumes hinzufügen.

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol Aktionen für die Zugriffsgruppe, der Sie Volumes hinzufügen möchten.
3. Klicken Sie auf die Schaltfläche **Bearbeiten**.
4. Wählen Sie unter Volumes hinzufügen ein Volume aus der Liste **Volumes** aus.

   Sie können weitere Volumes hinzufügen, indem Sie diesen Schritt wiederholen.

5. Klicken Sie Auf **Änderungen Speichern**.

Volumes aus einer Zugriffsgruppe entfernen

Wenn Sie ein Volume aus einer Zugriffsgruppe entfernen, hat die Gruppe keinen Zugriff mehr auf dieses Volume.

Das Ändern von CHAP-Einstellungen in einem Konto oder das Entfernen von Initiatoren oder Volumes aus einer Zugriffsgruppe kann dazu führen, dass Initiatoren unerwartet den Zugriff auf Volumes verlieren. Um zu überprüfen, ob der Volume-Zugriff nicht unerwartet verloren geht, melden Sie sich iSCSI-Sitzungen ab, die von einem Konto oder einer Zugriffsgruppenänderung betroffen sind, und überprüfen Sie, ob die Initiatoren nach Abschluss der Änderungen an den Initiatoreinstellungen und den Cluster-Einstellungen eine Verbindung zu Volumes herstellen können.

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol Aktionen für die Zugriffsgruppe, aus der Sie Volumes entfernen möchten.
3. Klicken Sie Auf **Bearbeiten**.
4. Klicken Sie unter Volumes hinzufügen im Dialogfeld **Volume Access Group** bearbeiten auf den Pfeil in der Liste **angehängte Volumes**.
5. Wählen Sie den gewünschten Datenträger aus der Liste aus und klicken Sie auf das Symbol **x**, um das Volume aus der Liste zu entfernen.

   Sie können weitere Volumes entfernen, indem Sie diesen Schritt wiederholen.

6. Klicken Sie Auf **Änderungen Speichern**.

Erstellen eines Initiators

Sie können iSCSI- oder Fibre Channel-Initiatoren erstellen und diese optional Aliase zuweisen.

Sie können auch initator-basierte CHAP-Attribute zuweisen, indem Sie einen API-Aufruf verwenden. Um einen CHAP-Kontonamen und Anmeldeinformationen pro Initiator hinzuzufügen, müssen Sie den verwenden `CreateInitiator` API-Aufruf zum Entfernen und Hinzufügen von CHAP-Zugriff und -Attributen. Der Initiatorzugriff kann auf ein oder mehrere VLANs beschränkt werden, indem ein oder mehrere virtuelle Netzwerk-IDs über das angegeben werden `CreateInitiators` Und `ModifyInitiators` API-Aufrufe. Wenn keine virtuellen Netzwerke angegeben werden, kann der Initiator auf alle Netzwerke zugreifen.

Für Details siehe die API-Referenzinformationen. "Storage-Management mit der Element API"

Schritte

1. Klicken Sie Auf **Management** > **Initiatoren**.
2. Klicken Sie Auf **Initiator Erstellen**.
3. Führen Sie die Schritte aus, um einen einzelnen Initiator oder mehrere Initiatoren zu erstellen:

Option	Schritte
Erstellen eines einzelnen Initiators	a. Klicken Sie auf **Einen einzelnen Initiator erstellen**. b. Geben Sie im Feld **IQN/WWPN** den IQN oder WWPN für den Initiator ein. c. Geben Sie im Feld **Alias** einen Anzeigenamen für den Initiator ein. d. Klicken Sie Auf **Initiator Erstellen**.

Option	Schritte
Erstellen Sie mehrere Initiatoren	a. Klicken Sie Auf **Bulk Create Initiatoren**. b. Geben Sie eine Liste von IQNs oder WWPNs in das Textfeld ein. c. Klicken Sie Auf **Initiatoren Hinzufügen**. d. Wählen Sie einen Initiator aus der Ergebnisliste aus, und klicken Sie in der Spalte **Alias** auf das entsprechende Add-Symbol, um einen Alias für den Initiator hinzuzufügen. e. Klicken Sie auf das Häkchen, um den neuen Alias zu bestätigen. f. Klicken Sie Auf **Initiatoren Erstellen**.

Bearbeiten Sie einen Initiator

Sie können den Alias eines bestehenden Initiators ändern oder einen Alias hinzufügen, wenn einer noch nicht vorhanden ist.

Um einen CHAP-Kontonamen und Anmeldeinformationen pro Initiator hinzuzufügen, müssen Sie den verwenden `ModifyInitiator` API-Aufruf zum Entfernen und Hinzufügen von CHAP-Zugriff und -Attributen.

Sehen"Storage-Management mit der Element API" .

Schritte

1. Klicken Sie Auf **Management** > **Initiatoren**.
2. Klicken Sie auf das Symbol Aktionen für den Initiator, den Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.
4. Geben Sie im Feld **Alias** einen neuen Alias für den Initiator ein.
5. Klicken Sie Auf **Änderungen Speichern**.

Fügen Sie einen einzelnen Initiator einer Volume-Zugriffsgruppe hinzu

Sie können einem bestehenden Volume-Zugriffsgruppen einen Initiator hinzufügen.

Wenn Sie einer Volume-Zugriffsgruppe einen Initiator hinzufügen, hat der Initiator Zugriff auf alle Volumes in dieser Volume-Zugriffsgruppe.

Sie können den Initiator für jedes Volume finden, indem Sie auf das Aktionen-Symbol klicken und dann **Details anzeigen** für das Volume in der Liste der aktiven Volumes auswählen.

Wenn Sie Initiator-basiertes CHAP verwenden, können Sie CHAP-Anmeldeinformationen für einen einzelnen Initiator in einer Volume-Zugriffsgruppe hinzufügen, wodurch mehr Sicherheit gewährleistet wird. Damit können Sie diese Option für bereits vorhandene Volume Access Groups anwenden.

Schritte

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol **Aktionen** für die Zugriffsgruppe, die Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.

4. So fügen Sie der Zugriffsgruppe für Volumes einen Fibre Channel-Initiator hinzu:

   a. Wählen Sie unter Initiatoren hinzufügen einen vorhandenen Fibre Channel-Initiator aus der Liste **Unbound Fibre Channel Initiatoren** aus.

   b. Klicken Sie auf **FC-Initiator hinzufügen**.

   Sie können während dieses Schritts einen Initiator erstellen, wenn Sie auf den Link **Initiator erstellen** klicken, einen Initiatornamen eingeben und auf **Erstellen** klicken. Das System fügt den Initiator nach dem Erstellen automatisch der Liste **Initiatoren** hinzu.

   Ein Beispiel für das Format:

```
5f:47:ac:c0:5c:74:d4:02
```

5. Um der Volume Access Group einen iSCSI-Initiator hinzuzufügen, wählen Sie unter Add-Initiatoren einen bestehenden Initiator aus der Liste **Initiatoren** aus.

   Sie können während dieses Schritts einen Initiator erstellen, wenn Sie auf den Link **Initiator erstellen** klicken, einen Initiatornamen eingeben und auf **Erstellen** klicken. Das System fügt den Initiator nach dem Erstellen automatisch der Liste **Initiatoren** hinzu.

   Das akzeptierte Format eines Initiator-IQN lautet wie folgt: iqn.yyy-mm, wobei y und m Ziffern sind, gefolgt von Text, der nur Ziffern, alphabetische Kleinbuchstaben, einen Punkt (.), einen Doppelpunkt (:) oder Strich (-) enthalten darf.

   Ein Beispiel für das Format:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

   Den Initiator IQN für jedes Volume finden Sie auf der Seite **Verwaltung** > **Volumes** Aktive Volumes. Klicken Sie dazu auf das Aktionen-Symbol und wählen Sie dann **Details anzeigen** für das Volume aus.

6. Klicken Sie Auf **Änderungen Speichern**.

Fügen Sie einer Volume-Zugriffsgruppe mehrere Initiatoren hinzu

Sie können einer vorhandenen Volume-Zugriffsgruppe mehrere Initiatoren hinzufügen, um den Zugriff auf Volumes in der Volume-Zugriffsgruppe mit oder ohne CHAP-Authentifizierung zu ermöglichen.

Wenn Sie einer Volume-Zugriffsgruppe Initiatoren hinzufügen, haben die Initiatoren Zugriff auf alle Volumes in dieser Volume-Zugriffsgruppe.

Sie können den Initiator für jedes Volume finden, indem Sie auf das Aktionen-Symbol und dann **Details anzeigen** für das Volume in der Liste der aktiven Volumes klicken.

Sie können einer vorhandenen Volume-Zugriffsgruppe mehrere Initiatoren hinzufügen, um den Zugriff auf

Volumes zu ermöglichen und jedem Initiator innerhalb dieser Volume-Zugriffsgruppe eindeutige CHAP-Anmeldeinformationen zuzuweisen. Damit können Sie diese Option für bereits vorhandene Volume Access Groups anwenden.

Sie können initator-basierte CHAP-Attribute mit einem API-Aufruf zuweisen. Um einen CHAP-Kontonamen und Anmeldeinformationen pro Initiator hinzuzufügen, müssen Sie den API-Aufruf zum ModifyInitiator verwenden, um CHAP-Zugriff und -Attribute zu entfernen und hinzuzufügen.

Weitere Einzelheiten finden Sie unter"Storage-Management mit der Element API" .

Schritte

1. Klicken Sie Auf **Management** > **Initiatoren**.
2. Wählen Sie die Initiatoren aus, die einer Zugriffsgruppe hinzugefügt werden sollen.
3. Klicken Sie auf die Schaltfläche **Massenaktionen**.
4. Klicken Sie auf **zu Volume Access Group hinzufügen**.
5. Wählen Sie im Dialogfeld zu Volume Access Group hinzufügen eine Zugriffsgruppe aus der Liste **Volume Access Group** aus.
6. Klicken Sie Auf **Hinzufügen**.

Entfernen Sie Initiatoren aus einer Zugriffsgruppe

Wenn Sie einen Initiator aus einer Zugriffsgruppe entfernen, kann er nicht mehr auf die Volumes in dieser Volume-Zugriffsgruppe zugreifen. Der normale Account-Zugriff auf das Volume wird nicht unterbrochen.

Das Ändern von CHAP-Einstellungen in einem Konto oder das Entfernen von Initiatoren oder Volumes aus einer Zugriffsgruppe kann dazu führen, dass Initiatoren unerwartet den Zugriff auf Volumes verlieren. Um zu überprüfen, ob der Volume-Zugriff nicht unerwartet verloren geht, melden Sie sich iSCSI-Sitzungen ab, die von einem Konto oder einer Zugriffsgruppenänderung betroffen sind, und überprüfen Sie, ob die Initiatoren nach Abschluss der Änderungen an den Initiatoreinstellungen und den Cluster-Einstellungen eine Verbindung zu Volumes herstellen können.

Schritte

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol **Aktionen** für die Zugriffsgruppe, die Sie entfernen möchten.
3. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
4. Klicken Sie unter Add Initiatoren im Dialogfeld **Edit Volume Access Group** auf den Pfeil in der Liste **Initiatoren**.
5. Wählen Sie für jeden Initiator das x-Symbol aus, das Sie aus der Zugriffsgruppe entfernen möchten.
6. Klicken Sie Auf **Änderungen Speichern**.

Löschen Sie eine Zugriffsgruppe

Sie können eine Zugriffsgruppe löschen, wenn sie nicht mehr benötigt wird. Sie müssen Initiator-IDs und Volume-IDs nicht aus der Volume-Zugriffsgruppe löschen, bevor Sie die Gruppe löschen. Nachdem Sie die Zugriffsgruppe gelöscht haben, wird der Gruppenzugriff auf die Volumes abgebrochen.

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol **Aktionen** für die Zugriffsgruppe, die Sie löschen möchten.
3. Klicken Sie im Menü Ergebnis auf **Löschen**.
4. Um auch die Initiatoren zu löschen, die dieser Zugriffsgruppe zugeordnet sind, aktivieren Sie das Kontrollkästchen **Initiatoren löschen in dieser Zugriffsgruppe**.
5. Bestätigen Sie die Aktion.

Löschen eines Initiators

Sie können einen Initiator löschen, nachdem er nicht mehr benötigt wird. Wenn Sie einen Initiator löschen, wird dieser vom System aus einer zugehörigen Volume-Zugriffsgruppe entfernt. Verbindungen, die den Initiator verwenden, bleiben gültig, bis die Verbindung zurückgesetzt wird.

Schritte

1. Klicken Sie Auf **Management** > **Initiatoren**.
2. Führen Sie die Schritte zum Löschen eines einzelnen Initiators oder mehrerer Initiatoren durch:

Option	Schritte
Löschen Sie den einzelnen Initiator	a. Klicken Sie auf das Symbol **Aktionen** für den Initiator, den Sie löschen möchten. b. Klicken Sie Auf **Löschen**. c. Bestätigen Sie die Aktion.
Löschen Sie mehrere Initiatoren	a. Aktivieren Sie die Kontrollkästchen neben den Initiatoren, die Sie löschen möchten. b. Klicken Sie auf die Schaltfläche **Massenaktionen**. c. Wählen Sie im Menü Ergebnis die Option **Löschen** aus. d. Bestätigen Sie die Aktion.

Sichern Sie Ihre Daten

Sichern Sie Ihre Daten

Die NetApp Element Software ermöglicht die Datensicherung auf unterschiedliche Weise mit Funktionen wie Snapshots für einzelne Volumes oder Volume-Gruppen, mit Replizierung zwischen Clustern und Volumes auf Element sowie mit Replizierung auf ONTAP Systemen.

- **Snapshots**

  Bei der Datensicherung nur mit Snapshots werden geänderte Daten zu einem bestimmten Zeitpunkt in ein Remote-Cluster repliziert. Es werden nur die Snapshots repliziert, die auf dem Quellcluster erstellt wurden. Aktive Schreibvorgänge vom Quell-Volume sind nicht.

Nutzen Sie Volume Snapshots zur Datensicherung

- **Remote-Replikation zwischen Clustern und Volumes, die auf Element** ausgeführt werden

  Sie können Volume-Daten synchron oder asynchron aus einem der beiden Cluster in einem Cluster-Paar replizieren, die beide im Element für Failover- und Failback-Szenarien ausgeführt werden.

  Remote-Replizierung zwischen Clustern mit NetApp Element Software

- **Replizierung zwischen Element und ONTAP Clustern mit SnapMirror Technologie**

  Mit der NetApp SnapMirror Technologie können Snapshots repliziert werden, die für Disaster Recovery mithilfe von Element in ONTAP erstellt wurden. In einer SnapMirror Beziehung stellt Element einen Endpunkt dar, und ONTAP ist der andere.

  SnapMirror Replizierung zwischen Element und ONTAP Clustern

- **Sichern und Wiederherstellen von Volumes aus SolidFire-, S3- oder Swift-Objektspeichern**

  Backups und Restores von Volumes auf anderen SolidFire Storage sowie sekundäre Objektspeicher, die mit Amazon S3 oder OpenStack Swift kompatibel sind.

  Backup und Restore von Volumes in SolidFire-, S3- oder Swift-Objektspeichern

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Nutzen Sie Volume Snapshots zur Datensicherung

Nutzen Sie Volume Snapshots zur Datensicherung

Ein Volume Snapshot ist eine zeitpunktgenaue Kopie eines Volumes. Sie können einen Snapshot eines Volumes erstellen und den Snapshot später verwenden, wenn Sie ein Volume zurück in den Zustand verschieben müssen, in dem es zum Zeitpunkt der Snapshot-Erstellung war.

Snapshots ähneln denen von Volume-Klonen. Allerdings sind Snapshots lediglich Replikate von Volume-Metadaten. Sie können also nicht mounten oder darauf schreiben. Das Erstellen eines Volume-Snapshots nimmt ebenfalls nur eine geringe Menge an Systemressourcen und Platz in Anspruch, sodass die Snapshot-Erstellung schneller als das Klonen erfolgt.

Sie können einen Snapshot eines einzelnen Volumes oder einer Gruppe von Volumes erstellen.

Optional können Sie Snapshots in einem Remote-Cluster replizieren und als Backup-Kopie des Volume verwenden. Dies ermöglicht Ihnen, ein Rollback eines Volumes zu einem bestimmten Zeitpunkt mithilfe des replizierten Snapshots durchzuführen. Alternativ können Sie aus einem replizierten Snapshot einen Klon eines Volumes erstellen.

Weitere Informationen

- Individuelle Volume Snapshots zur Datensicherung

- Gruppen-Snapshots für Datenschutzaufgabe wird verwendet
- Planen eines Snapshots

Individuelle Volume Snapshots zur Datensicherung

Individuelle Volume Snapshots zur Datensicherung

Ein Volume Snapshot ist eine zeitpunktgenaue Kopie eines Volumes. Sie können ein einzelnes Volume anstelle einer Gruppe von Volumes für den Snapshot verwenden.

Weitere Informationen

- Erstellen eines Volume-Snapshots
- Bearbeiten der Snapshot-Aufbewahrung
- Löschen eines Snapshots
- Klonen eines Volumes aus einem Snapshot
- Rollback eines Volumes zu einem Snapshot
- Sichern eines Volume-Snapshots in einem Amazon S3-Objektspeicher
- Ein Volume Snapshot wird in einem OpenStack Swift Objektspeicher gesichert
- Sichern eines Volume Snapshots auf einem SolidFire Cluster

Erstellen eines Volume-Snapshots

Sie können einen Snapshot eines aktiven Volumes erstellen, um das Volume Image zu einem beliebigen Zeitpunkt beizubehalten. Sie können bis zu 32 Snapshots für ein einzelnes Volume erstellen.

1. Klicken Sie Auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol **Aktionen** für das Volumen, das Sie für den Snapshot verwenden möchten.
3. Wählen Sie im Menü Ergebnis die Option **Snapshot** aus.
4. Geben Sie im Dialogfeld **Snapshot des Volumes erstellen** den neuen Snapshot-Namen ein.
5. **Optional:** Aktivieren Sie das Kontrollkästchen **Snapshot in Replikation einschließen, wenn gepaart** aktiviert ist, um sicherzustellen, dass der Snapshot bei der Replikation erfasst wird, wenn das übergeordnete Volume gekoppelt ist.
6. Um die Aufbewahrung für den Snapshot festzulegen, wählen Sie eine der folgenden Optionen aus:
   - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
   - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnboxen, um eine Zeitdauer für das System auszuwählen, um den Snapshot zu behalten.
7. So erstellen Sie einen einzigen, sofortigen Snapshot:
   a. Klicken Sie Auf **Momentaufnahme Jetzt Aufnehmen**.
   b. Klicken Sie Auf**Snapshot Erstellen**.
8. So planen Sie die Ausführung des Snapshots für einen späteren Zeitpunkt:
   a. Klicken Sie Auf **Snapshot Zeitplan Erstellen**.

b. Geben Sie einen **neuen Terminplannamen** ein.

c. Wählen Sie aus der Liste einen **Terminplantyp** aus.

d. **Optional:** Aktivieren Sie das Kontrollkästchen **wiederkehrender Zeitplan**, um den geplanten Snapshot regelmäßig zu wiederholen.

e. Klicken Sie Auf **Zeitplan Erstellen**.

Weitere Informationen

Planen Sie einen Snapshot

Bearbeiten der Snapshot-Aufbewahrung

Sie können den Aufbewahrungszeitraum für einen Snapshot ändern, um zu steuern, wann oder ob das System Snapshots löscht. Die von Ihnen angegebene Aufbewahrungsdauer beginnt, wenn Sie das neue Intervall eingeben. Wenn Sie einen Aufbewahrungszeitraum festlegen, können Sie einen Zeitraum auswählen, der zum aktuellen Zeitpunkt beginnt (die Aufbewahrung wird nicht aus der Snapshot-Erstellungszeit berechnet). Sie können Intervalle in Minuten, Stunden und Tagen festlegen.

Schritte

1. Klicken Sie Auf **Datenschutz** > **Snapshots**.
2. Klicken Sie auf das Symbol **Aktionen** für den zu bearbeitenden Snapshot.
3. Klicken Sie im Menü Ergebnis auf **Bearbeiten**.
4. **Optional:** Aktivieren Sie das Kontrollkästchen**Snapshot in Replikation einschließen, wenn gekoppelt**, um sicherzustellen, dass der Snapshot bei der Replikation erfasst wird, wenn das übergeordnete Volume gekoppelt ist.
5. **Optional:** Wählen Sie eine Aufbewahrungsoption für den Snapshot:
   - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
   - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnkästen, um eine Zeitdauer für das System auszuwählen, um den Snapshot beizubehalten.
6. Klicken Sie Auf **Änderungen Speichern**.

Löschen Sie einen Snapshot

Sie können einen Volume-Snapshot aus einem Storage-Cluster löschen, auf dem Element Software ausgeführt wird. Wenn Sie einen Snapshot löschen, entfernt das System ihn sofort.

Sie können Snapshots löschen, die aus dem Quellcluster repliziert werden. Wenn ein Snapshot beim Löschen mit dem Zielcluster synchronisiert wird, wird die synchrone Replikation abgeschlossen und der Snapshot wird aus dem Quellcluster gelöscht. Der Snapshot wird nicht aus dem Ziel-Cluster gelöscht.

Sie können auch Snapshots löschen, die vom Zielcluster zum Ziel repliziert wurden. Der gelöschte Snapshot wird in einer Liste von gelöschten Snapshots auf dem Ziel aufbewahrt, bis das System erkennt, dass Sie den Snapshot auf dem Quell-Cluster gelöscht haben. Wenn das Ziel erkennt, dass Sie den Quell-Snapshot gelöscht haben, wird die Replikation des Snapshots durch das Ziel gestoppt.

Wenn Sie einen Snapshot aus dem Quellcluster löschen, ist der Ziel-Cluster-Snapshot nicht betroffen (die umgekehrte ist auch wahr).

1. Klicken Sie Auf **Datenschutz** > **Snapshots**.
2. Klicken Sie auf das Symbol **Aktionen** für den zu löschenden Snapshot.
3. Wählen Sie im Menü Ergebnis die Option **Löschen** aus.
4. Bestätigen Sie die Aktion.

Klonen eines Volumes aus einem Snapshot

Sie können ein neues Volume aus einem Snapshot eines Volumes erstellen. Das wird verwendet, um ein neues Volume mithilfe der Snapshot-Informationen zu klonen. Dabei werden die Daten auf dem Volume zum Zeitpunkt der Erstellung des Snapshots verwendet. Dieser Prozess speichert Informationen über andere Snapshots des Volumes im neu erstellten Volume.

1. Klicken Sie Auf **Datenschutz** > **Snapshots**.
2. Klicken Sie auf das Symbol **Aktionen** für den Snapshot, den Sie für den Volume-Klon verwenden möchten.
3. Klicken Sie im Menü Ergebnis auf **Clone Volume from Snapshot**.
4. Geben Sie im Dialogfeld **Clone Volume from Snapshot** einen **Volume Name** ein.
5. Wählen Sie eine **Gesamtgröße** und Einheiten der Größe für das neue Volumen aus.
6. Wählen Sie für das Volume einen **Access**-Typ aus.
7. Wählen Sie in der Liste ein **Konto** aus, das mit dem neuen Volume verknüpft werden soll.
8. Klicken Sie Auf **Klonen Starten**.

Führen Sie ein Rollback eines Volumes zu einem Snapshot durch

Sie können ein Volume jederzeit auf einen vorherigen Snapshot zurück verschieben. Hierdurch werden alle Änderungen an dem Volume zurückgesetzt, die seit der Erstellung des Snapshots vorgenommen wurden.

Schritte

1. Klicken Sie Auf **Datenschutz** > **Snapshots**.
2. Klicken Sie auf das Symbol **Aktionen** für den Snapshot, den Sie für das Rollback des Volumes verwenden möchten.
3. Wählen Sie im Menü Ergebnis **Rollback Volume to Snapshot** aus.
4. **Optional:** zum Speichern des aktuellen Status des Volumens vor dem Rollback zum Snapshot:
   a. Wählen Sie im Dialogfeld **Rollback to Snapshot** den aktuellen Status des Volumes als Snapshot speichern* aus.
   b. Geben Sie einen Namen für den neuen Snapshot ein.
5. Klicken Sie Auf **Rollback Snapshot**.

Sichern Sie einen Volume-Snapshot

Sichern Sie einen Volume-Snapshot

Sie können die integrierte Backup-Funktion verwenden, um einen Volume-Snapshot zu sichern. Sie können ein Backup von Snapshots aus einem SolidFire Cluster auf einem externen Objektspeicher oder auf einem anderen SolidFire Cluster erstellen. Wenn Sie einen Snapshot in einem externen Objektspeicher sichern, müssen Sie über eine Verbindung zum Objektspeicher verfügen, der Lese-/Schreibvorgänge ermöglicht.

- "Sichern Sie einen Volume Snapshot in einem Amazon S3-Objektspeicher"
- "Sichern Sie einen Volume Snapshot in einem OpenStack Swift Objektspeicher"
- "Sichern Sie einen Volume Snapshot auf einem SolidFire Cluster"

Sichern Sie einen Volume Snapshot in einem Amazon S3-Objektspeicher

Sie können ein Backup von SolidFire Snapshots auf externen Objektspeichern erstellen, die mit Amazon S3 kompatibel sind.

1. Klicken Sie Auf**Data Protection** > **Snapshots**.
2. Klicken Sie auf das Symbol **Aktionen** für den Snapshot, den Sie sichern möchten.
3. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
4. Wählen Sie im Dialogfeld * Integriertes Backup* unter **Backup in** die Option **S3** aus.
5. Wählen Sie eine Option unter **Datenformat** aus:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Geben Sie einen Hostnamen ein, der für den Zugriff auf den Objektspeicher im Feld **Hostname** verwendet werden soll.
7. Geben Sie im Feld **Zugriffsschlüssel-ID** eine Zugriffsschlüssel-ID für das Konto ein.
8. Geben Sie den geheimen Zugriffsschlüssel für das Konto im Feld * Secret Access Key* ein.
9. Geben Sie den S3-Bucket ein, in dem die Sicherung im Feld **S3 Bucket** gespeichert werden soll.
10. **Optional**: Geben Sie im Feld **Nametag** einen Namensschild ein, der dem Präfix angefügt werden soll.
11. Klicken Sie Auf **Lesen Starten**.

Sichern Sie einen Volume Snapshot in einem OpenStack Swift Objektspeicher

Sie können ein Backup von SolidFire Snapshots auf sekundären Objektspeichern erstellen, die mit OpenStack Swift kompatibel sind.

1. Klicken Sie Auf **Datenschutz** > **Snapshots**.
2. Klicken Sie auf das Symbol **Aktionen** für den Snapshot, den Sie sichern möchten.
3. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
4. Wählen Sie im Dialogfeld * Integriertes Backup* unter **Backup in** die Option **Swift** aus.
5. Wählen Sie eine Option unter **Datenformat** aus:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.

    - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Geben Sie eine **URL** ein, um auf den Objektspeicher zuzugreifen.
7. Geben Sie einen **Benutzername** für das Konto ein.
8. Geben Sie den **Authentifizierungsschlüssel** für das Konto ein.
9. Geben Sie den **Container** ein, in dem die Sicherung gespeichert werden soll.
10. **Optional**: Geben Sie einen **Nametag** ein.
11. Klicken Sie Auf **Lesen Starten**.

Sichern Sie einen Volume Snapshot auf einem SolidFire Cluster

Sie können ein Backup von Volume Snapshots in einem SolidFire Cluster auf einem Remote SolidFire Cluster erstellen.

Stellen Sie sicher, dass die Quell- und Ziel-Cluster gekoppelt sind.

Beim Backup oder Restore von einem Cluster auf ein anderes generiert das System einen Schlüssel, der als Authentifizierung zwischen den Clustern verwendet wird. Dieser Schreibschlüssel für das Massenvolumen ermöglicht es dem Quellcluster, sich beim Schreiben auf das Ziel-Volume mit dem Ziel-Cluster zu authentifizieren. Im Rahmen des Backup- oder Wiederherstellungsprozesses müssen Sie vor dem Start des Vorgangs einen Schreibschlüssel für das Massenvolumen vom Zielvolume generieren.

1. Klicken Sie auf dem Ziel-Cluster auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol **Aktionen** für das Zielvolume.
3. Klicken Sie im Menü Ergebnis auf **aus** wiederherstellen.
4. Wählen Sie im Dialogfeld * Integrierter Restore* unter **Wiederherstellen von** die Option **SolidFire** aus.
5. Wählen Sie unter **Datenformat** ein Datenformat aus:
    - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
    - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Klicken Sie Auf **Schlüssel Generieren**.
7. Kopieren Sie den Schlüssel aus der Box **Bulk Volume Write Key** in die Zwischenablage.
8. Klicken Sie im Quellcluster auf **Data Protection** > **Snapshots**.
9. Klicken Sie auf das Aktionen-Symbol für den Snapshot, den Sie für das Backup verwenden möchten.
10. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
11. Wählen Sie im Dialogfeld**Integriertes Backup** unter **Backup in** die Option **SolidFire** aus.
12. Wählen Sie im Feld **Datenformat** das gleiche Datenformat aus, das Sie zuvor ausgewählt haben.
13. Geben Sie die virtuelle Management-IP-Adresse des Clusters des Ziel-Volumes im Feld **Remote Cluster MVIP** ein.
14. Geben Sie den Benutzernamen für den Remote-Cluster in das Feld **Remote-Cluster-Benutzername** ein.
15. Geben Sie das Kennwort für den Remote-Cluster im Feld * Remote-Cluster-Kennwort* ein.
16. Fügen Sie im Feld **Bulk Volume Write Key** den Schlüssel ein, den Sie zuvor auf dem Ziel-Cluster generiert haben.
17. Klicken Sie Auf **Lesen Starten**.

Verwenden Sie Gruppen-Snapshots für die Datensicherung

Gruppen-Snapshots für Datenschutzaufgabe wird verwendet

Sie können einen Gruppen-Snapshot einer verwandten Gruppe von Volumes erstellen, um eine zeitpunktgenaue Kopie der Metadaten für jedes Volume aufzubewahren. Sie können den Gruppen-Snapshot zukünftig als Backup oder Rollback verwenden, um den Zustand der Volume-Gruppe in einen vorherigen Zustand wiederherzustellen.

Weitere Informationen

- Erstellen Sie einen Gruppen-Snapshot
- Gruppenschnappschüsse bearbeiten
- Mitglieder des Gruppenschnappschusses bearbeiten
- Löschen eines Gruppen-Snapshots
- Rollback von Volumes zu einem Gruppen-Snapshot
- Klonen mehrerer Volumes
- Mehrere Volumes aus einem Gruppen-Snapshot klonen

Snapshot-Details gruppieren

Die Seite Snapshots gruppieren auf der Registerkarte Datenschutz enthält Informationen über die Gruppen-Snapshots.

- **ID**

  Die vom System generierte ID für den Gruppen-Snapshot.

- **UUID**

  Die eindeutige ID des Gruppen-Snapshot.

- **Name**

  Benutzerdefinierter Name für den Gruppen-Snapshot.

- **Zeit Erstellen**

  Die Zeit, zu der der Gruppenschnappschuß erstellt wurde.

- **Status**

  Der aktuelle Status des Snapshots. Mögliche Werte:

  - Vorbereiten: Der Snapshot wird gerade für die Verwendung vorbereitet und ist noch nicht beschreibbar.
  - Fertig: Diese Momentaufnahme hat die Vorbereitung abgeschlossen und ist nun nutzbar.
  - Aktiv: Der Snapshot ist der aktive Verzweig.

- **# Volumen**

  Die Anzahl der Volumes in der Gruppe.

- **Bis** Aufbewahren

  Tag und Uhrzeit des Snapshots werden gelöscht.

- **Remote-Replikation**

  Gibt an, ob der Snapshot für die Replikation auf ein Remote-SolidFire-Cluster aktiviert ist oder nicht. Mögliche Werte:

  - Aktiviert: Der Snapshot ist für die Remote-Replikation aktiviert.
  - Deaktiviert: Der Snapshot ist für die Remote-Replikation nicht aktiviert.

Erstellen eines Gruppen-Snapshots

Sie können einen Snapshot einer Gruppe von Volumes erstellen und auch einen Gruppen-Snapshot-Zeitplan zur Automatisierung von Gruppen-Snapshots erstellen. Ein Snapshot einer einzelnen Gruppe kann konsistent bis zu 32 Volumen gleichzeitig erstellen.

Schritte

1. Klicken Sie Auf **Management** > **Volumes**.
2. Wählen Sie mithilfe der Kontrollkästchen mehrere Volumes für eine Volume-Gruppe aus.
3. Klicken Sie Auf **Massenaktionen**.
4. Klicken Sie Auf **Snapshot Gruppieren**.
5. Geben Sie im Dialogfeld „Snapshot von Volumes erstellen“ einen neuen Gruppennamen für den Snapshot ein.
6. **Optional:** Aktivieren Sie das Kontrollkästchen **jedes GruppenSnapshot-Mitglied in Replikation einschließen, wenn Sie die Replikation gekoppelt haben**, um sicherzustellen, dass jeder Snapshot bei der Replikation erfasst wird, wenn das übergeordnete Volume gekoppelt ist.
7. Wählen Sie eine Aufbewahrungsoption für den Gruppen-Snapshot:
   - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
   - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnboxen, um eine Zeitdauer für das System auszuwählen, um den Snapshot zu behalten.
8. So erstellen Sie einen einzigen, sofortigen Snapshot:
   a. Klicken Sie Auf **Gruppenmomentaufnahme Jetzt Aufnehmen**.
   b. Klicken Sie Auf **Gruppenmomentaufnahme Erstellen**.
9. So planen Sie die Ausführung des Snapshots für einen späteren Zeitpunkt:
   a. Klicken Sie Auf **Snapshot-Zeitplan Der Gruppe Erstellen**.
   b. Geben Sie einen **neuen Terminplannamen** ein.
   c. Wählen Sie einen **Terminplantyp** aus der Liste aus.
   d. **Optional:** Aktivieren Sie das Kontrollkästchen **wiederkehrender Zeitplan**, um den geplanten Snapshot regelmäßig zu wiederholen.
   e. Klicken Sie Auf **Zeitplan Erstellen**.

Gruppenschnappschüsse werden bearbeitet

Sie können die Replizierungs- und Aufbewahrungseinstellungen für vorhandene Gruppen-Snapshots bearbeiten.

1. Klicken Sie Auf **Datenschutz** > **Snapshots Gruppieren**.
2. Klicken Sie auf das Aktionen-Symbol für den Gruppen-Snapshot, den Sie bearbeiten möchten.
3. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
4. **Optional:** zum Ändern der Replikationseinstellung für den Gruppenschnappschuß:
   a. Klicken Sie neben **Aktuelle Replikation** auf **Bearbeiten**.
   b. Aktivieren Sie das Kontrollkästchen **jedes Gruppenmitglied in Replikation einschließen bei Paarung**, um sicherzustellen, dass jeder Snapshot bei der Replikation erfasst wird, wenn das übergeordnete Volume gekoppelt ist.
5. **Optional:** um die Aufbewahrungseinstellung für den Gruppenschnappschuß zu ändern, wählen Sie aus den folgenden Optionen:
   a. Klicken Sie neben **Aktuelle Aufbewahrung** auf **Bearbeiten**.
   b. Wählen Sie eine Aufbewahrungsoption für den Gruppen-Snapshot:
      - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
      - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnboxen, um eine Zeitdauer für das System auszuwählen, um den Snapshot zu behalten.
6. Klicken Sie Auf **Änderungen Speichern**.

Löschen eines Gruppen-Snapshots

Sie können einen Gruppen-Snapshot aus dem System löschen. Wenn Sie den Gruppen-Snapshot löschen, können Sie auswählen, ob alle mit der Gruppe verknüpften Snapshots als einzelne Snapshots gelöscht oder beibehalten werden.

Wenn Sie ein Volume oder einen Snapshot löschen, das Mitglied eines Gruppen-Snapshots ist, können Sie nicht mehr zum Gruppen-Snapshot zurückkehren. Sie können jedoch jedes Volume einzeln zurück verschieben.

1. Klicken Sie Auf **Datenschutz** > **Snapshots Gruppieren**.
2. Klicken Sie auf das Symbol Aktionen für den zu löschenden Snapshot.
3. Klicken Sie im Menü Ergebnis auf **Löschen**.
4. Wählen Sie im Bestätigungsdialogfeld eine der folgenden Optionen aus:
   - Klicken Sie auf **GruppenSnapshot und alle Mitglieder der Gruppe löschen**, um den Gruppen-Snapshot und alle Mitglieder-Snapshots zu löschen.
   - Klicken Sie auf **GruppenSnapshot-Mitglieder als einzelne Snapshots**, um den Gruppen-Snapshot zu löschen, aber alle Mitglieder-Snapshots zu behalten.
5. Bestätigen Sie die Aktion.

Rollback von Volumes zu einem Gruppen-Snapshot

Sie können jederzeit ein Rollback einer Gruppe von Volumes zu einem Gruppen-

Snapshot durchführen.

Beim Rollback einer Gruppe von Volumes werden alle Volumes in der Gruppe in den Zustand wiederhergestellt, in dem sie sich zum Zeitpunkt der Erstellung des Gruppen-Snapshots befanden. Bei einem Rollback werden auch Volume-Größen an die Größe des ursprünglichen Snapshots wiederhergestellt. Wenn das System ein Volume bereinigt hat, wurden auch alle Snapshots des entsprechenden Volumes zum Zeitpunkt der Löschung gelöscht. Das System stellt keine gelöschten Volume-Snapshots wieder her.

1. Klicken Sie Auf **Datenschutz** > **Snapshots Gruppieren**.
2. Klicken Sie auf das Symbol Aktionen für den Gruppen-Snapshot, den Sie für das Rollback des Volumes verwenden möchten.
3. Wählen Sie im Ergebnismenü **Rollback-Volumes in Gruppenaufnahme** aus.
4. **Optional**: Zum Speichern des aktuellen Status der Volumes vor dem Rollback zum Snapshot:
   a. Wählen Sie im Dialogfeld **Rollback to Snapshot** den aktuellen Status von **Volumes speichern als GruppenSnapshot** aus.
   b. Geben Sie einen Namen für den neuen Snapshot ein.
5. Klicken Sie Auf **Rollback Group Snapshot**.

Bearbeiten von Mitgliedern des Gruppenschnappschusses

Sie können die Aufbewahrungseinstellungen für Mitglieder eines bestehenden Gruppen-Snapshots bearbeiten.

1. Klicken Sie Auf **Datenschutz** > **Snapshots**.
2. Klicken Sie auf die Registerkarte **Mitglieder**.
3. Klicken Sie auf das Aktionen-Symbol für das Gruppenmitglied, das Sie bearbeiten möchten.
4. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
5. Um die Replikationseinstellung für den Snapshot zu ändern, wählen Sie eine der folgenden Optionen aus:
   - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
   - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnboxen, um eine Zeitdauer für das System auszuwählen, um den Snapshot zu behalten.
6. Klicken Sie Auf **Änderungen Speichern**.

Klonen mehrerer Volumes

Sie können mehrere Volume-Klone in einem einzigen Vorgang erstellen, um eine zeitpunktgenaue Kopie der Daten in einer Gruppe von Volumes zu erstellen.

Wenn Sie ein Volume klonen, erstellt das System einen Snapshot des Volume und erstellt dann aus den Daten im Snapshot ein neues Volume. Sie können den neuen Volume-Klon mounten und schreiben. Das Klonen mehrerer Volumes ist ein asynchroner Prozess und erfordert eine variable Zeit, abhängig von der Größe und Anzahl der zu klonenden Volumes.

Die Volume-Größe und die aktuelle Cluster-Last beeinflussen die Zeit, die zum Abschließen eines Klonvorgangs erforderlich ist.

Schritte

1. Klicken Sie Auf **Management** > **Volumes**.
2. Klicken Sie auf die Registerkarte **Active**.
3. Aktivieren Sie die Kontrollkästchen, um mehrere Volumes auszuwählen und eine Gruppe von Volumes zu erstellen.
4. Klicken Sie Auf **Massenaktionen**.
5. Klicken Sie im resultierenden Menü auf **Clone**.
6. Geben Sie im Dialogfeld **mehrere Volumes klonen** einen **New Volume Name Prefix** ein.

   Das Präfix wird auf alle Volumes in der Gruppe angewendet.

7. **Optional:** Wählen Sie ein anderes Konto aus, zu dem der Klon gehören wird.

   Wenn Sie kein Konto auswählen, weist das System dem aktuellen Volume-Konto die neuen Volumes zu.

8. **Optional:** Wählen Sie eine andere Zugriffsmethode für die Volumes im Klon aus.

   Wenn Sie keine Zugriffsmethode auswählen, verwendet das System den aktuellen Volumenzugriff.

9. Klicken Sie Auf **Klonen Starten**.

Klonen mehrerer Volumes aus einem Gruppen-Snapshot

Sie können eine Gruppe von Volumes aus einem zeitpunktgenauen Snapshot in Gruppen klonen. Für diesen Vorgang muss bereits ein Gruppen-Snapshot der Volumes vorhanden sein, da der Gruppen-Snapshot als Basis für die Erstellung der Volumes verwendet wird. Nachdem Sie die Volumes erstellt haben, können Sie sie wie jedes andere Volume im System verwenden.

Die Volume-Größe und die aktuelle Cluster-Last beeinflussen die Zeit, die zum Abschließen eines Klonvorgangs erforderlich ist.

1. Klicken Sie Auf **Datenschutz** > **Snapshots Gruppieren**.
2. Klicken Sie auf das Aktionen-Symbol für den Gruppen-Snapshot, den Sie für die Volume-Klone verwenden möchten.
3. Wählen Sie im Menü Ergebnis die Option **Volumes aus GruppenSnapshot** klonen.
4. Geben Sie im Dialogfeld **Clone Volumes from Group Snapshot** einen **New Volume Name Prefix** ein.

   Das Präfix wird auf alle Volumes angewendet, die aus dem Gruppen-Snapshot erstellt wurden.

5. **Optional:** Wählen Sie ein anderes Konto aus, zu dem der Klon gehören wird.

   Wenn Sie kein Konto auswählen, weist das System dem aktuellen Volume-Konto die neuen Volumes zu.

6. **Optional:** Wählen Sie eine andere Zugriffsmethode für die Volumes im Klon aus.

   Wenn Sie keine Zugriffsmethode auswählen, verwendet das System den aktuellen Volumenzugriff.

7. Klicken Sie Auf **Klonen Starten**.

Planen Sie einen Snapshot

Planen Sie einen Snapshot

Sie können Daten auf einem Volume oder einer Gruppe von Volumes schützen, indem Sie die Volume Snapshots in bestimmten Intervallen planen. Sie können entweder einzelne Volume-Snapshots planen oder Snapshots gruppieren, um automatisch auszuführen.

Wenn Sie einen Snapshot-Zeitplan konfigurieren, können Sie zwischen verschiedenen Zeitabständen wählen, die auf Wochentagen oder Tagen des Monats basieren. Sie können auch Tage, Stunden und Minuten festlegen, bevor der nächste Snapshot erstellt wird. Sie können die resultierenden Snapshots auf einem Remote-Storage-System speichern, wenn das Volume repliziert wird.

Weitere Informationen

- Erstellen eines Snapshot-Zeitplans
- Bearbeiten eines Snapshot-Zeitplans
- Löschen Sie einen Snapshot-Zeitplan
- Snapshot-Zeitplan kopieren

Einzelheiten zum Snapshot Zeitplan

Auf der Seite Data Protection > Schedules können Sie die folgenden Informationen in der Liste der Snapshot-Zeitpläne anzeigen.

- **ID**

  Die vom System generierte ID für den Snapshot.

- **Typ**

  Die Art des Zeitplans. Snapshot ist derzeit der einzige Typ, der unterstützt wird.

- **Name**

  Der Name, der dem Zeitplan beim Erstellen angegeben wurde. Snapshot-Planungsnamen können bis zu 223 Zeichen lang sein und a–z, 0–9 und Bindestrich (-) Zeichen enthalten.

- **Frequenz**

  Die Häufigkeit, mit der der Zeitplan ausgeführt wird. Die Häufigkeit kann in Stunden und Minuten, Wochen oder Monaten eingestellt werden.

- **Wiederkehrend**

  Angabe, ob der Zeitplan nur einmal oder in regelmäßigen Abständen ausgeführt werden soll.

- **Manuell Angehalten**

  Gibt an, ob der Zeitplan manuell angehalten wurde oder nicht.

- **Volume-IDs**

Die ID des Volumens, das der Zeitplan bei der Ausführung des Zeitplans verwendet.

- **Letzter Lauf**

  Das letzte Mal, als der Zeitplan ausgeführt wurde.

- **Status Der Letzten Ausführung**

  Das Ergebnis der letzten Planausführung. Mögliche Werte:

  - Erfolg
  - Ausfall

Erstellen eines Snapshot-Zeitplans

Sie können einen Snapshot eines Volumes oder Volumes so planen, dass er automatisch in bestimmten Intervallen erfolgt.

Wenn Sie einen Snapshot-Zeitplan konfigurieren, können Sie zwischen verschiedenen Zeitabständen wählen, die auf Wochentagen oder Tagen des Monats basieren. Sie können auch einen wiederkehrenden Zeitplan erstellen und die Tage, Stunden und Minuten vor dem nächsten Snapshot festlegen.

Wenn Sie einen Snapshot für einen Zeitraum planen, der nicht durch 5 Minuten teilbar ist, wird der Snapshot zum nächsten Zeitraum ausgeführt, der durch 5 Minuten teilbar ist. Wenn Sie beispielsweise einen Snapshot für die Ausführung um 12:42:00 UTC planen, wird dieser um 12:45:00 UTC ausgeführt. Ein Snapshot kann nicht in Intervallen von weniger als 5 Minuten ausgeführt werden.

Ab Element 12.5 können Sie die serielle Erstellung aktivieren und auswählen, um die Snapshots von der Benutzeroberfläche aus auf FIFO-Basis (First in First out) zu behalten.

- Die Option **Serienerstellung aktivieren** gibt an, dass jeweils nur ein Snapshot repliziert wird. Die Erstellung eines neuen Snapshots schlägt fehl, wenn noch eine vorherige Snapshot-Replikation ausgeführt wird. Wenn das Kontrollkästchen nicht aktiviert ist, ist eine Snapshot-Erstellung zulässig, wenn noch eine andere Snapshot-Replikation ausgeführt wird.
- Die **FIFO** Option bietet die Möglichkeit, eine konsistente Anzahl der neuesten Snapshots zu behalten. Wenn das Kontrollkästchen aktiviert ist, werden Snapshots auf FIFO-Basis beibehalten. Nachdem die Warteschlange der FIFO-Snapshots ihre maximale Tiefe erreicht hat, wird der älteste FIFO-Snapshot verworfen, wenn ein neuer FIFO-Snapshot eingefügt wird.

Schritte

1. Wählen Sie **Data Protection** > **Schedules**.
2. Wählen Sie **Zeitplan Erstellen**.
3. Geben Sie im Feld **Volume IDs CSV** eine einzelne Volume-ID oder eine kommagetrennte Liste von Volume-IDs ein, die in den Snapshot-Vorgang aufgenommen werden sollen.
4. Geben Sie einen neuen Planungsnamen ein.
5. Wählen Sie einen Zeitplantyp aus, und legen Sie den Zeitplan aus den verfügbaren Optionen fest.
6. **Optional:** Wählen Sie **wiederkehrender Zeitplan**, um den Snapshot-Zeitplan auf unbestimmte Zeit zu wiederholen.
7. **Optional:** Geben Sie im Feld **New Snapshot Name** einen Namen für den neuen Snapshot ein.

   Wenn Sie das Feld leer lassen, verwendet das System die Uhrzeit und das Datum der Erstellung des

Snapshots als Namen.

8. **Optional:** Aktivieren Sie das Kontrollkästchen **Snapshots in Replikation einschließen bei gepaarten**, um sicherzustellen, dass die Snapshots bei der Replikation erfasst werden, wenn das übergeordnete Volume gekoppelt ist.
9. **Optional:** Aktivieren Sie das Kontrollkästchen **serielle Erstellung aktivieren**, um sicherzustellen, dass jeweils nur ein Snapshot repliziert wird.
10. Um die Aufbewahrung für den Snapshot festzulegen, wählen Sie eine der folgenden Optionen aus:
    - **Optional:** Aktivieren Sie das Kontrollkästchen **FIFO (First in First Out)**, um eine konsistente Anzahl der neuesten Snapshots zu erhalten.
    - Wählen Sie * Keep Forever* aus, um den Snapshot auf dem System für unbestimmte Zeit zu behalten.
    - Wählen Sie **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnboxen, um eine Zeitdauer für das System auszuwählen, um den Snapshot beizubehalten.
11. Wählen Sie **Zeitplan Erstellen**.

Bearbeiten eines Snapshot-Zeitplans

Sie können vorhandene Snapshot-Zeitpläne ändern. Nach der Änderung verwendet der Zeitplan bei der nächsten Ausführung die aktualisierten Attribute. Alle durch den ursprünglichen Zeitplan erstellten Snapshots verbleiben im Storage-System.

Schritte

1. Klicken Sie Auf **Datenschutz** > **Termine**.
2. Klicken Sie auf das Symbol **Aktionen** für den zu ändernden Zeitplan.
3. Klicken Sie im Menü Ergebnis auf **Bearbeiten**.
4. Ändern Sie im Feld **Volume IDs CSV** die Einzel-Volume-ID oder die kommagetrennte Liste der Volume-IDs, die derzeit im Snapshot-Vorgang enthalten sind.
5. Um den Zeitplan anzuhalten oder fortzusetzen, wählen Sie eine der folgenden Optionen aus:
    - Um einen aktiven Zeitplan anzuhalten, wählen Sie in der Liste **Zeitplan manuell anhalten** die Option **Ja** aus.
    - Um einen angehaltenen Zeitplan fortzusetzen, wählen Sie in der Liste **Zeitplan manuell anhalten** die Option **Nein** aus.
6. Geben Sie bei Bedarf einen anderen Namen für den Zeitplan im Feld **Neuer Terminplanname** ein.
7. Um den Zeitplan an verschiedenen Wochentagen oder Monaten zu ändern, wählen Sie **Terminplantyp** aus und ändern Sie den Zeitplan aus den verfügbaren Optionen.
8. **Optional:** Wählen Sie **wiederkehrender Zeitplan**, um den Snapshot-Zeitplan auf unbestimmte Zeit zu wiederholen.
9. **Optional:** Geben Sie im Feld **New Snapshot Name** den Namen für den neuen Snapshot ein oder ändern Sie diesen.

   Wenn Sie das Feld leer lassen, verwendet das System die Uhrzeit und das Datum der Erstellung des Snapshots als Namen.

10. **Optional:** Aktivieren Sie das Kontrollkästchen **Snapshots in Replikation einschließen bei gepaarten**, um sicherzustellen, dass die Snapshots bei der Replikation erfasst werden, wenn das übergeordnete Volume gekoppelt ist.

11. Um die Aufbewahrungseinstellung zu ändern, wählen Sie eine der folgenden Optionen aus:
    - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
    - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnkästen, um eine Zeitdauer für das System auszuwählen, um den Snapshot beizubehalten.
12. Klicken Sie Auf **Änderungen Speichern**.

Snapshot-Zeitplan kopieren

Sie können einen Zeitplan kopieren und dessen aktuelle Attribute beibehalten.

1. Klicken Sie Auf **Datenschutz** > **Termine**.
2. Klicken Sie auf das Symbol Aktionen für den zu kopierenden Zeitplan.
3. Klicken Sie im Menü Ergebnis auf **Kopie erstellen**.

   Das Dialogfeld **Zeitplan erstellen** wird mit den aktuellen Attributen des Zeitplans ausgefüllt.
4. **Optional:** Geben Sie einen Namen und aktualisierte Attribute für den neuen Zeitplan ein.
5. Klicken Sie Auf **Zeitplan Erstellen**.

Löschen Sie einen Snapshot-Zeitplan

Sie können einen Snapshot-Zeitplan löschen. Nach dem Löschen des Zeitplans werden keine zukünftigen geplanten Snapshots ausgeführt. Alle Snapshots, die nach diesem Zeitplan erstellt wurden, verbleiben im Storage-System.

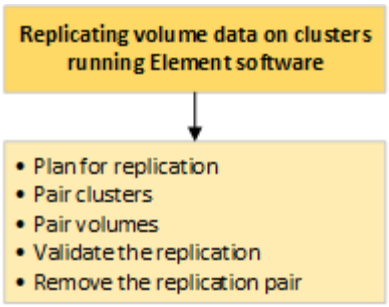
1. Klicken Sie Auf **Datenschutz** > **Termine**.
2. Klicken Sie für den zu löschenden Zeitplan auf das Symbol **Aktionen**.
3. Klicken Sie im Menü Ergebnis auf **Löschen**.
4. Bestätigen Sie die Aktion.

Remote-Replizierung zwischen Clustern mit NetApp Element Software

Remote-Replizierung zwischen Clustern mit NetApp Element Software

Bei Clustern mit Element Software ermöglicht Echtzeitreplizierung die schnelle Erstellung von Remote-Kopien von Volume-Daten. Ein Storage-Cluster kann mit bis zu vier anderen Storage-Clustern gekoppelt werden. Sie können Volume-Daten für Failover- und Failback-Szenarien synchron oder asynchron von einem Cluster in einem Cluster-Paar replizieren.

Der Replikationsprozess umfasst die folgenden Schritte:



- "Planen der Paarung von Clustern und Volumes für die Replizierung in Echtzeit"
- "Paarung von Clustern zur Replizierung"
- "Paar Volumes"
- "Volume-Replizierung validieren"
- "Löschen einer Volume-Beziehung nach der Replikation"
- "Managen Sie Volume-Beziehungen"

Planen der Paarung von Clustern und Volumes für die Replizierung in Echtzeit

Für die Echtzeitreplizierung müssen zwei Storage Cluster, auf denen Element Software ausgeführt wird, Volumes auf jedem Cluster gepaart werden und die Replizierung validiert werden. Nach Abschluss der Replikation sollten Sie die Volume-Beziehung löschen.

Was Sie benötigen

- Für ein oder beide Cluster, die gekoppelt werden, müssen Sie über Administratorrechte verfügen.
- Alle Node-IP-Adressen in Management- und Storage-Netzwerken für gepaarte Cluster werden miteinander verbunden.
- Die MTU aller verbundenen Nodes muss identisch sein und von einem End-to-End-System zwischen den Clustern unterstützt werden.
- Beide Speichercluster sollten eindeutige Cluster-Namen, MVIPs, SVIPs und alle Node-IP-Adressen haben.
- Der Unterschied zwischen den Element Software-Versionen auf den Clustern ist nicht größer als eine Hauptversion. Wenn der Unterschied größer ist, muss ein Cluster aktualisiert werden, um die Datenreplizierung durchzuführen.

> WAN Accelerator Appliances wurden von NetApp bei der Datenreplizierung nicht für den Einsatz qualifiziert. Diese Appliances beeinträchtigen die Komprimierung und Deduplizierung, wenn sie zwischen zwei Clustern, bei denen Daten repliziert werden, bereitgestellt werden. Stellen Sie sicher, dass Sie die Auswirkungen jeder WAN Accelerator Appliance vollständig qualifizieren, bevor Sie sie in einer Produktionsumgebung bereitstellen.

Weitere Informationen

- Paarung von Clustern zur Replizierung
- Paar Volumes
- Weisen Sie gepaarten Volumes eine Replikationsquelle und ein Replikationsziel zu

Paarung von Clustern zur Replizierung

Paarung von Clustern zur Replizierung

Sie müssen zwei Cluster als ersten Schritt mit der Echtzeitreplizierungsfunktion koppeln. Nachdem Sie zwei Cluster miteinander verbunden haben, können Sie aktive Volumes auf einem Cluster konfigurieren, sodass sie kontinuierlich zu einem zweiten Cluster repliziert werden. Dadurch profitieren Sie von kontinuierlicher Datensicherung (CDP).

Was Sie benötigen

- Für ein oder beide Cluster, die gekoppelt werden, müssen Sie über Administratorrechte verfügen.
- Alle Knoten-MIPs und Sips werden miteinander geroutet.
- Weniger als 2000 ms Paketumlauflatenz zwischen Clustern.
- Beide Speichercluster sollten eindeutige Cluster-Namen, MVIPs, SVIPs und alle Node-IP-Adressen haben.
- Der Unterschied zwischen den Element Software-Versionen auf den Clustern ist nicht größer als eine Hauptversion. Wenn der Unterschied größer ist, muss ein Cluster aktualisiert werden, um die Datenreplizierung durchzuführen.

> Die Cluster-Paarung erfordert eine vollständige Konnektivität zwischen den Nodes im Managementnetzwerk. Zur Replizierung ist die Verbindung zwischen den einzelnen Nodes im Storage-Cluster-Netzwerk erforderlich.

Ein Cluster kann zu bis zu vier anderen Clustern zur Replizierung von Volumes zusammengefasst werden. Sie können Cluster auch innerhalb der Cluster-Gruppe miteinander kombinieren.

Koppeln Sie Cluster mithilfe von MVIP oder einem Kopplschlüssel

Sie können ein Quell- und Zielcluster mithilfe des MVIP des Zielclusters koppeln, wenn auf beide Cluster-Administratoren Zugriff hat. Wenn der Zugriff des Cluster-Administrators nur auf einem Cluster in einem Cluster-Paar verfügbar ist, kann der Kopplungsschlüssel auf dem Ziel-Cluster verwendet werden, um die Cluster-Paarung abzuschließen.

1. Wählen Sie eine der folgenden Methoden, um Cluster zu koppeln:
   - "Koppeln Sie Cluster mit MVIP"Diese Methode ist anzuwenden, wenn auf beide Cluster ein Cluster-Administratorzugriff besteht. Bei dieser Methode wird der MVIP des entfernten Clusters verwendet, um zwei Cluster zu koppeln.
   - "Koppeln Sie Cluster mithilfe eines Kopplschlüssels"Verwenden Sie diese Methode, wenn der Clusteradministrator nur auf einen der Cluster Zugriff hat. Diese Methode generiert einen Kopplungsschlüssel, der auf dem Zielcluster verwendet werden kann, um die Clusterkopplung abzuschließen.

Weitere Informationen

Anforderungen an Netzwerk-Ports

Koppeln Sie Cluster mit MVIP

Sie können zwei Cluster für die Echtzeitreplikation koppeln, indem Sie das MVIP eines Clusters verwenden, um eine Verbindung mit dem anderen Cluster herzustellen. Der Zugriff auf beide Cluster-Administratoren ist zur Verwendung dieser Methode erforderlich.

Der Clusteradministrator-Benutzername und das Passwort werden zur Authentifizierung des Clusterzugriffs verwendet, bevor die Cluster gekoppelt werden können.

1. Wählen Sie auf dem lokalen Cluster die Option **Data Protection** > **Cluster Pairs** aus.
2. Klicken Sie Auf **Cluster-Paare**.
3. Klicken Sie auf **Pairing starten** und klicken Sie auf **Ja**, um anzuzeigen, dass Sie Zugriff auf den Remote-Cluster haben.
4. Geben Sie die MVIP-Adresse des Remote-Clusters ein.
5. Klicken Sie auf **Pairing auf Remote Cluster abschließen**.

   Geben Sie im Fenster **Authentifizierung erforderlich** den Cluster Administrator Benutzernamen und das Kennwort des Remote-Clusters ein.
6. Wählen Sie auf dem Remote-Cluster die Option **Data Protection** > **Cluster Pairs** aus.
7. Klicken Sie Auf **Cluster-Paare**.
8. Klicken Sie Auf **Pairing Abschließen**.
9. Klicken Sie auf die Schaltfläche * Pairing abschließen*.

Weitere Informationen

- Koppeln Sie Cluster mithilfe eines Kopplschlüssels
- "Koppeln von Clustern mithilfe von MVIP (Video)"

Koppeln Sie Cluster mithilfe eines Kopplschlüssels

Wenn Sie Zugriff auf einen Cluster-Administrator auf ein lokales Cluster, jedoch nicht auf das Remote-Cluster haben, können Sie die Cluster mithilfe eines Kopplungsschlüssels koppeln. Ein Kopplungsschlüssel wird auf einem lokalen Cluster generiert und dann sicher an einen Cluster-Administrator an einem Remote-Standort gesendet, um eine Verbindung herzustellen und die Cluster-Paarung zur Echtzeitreplizierung abzuschließen.

1. Wählen Sie auf dem lokalen Cluster die Option **Data Protection** > **Cluster Pairs** aus.
2. Klicken Sie Auf **Cluster-Paare**.
3. Klicken Sie auf **Pairing starten** und klicken Sie auf **Nein**, um anzuzeigen, dass Sie keinen Zugriff auf das Remote-Cluster haben.
4. Klicken Sie Auf **Schlüssel Generieren**.

   Diese Aktion generiert einen Textschlüssel für das Pairing und erstellt ein nicht konfiguriertes Clusterpaar auf dem lokalen Cluster. Wenn Sie den Vorgang nicht abschließen, müssen Sie das Cluster-Paar manuell löschen.
5. Kopieren Sie den Cluster-Kopplungsschlüssel in die Zwischenablage.
6. Der Kopplungsschlüssel kann dem Clusteradministrator am Remote-Cluster-Standort zugänglich gemacht werden.

Der Cluster-Kopplungsschlüssel enthält eine Version des MVIP, Benutzernamen, Kennwort und Datenbankinformationen, um Volume-Verbindungen für die Remote-Replikation zu ermöglichen. Dieser Schlüssel sollte sicher behandelt werden und nicht so gespeichert werden, dass ein versehentlicher oder ungesicherter Zugriff auf den Benutzernamen oder das Kennwort möglich wäre.

Ändern Sie keine Zeichen im Kopplungsschlüssel. Der Schlüssel wird ungültig, wenn er geändert wird.

7. Wählen Sie auf dem Remote-Cluster die Option **Data Protection** > **Cluster Pairs** aus.
8. Klicken Sie Auf **Cluster-Paare**.
9. Klicken Sie auf **Pairing abschließen** und geben Sie den Kopplungschlüssel in das Feld * Pairing Key* ein (Paste ist die empfohlene Methode).
10. Klicken Sie Auf **Pairing Abschließen**.

Weitere Informationen

- Koppeln Sie Cluster mit MVIP
- "Koppeln von Clustern mithilfe eines Cluster-Kopplungsschlüssels (Video)"

Überprüfen Sie die Verbindung des Cluster-Paars

Nach Abschluss der Cluster-Paarung möchten Sie möglicherweise die Verbindung zum Cluster-Paar überprüfen, um den Erfolg der Replizierung zu gewährleisten.

1. Wählen Sie auf dem lokalen Cluster die Option **Data Protection** > **Cluster Pairs** aus.
2. Überprüfen Sie im Fenster **Cluster-Paare**, ob das Cluster-Paar verbunden ist.
3. **Optional:** Navigieren Sie zurück zum lokalen Cluster und dem Fenster **Cluster Pairs** und überprüfen Sie, ob das Cluster-Paar verbunden ist.

Paar Volumes

Paar Volumes

Nachdem Sie eine Verbindung zwischen den Clustern in einem Cluster-Paar hergestellt haben, können Sie ein Volume auf einem Cluster mit einem Volume auf dem anderen Cluster des Paars koppeln. Wenn eine Volume-Pairing-Beziehung aufgebaut ist, müssen Sie angeben, welches Volume das Replikationsziel ist.

Sie können zwei Volumes für Echtzeitreplizierung kombinieren, die auf verschiedenen Storage-Clustern in einem verbundenen Cluster-Paar gespeichert sind. Nachdem Sie zwei Cluster miteinander verbunden haben, können Sie aktive Volumes auf einem Cluster konfigurieren, um kontinuierlich auf ein zweites Cluster zu replizieren. Dadurch erhalten Sie kontinuierliche Datensicherung (CDP). Sie können auch ein Volume als Quelle oder Ziel der Replikation zuweisen.

Volume-Paarungen sind immer eins zu eins. Nachdem ein Volume Teil einer Verbindung mit einem Volume auf einem anderen Cluster ist, können Sie es nicht mehr mit einem anderen Volume koppeln.

Was Sie benötigen

- Sie haben eine Verbindung zwischen Clustern in einem Cluster-Paar hergestellt.
- Sie haben Cluster-Administratorrechte für ein oder beide Cluster, die gekoppelt werden.

Schritte

1. Erstellung eines Ziel-Volumes mit Lese- oder Schreibzugriff
2. Koppeln von Volumes mithilfe einer Volume-ID oder eines Kopplungsschlüssels
3. Weisen Sie gepaarten Volumes eine Replikationsquelle und ein Replikationsziel zu

Erstellung eines Ziel-Volumes mit Lese- oder Schreibzugriff

Der Replikationsprozess umfasst zwei Endpunkte: Das Quell- und das Ziel-Volume. Wenn Sie das Ziel-Volume erstellen, wird das Volume automatisch auf den Lese-/Schreibmodus gesetzt, um die Daten während der Replikation zu akzeptieren.

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie Auf **Volume Erstellen**.
3. Geben Sie im Dialogfeld Neues Volume erstellen den Volume-Namen ein.
4. Geben Sie die Gesamtgröße des Volumes ein, wählen Sie eine Blockgröße für das Volume und wählen Sie das Konto aus, das Zugriff auf das Volume haben soll.
5. Klicken Sie Auf **Volume Erstellen**.
6. Klicken Sie im Fenster „aktiv“ auf das Aktionen-Symbol für das Volume.
7. Klicken Sie Auf **Bearbeiten**.
8. Ändern Sie die Kontozugriffsebene auf Replikationsziel.
9. Klicken Sie Auf **Änderungen Speichern**.

Koppeln von Volumes mithilfe einer Volume-ID oder eines Kopplungsschlüssels

Kombinieren Sie Volumes mit einer Volume-ID

Sie können ein Volume mit einem anderen Volume auf einem Remote-Cluster koppeln, wenn Sie über Cluster-Administratorrechte für beide Cluster verfügen, auf denen die Volumes gekoppelt werden sollen. Bei dieser Methode wird die Volume-ID des Volumes auf dem Remote-Cluster verwendet, um eine Verbindung herzustellen.

Was Sie benötigen

- Stellen Sie sicher, dass die Cluster, die die Volumes enthalten, gekoppelt sind.
- Erstellen Sie ein neues Volume auf dem Remote-Cluster.

> Sie können eine Replikationsquelle und ein Replikationsziel nach dem Pairing-Prozess zuweisen. Eine Replikationsquelle oder ein Replikationsziel kann ein Volume in einem Volume-Paar sein. Sie sollten ein Ziel-Volume erstellen, das keine Daten enthält und exakt die Merkmale des Quell-Volume hat, z. B. Größe, Einstellung der Blockgröße für die Volumes (512 oder 4 kb) und QoS-Konfiguration. Wenn Sie ein vorhandenes Volume als Replikationsziel zuweisen, werden die Daten auf diesem Volume überschrieben. Das Zielvolume kann größer oder gleich groß sein wie das Quellvolume, kann aber nicht kleiner sein.

- Die Ziel-Volume-ID kennen.

Schritte

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie auf das Symbol **Aktionen** für das Volume, das Sie koppeln möchten.
3. Klicken Sie Auf **Paar**.
4. Wählen Sie im Dialogfeld **Pair Volume** die Option **Pairing starten** aus.
5. Wählen Sie **i do** aus, um anzugeben, dass Sie Zugriff auf den Remote-Cluster haben.
6. Wählen Sie aus der Liste einen **Replikationsmodus** aus:
   - **Echtzeit (Asynchron)**: Schreibvorgänge werden dem Client bestätigt, nachdem sie auf dem Quellcluster erstellt wurden.
   - **Real-Time (Synchronous)**: Schreibvorgänge werden dem Client bestätigt, nachdem sie sowohl auf den Quell- als auch auf den Ziel-Clustern festgelegt sind.
   - **Nur Snapshots**: Nur Snapshots, die auf dem Quellcluster erstellt wurden, werden repliziert. Aktive Schreibvorgänge vom Quell-Volume werden nicht repliziert.
7. Wählen Sie aus der Liste einen Remote-Cluster aus.
8. Wählen Sie eine Remote-Volume-ID aus.
9. Klicken Sie Auf **Pairing Starten**.

   Das System öffnet eine Webbrowser-Registerkarte, die eine Verbindung mit der Element-UI des Remote-Clusters herstellt. Unter Umständen müssen Sie sich mit den Anmeldedaten des Cluster-Administrators im Remote-Cluster anmelden.

10. Wählen Sie in der Element-UI des Remote-Clusters die Option **Complete Pairing**.
11. Bestätigen Sie die Details unter **Volume Pairing bestätigen**.
12. Klicken Sie Auf **Pairing Abschließen**.

    Nachdem Sie die Paarung bestätigt haben, beginnen die beiden Cluster den Prozess, die Volumes zum Koppeln zu verbinden. Während des Pairings können Sie Meldungen in der Spalte **Volume Status** des Fensters **Volume Pairs** sehen. Das Volume-Paar wird angezeigt `PausedMisconfigured` Bis die Quelle und das Ziel des Volume-Paars zugewiesen sind.

    Nach erfolgreichem Abschluss der Paarung wird empfohlen, die Volumetabelle zu aktualisieren, um die **Pair**-Option aus der **Aktionen**-Liste für das gepaarte Volumen zu entfernen. Wenn Sie die Tabelle nicht aktualisieren, bleibt die Option **Paar** zur Auswahl verfügbar. Wenn Sie die Option **Pair** erneut auswählen, wird eine neue Registerkarte geöffnet, und da das Volume bereits gekoppelt ist, meldet das System einen `StartVolumePairing Failed: xVolumeAlreadyPaired` Fehlermeldung im Fenster **Pair Volume** der Element UI Seite.

Weitere Informationen

- Meldungen zur Volume-Kopplung
- Warnungen zum Volume-Pairing
- Weisen Sie gepaarten Volumes eine Replikationsquelle und ein Replikationsziel zu

Koppeln von Volumes mithilfe eines Kopplschlüssels

Wenn Sie nur über Clusteradministratorzugriff auf den Quellcluster verfügen (Sie besitzen keine Clusteradministrator-Anmeldeinformationen für einen Remotecluster), können Sie ein Volume mit einem anderen Volume auf einem Remotecluster mithilfe eines Kopplungsschlüssels koppeln.

Was Sie benötigen

- Stellen Sie sicher, dass die Cluster, die die Volumes enthalten, gekoppelt sind.
- Stellen Sie sicher, dass auf dem Remote-Cluster ein Volume zum Koppeln vorhanden ist.

> Sie können eine Replikationsquelle und ein Replikationsziel nach dem Pairing-Prozess zuweisen. Eine Replikationsquelle oder ein Replikationsziel kann ein Volume in einem Volume-Paar sein. Sie sollten ein Ziel-Volume erstellen, das keine Daten enthält und exakt die Merkmale des Quell-Volume hat, z. B. Größe, Einstellung der Blockgröße für die Volumes (512 oder 4 kb) und QoS-Konfiguration. Wenn Sie ein vorhandenes Volume als Replikationsziel zuweisen, werden die Daten auf diesem Volume überschrieben. Das Zielvolume kann größer oder gleich groß sein wie das Quellvolume, kann aber nicht kleiner sein.

Schritte

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie auf das Symbol **Aktionen** für das Volume, das Sie koppeln möchten.
3. Klicken Sie Auf **Paar**.
4. Wählen Sie im Dialogfeld **Pair Volume** die Option **Pairing starten** aus.
5. Wählen Sie * Ich nicht* aus, um anzugeben, dass Sie keinen Zugriff auf den Remote-Cluster haben.
6. Wählen Sie aus der Liste einen **Replikationsmodus** aus:
   - **Echtzeit (Asynchron)**: Schreibvorgänge werden dem Client bestätigt, nachdem sie auf dem Quellcluster erstellt wurden.
   - **Real-Time (Synchronous)**: Schreibvorgänge werden dem Client bestätigt, nachdem sie sowohl auf den Quell- als auch auf den Ziel-Clustern festgelegt sind.
   - **Nur Snapshots**: Nur Snapshots, die auf dem Quellcluster erstellt wurden, werden repliziert. Aktive Schreibvorgänge vom Quell-Volume werden nicht repliziert.
7. Klicken Sie Auf **Schlüssel Generieren**.

> Diese Aktion generiert einen Textschlüssel für das Koppeln und erstellt ein nicht konfiguriertes Volume-Paar auf dem lokalen Cluster. Wenn Sie den Vorgang nicht abschließen, müssen Sie das Volume-Paar manuell löschen.

8. Kopieren Sie den Kopplungsschlüssel in die Zwischenablage Ihres Computers.
9. Der Kopplungsschlüssel kann dem Cluster-Administrator am Remote-Cluster-Standort zugänglich gemacht werden.

> Der Volume-Kopplungsschlüssel sollte sicher behandelt werden und nicht so verwendet werden, dass ein versehentlicher oder ungesicherter Zugriff möglich wäre.

Ändern Sie keine Zeichen im Kopplungsschlüssel. Der Schlüssel wird ungültig, wenn er geändert wird.

10. Wählen Sie in der Remote Cluster Element UI die Option **Management** > **Volumes** aus.
11. Klicken Sie auf das Aktionen-Symbol für das Volume, das Sie koppeln möchten.
12. Klicken Sie Auf **Paar**.
13. Wählen Sie im Dialogfeld **Pair Volume** die Option **Complete Pairing** aus.
14. Fügen Sie den Kopplschlüssel aus dem anderen Cluster in die Box **Pairing Key** ein.
15. Klicken Sie Auf **Pairing Abschließen**.

    Nachdem Sie die Paarung bestätigt haben, beginnen die beiden Cluster den Prozess, die Volumes zum Koppeln zu verbinden. Während des Pairings können Sie Meldungen in der Spalte **Volume Status** des Fensters **Volume Pairs** sehen. Das Volume-Paar wird angezeigt `PausedMisconfigured` Bis die Quelle und das Ziel des Volume-Paars zugewiesen sind.

    Nach erfolgreichem Abschluss der Paarung wird empfohlen, die Volumetabelle zu aktualisieren, um die **Pair**-Option aus der **Aktionen**-Liste für das gepaarte Volumen zu entfernen. Wenn Sie die Tabelle nicht aktualisieren, bleibt die Option **Paar** zur Auswahl verfügbar. Wenn Sie die Option **Pair** erneut auswählen, wird eine neue Registerkarte geöffnet, und da das Volume bereits gekoppelt ist, meldet das System einen `StartVolumePairing Failed: xVolumeAlreadyPaired` Fehlermeldung im Fenster **Pair Volume** der Element UI Seite.

Weitere Informationen

- Meldungen zur Volume-Kopplung
- Warnungen zum Volume-Pairing
- Weisen Sie gepaarten Volumes eine Replikationsquelle und ein Replikationsziel zu

Weisen Sie gepaarten Volumes eine Replikationsquelle und ein Replikationsziel zu

Nachdem Volumes gekoppelt wurden, müssen Sie ein Quell-Volume und sein Replikationsziel-Volume zuweisen. Eine Replikationsquelle oder ein Replikationsziel kann ein Volume in einem Volume-Paar sein. Sie können dieses Verfahren auch verwenden, um Daten, die an ein Quell-Volume gesendet werden, zu einem Remote-Ziel-Volume umzuleiten, falls das Quell-Volume nicht mehr verfügbar ist.

Was Sie benötigen

Sie haben Zugriff auf die Cluster, die die Quell- und Ziel-Volumes enthalten.

Schritte

1. Vorbereiten des Quellvolumens:

    a. Wählen Sie aus dem Cluster, der das Volume enthält, das Sie als Quelle zuweisen möchten, **Management** > **Volumes** aus.

    b. Klicken Sie auf das Symbol **Aktionen** für das Volume, das Sie als Quelle zuweisen möchten, und klicken Sie auf **Bearbeiten**.

    c. Wählen Sie in der Dropdown-Liste **Zugriff** die Option **Lesen/Schreiben** aus.

Wenn Sie die Quell- und Zielzuweisung umkehren, führt diese Aktion dazu, dass das Volume-Paar die folgende Meldung anzeigt, bis ein neues Replikationsziel zugewiesen ist: `PausedMisconfigured`

Durch das Ändern des Zugriffs wird die Volume-Replizierung angehalten, und die Datenübertragung wird beendet. Vergewissern Sie sich, dass Sie diese Änderungen an beiden Standorten koordiniert haben.

a. Klicken Sie Auf **Änderungen Speichern**.

2. Bereiten Sie das Zielvolumen vor:
   a. Wählen Sie aus dem Cluster, der das Volume enthält, das Sie als Ziel zuweisen möchten, **Management** > **Volumes** aus.
   b. Klicken Sie auf das Aktionen-Symbol für das Volume, das Sie als Ziel zuweisen möchten, und klicken Sie auf **Bearbeiten**.
   c. Wählen Sie in der Dropdown-Liste **Zugriff** die Option **Replikationsziel** aus.

Wenn Sie ein vorhandenes Volume als Replikationsziel zuweisen, werden die Daten auf diesem Volume überschrieben. Es sollte ein neues Ziel-Volume verwendet werden, das keine Daten enthält und exakt die Merkmale des Quell-Volume hat, z. B. Größe, 512-e-Einstellung und QoS-Konfiguration. Das Zielvolume kann größer oder gleich groß sein wie das Quellvolume, kann aber nicht kleiner sein.

   d. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

- Kombinieren Sie Volumes mit einer Volume-ID
- Koppeln von Volumes mithilfe eines Kopplschlüssels

Volume-Replizierung validieren

Nach der Replizierung eines Volumes sollten Sie sicherstellen, dass die Quell- und Ziel-Volumes aktiv sind. Im aktiven Zustand werden Volumes gekoppelt. Die Daten werden vom Quell- an das Ziel-Volume gesendet, und die Daten werden im synchronen Modus gespeichert.

1. Wählen Sie in beiden Clustern die Option **Datenschutz** > **Volume Pairs** aus.
2. Vergewissern Sie sich, dass der Volume-Status aktiv ist.

Weitere Informationen

Warnungen zum Volume-Pairing

Löschen einer Volume-Beziehung nach der Replikation

Nachdem die Replikation abgeschlossen ist und Sie die Volume-Paar-Beziehung nicht mehr benötigen, können Sie die Volume-Beziehung löschen.

1. Wählen Sie **Data Protection** > **Volume Pairs**.
2. Klicken Sie auf das Symbol **Aktionen** für das Volume-Paar, das Sie löschen möchten.

3. Klicken Sie Auf **Löschen**.
4. Bestätigen Sie die Meldung.

Managen Sie Volume-Beziehungen

Unterbrechen Sie die Replikation

Sie können die Replizierung manuell unterbrechen, wenn Sie die I/O-Verarbeitung für kurze Zeit anhalten müssen. Möglicherweise möchten Sie die Replizierung unterbrechen, wenn die I/O-Verarbeitung stark zulasten und die Verarbeitungslast reduzieren soll.

1. Wählen Sie **Data Protection** > **Volume Pairs**.
2. Klicken Sie auf das Aktionen-Symbol für das Volume-Paar.
3. Klicken Sie Auf **Bearbeiten**.
4. Im Fensterbereich **Volume Pair bearbeiten** wird der Replikationsprozess manuell angehalten.

> Wenn Sie die Volume-Replikation manuell unterbrechen oder fortsetzen, wird die Übertragung der Daten beendet oder fortgesetzt. Vergewissern Sie sich, dass Sie diese Änderungen an beiden Standorten koordiniert haben.

5. Klicken Sie Auf **Änderungen Speichern**.

Ändern Sie den Modus der Replikation

Sie können die Volume-Paar-Eigenschaften bearbeiten, um den Replikationsmodus der Volume-Paar-Beziehung zu ändern.

1. Wählen Sie **Data Protection** > **Volume Pairs**.
2. Klicken Sie auf das Aktionen-Symbol für das Volume-Paar.
3. Klicken Sie Auf **Bearbeiten**.
4. Wählen Sie im Fensterbereich **Volume Pair bearbeiten** einen neuen Replikationsmodus aus:
   - **Echtzeit (Asynchron)**: Schreibvorgänge werden dem Client bestätigt, nachdem sie auf dem Quellcluster erstellt wurden.
   - **Real-Time (Synchronous)**: Schreibvorgänge werden dem Client bestätigt, nachdem sie sowohl auf den Quell- als auch auf den Ziel-Clustern festgelegt sind.
   - **Nur Snapshots**: Nur Snapshots, die auf dem Quellcluster erstellt wurden, werden repliziert. Aktive Schreibvorgänge vom Quell-Volume werden nicht repliziert. **Achtung:** die Änderung der Replikationsmodus ändert den Modus sofort. Vergewissern Sie sich, dass Sie diese Änderungen an beiden Standorten koordiniert haben.
5. Klicken Sie Auf **Änderungen Speichern**.

Volume-Paare löschen

Sie können ein Volume-Paar löschen, wenn Sie eine Paarverbindung zwischen zwei Volumes entfernen möchten.

1. Wählen Sie **Data Protection** > **Volume Pairs**.

2. Klicken Sie auf das Aktionen-Symbol für das Volume-Paar, das Sie löschen möchten.
3. Klicken Sie Auf **Löschen**.
4. Bestätigen Sie die Meldung.

Löschen eines Cluster-Paares

Sie können ein Cluster-Paar aus der Element-UI eines der Cluster im Paar löschen.

1. Klicken Sie Auf **Data Protection** > **Cluster Pairs**.
2. Auf das Aktionen-Symbol für ein Cluster-Paar klicken.
3. Klicken Sie im Menü Ergebnis auf **Löschen**.
4. Bestätigen Sie die Aktion.
5. Führen Sie die Schritte im zweiten Cluster in der Cluster-Paarung erneut aus.

Details zu dem Cluster-Paar

Die Seite Cluster-Paare auf der Registerkarte Datenschutz enthält Informationen zu Clustern, die gekoppelt wurden oder gerade gekoppelt werden. Das System zeigt Pairing- und Fortschrittsmeldungen in der Spalte Status an.

- **ID**

  Eine systemgenerierte ID für die einzelnen Cluster-Paare:

- **Remote Cluster Name**

  Der Name des anderen Clusters im Paar.

- * Remote MVIP*

  Die virtuelle Management-IP-Adresse des anderen Clusters im Paar.

- **Status**

  Replikationsstatus des Remote-Clusters

- **Replikation Von Volumes**

  Die Anzahl der Volumes des Clusters, die zur Replizierung gepaart werden.

- **UUID**

  Eine eindeutige ID, die jedem Cluster im Paar gegeben wurde.

Volumenpaare

Details zu Volume-Paaren

Die Seite Volume Pairs auf der Registerkarte Data Protection enthält Informationen zu Volumes, die gekoppelt wurden oder gerade gekoppelt werden. Das System zeigt Pairing- und Fortschrittsmeldungen in der Spalte Volume-Status an.

- **ID**

  Vom System generierte ID für das Volume:

- **Name**

  Der Name, der dem Volume bei seiner Erstellung gegeben wurde. Volume-Namen können bis zu 223 Zeichen lang sein und A-z, 0-9 und Bindestrich (-) enthalten.

- **Konto**

  Name des Kontos, der dem Volume zugewiesen wurde.

- **Volume-Status**

  Replikationsstatus des Volumes

- **Snapshot-Status**

  Status des Snapshot-Volumes.

- **Modus**

  Die Client-Schreibreplikationsmethode. Folgende Werte sind möglich:

  - Asynchron
  - Nur Snapshot
  - Synchron

- **Richtung**

  Richtung der Volume-Daten:

  - Quell-Volume-Symbol (→) Gibt an, dass Daten auf ein Ziel außerhalb des Clusters geschrieben werden.
  - Zielvolume-Symbol (←) Gibt an, dass Daten von einer externen Quelle auf das lokale Volume geschrieben werden.

- **Async Verzögerung**

  Dauer, seit das Volume zuletzt mit dem Remote-Cluster synchronisiert wurde. Wenn das Volume nicht gekoppelt ist, ist der Wert Null.

- * Remote Cluster*

  Name des Remote-Clusters, auf dem sich das Volume befindet.

- **Remote Volume ID**

  Volume-ID des Volumes im Remote-Cluster.

- **Remote Volume Name**

  Name, der dem Remotecomputer bei seiner Erstellung gegeben wurde.

Meldungen zur Volume-Kopplung

Sie können die Meldungen zur Volume-Kopplung während des ersten Pairing-Prozesses auf der Seite Volume Pairs auf der Registerkarte Data Protection anzeigen. Diese Meldungen können sowohl am Quell- als auch am Zielende des Paares in der Listenansicht „replizierte Volumes“ angezeigt werden.

- **PausedDisconnected**

  Zeitüberschreitung bei der Quellreplizierung oder Synchronisierung von RPCs. Die Verbindung zum Remote-Cluster wurde unterbrochen. Überprüfen Sie die Netzwerkverbindungen mit dem Cluster.

- **ResumingConnected**

  Die Synchronisierung der Remote-Replizierung ist jetzt aktiv. Mit dem Synchronisierungsprozess beginnen und auf Daten warten.

- **ResumingRRSync**

  Dem gekoppelten Cluster wird eine einzige Helix Kopie der Volume-Metadaten erstellt.

- **ResumingLocalSync**

  Dem gekoppelten Cluster wird eine doppelte Helix Kopie der Volume-Metadaten erstellt.

- **ResumingDataTransfer**

  Die Datenübertragung wurde fortgesetzt.

- * Aktiv*

  Volumes werden gekoppelt und Daten werden vom Quell-Volume an das Ziel-Volume gesendet, und die Daten werden synchron.

- **Frei**

  Es findet keine Replikationsaktivität statt.

Warnungen zum Volume-Pairing

Die Seite Thevolme Pairs auf der Registerkarte Datenschutz enthält diese Meldungen, nachdem Sie Volumes gepaart haben. Diese Meldungen können an den Quell- und Zielenden des Paares (sofern nicht anders angegeben) in der Listenansicht „replizierte Volumes“ angezeigt werden.

- * PausedClusterFull*

  Da das Ziel-Cluster voll ist, können die Quell-Replizierung und der Transfer von Massendaten nicht fortgesetzt werden. Die Meldung wird nur am Quellende des Paares angezeigt.

- **PausedExceedMaxSnapshotCount**

  Das Ziel-Volume verfügt bereits über die maximale Anzahl an Snapshots und kann keine zusätzlichen Snapshots replizieren.

- **PausedManual**

  Lokales Volume wurde manuell angehalten. Sie muss aufgehoben werden, bevor die Replikation fortgesetzt wird.

- **PausedManualRemote**

  Fernlautstärke befindet sich im manuellen Paused-Modus. Um das Remote-Volume vor dem Fortschreiten der Replikation zu unterbrechen, ist ein manueller Eingriff erforderlich.

- **PausedUnkonfiguriert**

  Warten auf eine aktive Quelle und ein aktives Ziel. Manuelle Eingriffe sind erforderlich, um die Replikation fortzusetzen.

- **PausedQoS**

  Ziel-QoS konnte eingehende I/O nicht aufrechterhalten. Automatische Wiederaufnahme der Replikation. Die Meldung wird nur am Quellende des Paares angezeigt.

- **PausedSlowLink**

  Langsame Verbindung wurde erkannt und die Replikation wurde angehalten. Automatische Wiederaufnahme der Replikation. Die Meldung wird nur am Quellende des Paares angezeigt.

- **PausedVolumeSizeMischmatch**

  Das Ziel-Volume ist nicht dieselbe Größe wie das Quell-Volume.

- **PausedXCopy**

  Ein SCSI XCOPY-Befehl wird an ein Quell-Volume übergeben. Der Befehl muss abgeschlossen sein, bevor die Replikation fortgesetzt werden kann. Die Meldung wird nur am Quellende des Paares angezeigt.

- **StoppedMiskonfiguriert**

  Es wurde ein permanenter Konfigurationsfehler erkannt. Das entfernte Volume wurde gelöscht oder entpaart. Es ist keine Korrekturmaßnahme möglich; es muss eine neue Paarung eingerichtet werden.

SnapMirror Replizierung zwischen Element und ONTAP Clustern (Element UI) verwenden

SnapMirror Replizierung zwischen Element und ONTAP Clustern (Element UI) verwenden

Sie können SnapMirror Beziehungen auf der Registerkarte Datensicherheit in der NetApp Element Benutzeroberfläche erstellen. Um dies in der Benutzeroberfläche zu sehen, muss die SnapMirror Funktionalität aktiviert sein.

IPv6 wird für die SnapMirror Replizierung zwischen NetApp Element Software und ONTAP Clustern nicht unterstützt.

"NetApp Video: SnapMirror für NetApp HCI und Element Software"

Systeme mit NetApp Element Software unterstützen SnapMirror Funktionen zum Kopieren und

Wiederherstellen von Snapshot Kopien mit NetApp ONTAP Systemen. Der Hauptgrund für den Einsatz dieser Technologie ist die Disaster Recovery von NetApp HCI auf ONTAP. Endpunkte sind ONTAP, ONTAP Select und Cloud Volumes ONTAP. Siehe TR-4641 NetApp HCI Datensicherung.

"Technischer Bericht 4641 zu NetApp HCI Datensicherung"

Weitere Informationen

- "Ihr Weg zur eigenen Data Fabric – mit NetApp HCI, ONTAP und konvergenter Infrastruktur"
- "Replizierung zwischen NetApp Element Software und ONTAP (ONTAP CLI)"

Übersicht über SnapMirror

Systeme mit NetApp Element Software unterstützen SnapMirror Funktionen zum Kopieren und Wiederherstellen von Snapshots mit NetApp ONTAP Systemen.

Systeme mit Element können direkt mit SnapMirror auf ONTAP Systemen ab 9.3 kommunizieren. Die NetApp Element API bietet Methoden zur Aktivierung der SnapMirror Funktion in Clustern, Volumes und Snapshots. Außerdem verfügt die Element UI über alle erforderlichen Funktionen zum Management von SnapMirror Beziehungen zwischen Element Software und ONTAP Systemen.

Von ONTAP stammende Volumes können in bestimmten Anwendungsfällen mit eingeschränkter Funktionalität zu Element Volumes repliziert werden. Weitere Informationen finden Sie unter "Replizierung zwischen Element Software und ONTAP (ONTAP CLI)".

Aktivieren Sie SnapMirror auf dem Cluster

Sie müssen die SnapMirror Funktion auf Cluster-Ebene manuell über die NetApp Element UI aktivieren. Im System ist die SnapMirror Funktion standardmäßig deaktiviert und wird im Rahmen einer neuen Installation oder eines Upgrades nicht automatisch aktiviert. Die Aktivierung der SnapMirror Funktion ist eine einmalige Konfigurationsaufgabe.

SnapMirror kann nur für Cluster aktiviert werden, auf denen Element Software in Verbindung mit Volumes auf einem NetApp ONTAP System verwendet wird. Sie sollten die SnapMirror Funktion nur aktivieren, wenn Ihr Cluster zur Verwendung mit NetApp ONTAP Volumes verbunden ist.

Was Sie benötigen

Der Storage Cluster muss die NetApp Element Software ausführen.

Schritte

1. Klicken Sie Auf **Cluster** > **Einstellungen**.
2. Suchen Sie die Cluster-spezifischen Einstellungen für SnapMirror.
3. Klicken Sie auf **SnapMirror aktivieren**.

   Durch die Aktivierung der SnapMirror Funktion wird die Konfiguration der Element Software endgültig geändert. Sie können die SnapMirror Funktion deaktivieren und nur die Standardeinstellungen wiederherstellen, indem Sie das Cluster wieder zum Werkseinstellungen zurücksetzen.

4. Klicken Sie auf **Ja**, um die SnapMirror-Konfigurationsänderung zu bestätigen.

Aktivieren Sie SnapMirror auf dem Volume

Sie müssen SnapMirror auf dem Volume in der Element UI aktivieren. Dies ermöglicht die Replikation von Daten auf festgelegte ONTAP-Volumes. Dies ist die Erlaubnis des Administrators des Clusters, auf dem die NetApp Element Software für SnapMirror ausgeführt wird, um ein Volume zu steuern.

Was Sie benötigen

- Sie haben SnapMirror in der Element UI für das Cluster aktiviert.
- Ein SnapMirror Endpunkt ist verfügbar.
- Das Volume muss mit einer Blockgröße von 512 E liegen.
- Das Volume ist nicht an der Remote-Replikation beteiligt.
- Der Volume-Zugriffstyp ist kein Replikationsziel.

Sie können diese Eigenschaft auch beim Erstellen oder Klonen eines Volumes festlegen.

Schritte

1. Klicken Sie Auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol **Aktionen** für das Volume, für das Sie SnapMirror aktivieren möchten.
3. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
4. Aktivieren Sie im Dialogfeld **Volume bearbeiten** das Kontrollkästchen **SnapMirror aktivieren**.
5. Klicken Sie Auf **Änderungen Speichern**.

Erstellen eines SnapMirror Endpunkts

Sie müssen einen SnapMirror Endpunkt in der NetApp Element-Benutzeroberfläche erstellen, bevor Sie eine Beziehung erstellen können.

Ein SnapMirror Endpunkt ist ein ONTAP Cluster, das als Replizierungsziel für ein Cluster dient, auf dem die Element Software ausgeführt wird. Bevor Sie eine SnapMirror Beziehung erstellen, erstellen Sie zuerst einen SnapMirror Endpunkt.

Es können bis zu vier SnapMirror Endpunkte in einem Storage-Cluster, auf dem die Element Software ausgeführt wird, erstellt und gemanagt werden.

Wenn ein vorhandener Endpunkt ursprünglich mit der API erstellt wurde und keine Anmeldedaten gespeichert wurden, können Sie den Endpunkt in der Element-UI sehen und dessen Existenz überprüfen. Er kann jedoch nicht über die Element-UI gemanagt werden. Dieser Endpunkt kann dann nur mit der Element-API gemanagt werden.

Einzelheiten zu den API-Methoden finden Sie unter "Storage-Management mit der Element API"Die

Was Sie benötigen

- Sie sollten SnapMirror in der Element UI für den Storage-Cluster aktiviert haben.
- Ihnen kennen die ONTAP-Anmeldedaten für den Endpunkt.

Schritte

1. Klicken Sie auf **Datensicherung** > **SnapMirror Endpunkte**.
2. Klicken Sie Auf **Endpunkt Erstellen**.
3. Geben Sie im Dialogfeld **Neuen Endpunkt erstellen** die Cluster-Management-IP-Adresse des ONTAP-Systems ein.
4. Geben Sie die mit dem Endpunkt verknüpften Anmeldedaten für den ONTAP-Administrator ein.
5. Lesen Sie weitere Details durch:
   - LIFs: Listet die ONTAP clusterübergreifende logische Schnittstellen auf, die zur Kommunikation mit Element verwendet werden.
   - Status: Zeigt den aktuellen Status des SnapMirror-Endpunkts an. Mögliche Werte sind: Verbunden, getrennt und nicht verwaltet.
6. Klicken Sie Auf **Endpunkt Erstellen**.

SnapMirror Beziehung erstellen

Sie müssen eine SnapMirror Beziehung in der NetApp Element UI erstellen.

> Wenn ein Volume für SnapMirror noch nicht aktiviert ist und Sie eine Beziehung aus der Element UI erstellen möchten, wird SnapMirror auf diesem Volume automatisch aktiviert.

Was Sie benötigen

SnapMirror ist auf dem Volume aktiviert.

Schritte

1. Klicken Sie Auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol **Aktionen** für das Volume, das Teil der Beziehung sein soll.
3. Klicken Sie auf **Erstellen Sie eine SnapMirror Beziehung**.
4. Wählen Sie im Dialogfeld **eine SnapMirror-Beziehung erstellen** einen Endpunkt aus der Liste **Endpunkt** aus.
5. Wählen Sie aus, ob die Beziehung mit einem neuen ONTAP Volume oder einem vorhandenen ONTAP Volume erstellt werden soll.
6. Um ein neues ONTAP Volume in der Element UI zu erstellen, klicken Sie auf **Neues Volume erstellen**.
   a. Wählen Sie für diese Beziehung die **Storage Virtual Machine** aus.
   b. Wählen Sie aus der Dropdown-Liste das **Aggregat** aus.
   c. Geben Sie im Feld **Volume Name Suffix** ein Suffix ein.

      > Das System erkennt den Namen des Quell-Volumes und kopiert ihn in das Feld **Volume Name**. Das Suffix, das Sie eingeben, fügt den Namen an.

   d. Klicken Sie Auf **Zielvolumen Erstellen**.
7. Um ein vorhandenes ONTAP-Volume zu verwenden, klicken Sie auf **vorhandenes Volume verwenden**.
   a. Wählen Sie für diese Beziehung die **Storage Virtual Machine** aus.
   b. Wählen Sie das Volume aus, das das Ziel für diese neue Beziehung ist.
8. Wählen Sie im Abschnitt **Beziehungsdetails** eine Richtlinie aus. Wenn in der ausgewählten Richtlinie Regeln beibehalten sind, werden in der Tabelle Regeln die Regeln und die zugehörigen Beschriftungen

angezeigt.

9. **Optional**: Wählen Sie einen Zeitplan aus.

   Dadurch wird festgelegt, wie oft die Beziehung Kopien erstellt.

10. **Optional**: Geben Sie im Feld **Limit Bandwidth to** die maximale Bandbreite ein, die von Datenübertragungen in Verbindung mit dieser Beziehung verbraucht werden kann.
11. Lesen Sie weitere Details durch:
    - **Zustand**: Aktueller Beziehungsstatus des Zielvolumens. Mögliche Werte sind:
      - Nicht initialisiert: Das Ziel-Volume wurde nicht initialisiert.
      - Snapmirrored: Das Ziel-Volume wurde initialisiert und ist bereit, SnapMirror Updates zu erhalten.
      - Broken-off: Der Zieldatenträger ist Lesen/Schreiben und Schnappschüsse sind vorhanden.
    - **Status**: Aktueller Status der Beziehung. Mögliche Werte sind inaktiv, übertragen, prüfen, stilllegen, stilllegen, Warteschlange, Vorbereitung, Fertigstellung, Abbruch und Abbrechen.
    - **Lag-Zeit**: Die Zeit in Sekunden, die das Zielsystem hinter das Quellsystem hinkt. Die Verzögerungszeit darf nicht länger als das Transferzeitintervall sein.
    - **Bandbreitenbegrenzung**: Die maximale Bandbreite, die von Datenübertragungen in Verbindung mit dieser Beziehung verbraucht werden kann.
    - **Letzter übertragen**: Zeitstempel des zuletzt übertragenen Snapshots. Klicken Sie auf, um weitere Informationen zu erhalten.
    - **Policy Name**: Der Name der ONTAP SnapMirror Politik für die Beziehung.
    - **Richtlinientyp**: Art der ONTAP-SnapMirror-Politik für die Beziehung ausgewählt. Mögliche Werte sind:
      - Async_Mirror
      - Mirror_Vault
    - **Terminplanname**: Name des bereits vorhandenen Zeitplans auf dem für diese Beziehung ausgewählten ONTAP-System.
12. Um die Initialisierung zu diesem Zeitpunkt nicht zu starten, stellen Sie sicher, dass das Kontrollkästchen **Initialisieren** nicht aktiviert ist.

    Initialisierung kann sehr zeitaufwendig sein. Möglicherweise möchten Sie dies in Zeiten geringerer Auslastung durchführen. Bei der Initialisierung wird ein Basistransfer durchgeführt. Es erstellt eine Snapshot Kopie des Quell-Volume und überträgt dann die Kopie sowie alle Datenblöcke, auf die er auf das Ziel-Volume verweist. Sie können den Initialisierungsprozess (und nachfolgende Updates) manuell initialisieren oder einen Zeitplan verwenden, um den Zeitplan zu starten.

13. Klicken Sie Auf **Beziehung Erstellen**.
14. Klicken Sie auf **Datensicherung** > **SnapMirror Beziehungen**, um diese neue SnapMirror Beziehung anzuzeigen.

Aktionen für SnapMirror Beziehungen

Auf der Seite SnapMirror Beziehungen auf der Registerkarte Datensicherung können Sie eine Beziehung konfigurieren. Die Optionen aus dem Aktionen-Symbol werden hier beschrieben.

- **Bearbeiten**: Bearbeitet die verwendete Richtlinie oder den Zeitplan für die Beziehung.
- **Löschen**: Löscht die SnapMirror-Beziehung. Diese Funktion löscht nicht das Zielvolume.
- **Initialize**: Führt den ersten Basistransfer der Daten durch, um eine neue Beziehung aufzubauen.
- **Update**: Führt eine On-Demand-Aktualisierung der Beziehung durch, repliziert neue Daten und Snapshot-Kopien, die seit der letzten Aktualisierung zum Ziel enthalten sind.
- **Quiesce**: Verhindert weitere Updates für eine Beziehung.
- **Fortsetzen**: Nimmt eine Beziehung auf, die stillgelegt wird.
- **Break**: Macht das Zielvolumen Lesen-Schreiben und stoppt alle aktuellen und zukünftigen Transfers. Legen Sie fest, dass Clients das ursprüngliche Quell-Volume nicht verwenden, da durch den umgekehrten Resync-Vorgang das ursprüngliche Quellvolumen schreibgeschützt ist.
- **Resync**: Stellt eine zerbrochene Beziehung in die gleiche Richtung wieder her, bevor die Pause stattfand.
- **Reverse Resync**: Automatisiert die notwendigen Schritte, um eine neue Beziehung in die entgegengesetzte Richtung zu erstellen und zu initialisieren. Dies kann nur geschehen, wenn die bestehende Beziehung in einem gebrochenen Zustand ist. Durch diesen Vorgang wird die aktuelle Beziehung nicht gelöscht. Das ursprüngliche Quell-Volume wird auf die zuletzt verwendete Snapshot Kopie zurückgesetzt und mit dem Ziel neu synchronisiert. Alle Änderungen, die seit der letzten erfolgreichen SnapMirror Aktualisierung auf dem ursprünglichen Quell-Volume vorgenommen werden, gehen verloren. Alle vorgenommenen Änderungen oder neu auf das aktuelle Ziel-Volume geschriebenen Daten werden zurück an das ursprüngliche Quell-Volume gesendet.
- **Abbrechen**: Bricht eine laufende Übertragung ab. Wenn ein SnapMirror Update für eine abgebrochene Beziehung ausgegeben wird, wird die Beziehung mit dem letzten Transfer vom letzten vor dem Abbrechen erstellten Neustart Checkpoint fortgesetzt.

SnapMirror-Labels

SnapMirror-Labels

Ein SnapMirror-Label dient als Marker für die Übertragung eines angegebenen Snapshots nach den Aufbewahrungsregeln der Beziehung.

Durch das Anwenden eines Labels auf einen Snapshot wird es als Ziel für die SnapMirror Replikation markiert. Aufgabe der Beziehung ist es, die Regeln beim Datentransfer durchzusetzen, indem der passende Snapshot ausgewählt, auf das Ziel-Volume kopiert und die korrekte Anzahl von Kopien aufbewahrt wird. Er bezieht sich auf die Richtlinie zur Bestimmung der Anzahl der Aufbewahrung und des Aufbewahrungszeitraums. Die Richtlinie kann eine beliebige Anzahl von Regeln haben, und jede Regel hat eine eindeutige Kennzeichnung. Dieses Etikett dient als Verbindung zwischen dem Snapshot und der Aufbewahrungsregel.

Es ist das SnapMirror-Label, das angibt, welche Regel für den ausgewählten Snapshot, den Gruppen-Snapshot oder den ausgewählten Zeitplan angewendet wird.

Fügen Sie SnapMirror-Beschriftungen zu Snapshots hinzu

Die SnapMirror-Beschriftungen geben die Snapshot-Aufbewahrungsrichtlinie auf dem SnapMirror-Endpunkt an. Sie können Snapshots mit Beschriftungen hinzufügen und sie gruppieren.

Sie können verfügbare Beschriftungen in einem Dialogfeld für eine vorhandene SnapMirror Beziehung oder in dem NetApp ONTAP System Manager anzeigen.

Wenn Sie einem Gruppen-Snapshot ein Etikett hinzufügen, werden alle vorhandenen Beschriftungen zu einzelnen Snapshots überschrieben.

Was Sie benötigen

- SnapMirror ist auf dem Cluster aktiviert.
- Die Beschriftung, die Sie hinzufügen möchten, ist bereits in ONTAP vorhanden.

Schritte

1. Klicken Sie auf **Data Protection** > **Snapshots** oder **Gruppen-Snapshots** Seite.
2. Klicken Sie auf das Symbol **Aktionen** für den Snapshot oder Gruppen-Snapshot, dem Sie ein SnapMirror-Etikett hinzufügen möchten.
3. Geben Sie im Dialogfeld **Snapshot bearbeiten** Text in das Feld **SnapMirror-Bezeichnung** ein. Das Etikett muss mit einem Regellabel in der Richtlinie für die SnapMirror Beziehung übereinstimmen.
4. Klicken Sie Auf **Änderungen Speichern**.

Fügen Sie SnapMirror-Beschriftungen zu Snapshot-Zeitplänen hinzu

Sie können SnapMirror Beschriftungen zu Snapshot-Zeitplänen hinzufügen, um sicherzustellen, dass eine SnapMirror-Richtlinie angewendet wird. Sie können verfügbare Labels aus einem vorhandenen SnapMirror-Beziehungsdialogfeld oder NetAppONTAP System Manager anzeigen.

Was Sie benötigen

- SnapMirror muss auf Cluster-Ebene aktiviert sein.
- Die Beschriftung, die Sie hinzufügen möchten, ist bereits in ONTAP vorhanden.

Schritte

1. Klicken Sie Auf **Datenschutz** > **Termine**.
2. Sie können einem Zeitplan auf eine der folgenden Arten ein SnapMirror-Label hinzufügen:

Option	Schritte
Erstellen eines neuen Zeitplans	a. Wählen Sie **Zeitplan Erstellen**. b. Geben Sie alle anderen relevanten Details ein. c. Wählen Sie **Zeitplan Erstellen**.
Ändern des vorhandenen Zeitplans	a. Klicken Sie auf das Symbol **Aktionen** für den Zeitplan, dem Sie eine Bezeichnung hinzufügen möchten, und wählen Sie **Bearbeiten**. b. Geben Sie im daraufhin angezeigten Dialogfeld Text in das Feld **SnapMirror Label** ein. c. Wählen Sie **Änderungen Speichern**.

Weitere Informationen

Erstellen eines Snapshot-Zeitplans

Disaster Recovery mit SnapMirror

Disaster Recovery mit SnapMirror

Bei einem Problem mit einem Volume oder Cluster, auf dem die NetApp Element Software ausgeführt wird, brechen Sie mithilfe der SnapMirror Funktion die Beziehung und ein Failover auf das Ziel-Volume ab.

Falls das ursprüngliche Cluster vollständig ausgefallen ist oder nicht vorhanden ist, wenden Sie sich an den NetApp Support, um weitere Unterstützung zu erhalten.

Führen Sie ein Failover von einem Element Cluster aus

Sie können ein Failover vom Element Cluster durchführen, um für Hosts auf der Zielseite das Lese-/Schreibvolume zu erhalten und auf diese zugreifen zu können. Bevor Sie ein Failover vom Element-Cluster durchführen, müssen Sie die SnapMirror Beziehung unterbrechen.

Verwenden Sie die Benutzeroberfläche von NetApp Element, um den Failover auszuführen. Wenn die Element-UI nicht verfügbar ist, können Sie auch den Befehl „Beziehungen unterbrechen“ mit ONTAP System Manager oder ONTAP CLI eingeben.

Was Sie benötigen

- Eine SnapMirror-Beziehung ist vorhanden und hat mindestens einen gültigen Snapshot auf dem Ziel-Volume.
- Aufgrund ungeplanter Ausfälle oder eines geplanten Ereignisses am primären Standort ist ein Failover auf das Ziel-Volume erforderlich.

Schritte

1. Klicken Sie in der Element UI auf **Data Protection** > **SnapMirror Relationships**.
2. Finden Sie die Beziehung zum Quellvolume, das Sie Failover ausführen möchten.
3. Klicken Sie auf das Symbol **Aktionen**.
4. Klicken Sie Auf **Pause**.
5. Bestätigen Sie die Aktion.

   Das Volume auf dem Ziel-Cluster verfügt jetzt über Lese- und Schreibzugriff, kann auf die Applikations-Hosts eingebunden werden, um die Produktions-Workloads wieder aufzunehmen. Durch diese Aktion wird die gesamte SnapMirror-Replikation angehalten. Die Beziehung zeigt einen Abbruch.

Führen Sie ein Failback zum Element durch

Erfahren Sie mehr über die Durchführung eines Failbacks zu Element.

Wenn das Problem auf der primären Seite gemindert wurde, müssen Sie das ursprüngliche Quell-Volume neu synchronisieren und zur NetApp Element Software zurückkehren. Die entsprechenden Schritte hängen davon ab, ob das ursprüngliche Quell-Volume noch vorhanden ist oder Sie ein Failback auf ein neu erstelltes Volume durchführen müssen.

SnapMirror Failback-Szenarien

Die Disaster Recovery-Funktion von SnapMirror wird in zwei Failback-Szenarien dargestellt. Diese gehen davon aus, dass die ursprüngliche Beziehung (unterbrochen) fehlgeschlagen ist.

Die Schritte aus den entsprechenden Verfahren werden zur Referenz hinzugefügt.

> In den hier gezeigten Beispielen lautet R1 = die ursprüngliche Beziehung, in der der Cluster, auf dem die NetApp Element Software ausgeführt wird, das ursprüngliche Quell-Volume (Element) ist und ONTAP das ursprüngliche Ziel-Volume (ONTAP). R2 und R3 stellen die inversen Beziehungen dar, die durch den umgekehrten Resync-Vorgang erstellt wurden.

Das folgende Bild zeigt das Failback-Szenario, wenn das Quell-Volume noch vorhanden ist:

Das folgende Bild zeigt das Failback-Szenario, wenn das Quell-Volume nicht mehr existiert:

Weitere Informationen

- Führen Sie ein Failback durch, wenn das Quell-Volume noch vorhanden ist
- Führen Sie ein Failback durch, wenn das Quell-Volume nicht mehr vorhanden ist
- SnapMirror Failback-Szenarien

Führen Sie ein Failback durch, wenn das Quell-Volume noch vorhanden ist

Sie können das ursprüngliche Quell-Volume neu synchronisieren und mit der NetApp Element Benutzeroberfläche zurück sichern. Dieses Verfahren gilt für Szenarien, in denen das ursprüngliche Quell-Volume noch vorhanden ist.

1. Suchen Sie in der Element UI die Beziehung, die Sie unterbrochen haben, um das Failover auszuführen.
2. Klicken Sie auf das Symbol Aktionen und klicken Sie auf **Resync rückwärts**.
3. Bestätigen Sie die Aktion.

> Die Operation Reverse Resync erzeugt eine neue Beziehung, in der die Rollen der ursprünglichen Quell- und Zielvolumen umgekehrt werden (dies führt zu zwei Beziehungen, wenn die ursprüngliche Beziehung besteht). Alle neuen Daten vom ursprünglichen Ziel-Volume werden im Rahmen der umgekehrten Resynchronisierung auf das ursprüngliche Quell-Volume übertragen. Sie können weiterhin auf das aktive Volume auf der Zielseite zugreifen und dort Daten schreiben, müssen aber alle Hosts auf das Quell-Volume trennen und ein SnapMirror Update durchführen, bevor Sie zur ursprünglichen primären Ressource zurückkehren.

4. Klicken Sie auf das Aktionen-Symbol der umgekehrten Beziehung, die Sie gerade erstellt haben, und klicken Sie auf **Aktualisieren**.

   Jetzt, da Sie die umgekehrte Resynchronisierung abgeschlossen haben und sichergestellt haben, dass keine aktiven Sitzungen mit dem Volume auf der Zielseite verbunden sind und die letzten Daten sich auf dem ursprünglichen primären Volume befinden, Sie können die folgenden Schritte durchführen, um das Failback abzuschließen und das ursprüngliche primäre Volume erneut zu aktivieren:

5. Klicken Sie auf das Aktionen-Symbol der umgekehrten Beziehung und klicken Sie auf **break**.
6. Klicken Sie auf das Aktionen-Symbol der ursprünglichen Beziehung und klicken Sie auf **Resync**.

> Das ursprüngliche primäre Volume kann nun gemountet werden, um die Produktions-Workloads auf dem ursprünglichen primären Volume wiederaufzunehmen. Die ursprüngliche SnapMirror Replizierung wird anhand der Richtlinie und des für die Beziehung konfigurierten Zeitplans fortgesetzt.

7. Nachdem Sie bestätigt haben, dass der ursprüngliche Beziehungsstatus “snapmirrored” lautet, klicken Sie auf das Aktionen-Symbol der inversen Beziehung und klicken Sie auf **Löschen**.

Weitere Informationen

SnapMirror Failback-Szenarien

Führen Sie ein Failback durch, wenn das Quell-Volume nicht mehr vorhanden ist

Sie können das ursprüngliche Quell-Volume neu synchronisieren und mit der NetApp Element Benutzeroberfläche zurück sichern. Dieser Abschnitt gilt für Szenarien, in denen das ursprüngliche Quell-Volume verloren wurde, das ursprüngliche Cluster jedoch weiterhin intakt ist. Anweisungen zur Wiederherstellung eines neuen Clusters finden Sie in der Dokumentation auf der NetApp Support Site.

Was Sie benötigen

- Sie verfügen über eine abgegebrochene Replizierungsbeziehung zwischen Element und ONTAP Volumes.
- Das Elementvolumen ist unwiederbringlich verloren.
- Der ursprüngliche Volume-Name wird als NICHT GEFUNDEN angezeigt.

Schritte

1. Suchen Sie in der Element UI die Beziehung, die Sie unterbrochen haben, um das Failover auszuführen.

   Best Practice: notieren Sie sich die SnapMirror Politik und planen Sie Einzelheiten zur ursprünglichen Abgebrochenen Beziehung. Diese Informationen sind erforderlich, wenn die Beziehung neu erstellt wird.

2. Klicken Sie auf das Symbol **Aktionen** und klicken Sie auf **Resync rückwärts**.
3. Bestätigen Sie die Aktion.

> Die Operation Reverse Resync erzeugt eine neue Beziehung, in der die Rollen des ursprünglichen Quellvolumens und des Zielvolumens umgekehrt werden (dies führt zu zwei Beziehungen, wenn die ursprüngliche Beziehung besteht). Da das ursprüngliche Volume nicht mehr vorhanden ist, erstellt das System ein neues Element Volume mit demselben Volume-Namen und derselben Volume-Größe wie das ursprüngliche Quell-Volume. Dem neuen Volume wird eine QoS-Standardrichtlinie namens SM-Recovery zugewiesen, die mit einem Standardkonto namens SM-Recovery verknüpft ist. Sie möchten das Konto und die QoS-Richtlinie für alle Volumes manuell bearbeiten, die von SnapMirror erstellt wurden, um die gelöschten ursprünglichen Quell-Volumes zu ersetzen.

Daten vom letzten Snapshot werden im Rahmen der umgekehrten Resynchronisierung auf das neue Volume übertragen. Sie können weiterhin auf die Daten zugreifen und diese auf die aktive Partition schreiben, aber Sie müssen alle Hosts auf den aktiven Volume trennen und ein SnapMirror-Update

durchführen, bevor Sie die ursprüngliche primäre Beziehung in einem späteren Schritt wieder herstellen. Nach Abschluss der Resynchronisierung und Sicherstellung, dass keine aktiven Sitzungen mit dem Volume auf der Zielseite verbunden sind und dass sich die letzten Daten auf dem ursprünglichen primären Volume befinden, fahren Sie mit den folgenden Schritten fort, um das Failback abzuschließen und das ursprüngliche primäre Volume erneut zu aktivieren:

4. Klicken Sie auf das Symbol **Aktionen** der inversen Beziehung, die während der Operation Reverse Resync erstellt wurde, und klicken Sie auf **break**.
5. Klicken Sie auf das Symbol **Aktionen** der ursprünglichen Beziehung, in der das Quellvolume nicht vorhanden ist, und klicken Sie auf **Löschen**.
6. Klicken Sie auf das Symbol **Aktionen** der umgekehrten Beziehung, die Sie in Schritt 4 gebrochen haben, und klicken Sie auf **Resync rückwärts**.
7. Dies kehrt die Quelle und das Ziel um und führt zu einer Beziehung mit der gleichen Volumenquelle und dem gleichen Volume-Ziel wie die ursprüngliche Beziehung.
8. Klicken Sie auf das Symbol **Aktionen** und **Bearbeiten**, um diese Beziehung mit der ursprünglichen QoS-Richtlinie und den Zeitplaneinstellungen zu aktualisieren, die Sie zur Kenntnis genommen haben.
9. Jetzt ist es sicher, die umgekehrte Beziehung zu löschen, die Sie in Schritt 6 umkehren.

Weitere Informationen

SnapMirror Failback-Szenarien

Transfer oder einmalige Migration von ONTAP zu Element durchführen

Wenn Sie SnapMirror für Disaster Recovery von einem SolidFire Storage-Cluster mit NetApp Element Software auf die ONTAP Software verwenden, ist Element normalerweise die Quelle und ONTAP das Ziel. In einigen Fällen kann das ONTAP Storage-System jedoch als Quelle und Element als Ziel fungieren.

- Es gibt zwei Szenarien:
  - Es besteht keine frühere Disaster Recovery-Beziehung. Befolgen Sie alle Schritte in diesem Verfahren.
  - Eine frühere Disaster-Recovery-Beziehung existiert, nicht jedoch zwischen den Volumes, die für diese Risikominderung verwendet werden. Befolgen Sie in diesem Fall nur die Schritte 3 und 4 unten.

Was Sie benötigen

- Der Ziel-Node für Element muss ONTAP zugänglich gemacht worden sein.
- Das Element Volume muss für die SnapMirror Replizierung aktiviert worden sein.

Sie müssen den Zielpfad des Elements in Form hospip:/lun/<id_number> angeben, wobei lun die tatsächliche Zeichenfolge „`lun`“ ist und id_number die ID des Element-Volumes ist.

Schritte

1. Erstellen Sie mithilfe von ONTAP die Beziehung zum Element Cluster:

```
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. Überprüfen Sie, ob die SnapMirror Beziehung mit dem ONTAP snapmirror show-Befehl erstellt wurde.

   Informationen zum Erstellen einer Replizierungsbeziehung in der ONTAP-Dokumentation und für eine vollständige Befehlssyntax finden Sie auf der ONTAP-man-Seite.

3. Verwenden der `ElementCreateVolume` API, Erstellung des Ziel-Volume und Einstellen des Ziel-Volume-Zugriffsmodus auf SnapMirror:

   Element Volume erstellen mithilfe der Element API

```
{
   "method": "CreateVolume",
   "params": {
        "name": "SMTargetVolumeTest2",
        "accountID": 1,
        "totalSize": 100000000000,
        "enable512e": true,
        "attributes": {},
        "qosPolicyID": 1,
        "enableSnapMirrorReplication": true,
        "access": "snapMirrorTarget"
    },
    "id": 1
}
```

4. Initialisieren Sie die Replikationsbeziehung mit dem ONTAP `snapmirror initialize` Befehl:

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

Replizierung zwischen NetApp Element Software und ONTAP (ONTAP CLI)

Replizierung zwischen der NetApp Element Software und ONTAP – Übersicht (ONTAP CLI)

Mit SnapMirror können Sie die Business Continuity auf einem Element System sicherstellen, indem Sie Snapshot Kopien eines Element Volumes auf ein ONTAP Ziel replizieren. Bei einem Ausfall am Element Standort können Sie Clients über das ONTAP System Daten bereitstellen und das Element System anschließend nach Wiederherstellung des Service wieder aktivieren.

Ab ONTAP 9.4 können Sie Snapshot Kopien einer auf einem ONTAP Node erstellten LUN zurück in ein Element System replizieren. Möglicherweise haben Sie während eines Ausfalls am Element Standort eine LUN erstellt oder eine LUN verwenden, um Daten von ONTAP auf Element Software zu migrieren.

Wenn Folgendes gilt, sollten Sie mit Element zu ONTAP Backups arbeiten:

- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie möchten die ONTAP Befehlszeilenschnittstelle (CLI) verwenden, nicht System Manager oder ein automatisiertes Scripting Tool.
- Sie verwenden iSCSI, um den Clients Daten bereitzustellen.

Weitere Informationen zur SnapMirror-Konfiguration oder zu Konzeptkonzepten finden Sie unter "Datensicherung im Überblick".

Allgemeines zur Replizierung zwischen Element und ONTAP

Ab ONTAP 9.3 können Sie SnapMirror verwenden, um Snapshot Kopien eines Element Volume auf ein ONTAP Ziel zu replizieren. Bei einem Ausfall am Element Standort können Sie Clients über das ONTAP System Daten bereitstellen und das Element Quell-Volume nach Wiederherstellung des Service erneut aktivieren.

Ab ONTAP 9.4 können Sie Snapshot Kopien einer auf einem ONTAP Node erstellten LUN zurück in ein Element System replizieren. Möglicherweise haben Sie während eines Ausfalls am Element Standort eine LUN erstellt oder eine LUN verwenden, um Daten von ONTAP auf Element Software zu migrieren.

Arten von Datensicherungsbeziehungen

SnapMirror bietet zwei Arten von Datensicherungsbeziehungen. Für jeden Typ erstellt SnapMirror vor der Initialisierung oder Aktualisierung der Beziehung eine Snapshot Kopie des Element Quell-Volume:

- In einer Datensicherheitsbeziehung *Disaster Recovery (DR)* enthält das Ziel-Volume nur die von SnapMirror erstellte Snapshot-Kopie, von der aus Sie im Falle einer Katastrophe am primären Standort weiterhin Daten bereitstellen können.
- In einer *langfristigen Aufbewahrung* Datensicherungsbeziehung enthält das Ziel-Volume von Element Software erstellte zeitpunktgenaue Snapshot Kopien sowie die von SnapMirror erstellte Snapshot Kopie. Möglicherweise möchten Sie monatliche Snapshot-Kopien aufbewahren, die beispielsweise über einen Zeitraum von 20 Jahren erstellt wurden.

Standardrichtlinien

Beim ersten Aufruf von SnapMirror führt es einen *Baseline-Transfer* vom Quell-Volume zum Ziel-Volume durch. Die Richtlinie *SnapMirror* definiert den Inhalt der Baseline und alle Updates.

Sie können eine Standard- oder benutzerdefinierte Richtlinie verwenden, wenn Sie eine Datensicherungsbeziehung erstellen. Der *Policy type* legt fest, welche Snapshot-Kopien aufgenommen werden und wie viele Kopien beibehalten werden sollen.

Die folgende Tabelle zeigt die Standardrichtlinien. Verwenden Sie die `MirrorLatest` Richtlinie zum Erstellen einer herkömmlichen DR-Beziehung. Verwenden Sie die `MirrorAndVault` `Unified7year` Richtlinie oder, um eine einheitliche Replizierungsbeziehung zu erstellen, bei der DR und langfristige Datenaufbewahrung auf demselben Ziel-Volume konfiguriert werden.

Richtlinie	Richtlinientyp	Verhalten aktualisieren

MirrorLatest	Asynchrone Spiegelung	Übertragen Sie die von SnapMirror erstellte Snapshot Kopie.
MirrorAndVault	Mirror-Vault	Übertragen Sie die von SnapMirror erstellte Snapshot Kopie und sämtliche weniger aktuellen Snapshot Kopien, die seit der letzten Aktualisierung erstellt wurden, sofern sie die SnapMirror-Bezeichnungen „`daily`“ oder „`weekly`“ haben.
Unified7 Jahr	Mirror-Vault	Übertragen Sie die von SnapMirror erstellte Snapshot Kopie und sämtliche weniger aktuellen Snapshot-Kopien, die seit der letzten Aktualisierung erstellt wurden, sofern sie die SnapMirror-Bezeichnungen „`daily`“, „`weekly `m`“ oder „ onthly`“ haben.

Vollständige Hintergrundinformationen zu SnapMirror-Richtlinien, einschließlich einer Anleitung zur Verwendung dieser Richtlinie, finden Sie unter "Datensicherung im Überblick".

Allgemeines zu SnapMirror-Beschriftungen

Für jede Richtlinie mit dem Richtlinientyp „`mmirror-Vault`“ muss eine Regel gelten, die angibt, welche Snapshot Kopien repliziert werden sollen. Die Regel “daily” zeigt beispielsweise an, dass nur Snapshot-Kopien, denen das SnapMirror-Label “daily” zugewiesen ist, repliziert werden sollen. Sie weisen das SnapMirror-Label zu, wenn Sie Element Snapshot Kopien konfigurieren.

Replizierung von einem Element Quell-Cluster zu einem ONTAP Ziel-Cluster

Sie können SnapMirror verwenden, um Snapshot Kopien eines Element Volumes auf einem ONTAP Zielsystem zu replizieren. Bei einem Ausfall am Element Standort können Sie Clients über das ONTAP System Daten bereitstellen und das Element Quell-Volume nach Wiederherstellung des Service erneut aktivieren.

Ein Element Volume ist in etwa dem einer ONTAP LUN entsprechenden Modus. SnapMirror erstellt eine LUN mit dem Namen des Element-Volume, wenn eine Datensicherungsbeziehung zwischen Element Software und ONTAP initialisiert wird. SnapMirror repliziert Daten in eine vorhandene LUN, wenn die LUN die Anforderungen für Element zur ONTAP Replizierung erfüllt.

Replikationsregeln:

- Ein ONTAP Volume kann nur Daten aus einem Element Volume enthalten.
- Es können keine Daten von einem ONTAP Volume auf mehrere Element Volumes repliziert werden.

Replizierung von einem ONTAP Quell-Cluster zu einem Element Ziel-Cluster

Ab ONTAP 9.4 können Sie Snapshot Kopien einer auf einem ONTAP System erstellten LUN zurück in ein Element Volume replizieren:

- Wenn bereits eine SnapMirror Beziehung zwischen einer Element Quelle und einem ONTAP Ziel vorhanden ist, wird eine beim Bereitstellen von Daten vom Ziel erstellte LUN automatisch repliziert, sobald die Quelle reaktiviert wird.
- Andernfalls müssen Sie eine SnapMirror Beziehung zwischen dem ONTAP Quell-Cluster und dem Element Ziel-Cluster erstellen und initialisieren.

Replikationsregeln:

- Die Replizierungsbeziehung muss über eine Richtlinie vom Typ „`async-Mirror`“ verfügen.

  Richtlinien vom Typ “mmirror-Vault” werden nicht unterstützt.

- Es werden nur iSCSI LUNs unterstützt.
- Es kann nicht mehr als eine LUN aus einem ONTAP Volume in ein Element Volume repliziert werden.
- Eine LUN kann nicht von einem ONTAP Volume auf mehrere Element Volumes repliziert werden.

Voraussetzungen

Sie müssen die folgenden Aufgaben abgeschlossen haben, bevor Sie eine Datensicherungsbeziehung zwischen Element und ONTAP konfigurieren:

- Auf dem Element Cluster muss die NetApp Element Softwareversion 10.1 oder höher ausgeführt werden.
- Der ONTAP Cluster muss ONTAP 9.3 oder höher ausführen.
- SnapMirror muss auf dem ONTAP Cluster lizenziert sein.
- Sie müssen Volumes auf dem Element und ONTAP Cluster konfigurieren, die groß genug sind, um erwartete Datentransfers zu verarbeiten.
- Wenn Sie den Richtlinientyp „`mmirror-Vault`“ verwenden, muss für die Replikation der Element Snapshot-Kopien ein SnapMirror-Label konfiguriert sein.

  Sie können diese Aufgabe nur im oder mit der ausführen"Web-UI der Element Software""API-Methoden".

- Sie müssen sicherstellen, dass Port 5010 verfügbar ist.
- Wenn Sie bereits sehen, dass ein Ziel-Volume möglicherweise verschoben werden muss, müssen Sie sicherstellen, dass eine vollständige Mesh-Konnektivität zwischen Quelle und Ziel besteht. Jeder Node im Element Quell-Cluster muss in der Lage sein, mit jedem Node im ONTAP Ziel-Cluster zu kommunizieren.

Support-Details

Die folgende Tabelle enthält Support-Details für Element- zu ONTAP-Backups.

Ressource oder Funktion	Support-Details

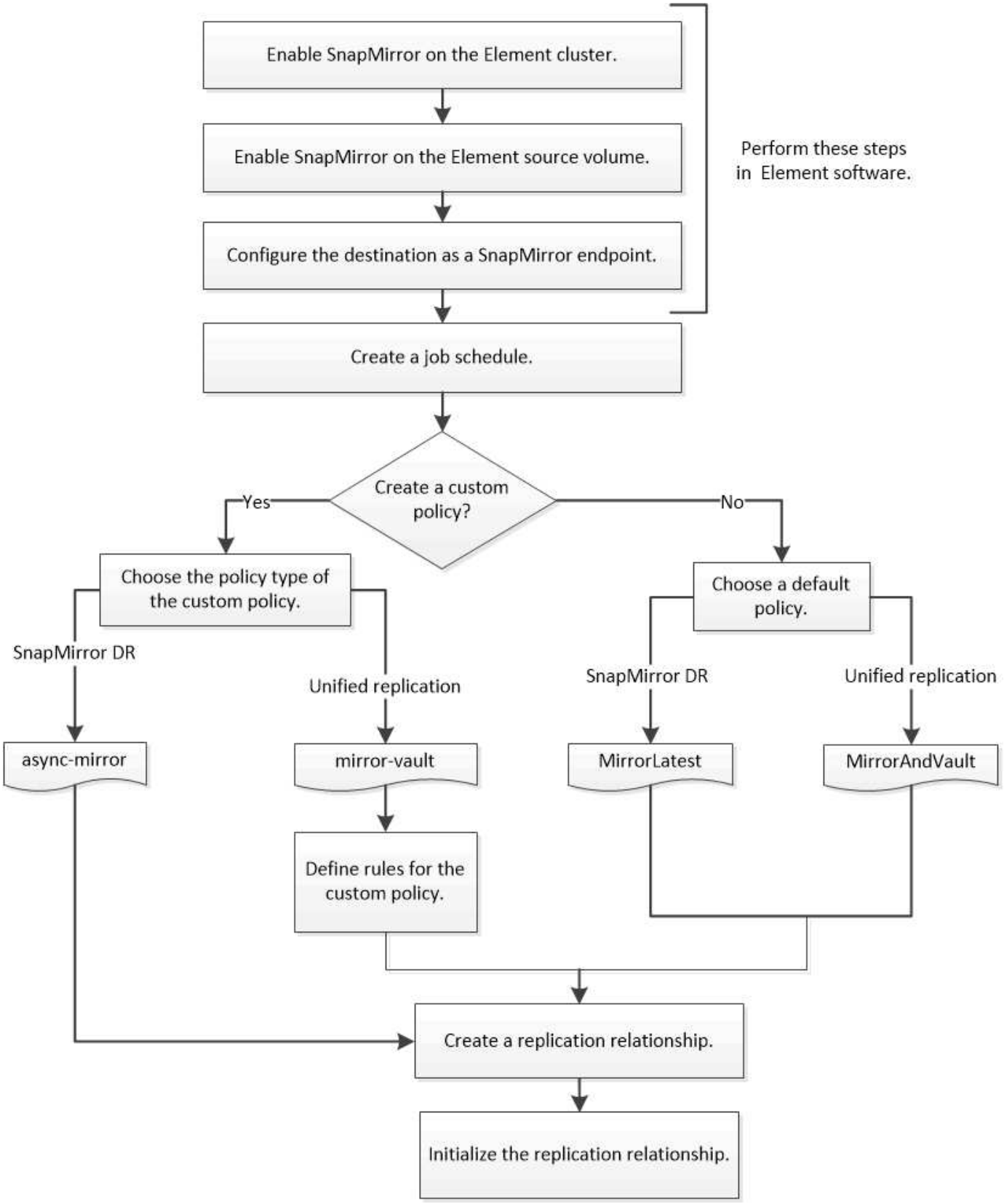
SnapMirror	• Die SnapMirror Wiederherstellungsfunktion wird nicht unterstützt. • Die `MirrorAllSnapshots` `XDPDefault` Richtlinien und werden nicht unterstützt. • Der Richtlinientyp „`Vault`“ wird nicht unterstützt. • Die systemdefinierte Regel „`all_Source_Snapshots`“ wird nicht unterstützt. • Der Richtlinientyp „`mmirror-Vault`“ wird nur zur Replikation von Element Software auf ONTAP unterstützt. Verwenden Sie „`Async-Mirror`“ für die Replizierung von ONTAP zu Element Software. • Die `-schedule` `-prefix` Optionen und für `snapmirror policy add-rule` werden nicht unterstützt. • Die `-preserve` `-quick-resync` Optionen und für `snapmirror resync` werden nicht unterstützt. • Storage-Effizienz bleibt erhalten. • Fan-out- und Kaskadenschutz-Implementierungen werden nicht unterstützt.
ONTAP	• ONTAP Select wird ab ONTAP 9.4 und Element 10.3 unterstützt. • Cloud Volumes ONTAP wird ab ONTAP 9.5 und Element 11.0 unterstützt.
Element	• Die maximale Volume-Größe beträgt 8 tib. • Die Volume-Blockgröße muss 512 Byte sein. Eine Blockgröße von 4 KB wird nicht unterstützt. • Die Volume-Größe muss ein Vielfaches von 1 MiB sein. • Volume-Attribute werden nicht erhalten. • Die maximale Anzahl der zu replizierenden Snapshot Kopien ist 30.
Netzwerk	• Pro Übertragung ist eine einzelne TCP-Verbindung zulässig. • Der Element-Node muss als IP-Adresse angegeben werden. Die Suche nach DNS-Hostnamen wird nicht unterstützt. • IPspaces werden nicht unterstützt.
SnapLock	SnapLock Volumes werden nicht unterstützt.
FlexGroup	FlexGroup Volumes werden nicht unterstützt.
SVM-DR	ONTAP Volumes in einer SVM-DR-Konfiguration werden nicht unterstützt.
MetroCluster	ONTAP Volumes in einer MetroCluster Konfiguration werden nicht unterstützt.

Workflow für die Replizierung zwischen Element und ONTAP

Unabhängig davon, ob Daten von Element zu ONTAP oder von ONTAP zu Element

repliziert werden, müssen Sie einen Job-Zeitplan konfigurieren, eine Richtlinie festlegen und die Beziehung erstellen und initialisieren. Sie können eine Standard- oder eine benutzerdefinierte Richtlinie verwenden.

Der Workflow setzt voraus, dass Sie die in aufgeführten erforderlichen Aufgaben abgeschlossen haben"Voraussetzungen". Vollständige Hintergrundinformationen zu SnapMirror-Richtlinien, einschließlich einer Anleitung zur Verwendung dieser Richtlinie, finden Sie unter "Datensicherung im Überblick".



SnapMirror in Element Software aktivieren

Aktivieren Sie SnapMirror auf dem Element Cluster

Sie müssen SnapMirror auf dem Element-Cluster aktivieren, bevor Sie eine

Replizierungsbeziehung erstellen können. Sie können diese Aufgabe nur in der Web-Benutzeroberfläche der Element-Software oder über die ausführen"API-Methode".

Bevor Sie beginnen

- Auf dem Element Cluster muss die NetApp Element Softwareversion 10.1 oder höher ausgeführt werden.
- SnapMirror kann nur für Element Cluster aktiviert werden, die in NetApp ONTAP Volumes verwendet werden.

Über diese Aufgabe

Das Element System wird standardmäßig mit SnapMirror deaktiviert. SnapMirror wird im Rahmen einer neuen Installation oder eines Upgrades nicht automatisch aktiviert.

Nach der Aktivierung kann SnapMirror nicht deaktiviert werden. Sie können die SnapMirror Funktion nur deaktivieren und die Standardeinstellungen wiederherstellen, indem Sie das Cluster wieder an das Werkseinstellungen zurücksetzen.

Schritte

1. Klicken Sie Auf **Cluster** > **Einstellungen**.
2. Suchen Sie die Cluster-spezifischen Einstellungen für SnapMirror.
3. Klicken Sie auf **SnapMirror aktivieren**.

Aktivieren Sie SnapMirror auf dem Element Quell-Volume

Sie müssen SnapMirror auf dem Element Quell-Volume aktivieren, bevor Sie eine Replizierungsbeziehung erstellen können. Sie können diese Aufgabe nur in der Webbenutzeroberfläche der Element-Software oder mit den Methoden und "ModifyVolumes" API ausführen"UmfyVolume".

Bevor Sie beginnen

- SnapMirror muss auf dem Element Cluster aktiviert sein.
- Die Volume-Blockgröße muss 512 Byte sein.
- Das Volume darf nicht an der Remote-Replizierung von Element beteiligt sein.
- Der Zugriffstyp des Volumes darf nicht „`Replikationsziel`“ sein.

Über diese Aufgabe

Für das folgende Verfahren wird vorausgesetzt, dass das Volume bereits vorhanden ist. Sie können SnapMirror auch beim Erstellen oder Klonen eines Volumes aktivieren.

Schritte

1. Wählen Sie **Management** > **Volumes**.
2. Wählen Sie die Schaltfläche für die Lautstärke.
3. Wählen Sie im Dropdown-Menü die Option **Bearbeiten** aus.
4. Wählen Sie im Dialogfeld **Volume bearbeiten** die Option **SnapMirror aktivieren** aus.
5. Wählen Sie **Änderungen Speichern**.

Erstellen eines SnapMirror Endpunkts

Bevor Sie eine Replikationsbeziehung erstellen können, müssen Sie einen SnapMirror -Endpunkt erstellen. Diese Aufgabe kann nur in der Web-Benutzeroberfläche der Element-Software oder mithilfe der "SnapMirror API-Methoden"Die

Bevor Sie beginnen

SnapMirror muss auf dem Element Cluster aktiviert sein.

Schritte

1. Klicken Sie auf **Datensicherung** > **SnapMirror Endpunkte**.
2. Klicken Sie Auf **Endpunkt Erstellen**.
3. Geben Sie im Dialogfeld **Neuen Endpunkt erstellen** die IP-Adresse für die ONTAP-Clusterverwaltung ein.
4. Geben Sie die Benutzer-ID und das Passwort des ONTAP Cluster-Administrators ein.
5. Klicken Sie Auf **Endpunkt Erstellen**.

Konfigurieren einer Replikationsbeziehung

Erstellen eines Replikationsauftrags

Unabhängig davon, ob Daten von Element zu ONTAP oder von ONTAP zu Element repliziert werden, müssen Sie einen Job-Zeitplan konfigurieren, eine Richtlinie festlegen und die Beziehung erstellen und initialisieren. Sie können eine Standard- oder eine benutzerdefinierte Richtlinie verwenden.

Sie können mit dem `job schedule cron create` Befehl einen Replikationsjob-Zeitplan erstellen. Der Job-Zeitplan legt fest, wann SnapMirror die Datensicherungsbeziehung automatisch aktualisiert, denen der Zeitplan zugewiesen ist.

Über diese Aufgabe

Sie weisen beim Erstellen einer Datensicherungsbeziehung einen Job-Zeitplan zu. Wenn Sie keinen Job-Zeitplan zuweisen, müssen Sie die Beziehung manuell aktualisieren.

Schritt

1. Job-Zeitplan erstellen:

   ```
   job schedule cron create -name job_name -month month -dayofweek day_of_week
   -day day_of_month -hour hour -minute minute
   ```

   Für `-month`, `-dayofweek` und `-hour` können Sie festlegen `all`, dass der Job jeden Monat, Wochentag und jede Stunde ausgeführt werden soll.

   Ab ONTAP 9.10.1 können Sie den Vserver für Ihren Job-Zeitplan angeben:

   ```
   job schedule cron create -name job_name -vserver Vserver_name -month month
   -dayofweek day_of_week -day day_of_month -hour hour -minute minute
   ```

   Im folgenden Beispiel wird ein Jobzeitplan mit dem Namen erstellt `my_weekly`, der samstags um 3:00 Uhr ausgeführt wird:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

Anpassen einer Replizierungsrichtlinie

Erstellen Sie eine benutzerdefinierte Replikationsrichtlinie

Sie können eine Standard- oder benutzerdefinierte Richtlinie verwenden, wenn Sie eine Replikationsbeziehung erstellen. Für eine benutzerdefinierte einheitliche Replikationsrichtlinie müssen Sie eine oder mehrere *rules* definieren, die festlegen, welche Snapshot-Kopien während der Initialisierung und Aktualisierung übertragen werden.

Sie können eine benutzerdefinierte Replikationsrichtlinie erstellen, wenn die Standardrichtlinie für eine Beziehung nicht geeignet ist. Möglicherweise möchten Sie Daten z. B. in einer Netzwerkübertragung komprimieren oder die Anzahl der Versuche, die SnapMirror unternimmt, um Snapshot-Kopien zu übertragen, ändern.

Über diese Aufgabe

Der Typ_Policy_ der Replikationsrichtlinie bestimmt die Art der von ihr unterstützten Beziehung. In der folgenden Tabelle sind die verfügbaren Richtlinientypen aufgeführt.

Richtlinientyp	Beziehungstyp
Asynchrone Spiegelung	SnapMirror DR
Mirror-Vault	Einheitliche Replizierung

Schritt

1. Erstellen einer benutzerdefinierten Replizierungsrichtlinie:

   ```
   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
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Ab ONTAP 9.5 können Sie mithilfe des Parameters den Zeitplan für die Erstellung eines gemeinsamen Zeitplans für Snapshot-Kopien für synchrone SnapMirror-Beziehungen festlegen `-common-snapshot -schedule`. Standardmäßig beträgt der allgemeine Zeitplan für synchrone SnapMirror Beziehungen für Snapshot Kopien eine Stunde. Sie können einen Wert zwischen 30 Minuten und zwei Stunden für den Zeitplan für Snapshot-Kopien für synchrone SnapMirror-Beziehungen angeben.

   Im folgenden Beispiel wird eine benutzerdefinierte Replizierungsrichtlinie für SnapMirror DR erstellt, die Netzwerkkomprimierung für Datentransfers ermöglicht:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network compression
enabled" -is-network-compression-enabled true
```

Im folgenden Beispiel wird eine benutzerdefinierte Replizierungsrichtlinie für einheitliche Replizierung erstellt:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy my_unified
-type mirror-vault
```

Nachdem Sie fertig sind

Für die Richtlinienarten „mmirror-Vault“ müssen Sie Regeln definieren, die festlegen, welche Snapshot-Kopien während der Initialisierung und Aktualisierung übertragen werden.

`snapmirror policy show`Überprüfen Sie mit dem Befehl, ob die SnapMirror-Richtlinie erstellt wurde. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Definieren Sie eine Regel für eine Richtlinie

Für benutzerdefinierte Richtlinien mit dem Richtlinientyp „mmirror-Vault“ müssen Sie mindestens eine Regel definieren, die festlegt, welche Snapshot-Kopien während der Initialisierung und Aktualisierung übertragen werden. Sie können auch Regeln für Standardrichtlinien mit dem Richtlinientyp „mmirror-Vault“ definieren.

Über diese Aufgabe

Für jede Richtlinie mit dem Richtlinientyp „mmirror-Vault“ muss eine Regel gelten, die angibt, welche Snapshot Kopien repliziert werden sollen. Die Regel „bi-monthly“ gibt beispielsweise an, dass nur Snapshot Kopien, denen das SnapMirror-Label „bi-monthly“ zugewiesen ist, repliziert werden sollen. Sie weisen das SnapMirror-Label zu, wenn Sie Element Snapshot Kopien konfigurieren.

Jeder Richtlinientyp ist einer oder mehreren systemdefinierten Regeln zugeordnet. Diese Regeln werden einer Richtlinie automatisch zugewiesen, wenn Sie ihren Richtlinientyp angeben. Die folgende Tabelle zeigt die systemdefinierten Regeln.

Systemdefinierte Regel	Wird in Richtlinientypen verwendet	Ergebnis
sm_erstellt	Asynchrone Spiegelung, Spiegelung/Vaulting	Bei der Initialisierung und Aktualisierung wird eine von SnapMirror erstellte Snapshot Kopie übertragen.

Täglich	Mirror-Vault	Neue Snapshot-Kopien auf der Quelle mit dem SnapMirror-Label “daily” werden bei Initialisierung und Aktualisierung übernommen.
Wöchentlich	Mirror-Vault	Neue Snapshot-Kopien auf der Quelle mit dem SnapMirror-Label „`Weekly`“ werden bei der Initialisierung und Aktualisierung übertragen.
Monatlich	Mirror-Vault	Neue Snapshot-Kopien auf der Quelle mit dem SnapMirror-Label „`mmonthly`“ werden bei der Initialisierung und dem Update übertragen.

Sie können bei Bedarf zusätzliche Regeln für Standard- oder benutzerdefinierte Richtlinien festlegen. Beispiel:

- Für die Standardrichtlinie `MirrorAndVault` können Sie eine Regel mit dem Namen „`bi-monthly`“ erstellen, um die Snapshot-Kopien der Quelle mit dem SnapMirror-Label „`bi-monthly`“ abzugleichen.
- Für eine benutzerdefinierte Richtlinie mit dem Richtlinientyp „`mmirror-Vault`“ können Sie eine Regel mit dem Namen „`bi-Weekly`“ erstellen, um Snapshot-Kopien auf der Quelle mit dem SnapMirror-Label „`bi-Weekly`“ abzugleichen.

Schritt

1. Definieren Sie eine Regel für eine Richtlinie:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird `bi-monthly` der Standardrichtlinie eine Regel mit dem Label SnapMirror hinzugefügt `MirrorAndVault`:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   Im folgenden Beispiel wird `bi-weekly` der benutzerdefinierten `my_snapvault` Richtlinie eine Regel mit der Beschriftung „SnapMirror“ hinzugefügt:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_snapvault -snapmirror-label bi-weekly -keep 26
   ```

   Im folgenden Beispiel wird `app_consistent` der benutzerdefinierten `Sync` Richtlinie eine Regel mit der Beschriftung „SnapMirror“ hinzugefügt:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

Sie können dann Snapshot-Kopien vom Quell-Cluster replizieren, die mit dem SnapMirror-Label übereinstimmen:

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Erstellen einer Replikationsbeziehung

Erstellen einer Beziehung von einer Element Quelle zu einem ONTAP Ziel

Die Beziehung zwischen dem Quell-Volume im primären Storage und dem Ziel-Volume im sekundären Storage wird als „*Data Protection Relationship*“ bezeichnet. Mit dem `snapmirror create` Befehl können Sie eine Datensicherungsbeziehung von einer Element Quelle zu einem ONTAP Ziel oder von einer ONTAP Quelle zu einem Element Ziel erstellen.

Sie können SnapMirror verwenden, um Snapshot Kopien eines Element Volumes auf einem ONTAP Zielsystem zu replizieren. Bei einem Ausfall am Element Standort können Sie Clients über das ONTAP System Daten bereitstellen und das Element Quell-Volume nach Wiederherstellung des Service erneut aktivieren.

Bevor Sie beginnen

- Der Element-Node, der das zu replizierende Volume enthält, muss ONTAP zugänglich gemacht werden.
- Das Element Volume muss für die SnapMirror Replizierung aktiviert worden sein.
- Wenn Sie den Richtlinientyp „`mmirror-Vault`“ verwenden, muss für die Replikation der Element Snapshot-Kopien ein SnapMirror-Label konfiguriert sein.

> Sie können diese Aufgabe nur im oder mit der ausführen"Web-UI der Element Software""API-Methoden".

Über diese Aufgabe

Sie müssen den Quellpfad des Elements im Formular angeben `<hostip:>/lun/<name>`, wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ ist und `name` der Name des Element-Volumes ist.

Ein Element Volume ist in etwa dem einer ONTAP LUN entsprechenden Modus. SnapMirror erstellt eine LUN mit dem Namen des Element-Volume, wenn eine Datensicherungsbeziehung zwischen Element Software und ONTAP initialisiert wird. SnapMirror repliziert Daten in eine vorhandene LUN, wenn die LUN die Anforderungen für die Replizierung von Element Software zu ONTAP erfüllt.

Replikationsregeln:

- Ein ONTAP Volume kann nur Daten aus einem Element Volume enthalten.
- Es können keine Daten von einem ONTAP Volume auf mehrere Element Volumes repliziert werden.

In ONTAP 9 3 und älteren Versionen kann ein Ziel-Volume bis zu 251 Snapshot-Kopien enthalten. In ONTAP 9.4 und höher kann ein Ziel-Volume bis zu 1019 Snapshot Kopien enthalten.

Schritt

1. Erstellen Sie vom Ziel-Cluster eine Replizierungsbeziehung von einer Elementquelle zu einem ONTAP Ziel:

   ```
   snapmirror create -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume> -type XDP -schedule schedule -policy
   <policy>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird eine SnapMirror DR-Beziehung mithilfe der Standardrichtlinie erstellt `MirrorLatest`:

   ```
   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
   ```

   Im folgenden Beispiel wird mithilfe der Standardrichtlinie eine einheitliche Replizierungsbeziehung erstellt `MirrorAndVault`:

   ```
   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
   ```

   Im folgenden Beispiel wird mithilfe der `Unified7year` Richtlinie eine einheitliche Replizierungsbeziehung erstellt:

   ```
   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
   ```

   Im folgenden Beispiel wird mithilfe der benutzerdefinierten `my_unified` Richtlinie eine einheitliche Replizierungsbeziehung erstellt:

   ```
   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
   ```

Nachdem Sie fertig sind

`snapmirror show`Überprüfen Sie mit dem Befehl, ob die SnapMirror Beziehung erstellt wurde. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Erstellen einer Beziehung von einer ONTAP Quelle zu einem Element Ziel

Ab ONTAP 9.4 können Sie SnapMirror verwenden, um Snapshot Kopien einer auf einer ONTAP Quelle erstellten LUN zurück zu einem Element Ziel zu replizieren. Möglicherweise verwenden Sie die LUN, um Daten von ONTAP zu Element Software zu migrieren.

Bevor Sie beginnen

- Der Ziel-Node für Element muss ONTAP zugänglich gemacht worden sein.
- Das Element Volume muss für die SnapMirror Replizierung aktiviert worden sein.

Über diese Aufgabe

Sie müssen den Element-Zielpfad im Formular angeben `<hostip:>/lun/<name>`, wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ ist und `name` der Name des Element-Volumes ist.

Replikationsregeln:

- Die Replizierungsbeziehung muss über eine Richtlinie vom Typ „`async-Mirror`“ verfügen.

  Sie können eine Standard- oder eine benutzerdefinierte Richtlinie verwenden.

- Es werden nur iSCSI LUNs unterstützt.
- Es kann nicht mehr als eine LUN aus einem ONTAP Volume in ein Element Volume repliziert werden.
- Eine LUN kann nicht von einem ONTAP Volume auf mehrere Element Volumes repliziert werden.

Schritt

1. Replizierungsbeziehung von einer ONTAP-Quelle zu einem Element-Ziel erstellen:

   ```
   snapmirror create -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -type XDP -schedule schedule -policy
   <policy>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird eine SnapMirror DR-Beziehung mithilfe der Standardrichtlinie erstellt `MirrorLatest`:

   ```
   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
   ```

Im folgenden Beispiel wird mithilfe der benutzerdefinierten `my_mirror` Richtlinie eine SnapMirror DR-Beziehung erstellt:

```
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
```

Nachdem Sie fertig sind

`snapmirror show`Überprüfen Sie mit dem Befehl, ob die SnapMirror Beziehung erstellt wurde. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Initialisieren Sie eine Replikationsbeziehung

Bei allen Beziehungstypen führt die Initialisierung eine *Baseline Transfer* durch: Es erstellt eine Snapshot Kopie des Quell-Volume und überträgt dann die Kopie mit allen Datenblöcken, die es auf das Ziel-Volume verweist.

Bevor Sie beginnen

- Der Element-Node, der das zu replizierende Volume enthält, muss ONTAP zugänglich gemacht werden.
- Das Element Volume muss für die SnapMirror Replizierung aktiviert worden sein.
- Wenn Sie den Richtlinientyp „`mmirror-Vault`“ verwenden, muss für die Replikation der Element Snapshot-Kopien ein SnapMirror-Label konfiguriert sein.

Sie können diese Aufgabe nur im oder mit der ausführen"Web-UI der Element Software""API-Methoden".

Über diese Aufgabe

Sie müssen den Quellpfad des Elements im Formular angeben `<hostip:>/lun/<name>`, wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ ist und *`name`* der Name des Element-Volumes ist.

Initialisierung kann sehr zeitaufwendig sein. Möglicherweise möchten Sie den Basistransfer in Zeiten geringerer Auslastung durchführen.

Wenn die Initialisierung einer Beziehung von einer ONTAP Quelle zu einem Element Ziel aus irgendeinem Grund fehlschlägt, wird sie weiterhin fehlschlagen, selbst wenn Sie das Problem behoben haben (z. B. ein ungültiger LUN-Name). Die Behelfslösung sieht wie folgt aus:

1. Löschen Sie die Beziehung.
2. Löschen Sie das Element Ziel-Volume.
3. Erstellung eines neuen Element Ziel-Volume
4. Erstellen und Initialisieren einer neuen Beziehung von der ONTAP Quelle auf das Ziel-Volume des Element

Schritt

1. Initialisieren einer Replikationsbeziehung:

   `snapmirror initialize -source-path <hostip:>/lun/<name> -destination-path <SVM:volume|cluster://SVM/volume>`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel initialisiert die Beziehung zwischen dem Quell-Volume `0005` an der IP-Adresse 10.0.0.11 und dem Ziel-Volume `volA_dst` auf `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Stellen Sie Daten von einem SnapMirror DR-Ziel-Volume bereit

Das Zielvolumen schreibbar machen

Wenn der primäre Standort für eine SnapMirror DR-Beziehung aufgrund einer Katastrophe deaktiviert wird, können Sie Daten vom Ziel-Volume mit minimaler Unterbrechung bereitstellen. Sie können das Quell-Volume neu aktivieren, wenn der Service am primären Standort wiederhergestellt ist.

Sie müssen das Ziel-Volume schreibbar machen, bevor Sie Daten vom Volume an die Clients bereitstellen können. Mit dem `snapmirror quiesce` Befehl können Sie geplante Transfers am Ziel stoppen, mit dem `snapmirror abort` Befehl die laufenden Transfers stoppen und mit dem `snapmirror break` Befehl das Ziel schreibbar machen.

Über diese Aufgabe

Sie müssen den Quellpfad des Elements im Formular angeben `<hostip:>/lun/<name>`, wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ ist und `name` der Name des Element-Volumes ist.

Schritte

1. Geplante Transfers zum Ziel anhalten:

   `snapmirror quiesce -source-path <hostip:>/lun/<name> -destination-path <SVM:volume>|<cluster://SVM/volume>`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden geplante Übertragungen zwischen dem Quell-Volume `0005` an der IP-Adresse 10.0.0.11 und dem Ziel-Volume `volA_dst` am angehalten `svm_backup`:

   ```
   cluster_dst::> snapmirror quiesce -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

2. Laufende Transfers zum Ziel anhalten:

   `snapmirror abort -source-path <hostip:>/lun/<name> -destination-path`

`<SVM:volume>|<cluster://SVM/volume>`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel stoppt laufende Transfers zwischen dem Quell-Volume `0005` an der IP-Adresse 10.0.0.11 und dem Ziel-Volume `volA_dst` auf `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

3. SnapMirror DR-Beziehung unterbrechen:

   `snapmirror break -source-path <hostip:>/lun/<name> -destination-path <SVM:volume>|<cluster://SVM/volume>`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `0005` bei IP-Adresse 10.0.0.11 und dem Ziel-Volume `volA_dst` auf `svm_backup` und dem Ziel-Volume `volA_dst` auf unterbrochen `svm_backup`:

   ```
   cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Ziel-Volume für Datenzugriff konfigurieren

Nachdem das Ziel-Volume schreibbar gemacht wurde, muss das Volume für den Datenzugriff konfiguriert werden. SAN-Hosts können auf die Daten vom Ziel-Volume zugreifen, bis das Quell-Volume erneut aktiviert ist.

1. Ordnen Sie die Element LUN der entsprechenden Initiatorgruppe zu.
2. Erstellen Sie iSCSI-Sitzungen von den SAN-Host-Initiatoren zu den SAN-LIFs.
3. Führen Sie auf dem SAN-Client einen erneuten Speicherscan durch, um die verbundene LUN zu erkennen.

Aktivieren Sie das ursprüngliche Quellvolume erneut

Sie können die ursprüngliche Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes wiederherstellen, wenn Sie nicht mehr Daten vom Bestimmungsort bereitstellen müssen.

Über diese Aufgabe

Für das folgende Verfahren wird vorausgesetzt, dass die Basis im ursprünglichen Quell-Volume intakt ist. Wenn die Baseline nicht intakt ist, müssen Sie die Beziehung zwischen dem Volume, das Sie Daten vom und dem ursprünglichen Quell-Volume bereitstellen, erstellen und initialisieren, bevor Sie den Vorgang durchführen.

Sie müssen den Quellpfad des Elements im Formular angeben `<hostip:>/lun/<name>`, wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ ist und `name` der Name des Element-Volumes ist.

Ab ONTAP 9.4 werden Snapshot Kopien einer LUN, die erstellt wurden, während Sie Daten vom ONTAP Ziel bereitstellen, automatisch repliziert, wenn die Element Quelle neu aktiviert wird.

Replikationsregeln:

- Es werden nur iSCSI LUNs unterstützt.
- Es kann nicht mehr als eine LUN aus einem ONTAP Volume in ein Element Volume repliziert werden.
- Eine LUN kann nicht von einem ONTAP Volume auf mehrere Element Volumes repliziert werden.

Schritte

1. Löschen Sie die ursprüngliche Datensicherungsbeziehung:

   ```
   snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -policy <policy>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die Beziehung zwischen dem ursprünglichen Quell-Volume, `0005` an der IP-Adresse 10.0.0.11, und dem Volume, von dem Sie Daten bereitstellen, `volA_dst` am gelöscht `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path 10.0.0.11:/lun/0005
   -policy MirrorLatest -destination-path svm_backup:volA_dst
   ```

2. Umkehren der ursprünglichen Datensicherungsbeziehung:

   ```
   snapmirror resync -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -policy <policy>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Auch wenn die Resynchronisierung keinen Basistransfer erfordert, kann sie zeitaufwendig sein. Möglicherweise möchten Sie die Neusynchronisierung in Zeiten nach außerhalb der Stoßzeiten durchführen.

   Im folgenden Beispiel wird die Beziehung zwischen dem ursprünglichen Quell-Volume, `0005` an der IP-Adresse 10.0.0.11, und dem Volumen, von dem Sie Daten bereitstellen, `volA_dst` auf umgekehrt `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
   ```

3. Aktualisierung der umgekehrten Beziehung:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name>
   ```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

> Der Befehl schlägt fehl, wenn auf der Quelle und dem Ziel keine gemeinsame Snapshot Kopie vorhanden ist. Verwenden Sie `snapmirror initialize` , um die Beziehung neu zu initialisieren.

Im folgenden Beispiel wird die Beziehung zwischen dem Volume, das Sie Daten von, `volA_dst` auf `svm_backup`, und dem ursprünglichen Quell-Volume `0005` an der IP-Adresse 10.0.0.11 bereitstellen, aktualisiert:

```
cluster_dst::> snapmirror update -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

4. Geplante Transfers für die umgekehrte Beziehung stoppen:

   ```
   snapmirror quiesce -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden geplante Übertragungen zwischen dem Volume, das Sie Daten von, `volA_dst` auf `svm_backup` und dem ursprünglichen Quell-Volume `0005` an der IP-Adresse 10.0.0.11 bereitstellen, gestoppt:

   ```
   cluster_dst::> snapmirror quiesce -source-path svm_backup:volA_dst
   -destination-path 10.0.0.11:/lun/0005
   ```

5. Laufende Transfers für die umgekehrte Beziehung stoppen:

   ```
   snapmirror abort -source-path <SVM:volume>|<cluster://SVM/volume> -destination
   -path <hostip:>/lun/<name>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel stoppt laufende Übertragungen zwischen dem Volumen, das Sie Daten von, `volA_dst` auf `svm_backup`, und dem ursprünglichen Quell-Volume `0005` an der IP-Adresse 10.0.0.11 bereitstellen:

   ```
   cluster_dst::> snapmirror abort -source-path svm_backup:volA_dst
   -destination-path 10.0.0.11:/lun/0005
   ```

6. Zerbrechen der umgekehrten Beziehung:

   ```
   snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume> -destination
   -path <hostip:>/lun/<name>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel wird die Beziehung zwischen dem Volumen, das Sie Daten von, `volA_dst` auf `svm_backup`, und dem ursprünglichen Quell-Volume `0005` an der IP-Adresse 10.0.0.11 bereitstellen, unterbrochen:

```
cluster_dst::> snapmirror break -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

7. Löschen Sie die umgekehrte Datensicherungsbeziehung:

   ```
   snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -policy <policy>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die umgekehrte Beziehung zwischen dem ursprünglichen Quell-Volume, `0005` an der IP-Adresse 10.0.0.11, und dem Volume, von dem Sie Daten bereitstellen, `volA_dst` am gelöscht `svm_backup`:

   ```
   cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
   ```

8. Wiederherstellung der ursprünglichen Datensicherungsbeziehung:

   ```
   snapmirror resync -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel stellt die Beziehung zwischen dem ursprünglichen Quell-Volume, `0005` bei der IP-Adresse 10.0.0.11, und dem ursprünglichen Ziel-Volume, `volA_dst` auf wieder her `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Nachdem Sie fertig sind

```
`snapmirror show`Überprüfen Sie mit dem Befehl, ob die SnapMirror
Beziehung erstellt wurde. Eine vollständige Befehlssyntax finden Sie in
der man-Page.
```

Aktualisieren Sie eine Replikationsbeziehung manuell

Möglicherweise müssen Sie eine Replikationsbeziehung manuell aktualisieren, wenn ein Update aufgrund eines Netzwerkfehlers fehlschlägt.

Über diese Aufgabe

Sie müssen den Quellpfad des Elements im Formular angeben `<hostip:>/lun/<name>`, wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ ist und `name` der Name des Element-Volumes ist.

Schritte

1. Manuelles Aktualisieren einer Replikationsbeziehung:

   ```
   snapmirror update -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   > Der Befehl schlägt fehl, wenn auf der Quelle und dem Ziel keine gemeinsame Snapshot Kopie vorhanden ist. Verwenden Sie `snapmirror initialize` , um die Beziehung neu zu initialisieren.

   Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `0005` an `volA_dst` der IP-Adresse 10.0.0.11 und dem Ziel-Volume auf aktualisiert `svm_backup`:

   ```
   cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Synchronisieren Sie eine Replikationsbeziehung neu

Sie müssen eine Replizierungsbeziehung neu synchronisieren, nachdem Sie ein Ziel-Volume schreibbar machen, nachdem ein Update fehlschlägt, weil eine gemeinsame Snapshot-Kopie nicht auf den Quell- und Ziel-Volumes vorhanden ist oder Sie die Replizierungsrichtlinie für die Beziehung ändern möchten.

Über diese Aufgabe

Auch wenn die Resynchronisierung keinen Basistransfer erfordert, kann sie zeitaufwendig sein. Möglicherweise möchten Sie die Neusynchronisierung in Zeiten nach außerhalb der Stoßzeiten durchführen.

Sie müssen den Quellpfad des Elements im Formular angeben `<hostip:>/lun/<name>`, wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ ist und `name` der Name des Element-Volumes ist.

Schritt

1. Neusynchronisierung der Quell- und Ziel-Volumes:

   ```
   snapmirror resync -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume> -type XDP -policy <policy>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `0005` an der IP-Adresse 10.0.0.11 und dem Ziel-Volume `volA_dst` auf neu synchronisiert `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

Backup und Restore von Volumes

Backup und Restore von Volumes

Backups und Restores von Volumes auf anderen SolidFire Storage sowie sekundäre Objektspeicher, die mit Amazon S3 oder OpenStack Swift kompatibel sind.

Wenn Sie Volumes aus OpenStack Swift oder Amazon S3 wiederherstellen, benötigen Sie Manifest-Informationen aus dem ursprünglichen Backup-Prozess. Wenn Sie ein Volume wiederherstellen, das auf einem SolidFire Storage-System gesichert wurde, sind keine Manifest-Informationen erforderlich.

Weitere Informationen

- Volumes werden in einem Amazon S3-Objektspeicher gesichert
- Volumes werden in einem OpenStack Swift Objektspeicher gesichert
- Sicherung eines Volumes auf einem SolidFire Storage-Cluster
- Wiederherstellung eines Volumes aus einem Backup auf einem Amazon S3-Objektspeicher
- Wiederherstellung eines Volumes aus dem Backup in einem OpenStack Swift Objektspeicher
- Wiederherstellung eines Volumes aus einem Backup auf einem SolidFire Storage-Cluster

Volumes werden in einem Amazon S3-Objektspeicher gesichert

Sie können Backups von Volumes auf externen Objektspeichern erstellen, die mit Amazon S3 kompatibel sind.

1. Klicken Sie Auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol Aktionen für das zu Sicherungsvolumen.
3. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
4. Wählen Sie im Dialogfeld * Integriertes Backup* unter **Backup in** die Option **S3** aus.
5. Wählen Sie eine Option unter **Datenformat** aus:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Geben Sie einen Hostnamen ein, der für den Zugriff auf den Objektspeicher im Feld **Hostname** verwendet werden soll.
7. Geben Sie im Feld **Zugriffsschlüssel-ID** eine Zugriffsschlüssel-ID für das Konto ein.
8. Geben Sie den geheimen Zugriffsschlüssel für das Konto im Feld * Secret Access Key* ein.
9. Geben Sie den S3-Bucket ein, in dem die Sicherung im Feld **S3 Bucket** gespeichert werden soll.
10. Geben Sie im Feld **Nametag** einen Namensschild ein, der an das Präfix angefügt werden soll.
11. Klicken Sie Auf **Lesen Starten**.

Volumes werden in einem OpenStack Swift Objektspeicher gesichert

Sie können ein Backup von Volumes auf externen Objektspeichern erstellen, die mit OpenStack Swift kompatibel sind.

1. Klicken Sie Auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol Aktionen, über das das Volume gesichert werden soll.
3. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
4. Wählen Sie im Dialogfeld * Integriertes Backup* unter **Backup in** die Option **Swift** aus.
5. Wählen Sie unter **Datenformat** ein Datenformat aus:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Geben Sie eine URL für den Zugriff auf den Objektspeicher im Feld **URL** ein.
7. Geben Sie im Feld **Benutzername** einen Benutzernamen für das Konto ein.
8. Geben Sie den Authentifizierungsschlüssel für das Konto im Feld **Authentifizierungsschlüssel** ein.
9. Geben Sie den Container ein, in dem das Backup im Feld **Container** gespeichert werden soll.
10. **Optional**: Geben Sie im Feld **Nametag** ein Namensschild ein, das an das Präfix angefügt werden soll.
11. Klicken Sie Auf **Lesen Starten**.

Sicherung eines Volumes auf einem SolidFire Storage-Cluster

Sie können ein Backup von Volumes in einem Cluster auf einem Remote-Cluster für Storage-Cluster mit Element Software erstellen.

Stellen Sie sicher, dass die Quell- und Ziel-Cluster gekoppelt sind.

Siehe "Paarung von Clustern zur Replizierung".

Beim Backup oder Restore von einem Cluster auf ein anderes generiert das System einen Schlüssel, der als Authentifizierung zwischen den Clustern verwendet wird. Dieser Schreibschlüssel für das Massenvolumen ermöglicht es dem Quellcluster, sich beim Schreiben auf das Ziel-Volume mit dem Ziel-Cluster zu authentifizieren. Im Rahmen des Backup- oder Wiederherstellungsprozesses müssen Sie vor dem Start des Vorgangs einen Schreibschlüssel für das Massenvolumen vom Zielvolume generieren.

1. Auf dem Ziel-Cluster * Management* > **Volumes**.
2. Klicken Sie auf das Aktionen-Symbol für das Ziel-Volume.
3. Klicken Sie im Menü Ergebnis auf **aus** wiederherstellen.
4. Wählen Sie im Dialogfeld * Integrierter Restore* unter **Wiederherstellen von** die Option **SolidFire** aus.
5. Wählen Sie eine Option unter **Datenformat** aus:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Klicken Sie Auf **Schlüssel Generieren**.
7. Kopieren Sie den Schlüssel aus der Box **Bulk Volume Write Key** in die Zwischenablage.
8. Gehen Sie auf dem Quellcluster zu **Management** > **Volumes**.

9. Klicken Sie auf das Symbol Aktionen, über das das Volume gesichert werden soll.
10. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
11. Wählen Sie im Dialogfeld * Integriertes Backup* unter **Backup in** die Option **SolidFire** aus.
12. Wählen Sie dieselbe Option aus, die Sie zuvor im Feld **Datenformat** ausgewählt haben.
13. Geben Sie die virtuelle Management-IP-Adresse des Clusters des Ziel-Volumes im Feld **Remote Cluster MVIP** ein.
14. Geben Sie den Benutzernamen für den Remote-Cluster in das Feld **Remote-Cluster-Benutzername** ein.
15. Geben Sie das Kennwort für den Remote-Cluster im Feld * Remote-Cluster-Kennwort* ein.
16. Fügen Sie im Feld **Bulk Volume Write Key** den Schlüssel ein, den Sie zuvor auf dem Ziel-Cluster generiert haben.
17. Klicken Sie Auf **Lesen Starten**.

Wiederherstellung eines Volumes aus einem Backup auf einem Amazon S3-Objektspeicher

Sie können ein Volume anhand einer Backup auf einem Amazon S3-Objektspeicher wiederherstellen.

1. Klicken Sie Auf **Berichterstellung** > **Ereignisprotokoll**.
2. Suchen Sie das Backup-Ereignis, das das Backup erstellt hat, das Sie wiederherstellen müssen.
3. Klicken Sie in der Spalte **Details** für die Veranstaltung auf **Details anzeigen**.
4. Kopieren Sie die Manifestinformationen in die Zwischenablage.
5. Klicken Sie Auf **Management** > **Volumes**.
6. Klicken Sie auf das Symbol Aktionen für das Volume, das Sie wiederherstellen möchten.
7. Klicken Sie im Menü Ergebnis auf **aus** wiederherstellen.
8. Wählen Sie im Dialogfeld * Integrierter Restore* unter **Wiederherstellen von** die Option **S3** aus.
9. Wählen Sie unter **Datenformat** die Option aus, die der Datensicherung entspricht:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
10. Geben Sie einen Hostnamen ein, der für den Zugriff auf den Objektspeicher im Feld **Hostname** verwendet werden soll.
11. Geben Sie im Feld **Zugriffsschlüssel-ID** eine Zugriffsschlüssel-ID für das Konto ein.
12. Geben Sie den geheimen Zugriffsschlüssel für das Konto im Feld * Secret Access Key* ein.
13. Geben Sie den S3-Bucket ein, in dem die Sicherung im Feld **S3 Bucket** gespeichert werden soll.
14. Fügen Sie die Manifest-Informationen in das Feld * Manifestieren* ein.
15. Klicken Sie Auf **Schreiben Starten**.

Wiederherstellung eines Volumes aus dem Backup in einem OpenStack Swift Objektspeicher

Sie können ein Volume aus einem Backup auf einem OpenStack Swift Objektspeicher wiederherstellen.

1. Klicken Sie Auf **Berichterstellung** > **Ereignisprotokoll**.

2. Suchen Sie das Backup-Ereignis, das das Backup erstellt hat, das Sie wiederherstellen müssen.
3. Klicken Sie in der Spalte **Details** für die Veranstaltung auf **Details anzeigen**.
4. Kopieren Sie die Manifestinformationen in die Zwischenablage.
5. Klicken Sie Auf **Management** > **Volumes**.
6. Klicken Sie auf das Symbol Aktionen für das Volume, das Sie wiederherstellen möchten.
7. Klicken Sie im Menü Ergebnis auf **aus** wiederherstellen.
8. Wählen Sie im Dialogfeld * Integrierter Restore* unter **Wiederherstellen von** die Option **Swift** aus.
9. Wählen Sie unter **Datenformat** die Option aus, die der Datensicherung entspricht:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
10. Geben Sie eine URL für den Zugriff auf den Objektspeicher im Feld **URL** ein.
11. Geben Sie im Feld **Benutzername** einen Benutzernamen für das Konto ein.
12. Geben Sie den Authentifizierungsschlüssel für das Konto im Feld **Authentifizierungsschlüssel** ein.
13. Geben Sie den Namen des Containers ein, in dem das Backup im Feld **Container** gespeichert ist.
14. Fügen Sie die Manifest-Informationen in das Feld * Manifestieren* ein.
15. Klicken Sie Auf **Schreiben Starten**.

Wiederherstellung eines Volumes aus einem Backup auf einem SolidFire Storage-Cluster

Sie können ein Volume aus einem Backup auf einem SolidFire Storage Cluster wiederherstellen.

Beim Backup oder Restore von einem Cluster auf ein anderes generiert das System einen Schlüssel, der als Authentifizierung zwischen den Clustern verwendet wird. Dieser Schreibschlüssel für das Massenvolumen ermöglicht es dem Quellcluster, sich beim Schreiben auf das Ziel-Volume mit dem Ziel-Cluster zu authentifizieren. Im Rahmen des Backup- oder Wiederherstellungsprozesses müssen Sie vor dem Start des Vorgangs einen Schreibschlüssel für das Massenvolumen vom Zielvolume generieren.

1. Klicken Sie auf dem Ziel-Cluster auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol Aktionen für das Volume, das Sie wiederherstellen möchten.
3. Klicken Sie im Menü Ergebnis auf **aus** wiederherstellen.
4. Wählen Sie im Dialogfeld * Integrierter Restore* unter **Wiederherstellen von** die Option **SolidFire** aus.
5. Wählen Sie unter **Datenformat** die Option aus, die der Datensicherung entspricht:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Klicken Sie Auf **Schlüssel Generieren**.
7. Kopieren Sie die **Massenvolume-Schreibschlüssel**-Informationen in die Zwischenablage.
8. Klicken Sie im Quellcluster auf **Verwaltung** > **Volumes**.
9. Klicken Sie auf das Aktionen-Symbol für das Volume, das Sie für die Wiederherstellung verwenden möchten.
10. Klicken Sie im Menü Ergebnis auf **Sichern nach**.

11. Wählen Sie im Dialogfeld * Integriertes Backup* unter **Sichern nach** die Option **SolidFire** aus.
12. Wählen Sie unter **Datenformat** die Option aus, die der Sicherung entspricht.
13. Geben Sie die virtuelle Management-IP-Adresse des Clusters des Ziel-Volumes im Feld **Remote Cluster MVIP** ein.
14. Geben Sie den Benutzernamen für den Remote-Cluster in das Feld **Remote-Cluster-Benutzername** ein.
15. Geben Sie das Kennwort für den Remote-Cluster im Feld * Remote-Cluster-Kennwort* ein.
16. Fügen Sie den Schlüssel aus Ihrer Zwischenablage in das Feld **Massenvolumenschreibschlüssel** ein.
17. Klicken Sie Auf **Lesen Starten**.

Konfigurieren Sie benutzerdefinierte Sicherungsdomänen

Bei Element-Clustern, die mehr als zwei Speicherknoten enthalten, können Sie benutzerdefinierte Schutzdomänen für jeden Knoten konfigurieren. Wenn Sie benutzerdefinierte Schutz-Domänen konfigurieren, müssen Sie einer Domäne alle Nodes im Cluster zuweisen.

Wenn Sie Protection Domains zuweisen, beginnt eine Datensynchronisation zwischen Nodes und einige Cluster-Vorgänge sind bis zum Abschluss der Datensynchronisierung nicht verfügbar. Nachdem eine benutzerdefinierte Schutzdomäne für ein Cluster konfiguriert wurde und Sie einen neuen Speicherknoten hinzufügen, können Sie keine Laufwerke für den neuen Knoten hinzufügen, bis Sie eine Schutzdomäne für den Knoten zuweisen und die Datensynchronisierung abschließen lassen. Besuchen Sie das "Dokumentation der Protection Domains" Um weitere Informationen zu Protection Domains zu erhalten.

Damit ein benutzerdefiniertes Protection Domain-Schema für ein Cluster nützlich sein kann, müssen alle Speicherknoten in jedem Chassis derselben benutzerdefinierten Protection Domain zugewiesen werden. Sie müssen so viele benutzerdefinierte Schutz-Domains wie nötig erstellen, damit dies der Fall sein kann (das kleinste mögliche benutzerdefinierte Schutz-Domain-Schema ist drei Domänen). Als Best Practice empfiehlt es sich, eine gleiche Anzahl von Knoten pro Domäne zu konfigurieren und sicherzustellen, dass jeder Knoten, der einer bestimmten Domäne zugewiesen ist, vom gleichen Typ ist.

Schritte

1. Klicken Sie Auf **Cluster** > **Knoten**.
2. Klicken Sie Auf **Schutzdomänen Konfigurieren**.

   Im Fenster **Benutzerdefinierte Schutzdomänen konfigurieren** können Sie die derzeit konfigurierten Schutzdomänen (sofern vorhanden) sowie die Protection Domain-Zuweisungen für einzelne Knoten anzeigen.

3. Geben Sie einen Namen für die neue benutzerdefinierte Schutzdomäne ein, und klicken Sie auf **Erstellen**.

   Wiederholen Sie diesen Schritt für alle neuen Protection Domains, die Sie erstellen müssen.

4. Klicken Sie für jeden Knoten in der Liste **Knoten zuweisen** auf die Dropdown-Liste in der Spalte **Schutzdomäne** und wählen Sie eine Schutzdomäne aus, die diesem Knoten zugewiesen werden soll.

Vergewissern Sie sich, dass Sie das Knoten- und Gehäuse-Layout, das benutzerdefinierte Schutz-Domain-Schema, das Sie konfiguriert haben, und die Auswirkungen des Schemas auf den Datenschutz kennen, bevor Sie die Änderungen anwenden. Wenn Sie ein Protection Domain-Schema anwenden und sofort Änderungen vornehmen müssen, könnte es einige Zeit dauern, bis Sie dies aufgrund der Datensynchronisierung durchführen können, die nach der Anwendung der Konfiguration erfolgt.

5. Klicken Sie Auf **Schutzdomänen Konfigurieren**.

Ergebnis

Je nach der Größe des Clusters kann die Datensynchronisation zwischen Domänen einige Zeit in Anspruch nehmen. Nach Abschluss der Datensynchronisation können Sie auf der Seite **Cluster** > **Nodes** die benutzerdefinierten Schutz-Domain-Zuweisungen anzeigen und das Element Web-UI-Dashboard zeigt den Schutzstatus des Clusters im Fensterbereich **Benutzerdefinierte Schutzdomäne-Funktionszustand** an.

Mögliche Fehler

Folgende Fehler werden möglicherweise nach dem Anwenden einer benutzerdefinierten Schutz-Domain-Konfiguration angezeigt:

Fehler	Beschreibung	Auflösung
SetProtectionDomainLayout fehlgeschlagen: ProtectionDomainLayout würde NodeID {9} unbrauchbar lassen. Standard- und nicht-Standardnamen können nicht zusammen verwendet werden.	Einem Knoten ist keine Schutzdomäne zugewiesen.	Weisen Sie dem Knoten eine Schutzdomäne zu.
SetProtectionDomainLayout fehlgeschlagen: Protection Domain type 'Custom' spaltet Protection Domain type 'Chassis'.	Einem Node in einem Multi-Node-Chassis wird eine Protection Domain zugewiesen, die sich von anderen Nodes im Chassis unterscheidet.	Stellen Sie sicher, dass alle Knoten im Chassis derselben Schutzdomäne zugewiesen sind.

Weitere Informationen

- "Benutzerdefinierte Sicherungsdomänen"
- "Storage-Management mit der Element API"

Fehler im System beheben

Systemereignisse

Zeigt Informationen zu Systemereignissen an

Sie können Informationen zu verschiedenen im System erkannten Ereignissen anzeigen. Das System aktualisiert die Ereignismeldungen alle 30 Sekunden. Im Ereignisprotokoll werden wichtige Ereignisse für das Cluster angezeigt.

1. Wählen Sie in der Element-UI die Option **Berichterstellung** > **Ereignisprotokoll**.

Für jedes Ereignis werden die folgenden Informationen angezeigt:

Element	Beschreibung
ID	Eindeutige ID, die jedem Ereignis zugeordnet ist.
Art Des Events	Der Typ des protokollierten Ereignisses, z. B. API-Ereignisse oder Klonereignisse.
Nachricht	Dem Ereignis zugeordnete Nachricht.
Details	Informationen, mit denen der Grund des Ereignisses ermittelt werden kann.
Service-ID	Der Dienst, der das Ereignis gemeldet hat (falls zutreffend).
Knoten	Der Node, der das Ereignis gemeldet hat (falls zutreffend).
Laufwerks-ID	Das Laufwerk, das das Ereignis gemeldet hat (falls zutreffend).
Ereigniszeit	Die Zeit, zu der das Ereignis aufgetreten ist.

Weitere Informationen

Ereignistypen

Ereignistypen

Das System meldet mehrere Ereignistypen. Jedes Ereignis ist ein Vorgang, den das System abgeschlossen hat. Ereignisse können Routine-, normale Ereignisse oder Ereignisse sein, die vom Administrator beachtet werden müssen. Die Spalte Ereignistypen auf der Seite Ereignisprotokoll gibt an, in welchem Teil des Systems das Ereignis aufgetreten ist.

Das System protokolliert keine schreibgeschützten API-Befehle im Ereignisprotokoll.

In der folgenden Liste werden die Arten von Ereignissen beschrieben, die im Ereignisprotokoll angezeigt werden:

- **ApiEvent**

  Ereignisse, die von einem Benutzer über eine API oder eine Web-Benutzeroberfläche initiiert werden, die Einstellungen ändern.

- **BinAssignmentsEvent**

Ereignisse im Zusammenhang mit der Zuordnung von Datenfächern. Fächer sind im Wesentlichen Container, in denen Daten gespeichert und über das gesamte Cluster hinweg zugeordnet sind.

- **BinSyncEvent**

  Systemereignisse zur Neuzuweisung von Daten zwischen Block-Services.

- **BsCheckEvent**

  Systemereignisse im Zusammenhang mit Blockserviceüberprüfungen.

- **BsKilEvent**

  Systemereignisse im Zusammenhang mit Blockdienstterminen.

- **BulkOpEvent**

  Ereignisse im Zusammenhang mit Vorgängen, die auf einem gesamten Volume ausgeführt werden, z. B. Backups, Wiederherstellungen, Snapshots oder Klone

- **KlonEvent**

  Ereignisse im Zusammenhang mit dem Klonen von Volumes.

- **ClusterMasterEvent**

  Ereignisse, die bei der Initialisierung des Clusters oder bei Änderungen der Konfiguration im Cluster angezeigt werden, z. B. Hinzufügen oder Entfernen von Nodes

- **cSumEvent**

  Ereignisse im Zusammenhang mit der Erkennung einer nicht übereinstimmenden Prüfsumme bei der Überprüfung der lückenlosen Prüfsumme.

  Dienste, die eine Prüfsummenkongruenz erkennen, werden automatisch angehalten und nach der Generierung dieses Ereignisses nicht neu gestartet.

- **Datenereignis**

  Ereignisse im Zusammenhang mit dem Lesen und Schreiben von Daten.

- **DbEvent**

  Veranstaltungen im Zusammenhang mit der globalen Datenbank, die von Ensemble-Knoten im Cluster gepflegt wird.

- **Auffahrt**

  Ereignisse in Verbindung mit Laufwerksoperationen

- **VerschlüsselungAtRestEvent**

  Ereignisse im Zusammenhang mit dem Verschlüsselungsvorgang auf einem Cluster.

- **EnsembleEvent**

Ereignisse, die sich auf die Erhöhung oder Verringerung der Anzahl der Knoten in einem Ensemble beziehen.

- **Fiber ChannelEvent**

  Ereignisse in Verbindung mit der Konfiguration von und Verbindungen zu den Nodes.

- **GcEvent**

  Ereignisse, die auf Prozessen zurückzuführen sind, werden alle 60 Minuten ausgeführt, um Speicher auf Blocklaufwerken zurückzugewinnen. Dieser Prozess wird auch als Garbage Collection bezeichnet.

- **IeEvent**

  Interner Systemfehler.

- **Installationsereignis**

  Automatische Softwareinstallationsereignisse. Die Software wird automatisch auf einem ausstehenden Node installiert.

- **ISCSIEvent**

  Ereignisse im Zusammenhang mit iSCSI-Problemen im System.

- **EndEvent**

  Ereignisse im Zusammenhang mit der Anzahl von Volumes oder virtuellen Volumes in einem Konto oder im Cluster, die sich dem maximal zulässigen Wert nähern.

- **WartungModeEvent**

  Ereignisse im Zusammenhang mit dem Wartungsmodus des Node, z. B. Deaktivieren des Node.

- **NetworkEvent**

  Ereignisse im Zusammenhang mit der Netzwerkfehlerberichterstattung für jede Schnittstelle der physischen Netzwerkschnittstelle (NIC).

  Diese Ereignisse werden ausgelöst, wenn eine Fehleranzahl für eine Schnittstelle einen Standardschwellenwert von 1000 in einem 10-minütigen Überwachungsintervall überschreitet. Diese Ereignisse gelten für Netzwerkfehler wie empfangene Fehlschläge, zyklische Redundanzprüfung (CRC)-Fehler, Längenfehler, Überlauffehler und Frame-Fehler.

- **HardwareEvent**

  Ereignisse im Zusammenhang mit Problemen, die auf Hardware-Geräten erkannt wurden.

- * Remote ClusterEvent*

  Ereignisse im Zusammenhang mit der Paarung von Remote-Clustern.

- **Termin**

  Ereignisse im Zusammenhang mit geplanten Snapshots.

- **ServiceEvent**

  Ereignisse im Zusammenhang mit dem Systemstatus.

- **SliceEvent**

  Ereignisse im Zusammenhang mit dem Slice Server, z. B. Entfernen eines Metadatenlaufwerks oder eines Volumes.

  Es gibt drei Arten von Ereignissen zur Umverteilung in Schichten, die Informationen über den Service enthalten, dem ein Volume zugewiesen wird:

  - Umdrehen: Ändern des primären Dienstes zu einem neuen primären Service

    ```
    sliceID oldPrimaryServiceID->newPrimaryServiceID
    ```

  - Verschieben: Ändern des sekundären Service zu einem neuen sekundären Service

    ```
    sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
    ```

  - Beschneidung: Entfernen eines Volumes aus einer Gruppe von Diensten

    ```
    sliceID {oldSecondaryServiceID(s)}
    ```

- **SnmpTrapEvent**

  Ereignisse im Zusammenhang mit SNMP-Traps.

- **StatEvent**

  Ereignisse in Verbindung mit Systemstatistiken.

- **TsEvent**

  Ereignisse im Zusammenhang mit dem Systemtransportdienst.

- **UnexpectedException**

  Ereignisse im Zusammenhang mit unerwarteten Systemausnahmen.

- **UreEvent**

  Ereignisse im Zusammenhang mit nicht behebbaren Lesefehlern, die beim Lesen vom Speichergerät auftreten.

- **VasaProviderEvent**

  Ereignisse in Verbindung mit einem VASA Provider (vSphere APIs for Storage Awareness)

Status der ausgeführten Aufgaben anzeigen

Sie können den Fortschritt und den Abschlussstatus der ausgeführten Aufgaben in der Web-Benutzeroberfläche anzeigen, die von den API-Methoden ListSyncJobs und ListBulkVolumeJobs gemeldet werden. Über die Registerkarte „Reporting“ der Element-Benutzeroberfläche können Sie auf die Seite „ausgeführte Aufgaben“ zugreifen.

Wenn eine große Anzahl von Aufgaben vorhanden ist, kann das System sie in Warteschlange stellen und in Batches ausführen. Auf der Seite laufende Aufgaben werden die aktuell synchronisierten Dienste angezeigt. Wenn eine Aufgabe abgeschlossen ist, wird sie durch die nächste Synchronisierungsaufgabe in der Warteschlange ersetzt. Die Synchronisierung von Aufgaben wird möglicherweise weiterhin auf der Seite laufende Aufgaben angezeigt, bis keine Aufgaben mehr abgeschlossen sind.

Auf der Seite laufende Aufgaben des Clusters, der das Ziel-Volume enthält, werden die Replikationsdaten für Volumes angezeigt, die die Replikation durchlaufen.

Systemwarnungen

Anzeigen von Systemmeldungen

Sie können Benachrichtigungen zu Cluster-Fehlern oder -Fehlern im System anzeigen. Warnmeldungen können Informationen, Warnungen oder Fehler sein und ein guter Indikator für die inwieweit das Cluster läuft. Die meisten Fehler lösen sich automatisch.

Sie können die API-Methode ListClusterStandards verwenden, um die Alarmüberwachung zu automatisieren. So können Sie über alle auftretenden Warnmeldungen benachrichtigt werden.

1. Wählen Sie in der Element-UI die Option **Berichterstellung** > **Alarme** aus.

   Das System aktualisiert die Alarme auf der Seite alle 30 Sekunden.

   Für jedes Ereignis werden die folgenden Informationen angezeigt:

Element	Beschreibung
ID	Eine eindeutige ID, die einer Cluster-Warnmeldung zugeordnet ist.

Schweregrad	Der Grad der Wichtigkeit des Alarms. Mögliche Werte: • Warnung: Ein kleines Problem, das bald Aufmerksamkeit erfordert. Upgrades des Systems sind weiterhin zulässig. • Fehler: Ein Ausfall, der zu einer Performance-Verschlechterung oder einem Verlust von Hochverfügbarkeit führen kann. Fehler sollten in der Regel den Dienst nicht anderweitig beeinträchtigen. • Kritisch: Ein schwerwiegender Fehler, der den Dienst beeinträchtigt. Das System kann keine API- oder Client-I/O-Anfragen bereitstellen. Ein Betrieb in diesem Zustand kann zu einem potenziellen Datenverlust führen. • BestPractice: Eine empfohlene Best Practice für die Systemkonfiguration wird nicht verwendet.
Typ	Die Komponente, die sich auf den Fehler auswirkt. Nodes, Laufwerk, Cluster, Service oder Volume können verwendet werden.
Knoten	Node-ID für den Node, auf den sich dieser Fehler bezieht. Bei Knoten- und Laufwerkfehlern enthalten, andernfalls auf - (Dash) gesetzt.
Laufwerks-ID	Laufwerk-ID für das Laufwerk, auf das sich dieser Fehler bezieht. Bei Fahrfehlern enthalten, ansonsten auf - (Dash) eingestellt.
Fehlercode	Ein beschreibenden Code, der angibt, was den Fehler verursacht hat.
Details	Eine Beschreibung des Fehlers mit zusätzlichen Details.
Datum	Datum und Uhrzeit der Fehlerprotokollierung.

2. Klicken Sie auf **Details anzeigen**, um eine individuelle Warnung anzuzeigen, um Informationen über den Alarm anzuzeigen.
3. Um die Details aller Warnmeldungen auf der Seite anzuzeigen, klicken Sie auf die Spalte Details.

   Nachdem das System eine Meldung beseitigt hat, werden alle Informationen über die Warnmeldung einschließlich des Datums, an dem sie behoben wurde, in den aufgelösten Bereich verschoben.

Weitere Informationen

- Cluster-Fehlercodes
- "Storage-Management mit der Element API"

Cluster-Fehlercodes

Das System meldet einen Fehler oder einen Status, der durch das Generieren eines Fehlercodes, der auf der Seite „Meldungen“ aufgeführt ist, von Interesse sein könnte. Anhand dieser Codes können Sie ermitteln, welche Komponente des Systems die Warnmeldung erfahren hat und warum die Warnmeldung generiert wurde.

In der folgenden Liste werden die verschiedenen Arten von Codes beschrieben:

- **AuthentifizierungServiceFault**

  Der Authentifizierungsdienst auf einem oder mehreren Clusterknoten funktioniert nicht wie erwartet.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **VerfügbarVirtualNetworkIPAdresseLow**

  Die Anzahl der virtuellen Netzwerkadressen im Block der IP-Adressen ist gering.

  Um diesen Fehler zu beheben, fügen Sie dem Block der virtuellen Netzwerkadressen weitere IP-Adressen hinzu.

- * BlockClusterFull*

  Es ist nicht ausreichend freier Block-Speicherplatz zur Unterstützung eines Single-Node-Verlusts vorhanden. Weitere Informationen zu Cluster-Auslastungsstufen finden Sie in der GetClusterFullThreshold API-Methode. Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Stage3Low (Warnung): Benutzerdefinierter Schwellenwert wurde überschritten. Passen Sie Cluster-Volleinstellungen an oder fügen Sie weitere Nodes hinzu.
  - Stage4Critical (Fehler): Es gibt nicht genügend Speicherplatz zur Wiederherstellung nach einem Ausfall eines 1 Node. Das Erstellen von Volumes, Snapshots und Klonen ist nicht zulässig.
  - Stage5CompletelyConsumed (kritisch)1; es sind keine Schreibzugriffe oder neue iSCSI-Verbindungen zulässig. Aktuelle iSCSI-Verbindungen werden beibehalten. Schreibzugriffe scheitern, bis mehr Kapazität dem Cluster hinzugefügt wird.

  Löschen oder löschen Sie Volumes, um diesen Fehler zu beheben, oder fügen Sie dem Storage-Cluster einen weiteren Storage-Node hinzu.

- **BlocksDegradiert**

  Blockdaten werden aufgrund eines Ausfalls nicht mehr vollständig repliziert.

Schweregrad	Beschreibung
Warnung	Auf nur zwei vollständige Kopien der Blockdaten kann zugegriffen werden.

Fehler	Auf nur eine vollständige Kopie der Blockdaten kann zugegriffen werden.
Kritisch	Auf vollständige Kopien der Blockdaten kann nicht zugegriffen werden.

Hinweis: der Warnstatus kann nur auf einem Triple Helix System auftreten.

Um diesen Fehler zu beheben, stellen Sie alle Offline Nodes oder Block-Services wieder her oder wenden Sie sich an den NetApp Support, um Unterstützung zu erhalten.

- **BlockServiceTooFull**

  Ein Block-Service benötigt zu viel Speicherplatz.

  Um diesen Fehler zu beheben, fügen Sie mehr bereitgestellte Kapazität hinzu.

- **BlockServiceUnHealthy**

  Ein Blockdienst wurde als fehlerhaft erkannt:

  - Schweregrad = Warnung: Es werden keine Maßnahmen ergriffen. Dieser Warnzeitraum läuft in cTimeUntilBSIsKilledMSec=330000 Millisekunden ab.
  - Schweregrad = Fehler: Das System setzt Daten automatisch zurück und repliziert seine Daten auf andere gesunde Laufwerke.
  - Schweregrad = kritisch: Es gibt fehlerhafte Blockdienste auf mehreren Knoten, die größer oder gleich der Replikationszahl sind (2 für Doppelhelix). Die Daten sind nicht verfügbar, und die bin-Synchronisierung wird nicht beendet.

    Prüfen Sie auf Probleme mit der Netzwerkverbindung und Hardwarefehler. Es gibt weitere Fehler, wenn bestimmte Hardwarekomponenten ausgefallen sind. Der Fehler wird gelöscht, wenn der Blockservice aufgerufen wird oder wenn der Dienst deaktiviert wurde.

- **BmcSelfTestFailed**

  Der Baseboard Management Controller (BMC) hat einen Selbsttest nicht bestanden.

  Wenden Sie sich an den NetApp Support, wenn Sie Hilfe benötigen.

  Bei einem Upgrade auf Element 12.5 oder höher wird der `BmcSelfTestFailed` Ein Fehler wird nicht bei einem Knoten generiert, der bereits über einen BMC-Fehler verfügt, oder wenn der BMC eines Knotens während des Upgrades ausfällt. Die BMCs, die die Selbsttests während des Upgrades nicht bestanden haben, geben eine aus `BmcSelfTestFailed` Warnfehler, nachdem das gesamte Cluster das Upgrade abgeschlossen hat.

- **ClockSkewExceedsFaultThreshold**

  Zeitverzerrung zwischen dem Cluster-Master und dem Node, der ein Token enthält, übersteigt den empfohlenen Schwellenwert. Storage Cluster kann die Zeitverzerrung zwischen den Nodes nicht automatisch korrigieren.

  Um diesen Fehler zu beheben, verwenden Sie NTP-Server, die intern zu Ihrem Netzwerk sind, anstatt die Installationsstandards. Wenn Sie einen internen NTP-Server verwenden, wenden Sie sich an den NetApp

Support.

- * ClusterCannotSync*

  Es ist ein nicht genügend Speicherplatz vorhanden, und Daten auf den Offline-Blockspeicherlaufwerken können nicht mit Laufwerken synchronisiert werden, die noch aktiv sind.

  Um diesen Fehler zu beheben, fügen Sie mehr Speicher hinzu.

- * ClusterFull*

  Es ist kein freier Speicherplatz im Storage-Cluster mehr verfügbar.

  Um diesen Fehler zu beheben, fügen Sie mehr Speicher hinzu.

- **ClusterIOPSAreüberProvistiert**

  Cluster-IOPS werden überprovisioniert. Die Summe aller minimalen QoS-IOPS ist größer als die erwarteten IOPS des Clusters. Eine minimale QoS kann nicht für alle Volumes gleichzeitig aufrechterhalten werden.

  Senken Sie zur Behebung dieses Problems die Mindesteinstellungen für QoS-IOPS für Volumes.

- **CpuThermalEventThreshold**

  Die Anzahl der thermischen CPU-Ereignisse auf einer oder mehreren CPUs überschreitet den konfigurierten Schwellenwert.

  Wenn innerhalb von zehn Minuten keine neuen thermischen CPU-Ereignisse erkannt werden, löst sich die Warnung.

- **AbleDriveSecurityFailed**

  Das Cluster ist nicht für das Aktivieren der Laufwerksicherheit konfiguriert (Verschlüsselung im Ruhezustand), aber mindestens ein Laufwerk ist die Laufwerksicherheit aktiviert, was bedeutet, dass die Laufwerksicherheit auf diesen Laufwerken deaktiviert ist. Dieser Fehler wird mit dem Schweregrad „`Warnung`“ protokolliert.

  Um diesen Fehler zu beheben, überprüfen Sie die Fehlerdetails aus dem Grund, warum die Laufwerksicherheit nicht deaktiviert werden konnte. Mögliche Gründe sind:

  - Der Verschlüsselungsschlüssel konnte nicht erworben werden. Untersuchen Sie das Problem mit dem Zugriff auf den Schlüssel oder den externen Schlüsselserver.
  - Der Vorgang zum Deaktivieren des Laufwerks ist fehlgeschlagen. Stellen Sie fest, ob der falsche Schlüssel möglicherweise erfasst wurde.

    Wenn keiner dieser Gründe den Fehler Gründe hat, muss das Laufwerk möglicherweise ausgetauscht werden.

  Sie können versuchen, ein Laufwerk wiederherzustellen, das die Sicherheit nicht erfolgreich deaktiviert, selbst wenn der richtige Authentifizierungsschlüssel angegeben ist. Entfernen Sie die Laufwerke aus dem System, indem Sie sie auf verfügbar verschieben, löschen Sie sie sicher auf dem Laufwerk, und verschieben Sie sie wieder in aktiv.

- **DisconnectedClusterpaar**

Ein Cluster-Paar ist getrennt oder falsch konfiguriert.

Überprüfen Sie die Netzwerkverbindung zwischen den Clustern.

- **Verbindung abschaltenRemoteNode**

  Ein Remote-Knoten ist entweder getrennt oder falsch konfiguriert.

  Überprüfen Sie die Netzwerkverbindung zwischen den Nodes.

- **DemconnectedSnapMirrorEndpoint**

  Ein Remote-SnapMirror-Endpunkt wird getrennt oder falsch konfiguriert.

  Überprüfen Sie die Netzwerkverbindung zwischen dem Cluster und dem Remote-SnapMirrorEndpoint.

- **Auffahrt verfügbar**

  Ein oder mehrere Laufwerke sind im Cluster verfügbar. Im Allgemeinen sollten alle Cluster alle Laufwerke hinzugefügt werden und keine im Status „verfügbar“. Sollte dieser Fehler unerwartet auftreten, wenden Sie sich an den NetApp Support.

  Um diesen Fehler zu beheben, fügen Sie alle verfügbaren Laufwerke zum Speicher-Cluster hinzu.

- * Auffahrt nicht möglich*

  Das Cluster gibt diesen Fehler zurück, wenn ein oder mehrere Laufwerke ausgefallen sind und einer der folgenden Bedingungen anzeigt:

  - Der Laufwerksmanager kann nicht auf das Laufwerk zugreifen.
  - Der Slice- oder Block-Service ist zu oft ausgefallen, vermutlich aufgrund von Lese- oder Schreibfehlern des Laufwerks und kann nicht neu gestartet werden.
  - Das Laufwerk fehlt.
  - Der Master-Service für den Node ist nicht verfügbar (alle Laufwerke im Node gelten als fehlend/ausgefallen).
  - Das Laufwerk ist gesperrt und der Authentifizierungsschlüssel für das Laufwerk kann nicht erworben werden.
  - Das Laufwerk ist gesperrt, und der Entsperrvorgang schlägt fehl.

    So lösen Sie dieses Problem:

  - Überprüfen Sie die Netzwerkverbindung für den Node.
  - Ersetzen Sie das Laufwerk.
  - Stellen Sie sicher, dass der Authentifizierungsschlüssel verfügbar ist.
- **DriveHealthFault**

  Die SMART-Integritätsprüfung auf einem Laufwerk ist fehlgeschlagen, sodass die Funktionen des Laufwerks verringert werden. Es gibt einen kritischen Schweregrad für diesen Fehler:

  - Laufwerk mit serieller Verbindung: <Seriennummer> in Steckplatz: <Node-Steckplatz><Laufwerksfach> hat die INTELLIGENTE allgemeine Integritätsprüfung nicht bestanden.

Um diesen Fehler zu beheben, ersetzen Sie das Laufwerk.

- **DriveWearFault**

  Die Restlebensdauer eines Laufwerks ist unter die Schwellenwerte gesunken, funktioniert aber immer noch.Es gibt zwei mögliche Schweregrade für diesen Fehler: Kritisch und Warnung:

  - Laufwerk mit serieller Verbindung: <Seriennummer> im Steckplatz: <Node-Steckplatz><Laufwerk-Steckplatz> verfügt über einen kritischen Verschleiß.
  - Laufwerk mit serieller Verbindung: <Seriennummer> im Steckplatz: <Node-Steckplatz><Laufwerksfach> verfügt über geringe Verschleißreserven.

    Um diesen Fehler zu beheben, tauschen Sie das Laufwerk bald aus.

- * DuplicateClusterMasterCandidates*

  Es wurden mehr als ein Master-Kandidat für Speichercluster erkannt.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **EnableDriveSecurityFailed**

  Das Cluster ist so konfiguriert, dass es Laufwerkssicherheit (Verschlüsselung im Ruhezustand) benötigt, die Laufwerkssicherheit konnte jedoch auf mindestens einem Laufwerk nicht aktiviert werden. Dieser Fehler wird mit dem Schweregrad „`Warnung`“ protokolliert.

  Um diesen Fehler zu beheben, überprüfen Sie die Fehlerdetails aus dem Grund, warum die Laufwerksicherheit nicht aktiviert werden konnte. Mögliche Gründe sind:

  - Der Verschlüsselungsschlüssel konnte nicht erworben werden. Untersuchen Sie das Problem mit dem Zugriff auf den Schlüssel oder den externen Schlüsselserver.
  - Der Vorgang zum Aktivieren ist auf dem Laufwerk fehlgeschlagen. Stellen Sie fest, ob der falsche Schlüssel möglicherweise erfasst wurde. Wenn keiner dieser Gründe den Fehler Gründe hat, muss das Laufwerk möglicherweise ausgetauscht werden.

  Sie können versuchen, ein Laufwerk wiederherzustellen, das die Sicherheit nicht erfolgreich aktiviert, selbst wenn der richtige Authentifizierungsschlüssel angegeben ist. Entfernen Sie die Laufwerke aus dem System, indem Sie sie auf verfügbar verschieben, löschen Sie sie sicher auf dem Laufwerk, und verschieben Sie sie wieder in aktiv.

- **EnsembleDegraded**

  Die Netzwerk-Konnektivität oder -Stromversorgung wurde auf einen oder mehrere der Ensemble-Knoten verloren.

  Um diesen Fehler zu beheben, stellen Sie die Netzwerkverbindung oder den Netzstrom wieder her.

- **Ausnahme**

  Ein Fehler wurde gemeldet, der sich nicht auf einen Routinefehler ausstellt. Diese Fehler werden nicht automatisch aus der Fehlerwarteschlange gelöscht.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **AusfallenSpaceTooFull**

Ein Blockservice reagiert nicht auf Datenschreibanfragen. Dadurch verfügt der Slice Service über keinen freien Speicherplatz zum Speichern ausgefallener Schreibvorgänge.

Um diesen Fehler zu beheben, stellen Sie die Funktion zur Wiederherstellung von Blockdiensten wieder her, damit Schreibvorgänge normal fortgesetzt werden und der fehlerhafte Speicherplatz aus dem Schichtdienst entfernt werden kann.

- **FanSensor**

  Ein Lüftersensor ist ausgefallen oder fehlt.

  Um diesen Fehler zu beheben, ersetzen Sie eine fehlerhafte Hardware.

- **Fiber ChannelAccessDegraded**

  Ein Fibre Channel-Node reagiert nicht auf andere Nodes im Storage-Cluster über einen bestimmten Zeitraum. In diesem Status gilt der Node als nicht ansprechbar und generiert einen Cluster-Fehler.

  Überprüfen Sie die Netzwerkverbindung.

- **FaserChannelAccessUnverfügbar**

  Alle Fibre-Channel-Nodes reagieren nicht mehr. Die Node-IDs werden angezeigt.

  Überprüfen Sie die Netzwerkverbindung.

- **FiberChannelActiveIxL**

  Die Anzahl der iXL-Nexus nähert sich dem unterstützten Limit von 8000 aktiven Sitzungen pro Fibre-Channel-Node.

  - Best Practice-Grenze ist 5500.
  - Warngrenze ist 7500.
  - Die maximale Obergrenze (nicht erzwungen) beträgt 8192.

  Um diesen Fehler zu beheben, reduzieren Sie die Anzahl der iXL Nexus unter dem Best Practice Limit von 5500.

- **Fiber ChannelConfig**

  Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - An einem PCI-Steckplatz befindet sich ein unerwarteter Fibre Channel-Port.
  - Es gibt ein unerwartetes Fibre Channel HBA-Modell.
  - Ein Problem mit der Firmware eines Fibre Channel HBA ist aufgetreten.
  - Ein Fibre-Channel-Port ist nicht online.
  - Bei der Konfiguration von Fibre Channel Passthrough müssen hartnäckige Probleme aufgetreten sein.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **FiberChannelIOPS**

  Die IOPS-Gesamtzahl nähert sich dem IOPS-Limit für Fibre Channel Nodes im Cluster. Die Grenzen sind:

- FC0025: 50.000 IOPS bei 4-KB-Blockgröße pro Fibre Channel Node.
- FCN001: Grenzwert von 625.000 OPS bei einer Blockgröße von 4 KB pro Fibre Channel Node.

Um diesen Fehler zu beheben, verteilen Sie die Last auf alle verfügbaren Fibre Channel Nodes.

- **FiberChannelStaticIxL**

  Die Anzahl der iXL-Nexus nähert sich dem unterstützten Limit von 16000 statischen Sitzungen pro Fibre-Channel-Node.

  - Best Practice-Grenze ist 11000.
  - Warngrenze ist 15000.
  - Die maximale Obergrenze (erzwungen) ist 16384.

  Um diesen Fehler zu beheben, reduzieren Sie die Anzahl der iXL Nexus unter dem Best Practice Limit von 11000.

- **DateiSystemkapazitätNiedrig**

  Auf einem der Dateisysteme ist nicht genügend Platz vorhanden.

  Um diesen Fehler zu beheben, fügen Sie dem Dateisystem mehr Kapazität hinzu.

- **FileSystemIsReadOnly**

  Ein Dateisystem ist in einen schreibgeschützten Modus umgestiegen.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **FipsDrivesMismatch**

  Ein Laufwerk ohne FIPS wurde physisch in einen FIPS-fähigen Storage-Node eingesetzt oder ein FIPS-Laufwerk wurde physisch in einen Storage-Node außerhalb von FIPS eingesetzt. Pro Node wird ein einziger Fehler generiert und alle betroffenen Laufwerke aufgelistet.

  Um diesen Fehler zu beheben, entfernen oder ersetzen Sie das nicht übereinstimmende Laufwerk oder die betreffenden Laufwerke.

- **FipsDriveOutOfCompliance**

  Das System hat erkannt, dass die Verschlüsselung im Ruhezustand nach Aktivierung der FIPS-Festplattenfunktion deaktiviert wurde. Dieser Fehler wird auch generiert, wenn die FIPS-Laufwerksfunktion aktiviert ist und ein Laufwerk oder ein Node außerhalb von FIPS im Storage-Cluster vorhanden ist.

  Um diesen Fehler zu beheben, aktivieren Sie die Verschlüsselung im Ruhezustand oder entfernen Sie die nicht-FIPS-Hardware aus dem Storage-Cluster.

- **FipsSelfTestFailure**

  Das FIPS-Subsystem hat während des Self-Tests einen Ausfall erkannt.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **HardwareConfigMismatch**

Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

- Die Konfiguration stimmt nicht mit der Knotendefinition überein.
- Für diesen Node-Typ gibt es eine falsche Laufwerksgröße.
- Es wurde ein nicht unterstütztes Laufwerk erkannt. Ein möglicher Grund ist, dass die installierte Element-Version dieses Laufwerk nicht erkennt. Es wird empfohlen, die Element Software auf diesem Node zu aktualisieren.
- Es stimmt nicht überein, dass die Laufwerk-Firmware nicht stimmt.
- Der Status für die Laufwerksverschlüsselung stimmt nicht mit dem Node überein.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **IdPCertificateExpiration**

  Das SSL-Zertifikat des Dienstanbieters des Clusters zur Verwendung mit einem Drittanbieter-Identitätsanbieter (IdP) nähert sich dem Ablaufdatum oder ist bereits abgelaufen. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Schweregrad	Beschreibung
Warnung	Das Zertifikat läuft innerhalb von 30 Tagen ab.
Fehler	Das Zertifikat läuft innerhalb von 7 Tagen ab.
Kritisch	Das Zertifikat läuft innerhalb von 3 Tagen ab oder ist bereits abgelaufen.

  Um diesen Fehler zu beheben, aktualisieren Sie das SSL-Zertifikat, bevor es abläuft. Verwenden Sie die UpdateIdpConfiguration API-Methode mit `refreshCertificateExpirationTime=true` Um das aktualisierte SSL-Zertifikat bereitzustellen.

- **Inkonsistenz BondModes**

  Die Bond-Modi auf dem VLAN-Gerät fehlen. Dieser Fehler zeigt den erwarteten Bond-Modus und den derzeit verwendeten Bond-Modus an.

- **Inkonsistent Mtus**

  Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Bond1G-Diskrepanz: Inkonsistente MTUs wurden an Bond1G-Schnittstellen erkannt.
  - Bond10G-Diskrepanz: Inkonsistente MTUs wurden an Bond10G-Schnittstellen erkannt.

  Dieser Fehler zeigt den betreffenden Node oder die betreffenden Knoten zusammen mit dem zugehörigen MTU-Wert an.

- **UnstimmigeDie Routenregeln**

  Die Routingregeln für diese Schnittstelle sind inkonsistent.

- **Inkonsistent SubnetMasken**

Die Netzwerkmaske auf dem VLAN-Gerät stimmt nicht mit der intern aufgezeichneten Netzwerkmaske für das VLAN überein. Dieser Fehler zeigt die erwartete Netzwerkmaske und die aktuell verwendete Netzwerkmaske an.

- **IncorrectBondPortCount**

  Die Anzahl der Bond-Ports ist falsch.

- **InvalidConfiguredFiberChannelNodeCount**

  Eine der beiden erwarteten Fibre-Channel-Node-Verbindungen ist beeinträchtigt. Dieser Fehler wird angezeigt, wenn nur ein Fibre-Channel-Knoten verbunden ist.

  Um diesen Fehler zu beheben, überprüfen Sie die Cluster-Netzwerkkonnektivität und die Netzwerkverkabelung und überprüfen Sie, ob Services ausgefallen sind. Falls keine Netzwerk- oder Serviceprobleme auftreten, wenden Sie sich an den NetApp Support, um einen Fibre Channel-Node zu ersetzen.

- **IrqBalanceFailed**

  Beim Versuch, Interrupts auszugleichen, ist eine Ausnahme aufgetreten.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **KmZertifizierungFault**
  - Das Zertifikat der Root Certification Authority (CA) nähert sich dem Ablaufdatum.

    Um diesen Fehler zu beheben, erwerben Sie ein neues Zertifikat von der Root CA mit Ablaufdatum mindestens 30 Tage aus und verwenden Sie ModifyKeyServerkmip, um das aktualisierte Root CA-Zertifikat bereitzustellen.

  - Das Clientzertifikat nähert sich dem Ablaufdatum.

    Um diesen Fehler zu beheben, erstellen Sie einen neuen CSR mit GetClientCertificateSigningRequest, lassen Sie ihn unterzeichnen, um sicherzustellen, dass das neue Ablaufdatum mindestens 30 Tage beträgt, und verwenden Sie ModifyKeyServerkmip, um das auslaufende KMIP-Clientzertifikat durch das neue Zertifikat zu ersetzen.

  - Das Zertifikat der Root Certification Authority (CA) ist abgelaufen.

    Um diesen Fehler zu beheben, erwerben Sie ein neues Zertifikat von der Root CA mit Ablaufdatum mindestens 30 Tage aus und verwenden Sie ModifyKeyServerkmip, um das aktualisierte Root CA-Zertifikat bereitzustellen.

  - Client-Zertifikat ist abgelaufen.

    Um diesen Fehler zu beheben, erstellen Sie einen neuen CSR mit GetClientCertificateSigningRequest, lassen Sie ihn unterzeichnen, um sicherzustellen, dass das neue Ablaufdatum mindestens 30 Tage beträgt, und verwenden Sie ModifyKeyServerkmip, um das abgelaufene KMIP-Clientzertifikat durch das neue Zertifikat zu ersetzen.

  - Fehler bei der Root Certification Authority (CA)-Zertifizierung.

    Um diesen Fehler zu beheben, überprüfen Sie, ob das richtige Zertifikat bereitgestellt wurde und, falls erforderlich, das Zertifikat von der Stammzertifizierungsstelle erneut erwerben. Verwenden Sie

ModifyKeyServerkmip, um das richtige KMIP-Client-Zertifikat zu installieren.

◦ Fehler beim Client-Zertifikat.

Um diesen Fehler zu beheben, überprüfen Sie, ob das korrekte KMIP-Client-Zertifikat installiert ist. Die Root-CA des Client-Zertifikats sollte auf dem EKS installiert werden. Verwenden Sie ModifyKeyServerkmip, um das richtige KMIP-Client-Zertifikat zu installieren.

- **KmipServerFault**
  - ◦ Verbindungsfehler

    Um diesen Fehler zu beheben, überprüfen Sie, ob der externe Schlüsselserver aktiv ist und über das Netzwerk erreichbar ist. Verwenden Sie TestKeyServerKimp und TestKeyProviderKmip, um Ihre Verbindung zu testen.

  - ◦ Authentifizierungsfehler

    Um diesen Fehler zu beheben, überprüfen Sie, ob die richtige Root-CA- und KMIP-Client-Zertifikate verwendet werden und ob der private Schlüssel und das KMIP-Client-Zertifikat übereinstimmen.

  - ◦ Serverfehler

    Um diesen Fehler zu beheben, überprüfen Sie die Details auf den Fehler. Möglicherweise ist aufgrund des zurückgegebenen Fehlers eine Fehlerbehebung auf dem externen Schlüsselserver erforderlich.

- * MemoryEccThreshold*

  Es wurden eine große Anzahl von korrigierbaren oder nicht korrigierbaren ECC-Fehlern erkannt. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Ereignis	Schweregrad	Beschreibung
Ein einzelnes DIMM cErrorCount erreicht cDimmCorrectableErrWarnThreshold.	Warnung	Korrigierbare ECC-Speicherfehler über dem Schwellenwert auf DIMM: <Prozessor> <DIMM Slot>
Ein einzelnes DIMM cErrorCount bleibt über cDimmCorrectableErrWarnThreshold bis cErrorFaultTimer für das DIMM abläuft.	Fehler	Korrektur von ECC-Speicherfehlern über dem Schwellenwert auf DIMM: <Processor> <DIMM>
Ein Speicher-Controller meldet cErrorCount über cMemCtlrCorrectableErrWarnThreshold und cMemCtlrCorrectableErrWarnDauer wird angegeben.	Warnung	Korrigierbare ECC-Speicherfehler oberhalb des Schwellenwerts für Speicher-Controller: <Prozessor> <Speicher-Controller>

Ein Speicher-Controller meldet cErrorCount über cMemCtlrCorrectableErrWarnThreshold bis cErrorFaultTimer für den Speicher-Controller abläuft.	Fehler	Korrektur von ECC-Speicherfehlern über dem Schwellenwert auf DIMM: <Processor> <DIMM>
Ein einzelnes DIMM meldet einen uErrorCount über Null, aber kleiner als cDimmUncorrectTableErrFaultThreshold.	Warnung	Nicht korrigierbarer ECC-Speicherfehler auf DIMM: <Prozessor> <DIMM Slot> erkannt
Ein einzelnes DIMM meldet einen uErrorCount von mindestens cDimmUncorrectTableErrFaultThreshold.	Fehler	Nicht korrigierbarer ECC-Speicherfehler auf DIMM: <Prozessor> <DIMM Slot> erkannt
Ein Speicher-Controller meldet einen uErrorCount über Null, aber kleiner als cMemCtlrUncorregictErrFaultThreshold.	Warnung	Nicht korrigierbarer ECC-Speicherfehler auf Speichercontroller: <Prozessor> <Speichercontroller> erkannt
Ein Speicher-Controller meldet einen uErrorCount von mindestens cMemCtlrUncorregictErrFaultThreshold.	Fehler	Nicht korrigierbarer ECC-Speicherfehler auf Speichercontroller: <Prozessor> <Speichercontroller> erkannt

Um diesen Fehler zu beheben, wenden Sie sich an den NetApp Support.

- **SpeichernUserageThreshold**

  Die Speicherauslastung ist über dem Normalwert. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

  Weitere Informationen zum Fehlertyp finden Sie in der Überschrift **Details** im Fehlerfehler.

Schweregrad	Beschreibung
Warnung	Der Systemspeicher ist schwach.
Fehler	Der Systemspeicher ist sehr gering.
Kritisch	Der Systemspeicher wird vollständig verbraucht.

Um diesen Fehler zu beheben, wenden Sie sich an den NetApp Support.

- * MetadataClusterFull*

Es ist nicht ausreichend freier Speicherplatz für Metadaten vorhanden, um einen Ausfall eines einzelnen Nodes zu unterstützen. Weitere Informationen zu Cluster-Auslastungsstufen finden Sie in der GetClusterFullThreshold API-Methode. Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Stage3Low (Warnung): Benutzerdefinierter Schwellenwert wurde überschritten. Passen Sie Cluster-Volleinstellungen an oder fügen Sie weitere Nodes hinzu.
  - Stage4Critical (Fehler): Es gibt nicht genügend Speicherplatz zur Wiederherstellung nach einem Ausfall eines 1 Node. Das Erstellen von Volumes, Snapshots und Klonen ist nicht zulässig.
  - Stage5CompletelyConsumed (kritisch)1; es sind keine Schreibzugriffe oder neue iSCSI-Verbindungen zulässig. Aktuelle iSCSI-Verbindungen werden beibehalten. Schreibzugriffe scheitern, bis mehr Kapazität dem Cluster hinzugefügt wird. Löschen oder Löschen von Daten oder Hinzufügen weiterer Nodes

Löschen oder löschen Sie Volumes, um diesen Fehler zu beheben, oder fügen Sie dem Storage-Cluster einen weiteren Storage-Node hinzu.

- **MtuCheckFailure**

  Ein Netzwerkgerät ist nicht für die richtige MTU-Größe konfiguriert.

  Um diesen Fehler zu beheben, stellen Sie sicher, dass alle Netzwerkschnittstellen und Switch-Ports für Jumbo Frames konfiguriert sind (MTUs mit einer Größe von bis zu 9000 Byte).

- **NetworkConfig**

  Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Eine erwartete Schnittstelle ist nicht vorhanden.
  - Es ist eine doppelte Schnittstelle vorhanden.
  - Eine konfigurierte Schnittstelle ist ausgefallen.
  - Ein Netzwerkneustart ist erforderlich.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **NoVerfügbarVirtualNetzwerkIPAddresses**

  Im Block der IP-Adressen sind keine virtuellen Netzwerkadressen verfügbar.

  - VirtualNetworkID # TAG(###) hat keine Speicher-IP-Adressen. Dem Cluster können keine weiteren Nodes hinzugefügt werden.

  Um diesen Fehler zu beheben, fügen Sie dem Block der virtuellen Netzwerkadressen weitere IP-Adressen hinzu.

- **NodeHardwareFault (Netzwerkschnittstelle <Name> ist ausgefallen oder das Kabel ist nicht angeschlossen)**

  Eine Netzwerkschnittstelle ist entweder ausgefallen oder das Kabel ist nicht angeschlossen.

  Um diesen Fehler zu beheben, überprüfen Sie die Netzwerkverbindung für den Knoten oder Knoten.

- **NodeHardwareFault (Laufwerksverschlüsselungsstatus entspricht dem Verschlüsselungsstatus des Node für das Laufwerk in Steckplatz <Node-Steckplatz><Laufwerkseinschub>)**

  Ein Laufwerk entspricht nicht den Verschlüsselungsfunktionen des in installierten Storage-Nodes.

- **NodeHardwareFault (Falscher <Laufwerkstyp> Laufwerksgröße <tatsächliche Größe> für das Laufwerk in Steckplatz <Node-Steckplatz><Laufwerkseinschub> für diesen Node-Typ - erwartete <erwartete Größe>)**

  Ein Storage-Node enthält ein Laufwerk, das die falsche Größe für diesen Node hat.

- **NodeHardwareFault (nicht unterstütztes Laufwerk in Steckplatz <Node Slot><Drive Slot> gefunden; Laufwerksstatistiken und Integritätsinformationen sind nicht verfügbar)**

  Ein Storage-Node enthält ein Laufwerk, das nicht unterstützt wird.

- **NodeHardwareFault (das Laufwerk in Slot <Node Slot><Drive Slot> sollte die Firmware-Version <erwartete Version> verwenden, wird aber nicht unterstützte Version <tatsächliche Version> verwenden)**

  Ein Speicherknoten enthält ein Laufwerk, auf dem eine nicht unterstützte Firmware-Version ausgeführt wird.

- **NoteWartungs-Modus**

  Ein Node wurde im Wartungsmodus versetzt. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Schweregrad	Beschreibung
Warnung	Gibt an, dass sich der Node noch im Wartungsmodus befindet.
Fehler	Zeigt an, dass der Wartungsmodus nicht deaktiviert wurde, wahrscheinlich aufgrund von fehlgeschlagenen oder aktiven Standardys.

  Um diesen Fehler zu beheben, deaktivieren Sie den Wartungsmodus nach Abschluss der Wartung. Wenn der Fehler auf der Fehlerebene weiterhin besteht, wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **NodeOffline**

  Element Software kann nicht mit dem angegebenen Node kommunizieren. Überprüfen Sie die Netzwerkverbindung.

- **NotusingLACPBondMode**

  LACP Bonding-Modus ist nicht konfiguriert.

  Um diesen Fehler zu beheben, verwenden Sie LACP Bonding bei der Implementierung von Storage-Nodes. Es kann zu Performance-Problemen kommen, wenn LACP nicht aktiviert und ordnungsgemäß konfiguriert ist.

- **NtpServerUnerreichbar**

  Das Storage-Cluster kann nicht mit dem angegebenen NTP-Server oder den angegebenen Servern kommunizieren.

Um diesen Fehler zu beheben, überprüfen Sie die Konfiguration für den NTP-Server, das Netzwerk und die Firewall.

- **NtpTimeNotInSync**

  Der Unterschied zwischen der Storage-Cluster-Zeit und der angegebenen NTP-Serverzeit ist zu groß. Der Speichercluster kann die Differenz nicht automatisch korrigieren.

  Um diesen Fehler zu beheben, verwenden Sie NTP-Server, die intern zu Ihrem Netzwerk sind, anstatt die Installationsstandards. Wenn Sie interne NTP-Server verwenden und das Problem weiterhin besteht, wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **NvramDeviceStatus**

  Ein NVRAM-Gerät weist einen Fehler auf, ist ausgefallen oder ist ausgefallen. Dieser Fehler weist folgende Schweregrade auf:

Schweregrad	Beschreibung
Warnung	Die Hardware hat eine Warnung erkannt. Dieser Zustand kann vorübergehend sein, z. B. eine Temperaturwarnung. • NvmLifetimeFehler • NvmLifetimeStatus • EnergiengySourceLifetimeStatus • EnergiengySourceTemperatureStatus • WarningThresholdExceped
Fehler	Die Hardware hat einen Fehler oder kritischen Status erkannt. Der Cluster-Master versucht, das Slice-Laufwerk aus dem Betrieb zu entfernen (dies erzeugt ein Ereignis zum Entfernen des Laufwerks). Wenn sekundäre Schichtdienste nicht verfügbar sind, wird das Laufwerk nicht entfernt. Zusätzlich zu den Warnungsebenen-Fehlern zurückgegebene Fehler: • Der Mount-Punkt für NVRAM-Gerät ist nicht vorhanden. • Die NVRAM-Gerätepartition ist nicht vorhanden. • Die NVRAM-Gerätepartition ist vorhanden, aber nicht angehängt.

Kritisch	Die Hardware hat einen Fehler oder kritischen Status erkannt. Der Cluster-Master versucht, das Slice-Laufwerk aus dem Betrieb zu entfernen (dies erzeugt ein Ereignis zum Entfernen des Laufwerks). Wenn sekundäre Schichtdienste nicht verfügbar sind, wird das Laufwerk nicht entfernt. • Persistenz verloren • ArmStatusSaveNArmed • CsaveStatusfehler

Ersetzen Sie alle fehlerhaften Hardware im Node. Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **PowerSupplyError**

  Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Es ist kein Netzteil vorhanden.
  - Ein Netzteil ist fehlgeschlagen.
  - Ein Netzteileingang fehlt oder außerhalb des zulässigen Bereichs liegt.

  Um diesen Fehler zu beheben, überprüfen Sie, ob alle Knoten mit redundanter Stromversorgung versorgt werden. Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **ProvisionedSpaceTooFull**

  Die insgesamt bereitgestellte Kapazität des Clusters ist zu voll.

  Um diesen Fehler zu beheben, fügen Sie mehr bereitgestellten Speicherplatz hinzu oder löschen und löschen Sie Volumes.

- **EntferntRepAsyncDelayExceeded**

  Die konfigurierte asynchrone Verzögerung der Replikation wurde überschritten. Überprüfen Sie die Netzwerkverbindung zwischen Clustern.

- **EntfernteRepClusterFull**

  Die Remote-Replikation der Volumes wurde angehalten, da der Ziel-Storage-Cluster zu voll ist.

  Um diesen Fehler zu beheben, geben Sie Speicherplatz auf dem Ziel-Storage-Cluster frei.

- **EntfernteRepSnapshotClusterFull**

  Die Remote-Replizierung der Snapshots wurde durch die Volumes unterbrochen, weil der Ziel-Storage-Cluster zu voll ist.

  Um diesen Fehler zu beheben, geben Sie Speicherplatz auf dem Ziel-Storage-Cluster frei.

- **EntferntRepSnapshotsExceedLimit**

  Die Volumes haben die Remote-Replizierung von Snapshots angehalten, da das Ziel-Storage-Cluster-

Volume seine Snapshot-Grenze überschritten hat.

Um diesen Fehler zu beheben, erhöhen Sie die Snapshot-Grenze auf dem Ziel-Speicher-Cluster.

- **Fehler beim PlaneActionError**

  Mindestens eine der geplanten Aktivitäten wurde ausgeführt, ist aber fehlgeschlagen.

  Der Fehler wird gelöscht, wenn die geplante Aktivität erneut ausgeführt wird und erfolgreich ist, wenn die geplante Aktivität gelöscht wird oder wenn die Aktivität angehalten und fortgesetzt wird.

- **SensorReadingFailed**

  Ein Sensor konnte nicht mit dem Baseboard Management Controller (BMC) kommunizieren.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **ServiceNotRunning**

  Ein erforderlicher Dienst wird nicht ausgeführt.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **SliceServiceTooFull**

  Einem Schichtdienst ist zu wenig provisionierte Kapazität zugewiesen.

  Um diesen Fehler zu beheben, fügen Sie mehr bereitgestellte Kapazität hinzu.

- **SchliceServiceUngesund**

  Das System hat erkannt, dass ein Schichtdienst ungesund ist und ihn automatisch stillsetzt.

  - Schweregrad = Warnung: Es werden keine Maßnahmen ergriffen. Dieser Warnzeitraum läuft in 6 Minuten ab.
  - Schweregrad = Fehler: Das System setzt Daten automatisch zurück und repliziert seine Daten auf andere gesunde Laufwerke.

  Prüfen Sie auf Probleme mit der Netzwerkverbindung und Hardwarefehler. Es gibt weitere Fehler, wenn bestimmte Hardwarekomponenten ausgefallen sind. Der Fehler wird gelöscht, wenn der Schichtdienst verfügbar ist oder wenn der Dienst deaktiviert wurde.

- **Sshenenabled**

  Der SSH-Service ist auf einem oder mehreren Nodes im Storage-Cluster aktiviert.

  Um diesen Fehler zu beheben, deaktivieren Sie den SSH-Service auf dem entsprechenden Node oder Nodes oder wenden Sie sich an den NetApp Support, um Unterstützung zu erhalten.

- **SslCertificateExpiration**

  Das mit diesem Knoten verknüpfte SSL-Zertifikat nähert sich dem Ablaufdatum oder ist abgelaufen. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Schweregrad	Beschreibung

Warnung	Das Zertifikat läuft innerhalb von 30 Tagen ab.
Fehler	Das Zertifikat läuft innerhalb von 7 Tagen ab.
Kritisch	Das Zertifikat läuft innerhalb von 3 Tagen ab oder ist bereits abgelaufen.

Um diesen Fehler zu beheben, erneuern Sie das SSL-Zertifikat. Wenden Sie sich bei Bedarf an den NetApp Support, um Hilfe zu erhalten.

- * Stranddecacity*

  Ein einzelner Node verursacht mehr als die Hälfte der Storage-Cluster-Kapazität.

  Um die Datenredundanz aufrechtzuerhalten, reduziert das System die Kapazität des größten Node, sodass einige seiner Blockkapazitäten ungenutzt (nicht verwendet) sind.

  Fügen Sie zur Behebung dieses Fehlers weitere Laufwerke zu vorhandenen Speicher-Nodes hinzu oder fügen Sie dem Cluster Storage-Nodes hinzu.

- **TempSensor**

  Ein Temperatursensor meldet höhere Temperaturen als normale Temperaturen. Dieser Fehler kann in Verbindung mit PowerSupplyError oder FanSensor Fehlern ausgelöst werden.

  Um diesen Fehler zu beheben, prüfen Sie, ob Luftstrombehinderungen in der Nähe des Storage-Clusters vorhanden sind. Wenden Sie sich bei Bedarf an den NetApp Support, um Hilfe zu erhalten.

- **Upgrade**

  Ein Upgrade läuft seit mehr als 24 Stunden.

  Setzen Sie das Upgrade fort, oder wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **UnresponsiveService**

  Ein Dienst reagiert nicht mehr.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **VirtualNetworkConfig**

  Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Eine Schnittstelle ist nicht vorhanden.
  - Ein falscher Namespace auf einer Schnittstelle.
  - Eine falsche Netzmaske ist vorhanden.
  - Eine falsche IP-Adresse ist vorhanden.
  - Eine Schnittstelle ist nicht verfügbar und wird nicht ausgeführt.
  - Es gibt eine überflüssige Schnittstelle auf einem Knoten.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **VolumesDegradiert**

  Die Replikation und Synchronisierung der sekundären Volumes ist nicht abgeschlossen. Die Meldung wird gelöscht, wenn die Synchronisierung abgeschlossen ist.

- **VolumesOffline**

  Ein oder mehrere Volumes im Storage-Cluster sind offline. Der Fehler **volumeDegraded** ist ebenfalls vorhanden.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

Zeigen Sie die Node-Performance-Aktivitäten an

Sie können Performance-Aktivitäten für jeden Node in einem grafischen Format anzeigen. Diese Information bietet Echtzeitstatistiken für CPU und Lese-/Schreib-I/O-Vorgänge pro Sekunde (IOPS) für jedes Laufwerk des Node. Das Auslastungsdiagramm wird alle fünf Sekunden aktualisiert, und das Laufwerksstatistiken-Diagramm aktualisiert alle zehn Sekunden.

1. Klicken Sie Auf **Cluster** > **Knoten**.
2. Klicken Sie auf **Aktionen** für den Knoten, den Sie anzeigen möchten.
3. Klicken Sie Auf **Details Anzeigen**.

Sie können bestimmte Punkte in der Zeit auf den Linien- und Balkendiagrammen sehen, indem Sie den Cursor über die Linie oder den Balken positionieren.

Volumenleistung

Anzeigen der Volume-Performance

Sie können detaillierte Performance-Informationen für alle Volumes im Cluster anzeigen. Sie können die Informationen nach der Volume-ID oder einer der Performance-Spalten sortieren. Sie können die Informationen auch nach bestimmten Kriterien filtern.

Sie können ändern, wie oft das System Performanceinformationen auf der Seite aktualisiert, indem Sie auf die Liste **Aktualisieren alle** klicken und einen anderen Wert auswählen. Das Standard-Aktualisierungsintervall ist 10 Sekunden, wenn das Cluster weniger als 1000 Volumes hat, andernfalls beträgt die Standardeinstellung 60 Sekunden. Wenn Sie einen Wert von „nie“ wählen, ist die automatische Aktualisierung der Seite deaktiviert.

Sie können die automatische Aktualisierung durch Klicken auf **Aktivieren der automatischen Aktualisierung** wieder aktivieren.

1. Wählen Sie in der Element UI die Option **Berichterstellung** > **Volume Performance**.
2. Klicken Sie in der Liste Volume auf das Aktionen-Symbol für ein Volume.
3. Klicken Sie Auf **Details Anzeigen**.

   Unten auf der Seite wird ein Fach mit allgemeinen Informationen zum Volume angezeigt.

4. Um weitere Informationen zum Volumen anzuzeigen, klicken Sie auf **Weitere Details**.

   Das System zeigt detaillierte Informationen sowie Performance-Diagramme für das Volume an.

Weitere Informationen

Volume Performance im Detail

Volume Performance im Detail

Auf der Seite Volume Performance auf der Registerkarte Reporting in der Element UI können Sie Performancestatistiken der Volumes anzeigen.

In der folgenden Liste werden die Details beschrieben, die Ihnen zur Verfügung stehen:

- **ID**

  Die vom System generierte ID für das Volume.

- **Name**

  Der Name, der dem Volume bei seiner Erstellung gegeben wurde.

- **Konto**

  Der Name des Kontos, das dem Volume zugewiesen wurde.

- **Zugriffsgruppen**

  Der Name der Zugriffsgruppe oder der Gruppen des Volumes, der das Volume angehört.

- **Volume-Nutzung**

  Ein Prozentwert, der beschreibt, wie viel der Client das Volume verwendet.

  Mögliche Werte:

  - 0 = der Client verwendet das Volume nicht
  - 100 = der Client verwendet das Maximum
  - >100 = der Kunde verwendet den Burst

- **IOPS insgesamt**

  Gesamtzahl der derzeit ausgeführten IOPS (Lese- und Schreibvorgänge) gegenüber dem Volume

- **Lese-IOPS**

  Gesamtzahl der Lese-IOPS, die derzeit auf dem Volume ausgeführt wird

- **Schreib-IOPS**

  Die Gesamtzahl der momentan ausgeführten Schreib-IOPS gegenüber dem Volume.

- **Gesamtdurchsatz**

Der aktuell ausgeführte Gesamtdurchsatz (Lese- und Schreibvorgänge) gegenüber dem Volume.

- **Lesedurchsatz**

  Gesamtmenge des aktuell ausgeführten Lese-Durchsatzes gegenüber dem Volume.

- **Schreibdurchsatz**

  Der Gesamtdurchsatz, der derzeit für das Volume ausgeführt wird.

- **Gesamte Latenz**

  Die durchschnittliche Zeit in Mikrosekunden, die Lese- und Schreibvorgänge auf einem Volume abzuschließen.

- **Leselatenz**

  Die durchschnittliche Zeit in Mikrosekunden, um Lesevorgänge in dem Volume in den letzten 500 Millisekunden abzuschließen.

- **Schreiblatenz**

  Der durchschnittliche Zeitaufwand in Mikrosekunden, um Schreibvorgänge in einem Volume in den letzten 500 Millisekunden abzuschließen.

- **Warteschlangentiefe**

  Die Anzahl der ausstehenden Lese- und Schreibvorgänge auf dem Volume.

- **Durchschnittliche I/O-Größe**

  Durchschnittliche Größe in Byte der letzten I/O-Vorgänge für das Volume in den letzten 500 Millisekunden.

iSCSI-Sitzungen

Anzeigen von iSCSI-Sitzungen

Sie können die iSCSI-Sitzungen anzeigen, die mit dem Cluster verbunden sind. Sie können die Informationen filtern, um nur die gewünschten Sitzungen einzubeziehen.

1. Wählen Sie in der Element UI die Option **Reporting** > **iSCSI-Sitzungen**.
2. Klicken Sie zum Anzeigen der Filterkriterien auf **Filter**.

Weitere Informationen

Details zur iSCSI-Sitzung

Details zur iSCSI-Sitzung

Sie können Informationen zu den iSCSI-Sitzungen anzeigen, die mit dem Cluster verbunden sind.

In der folgenden Liste werden die Informationen beschrieben, die Sie zu den iSCSI-Sitzungen finden können:

- **Knoten**

  Der Node, der die primäre Metadatenpartition für das Volume hostet.

- **Konto**

  Der Name des Kontos, zu dem das Volume gehört. Wenn der Wert leer ist, wird ein Strich (-) angezeigt.

- **Lautstärke**

  Der auf dem Node angegebene Volume-Name.

- **Volumen-ID**

  ID des Volumes, das mit der Ziel-IQN verknüpft ist.

- **Initiator-ID**

  Eine vom System generierte ID für den Initiator.

- **Initiator-Alias**

  Ein optionaler Name für den Initiator, der es einfacher macht, in einer langen Liste den Initiator zu finden.

- **Initator IP**

  Die IP-Adresse des Endpunkts, der die Sitzung initiiert.

- **Initiator-IQN**

  Der IQN des Endpunkts, der die Sitzung initiiert.

- **Ziel-IP**

  Die IP-Adresse des Node, der das Volume hostet.

- **Ziel-IQN**

  Der IQN des Volumes.

- **CHAP**

  Der CHAP-Algorithmus für eine iSCSI-Sitzung. Wenn kein CHAP-Algorithmus verwendet wird, wird ein Bindestrich (-) angezeigt. Verfügbar ab Element 12.8.

- **Erstellt Am**

  Datum, an dem die Sitzung eingerichtet wurde.

Fibre Channel-Sitzungen

Zeigen Sie Fibre-Channel-Sitzungen an

Sie können die Fibre Channel-Sitzungen (FC) anzeigen, die mit dem Cluster verbunden sind. Sie können Informationen so filtern, dass nur die Verbindungen berücksichtigt

werden, die im Fenster angezeigt werden sollen.

1. Wählen Sie in der Element-UI die Option **Reporting** > **FC-Sitzungen**.
2. Klicken Sie zum Anzeigen der Filterkriterien auf **Filter**.

Weitere Informationen

Details zur Fibre Channel-Sitzung

Details zur Fibre Channel-Sitzung

Sie können Informationen zu den aktiven Fibre Channel-Sitzungen (FC) finden, die mit dem Cluster verbunden sind.

In der folgenden Liste werden die Informationen beschrieben, die Sie über die mit dem Cluster verbundenen FC-Sitzungen finden:

- **Knoten-ID**

  Der Node, der die Sitzung für die Verbindung hostet.

- **Knotenname**

  Vom System generierter Node-Name.

- **Initiator-ID**

  Eine vom System generierte ID für den Initiator.

- **Initiator WWPN**

  Der weltweite Port-Name des Initiierenden.

- **Initiator-Alias**

  Ein optionaler Name für den Initiator, der es einfacher macht, in einer langen Liste den Initiator zu finden.

- **Ziel-WWPN**

  Der weltweite Zielname des Ports.

- **Volume Access Group**

  Name der Zugriffsgruppe des Volumes, der die Sitzung angehört.

- **Volume Access Group ID**

  Vom System generierte ID für die Zugriffsgruppe.

Fehlerbehebung bei Laufwerken

Fehlerbehebung bei Laufwerken

Fehlerhafte Solid State-Laufwerke (SSD) können durch ein Ersatzlaufwerk ersetzt

werden. SSDs für SolidFire Storage-Nodes sind Hot-Swap-fähig. Wenn Sie vermuten, dass eine SSD ausgefallen ist, wenden Sie sich an den NetApp Support, um den Fehler zu überprüfen und gehen Sie durch das entsprechende Lösungsverfahren. NetApp Support bietet Ihnen auch Ersatzlaufwerk nach Ihren Service Level Agreements.

So kann ein ausgefallenes Laufwerk eines aktiven Nodes entfernt und durch ein neues SSD-Laufwerk von NetApp ersetzt werden. Es wird nicht empfohlen, nicht ausgefallene Laufwerke in einem aktiven Cluster zu entfernen.

Sie sollten die von NetApp Support vorgeschlagenen vor-Ort-Ersatzteile aufrecht erhalten, um bei einem Ausfall einen sofortigen Austausch des Laufwerks zu ermöglichen.

> Wenn Sie zu Testzwecken einen Laufwerksausfall simulieren, indem Sie ein Laufwerk von einem Node entfernen, müssen Sie 30 Sekunden warten, bevor Sie das Laufwerk wieder in den Laufwerkschacht einsetzen.

Wenn ein Laufwerk ausfällt, verteilt Double Helix die Daten auf dem Laufwerk auf die Nodes, die im Cluster verbleiben. Mehrere Laufwerkausfälle auf demselben Node stellen kein Problem dar, da die Element Software vor zwei Kopien von Daten auf demselben Node schützt. Ein ausgefallenes Laufwerk führt zu den folgenden Ereignissen:

- Daten werden vom Laufwerk migriert.
- Die Gesamtkapazität des Clusters wird nach der Kapazität des Laufwerks verringert.
- Double Helix Datensicherung stellt sicher, dass zwei gültige Kopien der Daten vorhanden sind.

> SolidFire Storage-Systeme unterstützen das Entfernen eines Laufwerks nicht, wenn zu wenig Storage für die Datenmigration erforderlich ist.

Finden Sie weitere Informationen

- Entfernen ausgefallener Laufwerke aus dem Cluster
- Grundlegende Fehlersuche bei MDSS-Laufwerken
- Entfernen Sie MDSS-Laufwerke
- "Austausch von Laufwerken für SolidFire Storage-Nodes"
- "Austausch von Laufwerken für Storage-Nodes der Serie H600S"
- "H410S und H610S Hardware-Informationen"
- "Hardwareinformationen zur SF-Series"

Entfernen ausgefallener Laufwerke aus dem Cluster

Das SolidFire-System setzt ein Laufwerk in den Status „ausgefallen“, wenn die Selbstdiagnose des Laufwerks den Node angibt, an dem es ausgefallen ist, oder ob die Kommunikation mit dem Laufwerk fünf oder anderthalb Minuten lang unterbrochen wird. Das System zeigt eine Liste der ausgefallenen Laufwerke an. Sie müssen ein ausgefallenes Laufwerk von der Liste ausgefallener Laufwerke in der NetApp Element-Software entfernen.

Laufwerke in der Liste **Alerts** werden als **blockServiceUnHealthy** angezeigt, wenn ein Knoten offline ist.

Wenn der Node und seine Laufwerke beim Neustart innerhalb von fünf und anderthalb Minuten wieder online sind, werden die Laufwerke automatisch aktualisiert und fortgesetzt, wenn die aktiven Laufwerke im Cluster wieder verfügbar sind.

1. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke**.
2. Klicken Sie auf **fehlgeschlagen**, um die Liste der fehlgeschlagenen Laufwerke anzuzeigen.
3. Notieren Sie sich die Steckplatznummer des ausgefallenen Laufwerks.

   Sie benötigen diese Informationen, um das ausgefallene Laufwerk im Chassis zu finden.

4. Entfernen Sie die ausgefallenen Laufwerke mithilfe einer der folgenden Methoden:

Option	Schritte
Um einzelne Laufwerke zu entfernen	a. Klicken Sie auf **Aktionen** für das Laufwerk, das Sie entfernen möchten. b. Klicken Sie Auf **Entfernen**.
Um mehrere Laufwerke zu entfernen	a. Wählen Sie alle Laufwerke aus, die Sie entfernen möchten, und klicken Sie auf **Massenaktionen**. b. Klicken Sie Auf **Entfernen**.

Grundlegende Fehlersuche bei MDSS-Laufwerken

Metadaten (oder Slice)-Laufwerke können wiederhergestellt werden, indem sie zu dem Cluster hinzugefügt werden, wenn ein oder beide Metadaten-Laufwerke ausfallen. Sie können den Wiederherstellungsvorgang in der NetApp Element-Benutzeroberfläche ausführen, wenn die MDSS-Funktion bereits auf dem Knoten aktiviert ist.

Wenn es bei einem oder beiden Metadatenlaufwerken in einem Node zu einem Ausfall kommt, wird der Slice-Service heruntergefahren und Daten von beiden Laufwerken werden auf unterschiedlichen Laufwerken im Node gesichert.

In den folgenden Szenarien werden mögliche Fehler-Szenarien beschrieben und grundlegende Empfehlungen zur Behebung des Problems bereitgestellt:

Systemscheibe schlägt fehl

- In diesem Szenario wird der Steckplatz 2 überprüft und in einen verfügbaren Status zurückgeführt.
- Das Systemschichtlaufwerk muss neu befüllt werden, bevor der Schichtdienst wieder in den Online-Modus versetzt werden kann.
- Sie sollten das System-Slice-Laufwerk ersetzen, wenn das System-Slice-Laufwerk verfügbar ist, fügen Sie das Laufwerk und das Steckplatz-2-Laufwerk gleichzeitig hinzu.

Sie können das Laufwerk in Steckplatz 2 nicht selbst als Metadatenlaufwerk hinzufügen. Sie müssen beide Laufwerke gleichzeitig zum Node hinzufügen.

Steckplatz 2 fällt aus

- In diesem Szenario wird das Systemschichtlaufwerk überprüft und in einen verfügbaren Zustand zurückgeführt.
- Sie sollten Steckplatz 2 durch ein Ersatzlaufwerk ersetzen, wenn Steckplatz 2 verfügbar ist, fügen Sie das SystemSlice-Laufwerk und das Laufwerk Steckplatz 2 gleichzeitig hinzu.

System-Slice-Laufwerk und Steckplatz 2 schlägt fehl

- Sie sollten beide Systemscheiben-Laufwerke und Steckplatz 2 durch ein Ersatzlaufwerk ersetzen. Wenn beide Laufwerke verfügbar sind, fügen Sie das Systemlaufwerk und das Laufwerk Steckplatz 2 gleichzeitig hinzu.

Reihenfolge der Vorgänge

- Ersetzen Sie das ausgefallene Hardwarelaufwerk durch ein Ersatzlaufwerk (ersetzen Sie beide Laufwerke, wenn beide ausgefallen sind).
- Fügen Sie wieder Laufwerke zum Cluster hinzu, wenn sie wieder gefüllt wurden und sich in einem verfügbaren Zustand befinden.

Überprüfung des Betriebs

- Überprüfen Sie, ob die Laufwerke in Steckplatz 0 (oder intern) und Steckplatz 2 in der Liste „Aktive Laufwerke“ als Metadatenlaufwerke identifiziert werden.
- Vergewissern Sie sich, dass der gesamte Schichtausgleich abgeschlossen ist (es sind mindestens 30 Minuten lang keine weiteren Verschieben von Slices im Ereignisprotokoll vorhanden).

Finden Sie weitere Informationen

Fügen Sie MDSS-Laufwerke hinzu

Fügen Sie MDSS-Laufwerke hinzu

Sie können ein zweites Metadatenlaufwerk auf einem SolidFire-Knoten hinzufügen, indem Sie das Blocklaufwerk in Steckplatz 2 in ein Slice-Laufwerk konvertieren. Dies wird durch die Aktivierung der MDSS-Funktion (Multi-Drive Slice Service) erreicht. Um diese Funktion zu aktivieren, müssen Sie sich an den NetApp Support wenden.

Wenn Sie ein Slice-Laufwerk in einen verfügbaren Zustand bringen, muss möglicherweise ein ausgefallenes Laufwerk durch ein neues oder ein neues Ersatzlaufwerk ersetzt werden. Sie müssen das System-Slice-Laufwerk gleichzeitig hinzufügen, wenn Sie das Laufwerk für Steckplatz 2 hinzufügen. Wenn Sie versuchen, das Slice-Laufwerk für Steckplatz 2 allein oder vor dem Hinzufügen des Slice-Laufwerks hinzuzufügen, wird das System einen Fehler generieren.

1. Klicken Sie Auf **Cluster** > **Laufwerke**.
2. Klicken Sie auf **verfügbar**, um die Liste der verfügbaren Laufwerke anzuzeigen.
3. Wählen Sie die zu addieren Slice-Laufwerke aus.
4. Klicken Sie Auf **Massenaktionen**.
5. Klicken Sie Auf **Hinzufügen**.
6. Bestätigen Sie auf der Registerkarte * Aktive Laufwerke*, dass die Laufwerke hinzugefügt wurden.

Entfernen Sie MDSS-Laufwerke

Sie können die MDSS-Laufwerke (Slice Service) mit mehreren Laufwerken entfernen. Dieser Vorgang gilt nur, wenn der Knoten über mehrere Slice-Laufwerke verfügt.

> Wenn das System-Slice-Laufwerk und das Steckplatz-2-Laufwerk ausfallen, schaltet das System die Services ab und entfernt die Laufwerke. Wenn kein Ausfall auftritt und Sie die Laufwerke entfernen, müssen beide Laufwerke gleichzeitig entfernt werden.

1. Klicken Sie Auf **Cluster** > **Laufwerke**.
2. Klicken Sie auf der Registerkarte **Available** Drives auf das Kontrollkästchen für die zu entfernenden Slice Drives.
3. Klicken Sie Auf **Massenaktionen**.
4. Klicken Sie Auf **Entfernen**.
5. Bestätigen Sie die Aktion.

Fehlerbehebung für Nodes

Knoten aus einem Cluster entfernen

Sie können Nodes zu Wartungs- oder Austauschzwecken aus einem Cluster entfernen. Sie sollten die NetApp Element-UI oder -API verwenden, um Nodes zu entfernen, bevor Sie sie in den Offline-Modus versetzen.

Ein Überblick über das Verfahren zum Entfernen von Storage-Nodes:

- Stellen Sie sicher, dass im Cluster genügend Kapazität verfügbar ist, um eine Kopie der Daten auf dem Node zu erstellen.
- Entfernen Sie Laufwerke aus dem Cluster mithilfe der UI oder der RemoveDrives API-Methode.

  Daher werden Daten im System von Laufwerken des Node auf andere Laufwerke im Cluster migriert. Die Dauer dieses Prozesses hängt davon ab, wie viele Daten migriert werden müssen.

- Entfernen Sie den Node aus dem Cluster.

Beachten Sie die folgenden Überlegungen, bevor Sie einen Node herunterfahren oder hochfahren:

- Das Herunterfahren von Nodes und Clustern birgt Risiken, wenn die Performance nicht ordnungsgemäß erbracht wird.

  Das Herunterfahren eines Node sollte unter Anleitung von NetApp Support erfolgen.

- Wenn ein Node unter jeder Art von Herunterfahren länger als 5.5 Minuten ausgefallen ist, beginnt die Double Helix Datensicherung mit der Aufgabe, einzelne replizierte Blöcke auf einen anderen Node zu schreiben, um die Daten zu replizieren. In diesem Fall wenden Sie sich an den NetApp Support, um Hilfe bei der Analyse des ausgefallenen Nodes zu erhalten.
- Um einen Knoten sicher neu zu starten oder herunterzufahren, können Sie den API-Befehl Herunterfahren verwenden.
- Wenn ein Node sich in einem „down“ oder „Off“ befindet, müssen Sie den NetApp Support kontaktieren, bevor Sie ihn wieder in den Online-Status versetzen.

- Nachdem ein Node wieder online geschaltet wurde, müssen Sie die Laufwerke je nach Dauer des Service zurück zum Cluster hinzufügen.

Finden Sie weitere Informationen

"Austausch eines fehlerhaften SolidFire-Chassis"

"Austausch eines fehlerhaften H600S-Series-Knotens"

Schalten Sie ein Cluster aus

Gehen Sie wie folgt vor, um ein gesamtes Cluster herunterzufahren.

Schritte

1. (Optional) Wenden Sie sich an den NetApp Support, um Hilfe beim Abschluss der ersten Schritte zu erhalten.
2. Vergewissern Sie sich, dass alle I/O-Vorgänge angehalten wurden.
3. Trennen Sie alle iSCSI-Sitzungen:
   a. Navigieren Sie zur Management Virtual IP (MVIP)-Adresse auf dem Cluster, um die Element-UI zu öffnen.
   b. Beachten Sie die in der Liste Knoten aufgeführten Knoten.
   c. Führen Sie die Shutdown-API-Methode mit der Stopp-Option aus, die für jede Node-ID im Cluster angegeben ist.

> Wenn Sie das Cluster neu starten, müssen Sie bestimmte Schritte durchführen, um zu überprüfen, ob alle Nodes online sind:
>
> 1. Stellen Sie sicher, dass alle kritischen Schweregrad und `volumesOffline` Clusterfehler wurden behoben.
> 2. Warten Sie 10 bis 15 Minuten, bis sich das Cluster absetzen lässt.
> 3. Starten Sie, um die Hosts für den Zugriff auf die Daten aufzurufen.
>
> Wenn Sie beim Einschalten der Knoten mehr Zeit einplanen und überprüfen möchten, ob sie nach der Wartung ordnungsgemäß sind, wenden Sie sich an den technischen Support, um Hilfe bei der Verzögerung der Datensynchronisierung zu erhalten, um unnötige bin-Synchronisierung zu vermeiden.

Weitere Informationen

"Ordnungsgemäß Herunterfahren und Einschalten eines NetApp SolidFire/HCI Storage-Clusters"

Storage-Nodes: Dienstprogramme pro Node unterstützen

Storage-Nodes: Dienstprogramme pro Node unterstützen

Sie können die Dienstprogramme pro Node verwenden, um Netzwerkprobleme zu beheben, wenn die Standard-Monitoring-Tools der NetApp Element-Software nicht genügend Informationen zur Fehlerbehebung enthalten. Dienstprogramme pro Node bieten spezifische Informationen und Tools, die Sie bei der Fehlerbehebung bei

Netzwerkproblemen zwischen Nodes oder mit dem Management-Node unterstützen.

Weitere Informationen

- Über die UI pro Node können Sie auf Einstellungen pro Node zugreifen
- Details zu den Netzwerkeinstellungen in der Benutzeroberfläche pro Node
- Details zu den Cluster-Einstellungen erhalten Sie über die UI pro Node
- Führen Sie Systemtests über die UI pro Node aus
- Führen Sie Systemdienstprogramme über die UI pro Node aus

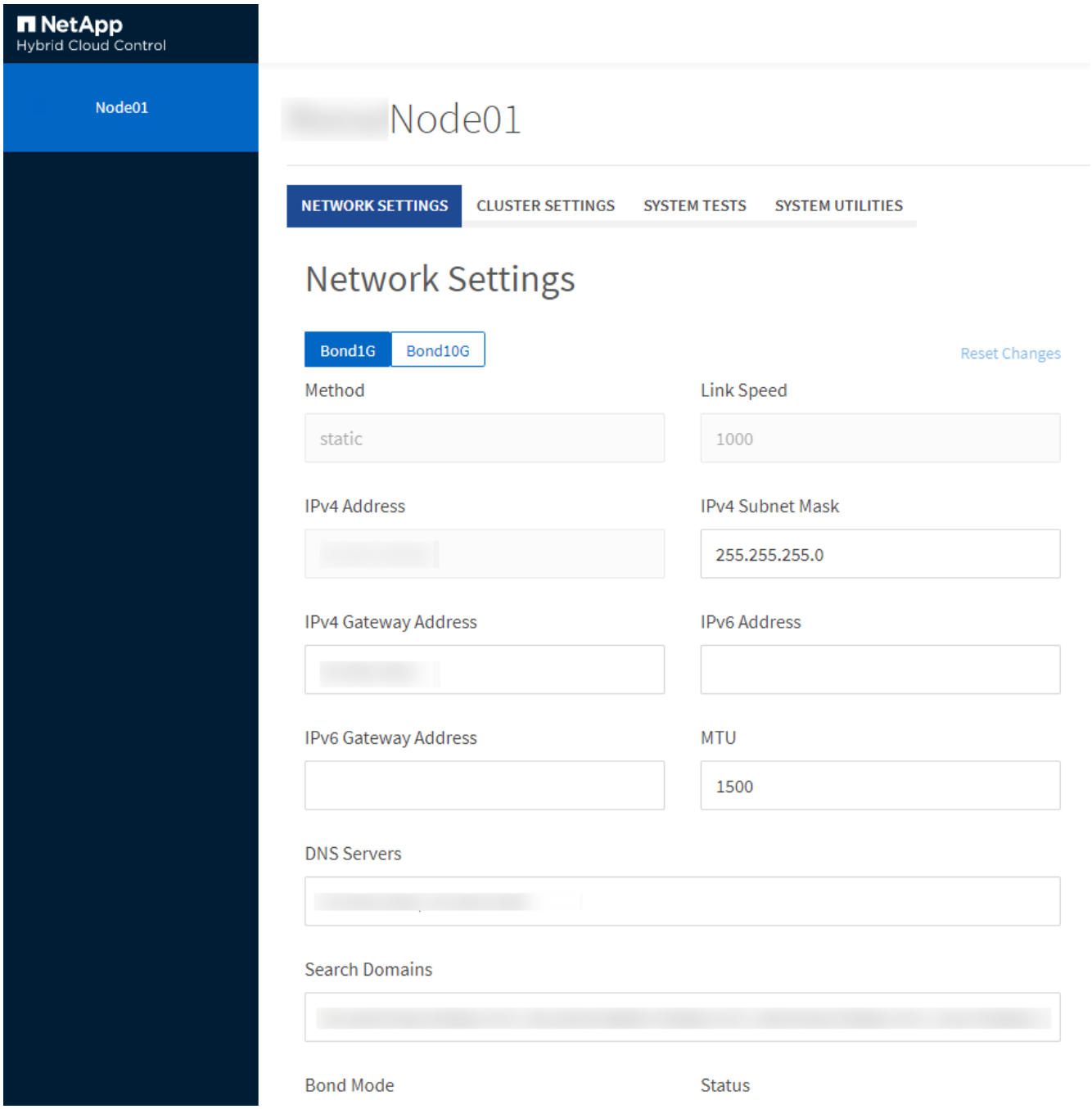
Über die UI pro Node können Sie auf Einstellungen pro Node zugreifen

Nach Eingabe der Management-Node-IP und Authentifizierung haben Sie in der Benutzeroberfläche per Node Zugriff auf Netzwerkeinstellungen, Cluster-Einstellungen sowie Systemtests und Dienstprogramme.

Wenn Sie die Einstellungen für einen Node in einem aktiven Status ändern möchten, der Teil eines Clusters ist, müssen Sie sich als Cluster-Administrator-Benutzer einloggen.

Sie sollten Nodes jeweils einzeln konfigurieren oder ändern. Sie sollten sicherstellen, dass die angegebenen Netzwerkeinstellungen den erwarteten Effekt haben und dass das Netzwerk stabil und gut funktioniert, bevor Sie Änderungen an einem anderen Node vornehmen.

1. Öffnen Sie die UI pro Node mit einer der folgenden Methoden:
   - Geben Sie die Management-IP-Adresse gefolgt von :442 in einem Browser-Fenster ein, und melden Sie sich mit einem Admin-Benutzernamen und -Passwort an.
   - Wählen Sie in der Element UI **Cluster** > **Nodes** aus und klicken Sie auf den Link Management-IP-Adresse für den Knoten, den Sie konfigurieren oder ändern möchten. Im geöffneten Browser-Fenster können Sie die Einstellungen des Node bearbeiten.



Details zu den Netzwerkeinstellungen in der Benutzeroberfläche pro Node

Sie können die Netzwerkeinstellungen des Storage-Nodes ändern, um dem Node einen neuen Satz an Netzwerkattributen zuzuweisen.

Die Netzwerkeinstellungen eines Speicherknotens können Sie auf der Seite **Netzwerkeinstellungen** einsehen, nachdem Sie sich beim Knoten angemeldet haben. (`https://<node_IP>:442/hcc/node/network-settings`). Sie können entweder die Einstellungen **Bond1G** (Verwaltung) oder **Bond10G** (Speicherung) auswählen. Die folgende Liste beschreibt die Einstellungen, die Sie ändern können, wenn sich ein Speicherknoten im Status „Verfügbar“, „Ausstehend“ oder „Aktiv“ befindet:

- **Methode**

  Die Methode zum Konfigurieren der Schnittstelle. Mögliche Methoden:

- Loopback: Wird verwendet, um die IPv4-Loopback-Schnittstelle zu definieren.
- Manuell: Wird verwendet, um Schnittstellen zu definieren, für die keine Konfiguration standardmäßig erfolgt.
- dhcp: Wird verwendet, um eine IP-Adresse über DHCP zu erhalten.
- Statisch: Zur Definition von Ethernet-Schnittstellen mit statisch zugewiesenen IPv4-Adressen.

- **Verbindungsgeschwindigkeit**

  Die von der virtuellen NIC ausgehandelte Geschwindigkeit.

- * IPv4-Adresse*

  Die IPv4-Adresse für das eth0-Netzwerk.

- **IPv4-Subnetzmaske**

  Adressbereiche des IPv4-Netzwerks.

- * IPv4 Gateway-Adresse*

  Netzwerkadresse des Routers für das Senden von Paketen aus dem lokalen Netzwerk.

- * IPv6-Adresse*

  Die IPv6-Adresse für das eth0-Netzwerk.

- * IPv6 Gateway-Adresse*

  Netzwerkadresse des Routers für das Senden von Paketen aus dem lokalen Netzwerk.

- **MTU**

  Größte Paketgröße, die ein Netzwerkprotokoll übertragen kann. Muss größer als oder gleich 1500 sein. Wenn Sie eine zweite Speicher-NIC hinzufügen, sollte der Wert 9000 sein.

- **DNS-Server**

  Für die Cluster-Kommunikation verwendete Netzwerkschnittstelle.

- **Domänen Suchen**

  Suche nach zusätzlichen MAC-Adressen, die dem System zur Verfügung stehen.

- **Bond-Modus**

  Dies kann einer der folgenden Modi sein:

  - ActivePassive (Standard)
  - ALB
  - LACP

- **Status**

  Mögliche Werte:

- UpAndRunning
- Runter
- Hoch

- **Virtual Network Tag**

  Das Tag wurde beim Erstellen des virtuellen Netzwerks zugewiesen.

- **Routen**

  Statische Routen zu bestimmten Hosts oder Netzwerken über die zugewiesene Schnittstelle, die die Routen für die Verwendung konfiguriert sind.

Details zu den Cluster-Einstellungen erhalten Sie über die UI pro Node

Sie können die Cluster-Einstellungen für einen Storage-Node nach der Cluster-Konfiguration überprüfen und den Node-Hostnamen ändern.

Die folgende Liste beschreibt die Clustereinstellungen für einen Speicherknoten, der auf der Seite **Clustereinstellungen** der Benutzeroberfläche pro Knoten angegeben ist. (`https://<node_IP>:442/hcc/node/cluster-settings`).

- * Rolle*

  Rolle, die der Node im Cluster hat. Mögliche Werte:

  - Storage: Storage oder Fibre Channel-Node
  - Management: Node ist ein Management-Node.

- **Hostname**

  Der Name des Node.

- * Cluster*

  Der Name des Clusters.

- **Cluster Mitgliedschaft**

  Status des Node. Mögliche Werte:

  - Verfügbar: Der Node ist keinem Cluster-Namen zugeordnet und ist noch nicht Teil eines Clusters.
  - Ausstehend: Der Node ist konfiguriert und kann einem bestimmten Cluster hinzugefügt werden. Für den Zugriff auf den Node ist keine Authentifizierung erforderlich.
  - PendingActive: Das System installiert gerade kompatible Software auf dem Knoten. Nach Abschluss der Migration wird der Node in den Status „aktiv“ verschoben.
  - Aktiv: Der Knoten nimmt an einem Cluster Teil. Zum Ändern des Node ist eine Authentifizierung erforderlich.

- **Version**

  Version der Element Software, die auf dem Node ausgeführt wird

- **Ensemble**

  Knoten, die Teil des Datenbankensembles sind.

- **Knoten-ID**

  ID wird zugewiesen, wenn dem Cluster ein Node hinzugefügt wird.

- * Clusterschnittstelle*

  Für die Cluster-Kommunikation verwendete Netzwerkschnittstelle.

- **Management-Schnittstelle**

  Management-Netzwerkschnittstelle. Dies ist standardmäßig Bond1G, kann aber auch Bond10G verwenden.

- **Storage-Schnittstelle**

  Storage-Netzwerk-Schnittstelle mit Bond10G.

- **Verschlüsselungsfähig**

  Gibt an, ob der Node die Laufwerkverschlüsselung unterstützt.

Führen Sie Systemtests über die UI pro Node aus

Sie können Änderungen an den Netzwerkeinstellungen testen, nachdem Sie sie zur Netzwerkkonfiguration übergeben haben. Sie können die Tests durchführen, um sicherzustellen, dass der Storage-Node stabil ist und ohne Probleme online geschaltet werden kann.

Sie haben sich bei der UI pro Node für den Storage-Node angemeldet.

1. Klicken Sie Auf **Systemtests**.
2. Klicken Sie neben dem Test, den Sie ausführen möchten, auf **Test ausführen** oder wählen Sie **Alle Tests ausführen**.

   Alle Testvorgänge können zeitaufwändig sein und sollten nur Richtung NetApp Support ausgeführt werden.

   - **Angeschlossenes Ensemble Testen**

     Testet und überprüft die Verbindung zu einem Datenbankensemble. Standardmäßig verwendet der Test das Ensemble für den Cluster, dem der Knoten zugeordnet ist. Alternativ können Sie auch ein anderes Ensemble zur Prüfung der Konnektivität bereitstellen.

   - * Testen Sie Connect Mvip*

     Sendet eine Pings der angegebenen MVIP-Adresse (Management Virtual IP) und führt dann einen einfachen API-Aufruf an das MVIP aus, um die Konnektivität zu überprüfen. Standardmäßig verwendet der Test das MVIP für das Cluster, dem der Node zugeordnet ist.

- * Testen Sie Connect Svip*

  Pings der angegebenen virtuellen Speicher-IP-Adresse (SVIP) mit ICMP-Paketen (Internet Control Message Protocol), die mit der auf dem Netzwerkadapter festgelegten Maximum Transmission Unit (MTU)-Größe übereinstimmen. Er stellt dann eine Verbindung zum SVIP als iSCSI-Initiator her. Standardmäßig verwendet der Test das SVIP für das Cluster, dem der Node zugeordnet ist.

- **Hardware-Konfiguration Testen**

  Testet die Richtigkeit aller Hardware-Konfigurationen, validiert die richtigen Firmware-Versionen und bestätigt, dass alle Laufwerke installiert und ordnungsgemäß ausgeführt werden. Dies ist das gleiche wie bei den werkseitigen Tests.

  Dieser Test ist ressourcenintensiv und sollte nur auf Anfrage des NetApp Supports ausgeführt werden.

- * Testen Sie Lokale Konnektivität*

  Testet die Verbindung zu allen anderen Knoten im Cluster, indem an jeden Knoten die Cluster-IP (CIP) pinging. Dieser Test wird nur auf einem Node angezeigt, wenn der Node Teil eines aktiven Clusters ist.

- **Test Lokalisieren Cluster**

  Überprüft, ob der Node das in der Cluster-Konfiguration angegebene Cluster finden kann.

- **Netzwerk-Konfiguration Testen**

  Stellt sicher, dass die konfigurierten Netzwerkeinstellungen mit den im System verwendeten Netzwerkeinstellungen übereinstimmen. Dieser Test dient nicht zur Erkennung von Hardwarefehlern, wenn ein Node aktiv an einem Cluster teilnimmt.

- **Ping Testen**

  Gibt eine angegebene Liste von Hosts aus oder, wenn keine angegeben werden, erstellt dynamisch eine Liste aller registrierten Nodes im Cluster und pings für einfache Konnektivität.

- **Remote-Verbindung Testen**

  Testet die Verbindung zu allen Knoten in Remote-gekoppelten Clustern durch Ping-Signal der Cluster-IP (CIP) an jedem Knoten. Dieser Test wird nur auf einem Node angezeigt, wenn der Node Teil eines aktiven Clusters ist.

Führen Sie Systemdienstprogramme über die UI pro Node aus

Über die UI pro Node kann der Storage-Node Supportpakete erstellen oder löschen, Konfigurationseinstellungen für Laufwerke zurücksetzen und Netzwerk- oder Cluster-Services neu starten.

Sie haben sich bei der UI pro Node für den Storage-Node angemeldet.

1. Klicken Sie Auf **Systemdienstprogramme**.
2. Klicken Sie auf die Schaltfläche für das Systemdienstprogramm, das Sie ausführen möchten.

◦ **Steuerleistung**

Neubooten, aus- und wieder einschalten oder den Node herunterfahren.

Dieser Vorgang führt zu einem vorübergehenden Verlust der Netzwerkverbindung.

Geben Sie die folgenden Parameter an:

- Aktion: Optionen umfassen Neustart und Anhalten (Ausschalten).
- Aufwachsverzögerung: Alle zusätzlichen Zeit, bevor der Node wieder online geht.

◦ **Node Logs Sammeln**

Erstellt ein Supportpaket unter dem Verzeichnis /tmp/Bundles des Node.

Geben Sie die folgenden Parameter an:

- Bundle-Name: Eindeutiger Name für jedes erstellte Support-Bundle. Wenn kein Name angegeben wird, werden „Supportbundle“ und der Node-Name als Dateiname verwendet.
- Zusätzliche Args: Dieser Parameter wird dem skript sf_Make_Support_Bundle zugeführt. Dieser Parameter sollte nur auf Anfrage des NetApp Support verwendet werden.
- Timeout sec: Geben Sie die Anzahl der Sekunden an, die auf jede einzelne Ping-Antwort warten sollen.

◦ **Node Logs Löschen**

Löscht alle aktuellen Supportpakete auf dem Knoten, die mit **Cluster Support Bundle erstellen** oder der CreateSupportBundle API-Methode erstellt wurden.

◦ **Laufwerke Zurücksetzen**

Initialisiert die Laufwerke und entfernt alle auf dem Laufwerk vorhandenen Daten. Sie können das Laufwerk in einem vorhandenen Knoten oder einem aktualisierten Knoten wiederverwenden.

Geben Sie den folgenden Parameter an:

- Laufwerke: Liste der Gerätenamen (keine Fahrerkennungen) zum Zurücksetzen.

◦ **Netzwerk-Konfiguration Zurücksetzen**

Unterstützt die Behebung von Netzwerkkonfigurationsproblemen für einen einzelnen Knoten und setzt die Netzwerkkonfiguration eines einzelnen Knotens auf die Werkseinstellungen zurück.

◦ **Knoten Zurücksetzen**

Setzt einen Knoten auf die Werkseinstellungen zurück. Alle Daten werden entfernt, die Netzwerkeinstellungen für den Node jedoch während dieses Vorgangs erhalten. Nodes können nur zurückgesetzt werden, wenn sie einem Cluster nicht zugewiesen sind und sich im verfügbaren Status befinden.

Bei Verwendung dieser Option werden alle Daten, Pakete (Software-Upgrades), Konfigurationen und Protokolldateien vom Knoten gelöscht.

◦ **Netzwerk Neu Starten**

Startet alle Netzwerkdienste auf einem Node neu.

> Dieser Vorgang kann zu einem vorübergehenden Verlust der Netzwerkverbindung führen.

- **Neustart Service**

  Startet die Element Softwareservices auf einem Node neu.

  > Dieser Vorgang kann zu einer temporären Node-Serviceunterbrechung führen. Sie sollten diesen Vorgang nur auf Anweisung des NetApp Supports durchführen.

  Geben Sie die folgenden Parameter an:

  - Dienst: Dienstname, der neu gestartet werden soll.
  - Aktion: Aktion, die auf dem Dienst ausgeführt werden soll. Die Optionen umfassen Start, Stopp und Neustart.

Arbeiten Sie mit dem Management-Node

Sie können den Management-Node (mNode) verwenden, um Systemservices zu aktualisieren, Cluster-Assets und -Einstellungen zu managen, Systemtests und Dienstprogramme auszuführen, Active IQ für das System-Monitoring zu konfigurieren und den NetApp Support-Zugriff zur Fehlerbehebung zu aktivieren.

> Als Best Practice wird nur ein Management Node mit einer VMware vCenter Instanz verknüpft, sodass nicht dieselben Storage- und Computing-Ressourcen oder vCenter Instanzen in mehreren Management Nodes definiert werden müssen.

Siehe "Dokumentation des Management-Node" Finden Sie weitere Informationen.

Erläuterung der Cluster-Auslastungsebenen

Der Cluster, auf dem Element Software ausgeführt wird, generiert Cluster-Fehler, um den Storage-Administrator zu warnen, wenn die Kapazität des Clusters knapp wird. Es gibt drei Ebenen der Cluster-Fülle, die alle in der NetApp Element UI angezeigt werden: Warnung, Fehler und kritisch.

Das System verwendet den BlockClusterFull-Fehlercode, um vor der Speicherfülle des Clusterblocks zu warnen. Sie können die Schweregrade für die Cluster-Fülle über die Registerkarte Meldungen der Element UI anzeigen.

Die folgende Liste enthält Informationen zum Schweregrad BlockClusterFull:

- **Warnung**

  Dies ist eine vom Kunden konfigurierbare Warnung, die angezeigt wird, wenn sich die Blockgröße des Clusters dem Fehlergrad nähert. Diese Stufe wird standardmäßig auf drei Prozent unter der Fehlerebene festgelegt und kann über die Element-UI und -API optimiert werden. Sie müssen so schnell wie möglich zusätzliche Kapazität hinzufügen oder Kapazität freisetzen.

- **Fehler**

  Wenn sich das Cluster in diesem Status befindet und ein Node verloren geht, ist nicht genügend Kapazität im Cluster vorhanden, um die Double Helix Datensicherung wiederherzustellen. Erstellung neuer Volumes, Klone und Snapshots werden allesamt gesperrt, während sich das Cluster in diesem Zustand befindet. Dies ist kein sicherer oder empfohlener Status für ein Cluster in. Sie müssen zusätzliche Kapazität hinzufügen oder Kapazität sofort freisetzen.

- * Kritisch*

  Dieser kritische Fehler ist aufgetreten, da das Cluster zu 100 Prozent verbraucht wird. Die Lösung befindet sich im schreibgeschützten Zustand und es können keine neuen iSCSI-Verbindungen zum Cluster hergestellt werden. Wenn Sie diese Phase erreichen, müssen Sie sofort freisetzen oder mehr Kapazität hinzufügen.

Das System verwendet den MetadaClusterFull Fehlercode, um über die Speicherfülle des Clusters zu warnen. Sie können die Cluster-Metadaten-Storage-Fülle im Abschnitt Cluster-Kapazität auf der Übersichtsseite der Registerkarte Berichterstellung in der Element UI anzeigen.

Die folgende Liste enthält Informationen zu den Schweregraden für MetadataClusterFull:

- **Warnung**

  Dies ist eine vom Kunden konfigurierbare Warnung, die angezeigt wird, wenn sich die Metatdatenkapazität des Clusters dem Schweregrad „Fehler“ nähert. Standardmäßig wird diese Ebene auf drei Prozent unter der Fehlerebene gesetzt und kann über die Element-API optimiert werden. Sie müssen so schnell wie möglich zusätzliche Kapazität hinzufügen oder Kapazität freisetzen.

- **Fehler**

  Wenn sich das Cluster in diesem Status befindet und ein Node verloren geht, ist nicht genügend Kapazität im Cluster vorhanden, um die Double Helix Datensicherung wiederherzustellen. Erstellung neuer Volumes, Klone und Snapshots werden allesamt gesperrt, während sich das Cluster in diesem Zustand befindet. Dies ist kein sicherer oder empfohlener Status für ein Cluster in. Sie müssen zusätzliche Kapazität hinzufügen oder Kapazität sofort freisetzen.

- * Kritisch*

  Dieser kritische Fehler ist aufgetreten, da das Cluster zu 100 Prozent verbraucht wird. Die Lösung befindet sich im schreibgeschützten Zustand und es können keine neuen iSCSI-Verbindungen zum Cluster hergestellt werden. Wenn Sie diese Phase erreichen, müssen Sie sofort freisetzen oder mehr Kapazität hinzufügen.

Folgendes gilt für Cluster-Schwellenwerte mit zwei Nodes:

- Metadaten-Fehler liegt 20 % unter dem kritischen Wert.
- Unter dem kritischen Block-Auslastungsfehler liegt ein Block-Laufwerk (einschließlich ungenutzter Kapazität). Das bedeutet, dass es sich um zwei Blocklaufwerke handelt, die weniger kritisch sind.

Management und Monitoring von Storage mit NetApp Hybrid Cloud Control

Fügen Sie Storage-Cluster mit NetApp Hybrid Cloud Control hinzu und managen Sie sie

Sie können Storage-Cluster zur Bestandsaufnahme der Management-Node-Ressourcen hinzufügen, sodass sie mittels NetApp Hybrid Cloud Control (HCC) gemanagt werden können. Der erste während der Systemeinrichtung hinzugefügte Storage Cluster ist der Standard "Autorisierende Storage-Cluster", Aber zusätzliche Cluster können mit HCC UI hinzugefügt werden.

Nach dem Hinzufügen eines Speicher-Clusters können Sie die Cluster-Performance überwachen, die Anmeldeinformationen für das Storage-Cluster für die verwaltete Ressource ändern oder ein Storage-Cluster aus der Asset-Bestandsaufnahme des Management-Nodes entfernen, wenn dieses nicht mehr mit HCC verwaltet werden muss.

Was Sie benötigen

- **Clusteradministrator-Berechtigungen**: Sie haben Berechtigungen als Administrator auf dem "Autorisierende Storage-Cluster". Das autoritäre Cluster ist das erste Cluster, das während der Systemeinrichtung zur Inventarisierung der Managementknoten hinzugefügt wird.
- **Element Software**: Die NetApp Element Software 11.3 oder höher wird in Ihrer Speichercluster-Version ausgeführt.
- **Management-Node**: Sie haben einen Management-Node mit Version 11.3 oder höher bereitgestellt.
- **Management Services**: Sie haben Ihr Management Services Bundle auf Version 2.17 oder höher aktualisiert.

Optionen

- Fügen Sie einen Storage-Cluster hinzu
- Bestätigen des Storage-Cluster-Status
- Bearbeiten der Anmeldedaten für das Storage-Cluster
- Entfernen eines Storage-Clusters
- Aktivieren und deaktivieren Sie den Wartungsmodus

Fügen Sie einen Storage-Cluster hinzu

Mit NetApp Hybrid Cloud Control können Sie dem Inventory der Management-Node-Ressourcen ein Storage-Cluster hinzufügen. Auf diese Weise können Sie den Cluster mithilfe der HCC-Benutzeroberfläche verwalten und überwachen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an und stellen Sie die autorisierenden Anmeldedaten des Storage-Cluster-Administrators bereit.
2. Wählen Sie im Dashboard oben rechts das Optionsmenü aus und wählen Sie **Konfigurieren**.
3. Wählen Sie im Fensterbereich **Storage Cluster Storage Cluster Details** aus.

4. Wählen Sie **Storage-Cluster Hinzufügen**.
5. Geben Sie die folgenden Informationen ein:
   - Virtuelle IP-Adresse für das Storage-Cluster-Management

     Es können nur Remote-Storage-Cluster hinzugefügt werden, die derzeit nicht von einem Management-Node gemanagt werden.

   - Benutzername und Passwort für den Storage Cluster
6. Wählen Sie **Hinzufügen**.

   Nachdem Sie das Storage-Cluster hinzugefügt haben, kann der Cluster-Bestand bis zu 2 Minuten dauern, bis die neue Ergänzung angezeigt wird. Möglicherweise müssen Sie die Seite in Ihrem Browser aktualisieren, um die Änderungen anzuzeigen.

Bestätigen des Storage-Cluster-Status

Über die Benutzeroberfläche von NetApp Hybrid Cloud Control können Sie den Verbindungsstatus von Storage-Cluster-Ressourcen überwachen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an und stellen Sie die autorisierenden Anmeldedaten des Storage-Cluster-Administrators bereit.
2. Wählen Sie im Dashboard oben rechts das Optionsmenü aus und wählen Sie **Konfigurieren**.
3. Überprüfen Sie den Status von Speicherclustern im Inventar.
4. Wählen Sie im Fensterbereich **Storage Cluster Storage Cluster Details** für weitere Details.

Bearbeiten der Anmeldedaten für das Storage-Cluster

Der Benutzername und das Passwort des Storage-Clusters können Sie über die Benutzeroberfläche von NetApp Hybrid Cloud Control bearbeiten.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an und stellen Sie die autorisierenden Anmeldedaten des Storage-Cluster-Administrators bereit.
2. Wählen Sie im Dashboard oben rechts das Optionsmenü aus und wählen Sie **Konfigurieren**.
3. Wählen Sie im Fensterbereich **Storage Cluster Storage Cluster Details** aus.
4. Wählen Sie für den Cluster das Menü **Aktionen** aus und wählen Sie **Cluster-Anmeldeinformationen bearbeiten**.
5. Aktualisieren Sie den Benutzernamen und das Passwort des Storage-Clusters.
6. Wählen Sie **Speichern**.

Entfernen eines Storage-Clusters

Durch Entfernen eines Storage-Clusters aus NetApp Hybrid Cloud Control wird das Cluster aus der Inventar des Management-Node entfernt. Nachdem Sie ein Storage-Cluster entfernt haben, kann der Cluster nicht mehr von HCC gemanagt werden. Sie können ihn nur aufrufen, indem Sie direkt zur Management-IP-Adresse navigieren.

Sie können das autorisierende Cluster nicht aus dem Bestand entfernen. Um den autorisierenden Cluster zu ermitteln, gehen Sie zu **Benutzerverwaltung > Benutzer**. Der autoritative Cluster wird neben der Überschrift **Benutzer** aufgelistet.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an und stellen Sie die autorisierenden Anmeldedaten des Storage-Cluster-Administrators bereit.
2. Wählen Sie im Dashboard oben rechts das Optionsmenü aus und wählen Sie **Konfigurieren**.
3. Wählen Sie im Fensterbereich **Storage Cluster Storage Cluster Details** aus.
4. Wählen Sie für den Cluster das Menü **Aktionen** aus und wählen Sie **Storage Cluster entfernen**.

   Durch die Auswahl von **Ja** wird der Cluster aus der Installation entfernt.

5. Wählen Sie **Ja**.

Aktivieren und deaktivieren Sie den Wartungsmodus

Wenn Sie einen Storage-Node für Wartungsarbeiten, wie z. B. Software-Upgrades oder Host-Reparaturen, offline schalten müssen, können Sie die Auswirkungen auf den Rest des Storage-Clusters durch auf ein Minimum minimieren Aktivieren Wartungsmodus für diesen Node. Wenn Sie Deaktivieren Im Wartungsmodus wird der Node überwacht, um sicherzustellen, dass bestimmte Kriterien erfüllt werden, bevor der Node aus dem Wartungsmodus wechselt.

Was Sie benötigen

- **Element Software**: Die NetApp Element Software 12.2 oder höher wird in Ihrer Speichercluster-Version ausgeführt.
- **Management-Node**: Sie haben einen Management-Node mit Version 12.2 oder höher bereitgestellt.
- **Management Services**: Sie haben Ihr Management Services Bundle auf Version 2.19 oder höher aktualisiert.
- Sie haben Zugriff auf die Anmeldung auf Administratorebene.

Wartungsmodus aktivieren

Sie können das folgende Verfahren verwenden, um den Wartungsmodus für einen Storage-Cluster-Node zu aktivieren.

Es kann sich nur ein Node gleichzeitig im Wartungsmodus befinden.

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser. Beispiel:

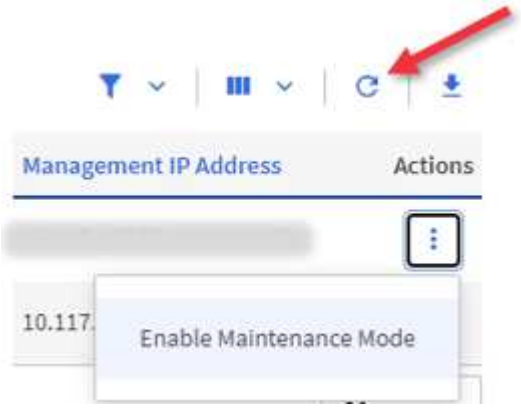
   ```
   https://[management node IP address]
   ```

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des SolidFire All-Flash-Storage-Cluster-Administrators bereitstellen.

Die Funktionsoptionen für den Wartungsmodus sind auf der schreibgeschützten Ebene deaktiviert.

3. Wählen Sie im blauen Feld links die SolidFire-All-Flash-Installation aus.
4. Wählen Sie im linken Navigationsbereich **Knoten** aus.
5. Um Informationen zum Speicherbestand anzuzeigen, wählen Sie **Speicherung**.
6. Aktivieren des Wartungsmodus auf einem Storage-Node:

Die Tabelle der Storage-Nodes wird automatisch alle zwei Minuten für Aktionen aktualisiert, die nicht von Benutzern initiiert wurden. Um sicherzustellen, dass Sie über den aktuellen Status verfügen, können Sie die Knoten-Tabelle aktualisieren, indem Sie das Aktualisierungssymbol oben rechts in der Knotentabelle verwenden.



a. Wählen Sie unter **Actions** die Option **Wartungsmodus aktivieren** aus.

   Während **Wartungsmodus** aktiviert wird, sind Aktionen im Wartungsmodus für den ausgewählten Knoten und alle anderen Knoten im selben Cluster nicht verfügbar.

Nachdem **Aktivieren des Wartungsmodus** abgeschlossen ist, wird in der Spalte **Knotenstatus** ein Schraubenschlüsselsymbol und der Text „**Wartungsmodus**“ für den Knoten angezeigt, der sich im Wartungsmodus befindet.

Wartungsmodus deaktivieren

Nachdem ein Knoten erfolgreich in den Wartungsmodus versetzt wurde, steht für diesen Knoten die Aktion **Wartungsmodus deaktivieren** zur Verfügung. Aktionen auf den anderen Nodes sind erst verfügbar, wenn der Wartungsmodus auf dem Node, der gerade gewartet wird, erfolgreich deaktiviert wurde.

Schritte

1. Wählen Sie für den Knoten im Wartungsmodus unter **Aktionen** die Option **Wartungsmodus deaktivieren** aus.

   Während **Wartungsmodus** deaktiviert wird, sind Aktionen im Wartungsmodus für den ausgewählten Knoten und alle anderen Knoten im selben Cluster nicht verfügbar.

   Nachdem **Wartungsmodus deaktivieren** abgeschlossen ist, wird in der Spalte **Knotenstatus aktiv** angezeigt.

Wenn sich ein Node im Wartungsmodus befindet, werden keine neuen Daten akzeptiert. Daher kann das Deaktivieren des Wartungsmodus länger dauern, da der Node die Daten wieder synchronisieren muss, bevor er den Wartungsmodus beenden kann. Je länger Sie im Wartungsmodus verbringen, desto länger kann es zum Deaktivieren des Wartungsmodus dauern.

Fehlerbehebung

Falls beim Aktivieren oder Deaktivieren des Wartungsmodus Fehler auftreten, wird oben in der Node-Tabelle ein Banner-Fehler angezeigt. Für weitere Informationen über den Fehler können Sie den auf dem Banner bereitgestellten Link **Details anzeigen** wählen, um zu zeigen, was die API zurückgibt.

Weitere Informationen

- "Erstellen und Managen von Storage-Cluster-Assets"
- "Dokumentation von SolidFire und Element Software"

Konfigurieren Sie vollständig qualifizierten Domänennamen Web UI-Zugriff

Mit SolidFire All-Flash-Speicher mit NetApp Element Software 12.2 oder höher können Sie unter Verwendung des vollständig qualifizierten Domain-Namens (FQDN) auf Webschnittstellen des Speicherclusters zugreifen. Wenn Sie den FQDN für den Zugriff auf Webbenutzerschnittstellen wie die Element-Web-UI, die Benutzeroberfläche per Node oder die Management-Node-Benutzeroberfläche verwenden möchten, müssen Sie zuerst eine Speichercluster-Einstellung hinzufügen, um den vom Cluster verwendeten FQDN zu identifizieren.

Durch diesen Prozess kann das Cluster eine Anmeldesitzung ordnungsgemäß umleiten und die Integration in externe Services wie Schlüsselmanager und Identitätsanbieter für die Multi-Faktor-Authentifizierung verbessern.

Was Sie benötigen

- Diese Funktion erfordert Element 12.2 oder höher.
- Für die Konfiguration dieser Funktion mit NetApp Hybrid Cloud Control REST-APIs sind Management-Services 2.15 oder höher erforderlich.
- Für die Konfiguration dieser Funktion mit der NetApp Hybrid Cloud Control UI sind Management-Services ab 2.19 erforderlich.
- Zur Verwendung VON REST-APIs müssen Sie einen Management-Node mit Version 11.5 oder höher bereitgestellt haben.
- Sie benötigen vollqualifizierte Domain-Namen für den Management-Node und jeden Storage-Cluster, die korrekt zur Management Node-IP-Adresse und den einzelnen Storage-Cluster-IP-Adressen auflösen.

Über NetApp Hybrid Cloud Control und DIE REST-API können Sie den FQDN-Webbenutzerzugriff konfigurieren oder entfernen. Sie können auch Fehler bei falsch konfigurierten FQDNs beheben.

- Konfigurieren Sie den FQDN-Web-UI-Zugriff mit NetApp Hybrid Cloud Control

- Konfigurieren Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API
- Entfernen Sie FQDN Web-UI-Zugriff mit NetApp Hybrid Cloud Control
- Entfernen Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API
- Fehlerbehebung

Konfigurieren Sie den FQDN-Web-UI-Zugriff mit NetApp Hybrid Cloud Control

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie das Menüsymbol oben rechts auf der Seite aus.
4. Wählen Sie **Konfigurieren**.
5. Wählen Sie im Fenster **vollqualifizierte Domänennamen** die Option **Einrichtung** aus.
6. Geben Sie im daraufhin angezeigten Fenster die FQDNs für den Managementknoten und jeden Speichercluster ein.
7. Wählen Sie **Speichern**.

   Im Fensterbereich **Fully Qualified Domain Names** werden alle Speichercluster mit dem zugehörigen MVIP und FQDN aufgelistet.

   > Nur verbundene Speichercluster mit dem FQDN-Satz werden im Fensterbereich **vollqualifizierte Domänennamen** aufgeführt.

Konfigurieren Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API

Schritte

1. Stellen Sie sicher, dass die Element-Speicherknoten und der mNode für die Netzwerkumgebung richtig konfiguriert sind, damit FQDNs in der Umgebung aufgelöst werden können. Um DNS einzustellen, wechseln Sie zur Benutzeroberfläche für Speicherknoten pro Knoten und zum Managementknoten und wählen Sie dann **Netzwerkeinstellungen** > **Managementnetzwerk** aus.
   a. UI pro Node für Storage-Nodes: `https://<storage_node_management_IP>:442`
   b. UI pro Node für den Management-Node: `https://<management_node_IP>:442`
2. Ändern Sie die Storage-Cluster-Einstellungen mithilfe der Element API.
   a. Greifen Sie auf die Element API zu, und erstellen Sie mithilfe der die folgende Clusterschnittstelle "CreateClusterSchnittstellenPräferenz" API-Methode, Einfügen des Clusters MVIP FQDN für den Vorzugswert:
      - Name: `mvip_fqdn`
      - Wert: `Fully Qualified Domain Name for the Cluster MVIP`

In diesem Beispiel ist FQDN=storagecluster.my.org:

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

3. Ändern Sie die Management-Node-Einstellungen mit der REST-API auf dem Management-Node:

   a. Rufen Sie die REST-API-UI für den Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode/2/`

      Beispiel:

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

   a. Klicken Sie auf **authorize** oder ein Schloss-Symbol und geben Sie den Cluster-Benutzernamen und das Passwort ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Klicken Sie auf **autorisieren**, um die Sitzung zu starten und dann das Fenster zu schließen.
   d. Wählen Sie in der Liste Server die Option aus `mnode2`.
   e. Klicken Sie auf **GET /settings**.
   f. Klicken Sie auf **Probieren Sie es aus**.
   g. Klicken Sie Auf **Ausführen**.
   h. Notieren Sie alle Proxyeinstellungen, die im Antwortkörper gemeldet wurden.
   i. Klicken Sie auf **PUT/settings**.
   j. Klicken Sie auf **Probieren Sie es aus**.
   k. Geben Sie im Bereich Text anfordern den Management-Node FQDN als Wert für das ein `mnode_fqdn` Parameter.
   l. Geben Sie alle Proxy-Einstellungswerte ein, die Sie zuvor in den verbleibenden Parametern im Anforderungskörper aufgezeichnet haben. Wenn Sie die Proxyparameter leer lassen oder nicht in den Text der Anforderung aufnehmen, werden die vorhandenen Proxyeinstellungen entfernt.
   m. Klicken Sie Auf **Ausführen**.

Entfernen Sie FQDN Web-UI-Zugriff mit NetApp Hybrid Cloud Control

Mit diesem Verfahren können Sie den FQDN-Webzugriff für den Managementknoten und die Speichercluster entfernen.

Schritte

1. Wählen Sie im Fenster **vollqualifizierte Domänennamen** die Option **Bearbeiten** aus.
2. Löschen Sie im resultierenden Fenster den Inhalt im Textfeld **FQDN**.
3. Wählen Sie **Speichern**.

   Das Fenster wird geschlossen, und der FQDN wird nicht mehr im Bereich **Fully Qualified Domain Names** aufgeführt.

Entfernen Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API

Schritte

1. Ändern Sie die Storage-Cluster-Einstellungen mithilfe der Element API.

   a. Greifen Sie auf die Element API zu und löschen Sie mithilfe der die folgende Clusterschnittstelle `DeleteClusterInterfacePreference` API-Methode:

      - Name: `mvip_fqdn`

        Beispiel:

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

2. Ändern Sie die Management-Node-Einstellungen mit der REST-API auf dem Management-Node:

   a. Rufen Sie die REST-API-UI für den Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode/2/`. Beispiel:

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

   b. Wählen Sie **authorize** oder ein Schloss-Symbol aus und geben Sie den Benutzernamen und das Kennwort des Element Clusters ein.

   c. Geben Sie die Client-ID als ein `mnode-client`.

   d. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

   e. Schließen Sie das Fenster.

   f. Wählen Sie **PUT /settings**.

   g. Wählen Sie **Probieren Sie es aus**.

   h. Geben Sie im Bereich des Anforderungskörpers keinen Wert für das ein `mnode_fqdn` Parameter. Geben Sie außerdem an, ob der Proxy verwendet werden soll (`true` Oder `false`) Für die `use_proxy` Parameter.

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

   i. Wählen Sie **Ausführen**.

Fehlerbehebung

Wenn FQDNs falsch konfiguriert sind, können Sie Probleme beim Zugriff auf den Managementknoten, einen Speichercluster oder beide haben. Verwenden Sie die folgenden Informationen, um die Fehlerbehebung zu unterstützen.

Problem	Ursache	Auflösung
• Beim Versuch, entweder mit dem FQDN auf den Management-Node oder den Speicher-Cluster zuzugreifen, wird ein Browserfehler angezeigt. • Sie können sich mit einer IP-Adresse nicht entweder beim Management-Node oder beim Storage-Cluster einloggen.	Der FQDN des Managementknoten und der FQDN des Speicherclusters sind beide falsch konfiguriert.	Verwenden Sie die REST-API-Anweisungen auf dieser Seite, um die FQDN-Einstellungen des Management-Nodes und Speicherclusters zu entfernen und erneut zu konfigurieren.
• Beim Versuch, auf den Speicher-Cluster-FQDN zuzugreifen, wird ein Browserfehler angezeigt. • Sie können sich mit einer IP-Adresse nicht entweder beim Management-Node oder beim Storage-Cluster einloggen.	Der FQDN des Managementknoten ist richtig konfiguriert, der Speichercluster-FQDN ist jedoch falsch konfiguriert.	Mithilfe der REST-API-Anweisungen auf dieser Seite können Sie die FQDN-Einstellungen des Speicherclusters entfernen und erneut konfigurieren
• Beim Versuch, auf den Verwaltungsknoten FQDN zuzugreifen, wird ein Browserfehler angezeigt. • Sie können sich mit einer IP-Adresse beim Management-Node und Storage-Cluster einloggen.	Der FQDN des Managementknoten ist falsch konfiguriert, der Speichercluster-FQDN ist jedoch korrekt konfiguriert.	Melden Sie sich bei NetApp Hybrid Cloud Control an, um die FQDN-Einstellungen des Managementknoten in der UI zu korrigieren, oder VERWENDEN Sie die REST-API-Anweisungen auf dieser Seite, um die Einstellungen zu korrigieren.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Erstellen und managen Sie Benutzerkonten mit NetApp Hybrid Cloud Control

In Element-basierten Storage-Systemen können maßgebliche Cluster-Benutzer erstellt werden, um Login-Zugriff auf NetApp Hybrid Cloud Control zu ermöglichen. Dies hängt von den Berechtigungen ab, die Sie „Administrator“ oder „schreibgeschützten“ Benutzern gewähren möchten. Neben Cluster-Benutzern gibt es auch Volume-Konten, über die Clients eine Verbindung zu Volumes auf einem Storage-Node herstellen können.

Verwalten Sie die folgenden Kontoarten:

- Managen von autorisierenden Cluster-Konten

- Volume-Konten verwalten

Aktivieren Sie LDAP

Um LDAP für jedes Benutzerkonto verwenden zu können, müssen Sie zunächst LDAP aktivieren.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Wählen Sie im Dashboard oben rechts das Options-Symbol aus und wählen Sie **Benutzerverwaltung**.
3. Wählen Sie auf der Seite Benutzer die Option **LDAP konfigurieren** aus.
4. Definieren Sie Ihre LDAP-Konfiguration.
5. Wählen Sie den Authentifizierungstyp Suchen und Bind oder Direct Bind aus.
6. Bevor Sie die Änderungen speichern, wählen Sie **LDAP-Anmeldung testen** oben auf der Seite, geben Sie den Benutzernamen und das Kennwort eines Benutzers ein, den Sie kennen, und wählen Sie **Test**.
7. Wählen Sie **Speichern**.

Managen von autorisierenden Cluster-Konten

"Autoritäre Benutzerkonten" Werden bei NetApp Hybrid Cloud Control über die Option „Benutzerverwaltung“ rechts oben gemanagt. Mithilfe dieser Kontoarten können Sie sich gegen alle Storage-Ressourcen authentifizieren, die mit einer NetApp Hybrid Cloud Control Instanz von Nodes und Clustern verbunden sind. Mit diesem Konto können Sie Volumes, Konten, Zugriffsgruppen und mehr über alle Cluster hinweg verwalten.

Erstellen Sie ein autorisierende Cluster-Konto

Erstellen Sie ein Konto mit NetApp Hybrid Cloud Control.

Mithilfe dieses Kontos können Kunden sich bei der Hybrid Cloud Control, der UI pro Node für das Cluster und dem Storage-Cluster in der NetApp Element Software anmelden.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Wählen Sie im Dashboard oben rechts das Options-Symbol aus und wählen Sie **Benutzerverwaltung**.
3. Wählen Sie **Benutzer Erstellen**.
4. Wählen Sie den Authentifizierungstyp von Cluster oder LDAP aus.
5. Führen Sie eine der folgenden Aktionen durch:
   - Wenn Sie LDAP ausgewählt haben, geben Sie den DN ein.

     Um LDAP zu verwenden, müssen Sie zunächst LDAP oder LDAPS aktivieren. Siehe Aktivieren Sie LDAP.

   - Wenn Sie Cluster als Auth-Typ ausgewählt haben, geben Sie einen Namen und ein Passwort für das neue Konto ein.
6. Wählen Sie entweder Administrator- oder schreibgeschützten Berechtigungen aus.

Um die Berechtigungen aus der NetApp Element-Software anzuzeigen, wählen Sie **ältere Berechtigungen anzeigen**. Wenn Sie eine Untergruppe dieser Berechtigungen auswählen, wird dem Konto Schreibberechtigung zugewiesen. Wenn Sie alle älteren Berechtigungen auswählen, wird dem Konto Administratorberechtigungen zugewiesen.

Um sicherzustellen, dass alle untergeordneten Gruppen Berechtigungen erben, erstellen Sie im LDAP-Server eine DN-Organisationsadministratorgruppe. Alle untergeordneten Konten dieser Gruppe übernehmen diese Berechtigungen.

7. Aktivieren Sie das Kontrollkästchen unter „Ich habe die NetApp Endbenutzer-Lizenzvereinbarung gelesen und akzeptiere sie“.
8. Wählen Sie **Benutzer Erstellen**.

Bearbeiten Sie ein autorisierende Cluster-Konto

Mit NetApp Hybrid Cloud Control können Sie die Berechtigungen oder das Passwort eines Benutzerkontos ändern.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Wählen Sie im Dashboard das Symbol oben rechts aus und wählen Sie **Benutzerverwaltung**.
3. Filtern Sie die Liste der Benutzerkonten optional durch Auswahl von **Cluster**, **LDAP** oder **IDP**.

   Wenn Sie Benutzer im Storage-Cluster mit LDAP konfiguriert haben, wird für diese Konten ein Benutzertyp mit „LDAP“ angezeigt. Wenn Benutzer auf dem Storage-Cluster mit IDP konfiguriert wurden, zeigen diese Konten einen Benutzertyp mit „IDP“.

4. Erweitern Sie in der Spalte **Aktionen** in der Tabelle das Menü für das Konto und wählen Sie **Bearbeiten**.
5. Nehmen Sie die erforderlichen Änderungen vor.
6. Wählen Sie **Speichern**.
7. Abmelden von NetApp Hybrid Cloud Control

Die Benutzeroberfläche von NetApp Hybrid Cloud Control dauert möglicherweise bis zu 2 Minuten, um den Bestand zu aktualisieren. Um den Bestand manuell zu aktualisieren, greifen Sie auf den Rest API UI Inventory Service zu `https://[management node IP]/inventory/1/` Und ausführen `GET /installations/{id}` Für den Cluster.

8. Melden Sie sich bei NetApp Hybrid Cloud Control an.

Löschen eines autorisierenden Benutzerkontos

Sie können ein oder mehrere Konten löschen, wenn sie nicht mehr benötigt werden. Sie können ein LDAP-Benutzerkonto löschen.

Sie können das primäre Administratorbenutzerkonto für das autorisierende Cluster nicht löschen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.

2. Wählen Sie im Dashboard das Symbol oben rechts aus und wählen Sie **Benutzerverwaltung**.
3. Erweitern Sie in der Spalte **Aktionen** in der Benutzertabelle das Menü für das Konto und wählen Sie **Löschen**.
4. Bestätigen Sie den Löschvorgang, indem Sie **Ja** wählen.

Volume-Konten verwalten

"Volume-Konten" Werden in der Tabelle NetApp Hybrid Cloud Control Volumes gemanagt. Diese Konten gelten nur für den Storage Cluster, auf dem sie erstellt wurden. Mit diesen Typen von Konten können Sie Berechtigungen für Volumes im gesamten Netzwerk festlegen, haben aber keine Auswirkungen außerhalb dieser Volumes.

Ein Volume-Konto enthält die CHAP-Authentifizierung, die für den Zugriff auf die ihm zugewiesenen Volumes erforderlich ist.

Erstellen eines Volume-Kontos

Erstellen Sie ein für dieses Volume spezifisches Konto.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Wählen Sie im Dashboard **Storage** > **Volumes** aus.
3. Wählen Sie die Registerkarte **Konten**.
4. Klicken Sie auf die Schaltfläche **Konto erstellen**.
5. Geben Sie einen Namen für das neue Konto ein.
6. Geben Sie im Abschnitt CHAP-Einstellungen die folgenden Informationen ein:
   - Initiatorschlüssel für CHAP-Node-Session-Authentifizierung
   - Zielschlüssel für CHAP-Knoten-Session-Authentifizierung

   Um ein Kennwort automatisch zu generieren, lassen Sie die Felder für Anmeldedaten leer.
7. Wählen Sie **Konto Erstellen**.

Bearbeiten eines Volume-Kontos

Sie können die CHAP-Informationen ändern und ändern, ob ein Konto aktiv oder gesperrt ist.

Das Löschen oder Sperren eines Kontos im Zusammenhang mit dem Managementknoten führt zu einem nicht zugänglichen Managementknoten.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Wählen Sie im Dashboard **Storage** > **Volumes** aus.
3. Wählen Sie die Registerkarte **Konten**.

4. Erweitern Sie in der Spalte **Aktionen** in der Tabelle das Menü für das Konto und wählen Sie **Bearbeiten**.
5. Nehmen Sie die erforderlichen Änderungen vor.
6. Bestätigen Sie die Änderungen, indem Sie **Ja** wählen.

Löschen Sie ein Volume-Konto

Löschen Sie ein Konto, das Sie nicht mehr benötigen.

Bevor Sie ein Volume-Konto löschen, löschen Sie zunächst alle Volumes, die dem Konto zugeordnet sind.

> Das Löschen oder Sperren eines Kontos im Zusammenhang mit dem Managementknoten führt zu einem nicht zugänglichen Managementknoten.

> Persistente Volumes, die mit Managementservices verbunden sind, werden einem neuen Konto bei der Installation oder bei einem Upgrade zugewiesen. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie die Volumes oder ihr zugehörigem Konto nicht. Wenn Sie diese Konten löschen, können Sie den Management-Node nicht mehr verwenden.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Wählen Sie im Dashboard **Storage** > **Volumes** aus.
3. Wählen Sie die Registerkarte **Konten**.
4. Erweitern Sie in der Spalte **Aktionen** in der Tabelle das Menü für das Konto und wählen Sie **Löschen**.
5. Bestätigen Sie den Löschvorgang, indem Sie **Ja** wählen.

Weitere Informationen

- "Informationen zu Accounts"
- "Arbeiten Sie mit Konten, die CHAP verwenden"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Erstellen und managen Sie Volumes mit NetApp Hybrid Cloud Control

Sie können ein Volume erstellen und das Volume einem bestimmten Konto zuordnen. Durch die Verknüpfung eines Volumes mit einem Konto erhält das Konto über die iSCSI-Initiatoren und CHAP-Anmeldeinformationen Zugriff auf das Volume.

Sie können die QoS-Einstellungen für ein Volume während der Erstellung festlegen.

Folgende Möglichkeiten zum Managen von Volumes in NetApp Hybrid Cloud Control:

- Erstellen eines Volumes
- Wenden Sie eine QoS-Richtlinie auf ein Volume an

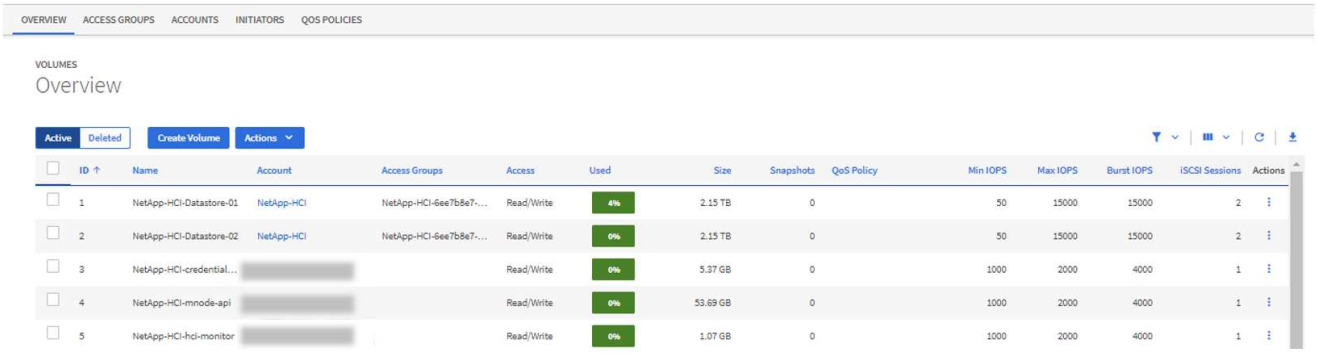
- Bearbeiten Sie ein Volume
- Volumes klonen
- Hinzufügen von Volumes zu einer Volume-Zugriffsgruppe
- Löschen Sie ein Volume
- Wiederherstellen eines gelöschten Volumes
- Löschen Sie ein gelöschtes Volume

Erstellen eines Volumes

Mit NetApp Hybrid Cloud Control können Sie ein Storage-Volume erstellen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie die Registerkarte **Bände** > **Übersicht**.



4. Wählen Sie **Lautstärke Erstellen**.
5. Geben Sie einen Namen für das neue Volume ein.
6. Geben Sie die Gesamtgröße des Volumes ein.

> Die standardmäßige Auswahl der Volume-Größe ist in GB. Sie können Volumes mit Größen erstellen, die in GB oder gib gemessen wurden: 1 GB = 1 000 000 000 Byte 1 gib = 1 073 741 824 Byte

7. Wählen Sie eine Blockgröße für das Volume aus.
8. Wählen Sie aus der Liste **Konto** das Konto aus, das Zugriff auf das Volume haben soll.

   Wenn kein Konto vorhanden ist, wählen Sie **Neues Konto erstellen**, geben Sie einen neuen Kontonamen ein und wählen Sie **Konto erstellen**. Das Konto wird erstellt und mit dem neuen Volumen in der **Konto** Liste verknüpft.

> Wenn mehr als 50 Konten vorhanden sind, wird die Liste nicht angezeigt. Beginnen Sie mit der Eingabe, und die automatische Vervollständigung zeigt Werte an, die Sie auswählen können.

9. Um die Servicequalität für das Volume zu konfigurieren, führen Sie einen der folgenden Schritte aus:

- Legen Sie unter **Quality of Service Settings** benutzerdefinierte Mindest-, Maximum- und Burst-Werte für IOPS fest oder verwenden Sie die Standard-QoS-Werte.
- Wählen Sie eine vorhandene QoS-Richtlinie aus, indem Sie die Option **Quality of Service Policy** zuweisen aktivieren und eine vorhandene QoS-Richtlinie aus der Ergebnisliste auswählen.
- Erstellen und Zuweisen einer neuen QoS-Richtlinie durch Aktivieren der Option **Quality of Service Policy** zuweisen und Auswählen von **Neue QoS-Richtlinie erstellen**. Geben Sie im daraufhin angezeigten Fenster einen Namen für die QoS-Richtlinie ein, und geben Sie anschließend QoS-Werte ein. Wählen Sie nach Abschluss **Quality of Service Policy**.

Volumes mit einem IOPS-Wert von max oder Burst über 20,000 IOPS erfordern möglicherweise eine hohe Warteschlangentiefe oder mehrere Sitzungen, um diesen IOPS-Level auf einem einzelnen Volume zu erreichen.

10. Wählen Sie **Lautstärke Erstellen**.

Wenden Sie eine QoS-Richtlinie auf ein Volume an

Mithilfe von NetApp Hybrid Cloud Control können Sie eine QoS-Richtlinie auf vorhandene Storage-Volumes anwenden. Wenn Sie stattdessen benutzerdefinierte QoS-Werte für ein Volume festlegen müssen, ist dies möglich Bearbeiten Sie ein Volume. Informationen zum Erstellen einer neuen QoS-Richtlinie finden Sie unter "Erstellung und Management von QoS-Richtlinien für Volumes".

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände** > **Übersicht**.
4. Wählen Sie ein oder mehrere Volumes aus, die einer QoS-Richtlinie zugeordnet werden sollen.
5. Wählen Sie oben in der Tabelle Volumes die Dropdown-Liste **Aktionen** aus, und wählen Sie **QoS-Richtlinie anwenden**.
6. Wählen Sie im resultierenden Fenster eine QoS-Richtlinie aus der Liste aus und wählen Sie **QoS-Richtlinie anwenden**.

> Wenn Sie QoS-Richtlinien für ein Volume verwenden, können Sie durch benutzerdefinierte QoS festlegen, dass die QoS-Richtlinie, die mit dem Volume verbunden ist, entfernt wird. Benutzerdefinierte QoS-Werte überschreiben QoS-Richtlinienwerte für Volume-QoS-Einstellungen.

Bearbeiten Sie ein Volume

Mit NetApp Hybrid Cloud Control lassen sich Volume-Attribute wie QoS-Werte, Volume-Größe und die Maßeinheit bearbeiten, mit der Byte-Werte berechnet werden. Außerdem haben Sie die Möglichkeit, den Kontozugriff für die Replizierungsnutzung zu ändern oder den Zugriff auf das Volume zu beschränken.

Über diese Aufgabe

Sie können die Größe eines Volume ändern, wenn unter den folgenden Bedingungen genügend Speicherplatz auf dem Cluster vorhanden ist:

- Normale Betriebsbedingungen.

- Volume-Fehler oder -Ausfälle werden gemeldet.
- Das Volume ist zu klonen.
- Das Volume wird neu synchronisiert.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände** > **Übersicht**.
4. Erweitern Sie in der Spalte **Aktionen** in der Tabelle Volumes das Menü für die Lautstärke und wählen Sie **Bearbeiten**.
5. Nehmen Sie die Änderungen nach Bedarf vor:

   a. Ändern Sie die Gesamtgröße des Volumes.

   Sie können die Volume-Größe vergrößern, aber nicht verkleinern. Sie können die Größe eines Volumes nur in einem einzigen Größenänderungs-Vorgang anpassen. Speicherbereinigung und Software-Upgrades unterbrechen die Größenänderung nicht.

   Wenn Sie die Volume-Größe für die Replikation anpassen, erhöhen Sie zuerst die Größe des Volumes, das als Replikationsziel zugewiesen wurde. Anschließend können Sie die Größe des Quellvolumens anpassen. Das Zielvolume kann größer oder gleich groß sein wie das Quellvolume, kann aber nicht kleiner sein.

   Die standardmäßige Auswahl der Volume-Größe ist in GB. Sie können Volumes mit Größen erstellen, die in GB oder gib gemessen wurden: 1 GB = 1 000 000 000 Byte 1 gib = 1 073 741 824 Byte

   b. Wählen Sie eine andere Zugriffsebene für Konten aus:
      - Schreibgeschützt
      - Lese-/Schreibzugriff
      - Gesperrt
      - Replizierungsziel

   c. Wählen Sie das Konto aus, das Zugriff auf das Volume haben soll.

      Beginnen Sie mit der Eingabe, und die automatische Vervollständigung zeigt mögliche Werte an, die Sie auswählen können.

      Wenn kein Konto vorhanden ist, wählen Sie **Neues Konto erstellen**, geben Sie einen neuen Kontonamen ein und wählen Sie **Erstellen**. Der Account wird erstellt und dem vorhandenen Volume zugeordnet.

   d. Ändern Sie die Servicequalität mit einer der folgenden Aktionen:
      i. Wählen Sie eine vorhandene Richtlinie aus.
      ii. Legen Sie unter „Benutzerdefinierte Einstellungen“ die Mindest-, Höchst- und Burst-Werte für IOPS fest oder verwenden Sie die Standardwerte.

Wenn Sie QoS-Richtlinien für ein Volume verwenden, können Sie durch benutzerdefinierte QoS festlegen, dass die QoS-Richtlinie, die mit dem Volume verbunden ist, entfernt wird. Durch benutzerdefinierte QoS werden die QoS-Richtlinienwerte für Volume-QoS-Einstellungen außer Kraft gesetzt.

Wenn Sie IOPS-Werte ändern, sollten Sie sich Dutzende oder Hunderte erhöhen. Eingabewerte erfordern gültige ganze Zahlen. Konfigurieren Sie Volumes mit einem extrem hohen Burst-Wert. So kann das System gelegentlich umfangreiche sequenzielle Workloads von großen Blöcken schneller verarbeiten und zugleich die anhaltenden IOPS für ein Volume einschränken.

6. Wählen Sie **Speichern**.

Volumes klonen

Sie können einen Klon eines einzelnen Storage Volumes erstellen oder eine Gruppe von Volumes klonen, um eine zeitpunktgenaue Kopie der Daten zu erstellen. Wenn Sie ein Volume klonen, erstellt das System einen Snapshot des Volume und erstellt dann eine Kopie der Daten, auf die der Snapshot verweist.

Bevor Sie beginnen

- Mindestens ein Cluster muss hinzugefügt und ausgeführt werden.
- Mindestens ein Volume wurde erstellt.
- Ein Benutzerkonto wurde erstellt.
- Der verfügbare nicht bereitgestellte Speicherplatz muss der Volume-Größe entsprechen oder größer sein.

Über diese Aufgabe

Das Cluster unterstützt bis zu zwei aktuell laufende Klonanforderungen pro Volume und bis zu 8 aktive Volume-Klonvorgänge gleichzeitig. Anforderungen, die über diese Grenzen hinausgehen, werden zur späteren Verarbeitung in die Warteschlange gestellt.

Das Klonen von Volumes ist ein asynchroner Prozess. Die erforderliche Zeit hängt von der Größe des Klonens des Volumes und der aktuellen Cluster-Last ab.

Geklonte Volumes übernehmen keine Zugriffsgruppenmitgliedschaft für Volumes vom Quell-Volume.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie die Registerkarte **Volumes** > **Übersicht** aus.
4. Wählen Sie jedes Volume aus, das Sie klonen möchten.
5. Wählen Sie oben in der Tabelle Volumes die Dropdown-Liste **Aktionen** aus, und wählen Sie **Klonen**.
6. Gehen Sie im daraufhin angezeigten Fenster wie folgt vor:

    a. Geben Sie ein Präfix für den Volume-Namen ein (optional).

    b. Wählen Sie den Zugriffstyp aus der Liste **Zugriff** aus.

c. Wählen Sie ein Konto aus, das dem neuen Volume-Klon zugeordnet werden soll (standardmäßig ist **aus Volume kopieren** ausgewählt, das dasselbe Konto verwendet, das das ursprüngliche Volume verwendet).

d. Wenn kein Konto vorhanden ist, wählen Sie **Neues Konto erstellen**, geben Sie einen neuen Kontonamen ein und wählen Sie **Konto erstellen**. Der Account wird erstellt und dem Volume zugeordnet.

Verwenden Sie beschreibende Best Practices für die Benennung. Dies ist besonders wichtig, wenn in Ihrer Umgebung mehrere Cluster oder vCenter Server verwendet werden.

Wenn Sie die Volume-Größe eines Klons erhöhen, führt dies zu einem neuen Volume mit zusätzlichem freien Speicherplatz am Ende des Volumes. Je nachdem, wie Sie das Volume verwenden, müssen Sie möglicherweise Partitionen erweitern oder neue Partitionen im freien Speicherplatz erstellen, um es zu nutzen.

a. Wählen Sie **Clone Volumes** Aus.

Der Zeitaufwand zum Abschluss eines Klonvorgangs wird von der Volume-Größe und der aktuellen Cluster-Last beeinflusst. Aktualisieren Sie die Seite, wenn das geklonte Volume nicht in der Liste der Volumes angezeigt wird.

Hinzufügen von Volumes zu einer Volume-Zugriffsgruppe

Sie können einer Volume-Zugriffsgruppe ein einzelnes Volume oder eine Gruppe von Volumes hinzufügen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände** > **Übersicht**.
4. Wählen Sie ein oder mehrere Volumes aus, die einer Volume-Zugriffsgruppe zugeordnet werden sollen.
5. Wählen Sie oben in der Tabelle Volumes die Dropdown-Liste **Aktionen** aus, und wählen Sie **zur Zugriffsgruppe hinzufügen**.
6. Wählen Sie im resultierenden Fenster eine Zugriffsgruppe für Volumes aus der Liste **Volume Access Group** aus.
7. Wählen Sie **Volumen Hinzufügen**.

Löschen Sie ein Volume

Ein oder mehrere Volumes können aus einem Element Storage-Cluster gelöscht werden.

Über diese Aufgabe

Gelöschte Volumes werden nicht sofort vom System gelöscht, sie bleiben etwa acht Stunden lang verfügbar. Nach acht Stunden werden sie gereinigt und sind nicht mehr verfügbar. Wenn Sie ein Volume wiederherstellen, bevor das System es bereinigt, wird das Volume wieder online geschaltet und die iSCSI-Verbindungen werden wiederhergestellt.

Wenn ein Volume, das zum Erstellen eines Snapshots verwendet wird, gelöscht wird, werden die zugehörigen Snapshots inaktiv. Wenn die gelöschten Quell-Volumes gelöscht werden, werden auch die zugehörigen inaktiven Snapshots aus dem System entfernt.

> Persistente Volumes, die mit Managementservices verbunden sind, werden bei der Installation oder bei einem Upgrade einem neuen Konto erstellt und zugewiesen. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie die Volumes oder ihr zugehörigem Konto nicht. Wenn Sie diese Volumes löschen, kann der Management-Node nicht mehr verwendet werden.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände** > **Übersicht**.
4. Wählen Sie ein oder mehrere zu löschende Volumes aus.
5. Wählen Sie oben in der Tabelle Volumes die Dropdown-Liste **Aktionen** aus, und wählen Sie **Löschen**.
6. Bestätigen Sie im daraufhin angezeigten Fenster die Aktion, indem Sie **Ja** auswählen.

Wiederherstellen eines gelöschten Volumes

Nach dem Löschen eines Storage Volume können Sie ihn weiterhin wiederherstellen, falls dies vor acht Stunden nach dem Löschen erfolgt.

Gelöschte Volumes werden nicht sofort vom System gelöscht, sie bleiben etwa acht Stunden lang verfügbar. Nach acht Stunden werden sie gereinigt und sind nicht mehr verfügbar. Wenn Sie ein Volume wiederherstellen, bevor das System es bereinigt, wird das Volume wieder online geschaltet und die iSCSI-Verbindungen werden wiederhergestellt.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände** > **Übersicht**.
4. Wählen Sie **Gelöscht**.
5. Erweitern Sie in der Spalte **Aktionen** der Tabelle Volumes das Menü für die Lautstärke und wählen Sie **Wiederherstellen**.
6. Bestätigen Sie den Vorgang, indem Sie **Ja** wählen.

Löschen Sie ein gelöschtes Volume

Nach dem Löschen von Storage Volumes bleiben diese für ungefähr acht Stunden verfügbar. Nach acht Stunden werden sie automatisch gereinigt und sind nicht mehr verfügbar. Wenn Sie die acht Stunden nicht warten möchten, können Sie sie löschen

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.

3. Wählen Sie **Bände** > **Übersicht**.
4. Wählen Sie **Gelöscht**.
5. Wählen Sie ein oder mehrere Volumes aus, die gelöscht werden sollen.
6. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie mehrere Volumen ausgewählt haben, wählen Sie oben in der Tabelle den Schnellfilter **Löschen** aus.
   - Wenn Sie ein einzelnes Volume ausgewählt haben, erweitern Sie in der Spalte **Aktionen** der Volumetabelle das Menü für die Lautstärke und wählen Sie **Löschen**.
7. Erweitern Sie in der Spalte **Aktionen** der Tabelle Volumes das Menü für die Lautstärke und wählen Sie **Löschen**.
8. Bestätigen Sie den Vorgang, indem Sie **Ja** wählen.

Weitere Informationen

- "Informationen zu Volumes"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Erstellung und Management von Volume-Zugriffsgruppen

Sie können neue Volume-Zugriffsgruppen erstellen, den Namen, zugehörige Initiatoren oder zugehörige Volumes von Zugriffsgruppen ändern oder vorhandene Volume-Zugriffsgruppen mithilfe von NetApp Hybrid Cloud Control löschen.

Was Sie benötigen

- Sie haben Administratorberechtigungen für dieses All-Flash-Storage-System von SolidFire.
- Sie haben Ihre Managementservices auf mindestens Version 2.15.28 aktualisiert. Das NetApp Hybrid Cloud Control Storage-Management ist in früheren Service-Bundle-Versionen nicht verfügbar.
- Stellen Sie sicher, dass Sie über ein logisches Benennungsschema für Volume-Zugriffsgruppen verfügen.

Fügen Sie eine Zugriffsgruppe für Volumes hinzu

Mit NetApp Hybrid Cloud Control können Sie einem Storage-Cluster eine Volume-Zugriffsgruppe hinzufügen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Zugriffsgruppen** aus.
5. Klicken Sie auf die Schaltfläche **Zugriffsgruppe erstellen**.
6. Geben Sie im daraufhin angezeigten Dialogfeld einen Namen für die Zugriffsgruppe des neuen Volumes ein.

7. (Optional) Wählen Sie im Abschnitt **Initiatoren** einen oder mehrere Initiatoren aus, die der neuen Zugriffsgruppe zugeordnet werden sollen.

   Wenn Sie einen Initiator der Volume-Zugriffsgruppe zuordnen, kann dieser Initiator ohne Authentifizierung auf jedes Volume in der Gruppe zugreifen.

8. (Optional) Wählen Sie im Abschnitt **Volumes** ein oder mehrere Volumes aus, die in diese Zugriffsgruppe aufgenommen werden sollen.
9. Wählen Sie **Zugriffsgruppe Erstellen**.

Bearbeiten Sie eine Zugriffsgruppe für Volumes

Sie können die Eigenschaften einer vorhandenen Volume-Zugriffsgruppe mit NetApp Hybrid Cloud Control bearbeiten. Sie können den Namen, zugeordnete Initiatoren oder zugehörige Volumes einer Zugriffsgruppe ändern.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Zugriffsgruppen** aus.
5. Erweitern Sie in der Spalte **Aktionen** der Tabelle der Zugriffsgruppen das Optionsmenü für die Zugriffsgruppe, die Sie bearbeiten müssen.
6. Wählen Sie im Optionsmenü die Option **Bearbeiten**.
7. Nehmen Sie alle erforderlichen Änderungen am Namen, den zugehörigen Initiatoren oder den zugehörigen Volumes vor.
8. Bestätigen Sie Ihre Änderungen, indem Sie **Speichern** wählen.
9. Überprüfen Sie in der Tabelle **Access Groups**, ob die Zugriffsgruppe Ihre Änderungen widerspiegelt.

Löschen Sie eine Zugriffsgruppe für Volumes

Sie können eine Volume-Zugriffsgruppe mithilfe von NetApp Hybrid Cloud Control entfernen und gleichzeitig die mit dieser Zugriffsgruppe verknüpften Initiatoren aus dem System entfernen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Zugriffsgruppen** aus.
5. Erweitern Sie in der Spalte **Aktionen** der Zugriffstabelle das Optionsmenü für die zu löschende Zugriffsgruppe.
6. Wählen Sie im Optionsmenü die Option **Löschen** aus.
7. Wenn Sie die Initiatoren, die der Zugriffsgruppe zugeordnet sind, nicht löschen möchten, deaktivieren Sie das Kontrollkästchen **Initiatoren löschen in dieser Zugriffsgruppe**.

8. Bestätigen Sie den Löschvorgang, indem Sie **Ja** auswählen.

Weitere Informationen

- "Erfahren Sie mehr über Volume Access Groups"
- "Hinzufügen eines Initiators zu einer Volume-Zugriffsgruppe"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Erstellen und Verwalten von Initiatoren

Verwenden Sie können "Initiatoren" Für CHAP-basierten und nicht kontenbasierten Zugriff auf Volumes. Sie können Initiatoren erstellen und löschen und ihnen freundliche Alias geben, um die Administration und den Zugriff auf Volumes zu vereinfachen. Wenn Sie einer Volume-Zugriffsgruppe einen Initiator hinzufügen, ermöglicht dieser Initiator den Zugriff auf alle Volumes in der Gruppe.

Was Sie benötigen

- Sie haben Cluster-Administrator-Anmeldedaten.
- Sie haben Ihre Managementservices auf mindestens Version 2.17 aktualisiert. Das NetApp Hybrid Cloud Control Initiator-Management ist in früheren Service-Bundle-Versionen nicht verfügbar.

Optionen

- Erstellen eines Initiators
- Fügen Sie Initiatoren zu einer Volume-Zugriffsgruppe hinzu
- Ändern eines Initiator-Alias
- Löschen Sie Initiatoren

Erstellen eines Initiators

Sie können iSCSI- oder Fibre Channel-Initiatoren erstellen und diese optional Aliase zuweisen.

Über diese Aufgabe

Das akzeptierte Format eines Initiator-IQN lautet `iqn.yyyy-mm` Wobei y und m Ziffern sind, gefolgt von Text, der nur Ziffern, Kleinbuchstaben, einen Punkt enthalten darf (`.`), Doppelpunkt (`:`) Oder Strich (`-`). Ein Beispiel für das Format:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

Das akzeptierte Format eines Fibre Channel Initiator-WWPN `:Aa:bB:CC:dd:11:22:33:44` Oder `AabBCCdd11223344`. Ein Beispiel für das Format:

```
5f:47:ac:c0:5c:74:d4:02
```

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Initiatoren** aus.
5. Wählen Sie die Schaltfläche **Initiatoren erstellen**.

Option	Schritte
Erstellen Sie einen oder mehrere Initiatoren	a. Geben Sie im Feld **IQN/WWPN** den IQN oder WWPN für den Initiator ein. b. Geben Sie im Feld **Alias** einen Anzeigenamen für den Initiator ein. c. (Optional) Wählen Sie **Initiator hinzufügen**, um neue Initiatorfelder zu öffnen, oder verwenden Sie stattdessen die Option Bulk create. d. Wählen Sie **Initiatoren Erstellen** Aus.
Initiatoren für Massenvorgänge erstellen	a. Wählen Sie **Bulk Add IQNs/WWPNs** aus. b. Geben Sie eine Liste von IQNs oder WWPNs in das Textfeld ein. Jeder IQN oder WWPN muss Komma oder Speicherplatz getrennt oder in seiner eigenen Zeile sein. c. Wählen Sie **IQNs/WWPNs hinzufügen**. d. (Optional) Fügen Sie jedem Initiator eindeutige Aliase hinzu. e. Entfernen Sie jeden Initiator aus der Liste, der in der Installation möglicherweise bereits vorhanden ist. f. Wählen Sie **Initiatoren Erstellen** Aus.

Fügen Sie Initiatoren zu einer Volume-Zugriffsgruppe hinzu

Sie können Initiatoren zu einer Volume-Zugriffsgruppe hinzufügen. Wenn Sie einer Volume-Zugriffsgruppe einen Initiator hinzufügen, ermöglicht der Initiator den Zugriff auf alle Volumes in dieser Volume-Zugriffsgruppe.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Initiatoren** aus.
5. Wählen Sie einen oder mehrere Initiatoren aus, die Sie hinzufügen möchten.

6. Wählen Sie **Aktionen > zur Zugriffsgruppe hinzufügen**.
7. Wählen Sie die Zugriffsgruppe aus.
8. Bestätigen Sie Ihre Änderungen, indem Sie **Initiator hinzufügen** wählen.

Ändern eines Initiator-Alias

Sie können den Alias eines bestehenden Initiators ändern oder einen Alias hinzufügen, wenn einer noch nicht vorhanden ist.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Initiatoren** aus.
5. Erweitern Sie in der Spalte **Aktionen** das Optionsmenü für den Initiator.
6. Wählen Sie **Bearbeiten**.
7. Nehmen Sie alle erforderlichen Änderungen am Alias vor oder fügen Sie einen neuen Alias hinzu.
8. Wählen Sie **Speichern**.

Löschen Sie Initiatoren

Sie können einen oder mehrere Initiatoren löschen. Wenn Sie einen Initiator löschen, wird dieser vom System aus einer zugehörigen Volume-Zugriffsgruppe entfernt. Verbindungen, die den Initiator verwenden, bleiben gültig, bis die Verbindung zurückgesetzt wird.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Initiatoren** aus.
5. Einen oder mehrere Initiatoren löschen:
   a. Wählen Sie einen oder mehrere Initiatoren aus, die Sie löschen möchten.
   b. Wählen Sie **Aktionen > Löschen**.
   c. Bestätigen Sie den Löschvorgang und wählen Sie **Ja**.

Weitere Informationen

- "Weitere Informationen zu Initiatoren"
- "Erfahren Sie mehr über Volume Access Groups"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Erstellung und Management von QoS-Richtlinien für Volumes

Mit einer QoS-Richtlinie (Quality of Service) können Sie eine standardisierte Quality-of-Service-Einstellung erstellen und speichern, die auf viele Volumes angewendet werden kann. Der ausgewählte Cluster muss zur Verwendung von QoS-Richtlinien Element 10.0 oder höher sein. Anderenfalls sind QoS-Richtlinienfunktionen nicht verfügbar.

Weitere Informationen zur Verwendung finden Sie in den SolidFire All-Flash-Storage-Konzepten "QoS-Richtlinien (QoS" Anstelle einzelner Volumes "QoS".

Mithilfe von NetApp Hybrid Cloud Control lassen sich QoS-Richtlinien erstellen und managen, indem folgende Aufgaben ausgeführt werden:

- Erstellen einer QoS-Richtlinie
- Wenden Sie eine QoS-Richtlinie auf ein Volume an
- Ändern der QoS-Richtlinienzuweisung eines Volumes
- Bearbeiten einer QoS-Richtlinie
- Löschen einer QoS-Richtlinie

Erstellen einer QoS-Richtlinie

Sie können QoS-Richtlinien erstellen und auf Volumes anwenden, die eine vergleichbare Performance aufweisen sollten.

Wenn Sie QoS-Richtlinien verwenden, verwenden Sie keine benutzerdefinierte QoS für ein Volume. Durch benutzerdefinierte QoS werden die QoS-Richtlinienwerte für Volume-QoS-Einstellungen überschrieben und angepasst.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard das Menü für Ihr Speichercluster.
3. Wählen Sie **Storage > Volumes**.
4. Wählen Sie die Registerkarte **QoS Policies**.
5. Wählen Sie **Create Policy**.
6. Geben Sie den **Policy Name** ein.

   Verwenden Sie beschreibende Best Practices für die Benennung. Dies ist besonders wichtig, wenn in Ihrer Umgebung mehrere Cluster oder vCenter Server verwendet werden.

7. Geben Sie die Werte für IOPS-Minimum, IOPS-Maximum und IOPS-Burst ein.
8. Wählen Sie **QoS-Richtlinie erstellen**.

   Für die Richtlinie wird eine System-ID generiert, und die Richtlinie wird auf der Seite QoS Policies mit ihren zugewiesenen QoS-Werten angezeigt.

Wenden Sie eine QoS-Richtlinie auf ein Volume an

Mithilfe von NetApp Hybrid Cloud Control kann einer vorhandenen QoS-Richtlinie ein Volume zugewiesen werden.

Was Sie benötigen

Die QoS-Richtlinie, die Sie zuweisen möchten, war Erstellt.

Über diese Aufgabe

Dieser Task beschreibt, wie eine QoS-Richtlinie einem einzelnen Volume durch Ändern der entsprechenden Einstellungen zugewiesen wird. Die neueste Version von NetApp Hybrid Cloud Control bietet keine Massenzuordnungsoption für mehr als ein Volume. Bis die Funktion für die Massen-Zuweisung in einer zukünftigen Version verfügbar ist, können Sie QoS-Richtlinien über die Element Web-UI oder das vCenter Plug-in in Bulk zuweisen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard das Menü für Ihr Speichercluster.
3. Wählen Sie **Storage > Volumes**.
4. Wählen Sie das Menü **Aktionen** neben dem Volumen, das Sie ändern möchten.
5. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
6. Aktivieren Sie im Dialogfeld **QoS-Richtlinie zuweisen** und wählen Sie die QoS-Richtlinie aus der Dropdown-Liste aus, die auf das ausgewählte Volume angewendet werden soll.

   Durch die Zuweisung von QoS werden alle zuvor angewandten QoS-Werte für Volumes außer Kraft gesetzt.

7. Wählen Sie **Speichern**.

Ändern der QoS-Richtlinienzuweisung eines Volumes

Sie können die Zuweisung einer QoS-Richtlinie aus einem Volume entfernen oder eine andere QoS-Richtlinie oder benutzerdefinierte QoS auswählen.

Was Sie benötigen

Das Volume, das Sie ändern möchten, ist Zugewiesen Eine QoS-Richtlinie

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard das Menü für Ihr Speichercluster.
3. Wählen Sie **Storage > Volumes**.
4. Wählen Sie das Menü **Aktionen** neben dem Volumen, das Sie ändern möchten.
5. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
6. Führen Sie im Dialogfeld einen der folgenden Schritte aus:
   - Deaktivieren Sie **Assign QoS Policy** und ändern Sie die **Min IOPS**, **Max IOPS** und **Burst IOPS**-Werte für die QoS einzelner Volumes.

Wenn QoS-Richtlinien deaktiviert sind, verwendet das Volume Standard-QoS-IOPS-Werte, sofern nichts anderes geändert wurde.

- Wählen Sie in der Dropdown-Liste eine andere QoS-Richtlinie aus, die auf das ausgewählte Volume angewendet werden soll.

7. Wählen Sie **Speichern**.

Bearbeiten einer QoS-Richtlinie

Sie können den Namen einer vorhandenen QoS-Richtlinie ändern oder die mit der Richtlinie verknüpften Werte bearbeiten. Das Ändern von Performance-Werten für die QoS-Richtlinie wirkt sich auf die QoS aller mit der Richtlinie verknüpften Volumes aus.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard das Menü für Ihr Speichercluster.
3. Wählen Sie **Storage > Volumes**.
4. Wählen Sie die Registerkarte **QoS Policies**.
5. Wählen Sie das Menü **Aktionen** neben der QoS-Richtlinie, die Sie ändern möchten.
6. Wählen Sie **Bearbeiten**.
7. Ändern Sie im Dialogfeld **QoS-Richtlinie bearbeiten** einen oder mehrere der folgenden Optionen:
   - **Name**: Der benutzerdefinierte Name für die QoS-Richtlinie.
   - **Minimum IOPS**: Die Mindestzahl an IOPS für das Volume garantiert. Standard = 50.
   - **Maximale IOPS**: Die maximale Anzahl von IOPS für das Volume zulässig. Standard = 15,000.
   - **Burst IOPS**: Die maximale Anzahl an IOPS über einen kurzen Zeitraum für das Volume zulässig. Standard = 15,000.
8. Wählen Sie **Speichern**.

Auf dem Link in der Spalte **aktive Volumes** können Sie eine Richtlinie auswählen, um eine gefilterte Liste der Volumes anzuzeigen, die dieser Richtlinie zugeordnet sind.

Löschen einer QoS-Richtlinie

Die QoS-Richtlinie kann gelöscht werden, wenn sie nicht mehr benötigt wird. Wenn Sie eine QoS-Richtlinie löschen, erhalten alle mit der Richtlinie zugewiesenen Volumes die QoS-Werte, die zuvor von der Richtlinie definiert wurden, jedoch als individuelle Volume-QoS. Jede Zuordnung zur Richtlinie „Gelöschte QoS“ wird entfernt.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard das Menü für Ihr Speichercluster.
3. Wählen Sie **Storage > Volumes**.
4. Wählen Sie die Registerkarte **QoS Policies**.

5. Wählen Sie das Menü **Aktionen** neben der QoS-Richtlinie, die Sie ändern möchten.
6. Wählen Sie **Löschen**.
7. Bestätigen Sie die Aktion.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Überwachen Sie Ihr SolidFire System mit NetApp Hybrid Cloud Control

Überwachen Sie die Speicherressourcen über das Hybrid Cloud Control Dashboard

Mit der NetApp Hybrid Cloud Control Dashboard können Sie alle Storage-Ressourcen auf einen Blick anzeigen. Darüber hinaus können Sie die Storage-Kapazität und die Storage-Performance überwachen.

> Wenn Sie zum ersten Mal eine neue NetApp Hybrid Cloud Control Session starten, kann es möglicherweise zu Verzögerungen beim Laden der NetApp Hybrid Cloud Control Dashboard-Ansicht kommen, wenn der Management-Node viele Cluster verwaltet. Die Ladezeit hängt von der Anzahl der Cluster ab, die aktiv vom Management-Node gemanagt werden. Bei späteren Starts erleben Sie schnellere Ladezeiten.

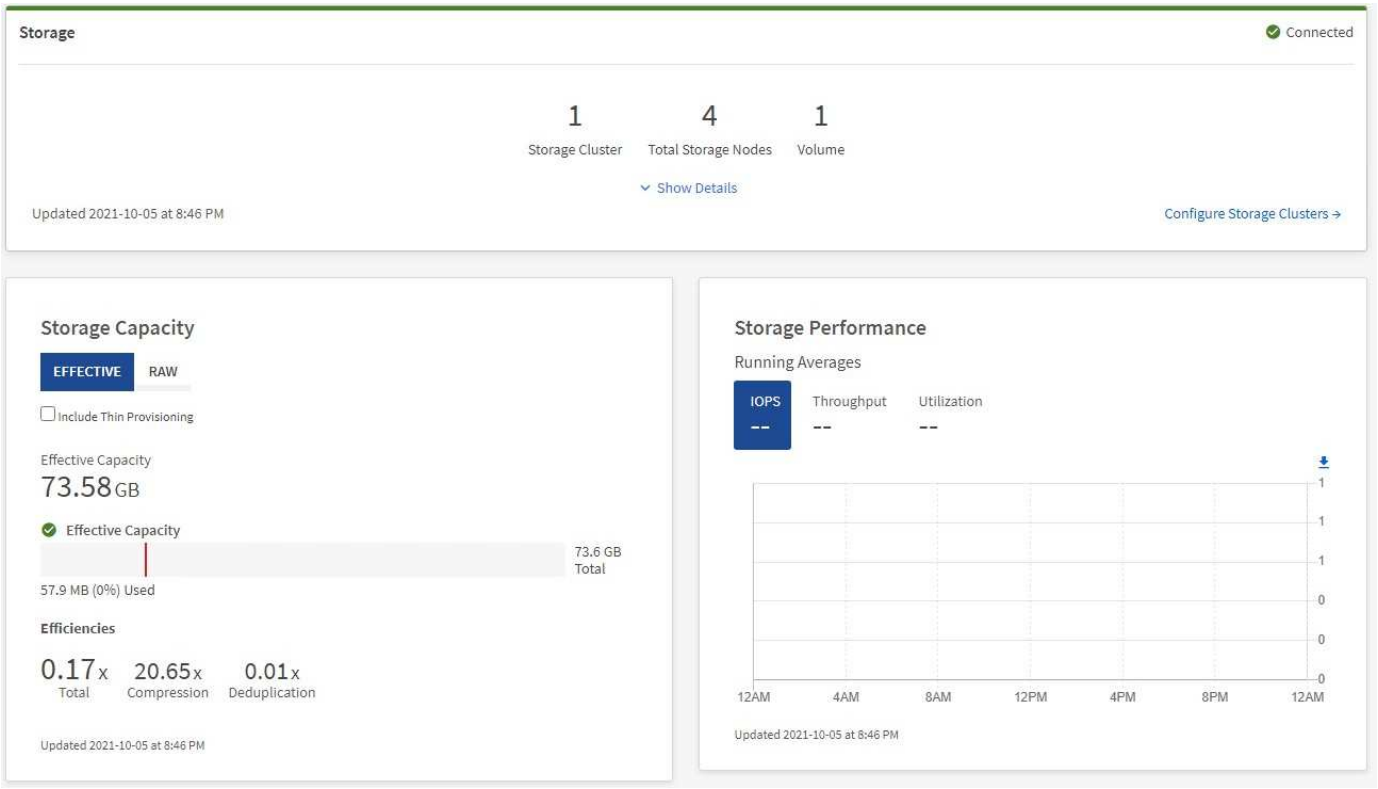
- Zugriff auf das NetApp HCC Dashboard
- Monitoring von Storage-Ressourcen
- Monitoring der Storage-Kapazität
- Monitoring der Storage-Performance

Zugriff auf das NetApp HCC Dashboard

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser. Beispiel:

```
https://[management node IP address]
```

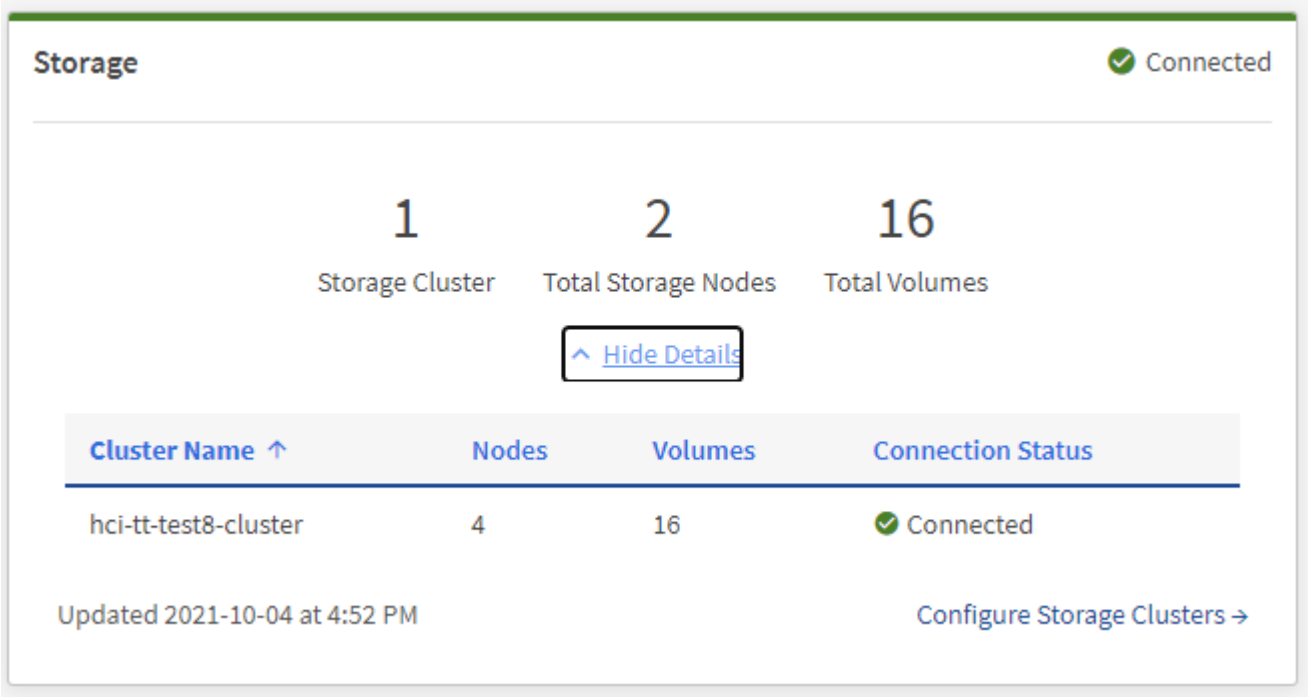
2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des SolidFire All-Flash-Storage-Cluster-Administrators bereitstellen.
3. Zeigen Sie das Hybrid Cloud Control Dashboard an.



Monitoring von Storage-Ressourcen

Nutzen Sie den Fensterbereich **Storage**, um Ihre gesamte Speicherumgebung anzuzeigen. Sie können die Anzahl der Storage-Cluster, Storage-Nodes und Volumes insgesamt überwachen.

Um Details anzuzeigen, wählen Sie im Bereich Speicher die Option **Details anzeigen**.



Die Gesamtzahl der Storage-Nodes enthält keine Witness-Nodes aus Storage-Clustern mit zwei Nodes. Die Witness-Nodes sind in die Nummer Nodes im Detailbereich für diesen Cluster enthalten.

Um die letzten Speichercluster-Daten anzuzeigen, verwenden Sie die Seite Speichercluster, auf der Abfragen häufiger durchgeführt werden als auf dem Dashboard.

Monitoring der Storage-Kapazität

Das Monitoring der Storage-Kapazität Ihrer Umgebung ist von entscheidender Bedeutung. Mit dem Teilfenster Storage-Kapazität können Sie die Effizienz Ihrer Storage-Kapazität bestimmen, wobei oder ohne aktivierte Komprimierung, Deduplizierung und Thin Provisioning-Funktionen die Effizienz erhöht wird.

Auf der Registerkarte **RAW** sehen Sie den gesamten verfügbaren physischen Speicherplatz in Ihrem Cluster sowie Informationen zum bereitgestellten Speicher auf der Registerkarte **EFFEKTIV**.

Schritte

1. Wählen Sie die Registerkarte * RAW* aus, um den gesamten physischen Speicherplatz anzuzeigen, der in Ihrem Cluster verwendet und verfügbar ist.

   Sehen Sie sich die vertikalen Linien an, um zu bestimmen, ob die genutzte Kapazität unter dem Wert „Warnung“, „Fehler“ oder „kritische Schwellenwerte“ liegt. Bewegen Sie den Mauszeiger über die Linien, um Details anzuzeigen.

   Sie können den Schwellenwert für Warnung festlegen, der standardmäßig 3% unter dem Fehlerschwellenwert liegt. Die Fehler- und kritischen Schwellenwerte sind voreingestellt und können nicht anhand des Designs konfiguriert werden. Der Fehlerschwellenwert gibt an, dass weniger als ein Knoten der Kapazität im Cluster verbleibt. Schritte zum Einstellen des Schwellenwerts finden Sie unter "Cluster-Schwellenwert wird eingestellt".

   Informationen zur entsprechenden Cluster-Schwellenwertelement-API finden Sie unter "„GetClusterFullThreshold“" In der Dokumentation *Element Software API*. Weitere Informationen zur Block- und Metadatenkapazität finden Sie unter "Allgemeines zu Cluster-Auslastungsebenen" In der Dokumentation *Element Software*.

2. Wählen Sie die Registerkarte * EFFECTIVE* aus, um Informationen über den insgesamt bereitgestellten Storage für verbundene Hosts anzuzeigen und Effizienzbewertungen anzuzeigen.
   a. Optional können Sie sich **mit Thin Provisioning** um Thin Provisioning-Effizienzraten im Balkendiagramm für die effektive Kapazität anzuzeigen.
   b. **Balkendiagramm für effektive Kapazität**: Prüfen Sie die vertikalen Linien, um festzustellen, ob Ihre verwendete Kapazität unter der Gesamtsumme oder weniger als Warnung, Fehler oder kritische Schwellenwerte liegt. Ähnlich wie die Registerkarte „Raw“ können Sie den Mauszeiger über die vertikalen Linien bewegen, um Details anzuzeigen.
   c. **Effizienz**: Prüfen Sie diese Bewertungen, um festzustellen, welche Vorteile die Effizienz Ihrer Storage-Kapazität durch aktivierte Komprimierung, Deduplizierung und Thin Provisioning-Funktionen erzielt wird. Wenn die Komprimierung beispielsweise „1,3x“ anzeigt, bedeutet dies, dass die Storage-Effizienz bei aktivierter Komprimierung 1.3-mal effizienter ist als ohne sie.

      Die Gesamteffizienz entspricht (maxUsedSpace * Efficiency Factor) / 2, wobei Efficiency Factor = (thinProvisioningFactor * deDuplicationFactor * comressionFactor). Wenn Thin Provisioning nicht aktiviert ist, wird dies nicht in der Gesamteffizienz berücksichtigt.

   d. Wenn die effektive Storage-Kapazität einen Fehler oder einen kritischen Schwellenwert überschreitet, sollten Sie die Daten auf dem System löschen.
3. Für weitere Analysen und historischen Kontext, schauen Sie sich "Details zum NetApp SolidFire Active IQ".

Monitoring der Storage-Performance

Sie können sich ansehen, wie viel IOPS oder Durchsatz Sie aus einem Cluster erhalten können, ohne die nützliche Performance dieser Ressource durch Verwendung des Teilfensters „Storage Performance“ zu überschreiten. Die Storage-Performance ist der Punkt, an dem die maximale Auslastung erreicht wird, bevor die Latenz zum Problem wird.

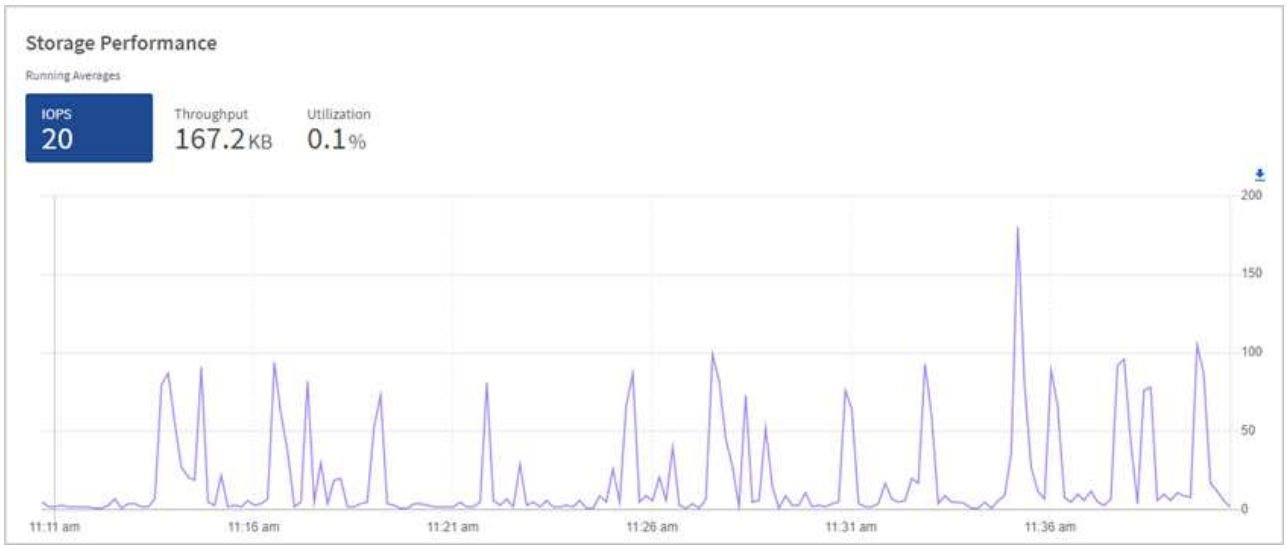
Im Bereich Storage Performance können Sie feststellen, ob die Performance an einem Punkt erreicht wird, an dem die Performance abnimmt, wenn sich die Workloads erhöhen.

Die Informationen in diesem Teilfenster werden alle 10 Sekunden aktualisiert und zeigen einen Durchschnitt aller Punkte im Diagramm an.

Details zur zugehörigen Element-API-Methode finden Sie im "GetClusterStats" Methode in der API-Dokumentation *Element Software*.

Schritte

1. Zeigen Sie das Teilfenster Speicher-Performance an. Zeigen Sie für Details den Mauszeiger auf Punkte im Diagramm.
   a. **IOPS** Registerkarte: Siehe die aktuellen Operationen pro Sekunde. Suchen Sie nach Trends in Daten oder Spitzen. Wenn Sie beispielsweise sehen, dass die maximale IOPS 160.000 beträgt und 100.000 freie oder verfügbare IOPS sind, ziehen Sie möglicherweise nach dem Hinzufügen weiterer Workloads zu diesem Cluster in Betracht. Wenn andererseits zu sehen ist, dass nur 140K verfügbar ist, können Sie unter Umständen Workloads auslagern oder Ihr System erweitern.



b. **Throughput** Tab: Monitoring-Muster oder Durchsatzspitzen. Überwachen Sie darüber hinaus kontinuierlich hohe Durchsatzwerte. Dies kann darauf hindeuten, dass sich die maximale Performance der Ressource nähert.

c. **Auslastung** Registerkarte: Überwachen Sie die Auslastung von IOPS in Bezug auf die insgesamt verfügbaren IOPS, die auf der Clusterebene zusammengefasst sind.

2. Werfen Sie weitere Analysen mit dem NetApp Element Plug-in für vCenter Server an die Storage-Performance.

   "Performance, die im NetApp Element Plug-in für vCenter Server dargestellt ist".

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Zeigen Sie Ihren Bestand auf der Seite Knoten an

Sie können Ihre Storage-Ressourcen in Ihrem System anzeigen und ihre IP-Adressen, Namen und Softwareversionen festlegen.

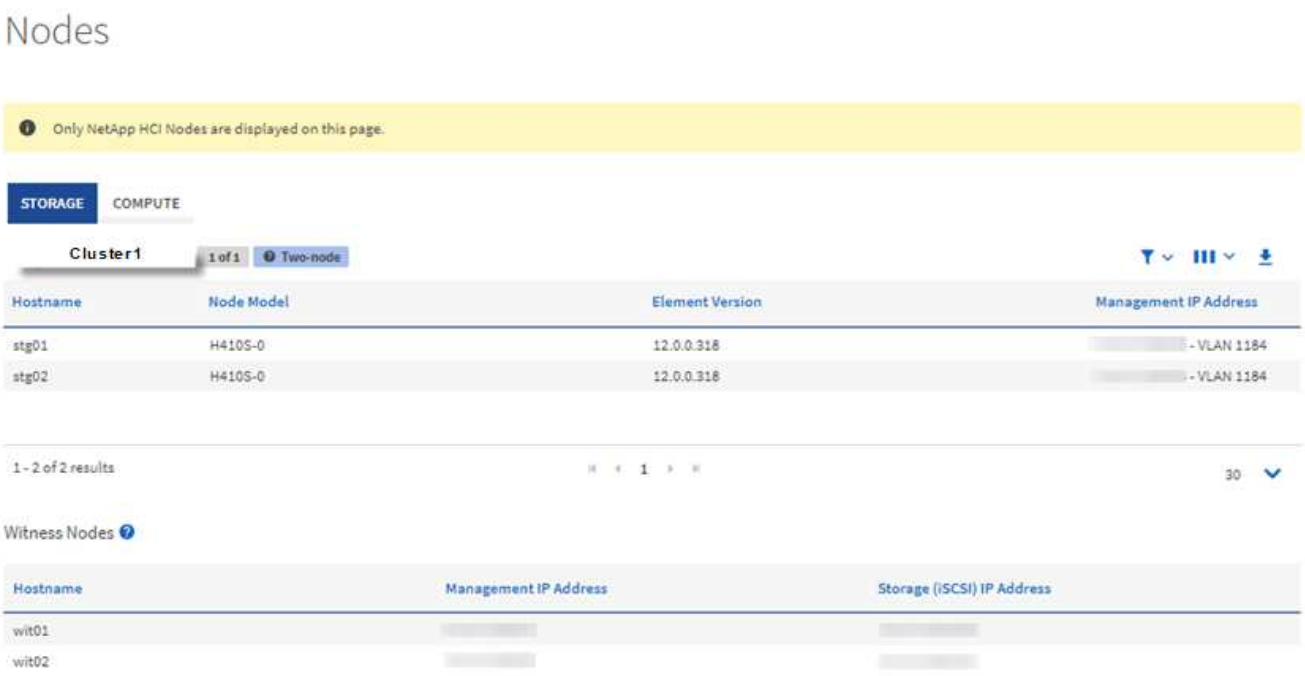
Sie können Storage-Informationen für Ihre Systeme mit mehreren Nodes anzeigen. Wenn "Benutzerdefinierte Sicherungsdomänen" Bei Zuordnung sehen Sie, welche Sicherungsdomänen spezifischen Nodes zugewiesen sind.

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser. Beispiel:

   ```
   https://[management node IP address]
   ```

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des SolidFire All-Flash-Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie in der linken Navigation **Knoten**.



Wenn Sie zum ersten Mal eine neue NetApp Hybrid Cloud Control Session starten, kann es möglicherweise zu einer Verzögerung beim Laden der Seite NetApp Hybrid Cloud Control Nodes kommen, wenn der Management-Node viele Cluster verwaltet. Die Ladezeit hängt von der Anzahl der Cluster ab, die aktiv vom Management-Node gemanagt werden. Bei späteren Starts erleben Sie schnellere Ladezeiten.

4. Überprüfen Sie auf der Seite Knoten auf der Registerkarte **Storage** die folgenden Informationen:
   a. Zwei-Knoten-Cluster: Auf der Registerkarte Speicher wird eine Bezeichnung „zwei-Knoten“ angezeigt und die zugehörigen Witness Nodes werden aufgelistet.
   b. Drei-Node-Cluster: Die Storage-Nodes und die zugehörigen Witness-Nodes werden aufgeführt. Bei Clustern mit drei Nodes wird ein Witness Node im Standby bereitgestellt, um im Falle eines Node-Ausfalls die Hochverfügbarkeit aufrechtzuerhalten.
   c. Cluster mit mindestens vier Nodes: Es werden Informationen für Cluster mit vier oder mehr Nodes angezeigt. Witness Nodes gelten nicht. Wenn Sie mit zwei oder drei Storage-Nodes begonnen und weitere Nodes hinzugefügt haben, werden die Witness-Nodes weiterhin angezeigt. Andernfalls wird die Tabelle Witness Nodes nicht angezeigt.
   d. Die Firmware-Bundle-Version: Ab Management Services Version 2.14 wird für diese Cluster die Firmware-Bundle-Version angezeigt, wenn auf Clustern mit Element 12.0 oder höher ausgeführt wird. Wenn die Knoten in einem Cluster unterschiedliche Firmware-Versionen enthalten, sehen Sie in der Spalte **Firmware Bundle Version multiple**.
   e. Benutzerdefinierte Schutz-Domänen: Wenn benutzerdefinierte Schutz-Domänen im Cluster verwendet werden, werden für jeden Node im Cluster benutzerdefinierte Schutz-Domain-Zuweisungen angezeigt. Wenn benutzerdefinierte Schutzdomänen nicht aktiviert sind, wird diese Spalte nicht angezeigt.
5. Sie haben verschiedene Möglichkeiten, die Informationen auf diesen Seiten zu bearbeiten:
   a. Um die Liste der Elemente in den Ergebnissen zu filtern, wählen Sie das **Filter**-Symbol und wählen Sie die Filter aus. Sie können auch Text für den Filter eingeben.
   b. Um Spalten ein- oder auszublenden, wählen Sie das Symbol **Spalten anzeigen/ausblenden** aus.
   c. Um die Tabelle herunterzuladen, wählen Sie das Symbol **Download**.

Zur Anzeige der Storage-Anzahl bietet das NetApp Hybrid Cloud Control (HCC) Dashboard. Siehe "Überwachen Sie Speicherressourcen mit dem HCC Dashboard".

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Überwachung von Volumes auf Ihrem Storage-Cluster

Das SolidFire System stellt mithilfe von Volumes Storage bereit. Volumes sind Blockgeräte, auf die über das Netzwerk von iSCSI- oder Fibre Channel-Clients zugegriffen wird. Details zu Zugriffsgruppen, Konten, Initiatoren, genutzter Kapazität, Snapshot Datensicherungsstatus, Anzahl von iSCSI-Sitzungen und der QoS-Richtlinie (Quality of Service) für dieses Volume lassen sich überwachen.

Sie können auch Details zu aktiven und gelöschten Volumes anzeigen.

In dieser Ansicht sollten Sie zunächst die Spalte „verwendete Kapazität“ überwachen.

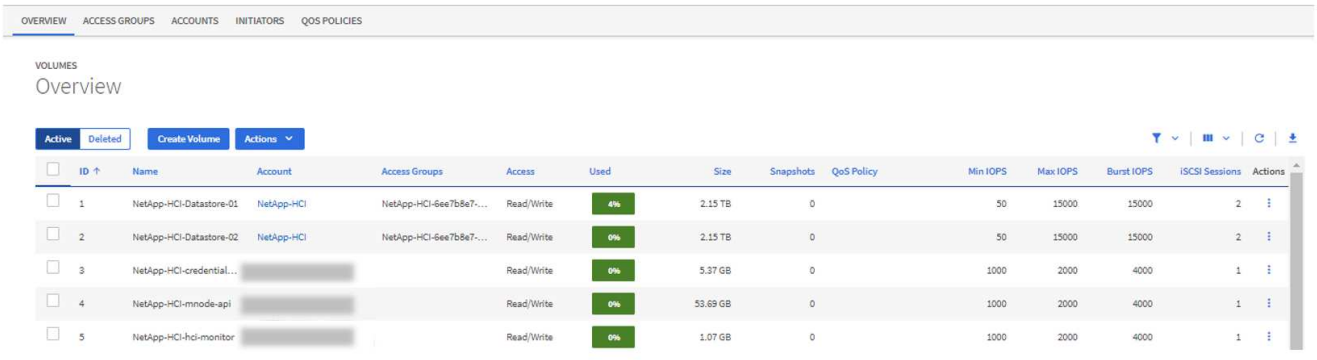
Sie können nur dann auf diese Informationen zugreifen, wenn Sie über Administratorrechte für NetApp Hybrid Cloud Control verfügen.

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser. Beispiel:

```
https://[management node IP address]
```

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des SolidFire All-Flash-Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie im blauen Feld links die SolidFire All-Flash-Storage-Installation aus.
4. Wählen Sie im linken Navigationsbereich den Cluster aus und wählen Sie **Storage** > **Volumes**.



5. Verwenden Sie auf der Seite Volumes die folgenden Optionen:

a. Filtern Sie die Ergebnisse, indem Sie das Symbol **Filter** wählen.

b. Durch Auswahl des Symbols **Ausblenden/Anzeigen** können Sie Spalten ausblenden oder anzeigen.

c. Aktualisieren Sie die Daten, indem Sie das Symbol **Aktualisieren** auswählen.

d. Laden Sie eine CSV-Datei herunter, indem Sie auf das Symbol **Download** klicken.

6. Überwachen Sie die Spalte „verwendete Kapazität“. Wenn Warnungs-, Fehler- oder kritische Schwellenwerte erreicht werden, steht die Farbe für den Status der verwendeten Kapazität:

   a. Warnung - Gelb

   b. Fehler - Orange

   c. Kritisch – Rot

7. Wählen Sie in der Ansicht Volumes die Registerkarten aus, um weitere Details zu den Volumes anzuzeigen:

   a. **Access Groups**: Sie können die Volume Access Groups sehen, die von Initiatoren einer Sammlung von Volumes für gesicherten Zugriff zugeordnet sind.

      Siehe Informationen zu "Volume-Zugriffsgruppen".

   b. **Konten**: Sie können die Benutzerkonten sehen, die es Clients ermöglichen, sich mit Volumes auf einem Knoten zu verbinden. Wenn Sie ein Volume erstellen, wird es einem bestimmten Benutzerkonto zugewiesen.

      Siehe Informationen zu "Benutzerkonten für SolidFire All-Flash-Storage-Systeme".

   c. **Initiatoren**: Sie können den iSCSI-Initiator IQN oder Fibre Channel-WWPNs für das Volume sehen. Jeder IQN, der einer Zugriffsgruppe hinzugefügt wird, kann auf jedes Volume in der Gruppe zugreifen, ohne dass eine CHAP-Authentifizierung erforderlich ist. Jeder zu einer Zugriffsgruppe hinzugefügte WWPN ermöglicht den Fibre-Channel-Netzwerkzugriff auf Volumes in der Zugriffsgruppe.

   d. **QoS-Richtlinien**: Sie sehen die QoS-Richtlinie, die auf das Volume angewendet wird. Eine QoS-Richtlinie wendet standardisierte Einstellungen für IOPS-Minimum, IOPS-Maximum und IOPS-Burst auf mehrere Volumes an.

      Siehe Informationen über "Performance- und QoS-Richtlinien"Die

Weitere Informationen

- "SolidFire- und Element-Dokumentation"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Sammelt Protokolle für die Fehlerbehebung

Falls Sie Probleme bei der Installation Ihrer SolidFire All-Flash-Storage haben, können Sie Protokolle erfassen, die Sie an NetApp Support senden, um eine Hilfe bei der Diagnose zu erhalten. Entweder NetApp Hybrid Cloud Control oder DIE REST-API zur Erfassung von Protokollen auf einem Element System.

Was Sie benötigen

- Stellen Sie sicher, dass auf Ihrer Speichercluster-Version die NetApp Element-Software 11.3 oder höher

ausgeführt wird.

- Stellen Sie sicher, dass Sie einen Management-Node mit Version 11.3 oder höher bereitgestellt haben.

Optionen für die Protokollerfassung

Wählen Sie eine der folgenden Optionen:

- Verwenden Sie NetApp Hybrid Cloud Control zum Erfassen von Protokollen
- VERWENDEN Sie die REST API zum Erfassen von Protokollen

Verwenden Sie NetApp Hybrid Cloud Control zum Erfassen von Protokollen

Der Protokolleinfassungsbereich ist über das NetApp Hybrid Cloud Control Dashboard zugänglich.

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser. Beispiel:

   ```
   https://[management node IP address]
   ```

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie im Dashboard oben rechts das Menü aus.
4. Wählen Sie **Protokolle Sammeln**.

   Wenn Sie zuvor Protokolle gesammelt haben, können Sie das vorhandene Protokollpaket herunterladen oder eine neue Protokollsammlung starten.

5. Wählen Sie im Dropdown-Menü **Datumsbereich** einen Datumsbereich aus, um festzulegen, welche Daten die Protokolle enthalten sollen.

   Wenn Sie ein benutzerdefiniertes Startdatum angeben, können Sie das Datum auswählen, um den Datumsbereich zu beginnen. Protokolle werden von diesem Datum bis zur aktuellen Zeit gesammelt.

6. Wählen Sie im Abschnitt **Log Collection** die Art der Protokolldateien aus, die das Protokollpaket enthalten soll.

   Bei Storage-Protokollen können Sie die Liste der Storage-Nodes erweitern und einzelne Nodes auswählen, aus denen Protokolle (oder alle Nodes in der Liste) erfasst werden sollen.

7. Wählen Sie **Protokolle sammeln**, um die Protokollsammlung zu starten.

   Die Protokollerfassung wird im Hintergrund ausgeführt, und auf der Seite wird der Fortschritt angezeigt.

   > Abhängig von den gesammelten Protokollen bleibt der Fortschrittsbalken möglicherweise für einige Minuten bei einem bestimmten Prozentsatz oder läuft an einigen Punkten sehr langsam voran.

8. Wählen Sie **Protokolle herunterladen**, um das Protokollpaket herunterzuladen.

   Das Protokollpaket befindet sich in einem komprimierten UNIX .tgz-Dateiformat.

VERWENDEN Sie die REST API zum Erfassen von Protokollen

Sie können REST API zum Sammeln von Element-Protokollen verwenden.

Schritte

1. Suchen Sie die Storage Cluster ID:
   a. Öffnen Sie die REST-API-UI für den Management-Node:

      ```
      https://[management node IP]/logs/1/
      ```

   b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
      ii. Geben Sie die Client-ID als ein `mnode-client` Wenn der Wert nicht bereits ausgefüllt ist.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
2. Protokolle aus Element erfassen:
   a. Wählen Sie **POST/Bundle**.
   b. Wählen Sie **Probieren Sie es aus**.
   c. Ändern Sie die Werte der folgenden Parameter im Feld **Request Body**, je nachdem, welche Protokolltypen Sie erfassen müssen und für welchen Zeitraum:

Parameter	Typ	Beschreibung
`modifiedSince`	Datumszeichenfolge	Schließen Sie nur Protokolle ein, die nach diesem Datum und dieser Uhrzeit geändert wurden. Der Wert "2020-07-14T20:19:00.000Z" definiert beispielsweise ein Startdatum vom 14. Juli 2020 um 20:19 UTC.
`mnodeLogs`	Boolesch	Setzen Sie diesen Parameter auf `true` Um Management-Node-Protokolle einzuschließen.
`storageCrashDumps`	Boolesch	Setzen Sie diesen Parameter auf `true` Um Absturzprotokolle für den Storage-Node einzuschließen.
`storageLogs`	Boolesch	Setzen Sie diesen Parameter auf `true` Um Protokolle für Storage-Nodes einzubeziehen.

Parameter	Typ	Beschreibung
`storageNodeIds`	UUID-Array	Wenn `storageLogs` Ist auf festgelegt `true`, Füllen Sie diesen Parameter mit den Storage-Cluster-Node-IDs aus, um die Protokollerfassung auf diese spezifischen Storage-Nodes zu begrenzen. Verwenden Sie die `GET https://[management node IP]/logs/1/bundle/options` endpunkt zeigt alle möglichen Knoten-IDs, die Sie verwenden können.

d. Wählen Sie **Ausführen**, um die Protokollerfassung zu starten. Die Antwort sollte eine ähnliche Antwort wie die folgende zurückgeben:

```
{
  "_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. Überprüfen Sie den Status der Aufgabe zur Protokollerfassung:
   a. Wählen Sie **GET /Bundle** aus.
   b. Wählen Sie **Probieren Sie es aus**.
   c. Wählen Sie **Ausführen** aus, um einen Status der Sammelaufgabe zurückzugeben.
   d. Blättern Sie zum unteren Rand des Antwortkörpers.

      Sie sollten ein sehen `percentComplete` Attribut, in dem der Fortschritt der Sammlung beschrieben wird. Wenn die Sammlung abgeschlossen ist, wird der angezeigt `downloadLink` Das Attribut enthält den vollständigen Download-Link einschließlich des Dateinamens des Protokollpakets.

   e. Kopieren Sie den Dateinamen am Ende des `downloadLink` Attribut.
4. Laden Sie das gesammelte Protokollpaket herunter:
   a. Wählen Sie **GET /Bundle/{filename}**.
   b. Wählen Sie **Probieren Sie es aus**.
   c. Fügen Sie den Dateinamen ein, den Sie zuvor in den kopiert haben `filename` Textfeld für Parameter.
   d. Wählen Sie **Ausführen**.

      Nach der Ausführung wird im Bereich Response Body ein Download-Link angezeigt.

   e. Wählen Sie **Datei herunterladen** und speichern Sie die resultierende Datei auf Ihrem Computer.

Das Protokollpaket befindet sich in einem komprimierten UNIX .tgz-Dateiformat.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Storage-Management mit Element API

Element API-Software

Erfahren Sie mehr über die Speicherverwaltung mit der Element API.

Die Element-API basiert auf dem JSON-RPC-Protokoll über HTTPS. JSON-RPC ist ein einfaches textbasiertes RPC-Protokoll, das auf dem schlanken JSON-Datenwechselformat basiert. Client-Bibliotheken sind für alle wichtigen Programmiersprachen verfügbar.

API-Anforderungen können über HTTPS-POSTANFORDERUNGEN an den API-Endpunkt gestellt werden. Der Text der POST-Anforderung ist ein JSON-RPC Request-Objekt. Derzeit unterstützt die API keine Batchanforderungen (mehrere Anforderungsobjekte in einem EINZELNEN POST). Beim Senden von API-Anforderungen müssen Sie „Application/json-rpc“ als Inhaltstyp der Anfrage verwenden und sicherstellen, dass der Körper nicht formcodiert ist.

> Die Element Web-UI nutzt die in diesem Dokument beschriebenen API-Methoden. Sie können API-Vorgänge in der Benutzeroberfläche überwachen, indem Sie das API-Protokoll aktivieren. Dadurch können Sie die Methoden anzeigen, die an das System ausgegeben werden. Sie können sowohl Anfragen als auch Antworten aktivieren, um zu sehen, wie das System auf die ausgestellten Methoden antwortet.

Sofern nicht anders angegeben, gelten alle Datumstrings in den API-Antworten im UTC+0-Format.

> Wenn der Storage-Cluster stark ausgelastet ist oder Sie zahlreiche aufeinander folgende API-Anfragen ohne dazwischenende Verzögerungen senden, schlägt die Methode unter Umständen fehl und gibt den Fehler „xDBVersionMismatch“ zurück. In diesem Fall wiederholen Sie den Methodenaufruf.

Gemeinsame Objekte

Die API der Element Software verwendet JSON-Objekte, um organisierte Datenkonzepte darzustellen. Viele dieser API-Methoden nutzen diese Objekte für die Dateneingabe und -Ausgabe. Dieser Abschnitt dokumentiert diese häufig verwendeten Objekte; Objekte, die nur in einer einzigen Methode verwendet werden, werden mit dieser Methode anstelle von in diesem Abschnitt dokumentiert.

"Lerne gängige Gegenstände kennen"

Gängige Methoden

Häufig verwendete Methoden sind Methoden zum Abrufen von Informationen über das Storage-Cluster, die API selbst oder fortlaufende API-Vorgänge.

"Lernen Sie gängige Methoden kennen"

Account-API-Methoden

Mit Kontomethoden können Sie Konto- und Sicherheitsinformationen hinzufügen, entfernen, anzeigen und ändern.

"Erfahren Sie mehr über die API-Methoden für Konten."

Administrator-API-Methoden

Mithilfe von Administrator-API-Methoden können Storage-Cluster-Administratoren Storage-Cluster-Administratoren erstellen, ändern, anzeigen und entfernen sowie Zugriffsebenen und Berechtigungen für Benutzer mit Zugriff auf ein Storage-Cluster zuweisen.

"Erfahren Sie mehr über die Administrator-API-Methoden."

Cluster-API-Methoden

Mithilfe der Cluster-API-Methoden der Element Software können Sie die Konfiguration und Topologie des Storage-Clusters und der Nodes, die zu einem Storage-Cluster gehören, managen.

Einige Cluster-API-Methoden werden auf Nodes ausgeführt, die Teil eines Clusters sind oder für die Verbindung zu einem Cluster konfiguriert wurden. Sie können einem neuen Cluster oder einem vorhandenen Cluster Nodes hinzufügen. Nodes, die zu einem Cluster hinzugefügt werden können, befinden sich in einem „ausstehend“, was bedeutet, dass sie konfiguriert, jedoch noch nicht dem Cluster hinzugefügt wurden.

"Erfahren Sie mehr über Cluster-API-Methoden."

API-Methoden zur Clustererstellung

Sie können diese API-Methoden verwenden, um ein Storage-Cluster zu erstellen. Alle diese Methoden müssen auf einem einzelnen Node gegen den API-Endpunkt eingesetzt werden.

"Erfahren Sie mehr über die API-Methoden zur Clustererstellung."

Drive-API-Methoden

Mit den Drive-API-Methoden können Laufwerke hinzugefügt und gemanagt werden, die einem Storage-Cluster zur Verfügung stehen. Wenn Sie dem Storage-Cluster einen Storage-Node hinzufügen oder neue Laufwerke in einem vorhandenen Storage-Node installieren, können die Laufwerke dem Storage-Cluster hinzugefügt werden.

"Erfahren Sie mehr über die Drive-API-Methoden."

Fibre Channel-API-Methoden

Fibre Channel-API-Methoden können zum Hinzufügen, Ändern oder Entfernen von Fibre Channel-Node-Mitgliedern eines Storage-Clusters verwendet werden.

"Erfahren Sie mehr über Fibre Channel API-Methoden"

Initiator-API-Methoden

Mithilfe von Initiator-Methoden können Sie iSCSI-Initiator-Objekte hinzufügen, entfernen, anzeigen und ändern, die die Kommunikation zwischen dem Speichersystem und externen Speicher-Clients behandeln.

"Erfahren Sie mehr über die Initiator-API-Methoden."

LDAP-API-Methoden

Sie können das Lightweight Directory Access Protocol (LDAP) verwenden, um den Zugriff auf Element Storage zu authentifizieren. Mit den in diesem Abschnitt beschriebenen LDAP-API-Methoden können Sie den LDAP-Zugriff auf das Storage-Cluster konfigurieren.

"Erfahren Sie mehr über die LDAP-API-Methoden."

Multi-Faktor-Authentifizierungs-API-Methoden

Sie können Multi-Faktor-Authentifizierung (MFA) verwenden, um Benutzersitzungen über einen Drittanbieter-Identitätsanbieter (IdP) über die Security Assertion Markup Language (SAML) zu verwalten.

"Erfahren Sie mehr über API-Methoden zur Multi-Faktor-Authentifizierung."

API-Methoden für die Sitzungsauthentifizierung

Sie können die sitzungsbasierte Authentifizierung verwenden, um Benutzersitzungen zu verwalten.

"Erfahren Sie mehr über die API-Methoden zur Sitzungsauthentifizierung."

Node-API-Methoden

Sie können Node-API-Methoden verwenden, um einzelne Nodes zu konfigurieren. Diese Methoden arbeiten auf einzelnen Nodes, die konfiguriert werden müssen, konfiguriert sind, aber noch nicht an einem Cluster beteiligt sind oder aktiv an einem Cluster teilnehmen. Mithilfe von Node-API-Methoden können Sie Einstellungen für einzelne Nodes und das Cluster-Netzwerk, das zur Kommunikation mit dem Node verwendet wird, anzeigen und ändern. Sie müssen diese Methoden für einzelne Nodes ausführen. Sie können keine API-Methoden pro Node für die Adresse des Clusters ausführen.

"Lernen Sie die Node-API-Methoden kennen."

Replizierungs-API-Methoden

Mit den Replication-API-Methoden können Sie zwei Cluster verbinden, um einen kontinuierlichen Datenschutz (CDP) zu ermöglichen. Wenn Sie zwei Cluster verbinden, können aktive Volumes innerhalb eines Clusters kontinuierlich auf ein zweites Cluster repliziert werden, um eine Datenwiederherstellung bereitzustellen. Durch das Pairing von Volumes zur Replikation können Sie Ihre Daten vor Ereignissen schützen, die den Zugriff auf diese Dateien möglicherweise nicht ermöglichen.

"Erfahren Sie mehr über die Replikations-API-Methoden."

Sicherheits-API-Methoden

Sie können Element Software in externe, sicherheitsbezogene Services wie einen externen Verschlüsselungsmanagementserver integrieren. Mit diesen sicherheitsbezogenen Methoden können Sie Sicherheitsfunktionen für Komponenten wie externes Verschlüsselungsmanagement für die Verschlüsselung im Ruhezustand konfigurieren.

"Erfahren Sie mehr über Sicherheits-API-Methoden."

SnapMirror API-Methoden

Die SnapMirror API-Methoden werden von der Element Web-Benutzeroberfläche zum Management von Snapshots verwendet, die mit Remote-ONTAP-Systemen gespiegelt wurden. Diese Methoden sind nur für die

Verwendung durch Element Web UI gedacht. Wenn Sie API-Zugriff auf die SnapMirror-Funktion benötigen, verwenden Sie die ONTAP-APIs. Beispiele für Anfragen und Rückgabeverfahren werden nicht für SnapMirror API-Methoden zur Verfügung gestellt.

"Erfahren Sie mehr über die SnapMirror API-Methoden."

Methoden für die Systemkonfiguration-API

Mit Systemkonfigurations-API-Methoden können Sie Konfigurationswerte abrufen und festlegen, die für alle Knoten im Cluster gelten.

"Erfahren Sie mehr über die API-Methoden zur Systemkonfiguration."

Mandantenfähige Netzwerk-API-Methoden

Das mandantenfähige Netzwerk in Element Storage-Clustern ermöglicht den Datenverkehr zwischen mehreren Clients, die sich in separaten logischen Netzwerken befinden, ohne Layer-3-Routing mit einem Element Storage-Cluster verbunden werden.

Verbindungen zum Storage-Cluster sind im Netzwerk-Stack durch VLAN-Tagging getrennt.

Voraussetzungen für die Einrichtung eines mandantenfähigen virtuellen Netzwerks

- Sie müssen den Block der Client-Netzwerk-IP-Adressen identifiziert haben, die den virtuellen Netzwerken auf den Storage-Nodes zugewiesen werden sollen.
- Sie müssen eine SVIP-Adresse (Client Storage Network IP) für den gesamten Storage-Datenverkehr als Endpunkt angegeben haben.

Reihenfolge der Vorgänge virtueller Netzwerke

1. Verwenden Sie die AddVirtualNetwork-Methode, um die IP-Adressen, die Sie eingeben, in Massen bereitzustellen.

   Nachdem Sie ein virtuelles Netzwerk hinzugefügt haben, führt der Cluster automatisch die folgenden Schritte aus:

   - Jeder Storage-Node erstellt eine virtuelle Netzwerkschnittstelle.
   - Jedem Speicherknoten wird eine VLAN-Adresse zugewiesen, die über das virtuelle SVIP weitergeleitet werden kann.
   - Bei einem Neubooten eines Node bleiben VLAN-IP-Adressen auf jedem Node erhalten.
2. Wenn die virtuelle Netzwerkschnittstelle und die VLAN-Adressen zugewiesen wurden, können Sie dem virtuellen SVIP Client-Netzwerkverkehr zuweisen.

"Erfahren Sie mehr über Multitenant-Netzwerk-API-Methoden"

Volume-API-Methoden

Mit Element Software für die Volume-API-Methoden können Sie Volumes managen, die sich auf einem Storage-Node befinden. Mit diesen Methoden können Sie Volumes erstellen, ändern, klonen und löschen. Sie können auch Volume-API-Methoden verwenden, um Datenmessungen für ein Volume zu erfassen und anzuzeigen.

"Erfahren Sie mehr über die Volume-API-Methoden."

API-Methoden für Volume-Zugriffsgruppen

Mit Methoden für Volume-Zugriffsgruppen können Sie Volume-Zugriffsgruppen hinzufügen, entfernen, anzeigen und ändern. Dabei handelt es sich um Sammlungen von Volumes, auf die Benutzer über iSCSI- oder Fibre-Channel-Initiatoren zugreifen können.

"Erfahren Sie mehr über die API-Methoden für Volumenzugriffsgruppen."

Volume Snapshot-API-Methoden

Mit Element Software Volume Snapshot-API-Methoden können Sie Volume-Snapshots verwalten. Mithilfe der API-Methoden für den Volume-Snapshot können Volume-Snapshots erstellt, geändert, geklont und gelöscht werden.

"Erfahren Sie mehr über die API-Methoden für Volume-Snapshots."

API-Methoden für virtuelle Volumes

Mit Element Software können Sie Virtual Volume API-Methoden (VVols) managen. Vorhandene VVols können mit diesen API-Methoden angezeigt werden sowie Storage Container für virtuelle Volumes erstellen, ändern und löschen. Obwohl Sie diese Methoden nicht zum Betrieb auf normalen Volumes verwenden können, können Sie die normalen Volume-API-Methoden verwenden, um Informationen über VVols aufzulisten.

"Erfahren Sie mehr über die API-Methoden für virtuelle Volumes."

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Fordern Sie Objektmitglieder an

Jede Element Software-API-Anforderung besitzt die folgenden grundlegenden Komponenten:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Methode	Name der anzurufenden Methode.	Zeichenfolge	Keine	Ja.
Parameter	Objekt, das die Parameter für die aufgerufene Methode enthält. Benannte Parameter sind erforderlich. Positionsparameter (als Array übergeben) sind nicht zulässig.	JSON-Objekt	{}	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
id	Die Kennung, die für die Antwort der Anforderung verwendet wurde, wurde im Ergebnis zurückgegeben.	Zeichenfolge oder Ganzzahl	{}	Nein

Mitglieder des Antwortobjekts

Jeder Element Software-API-Antwortkörper hat die folgenden grundlegenden Bestandteile:

Name	Beschreibung	Typ
Ergebnis	Das von der Methode zurückgegebene Objekt. Das System gibt ein Objekt mit benannten Mitgliedern zurück, die dem dokumentierten Rückgabewert der Methode entsprechen. Dieses Mitglied ist nicht vorhanden, wenn ein Fehler aufgetreten ist.	JSON-Objekt
Fehler	Das Objekt wird bei Auftreten eines Fehlers zurückgegeben. Dieses Mitglied ist nur vorhanden, wenn ein Fehler aufgetreten ist.	Objekt
id	Eine Kennung, die der Anforderung der Antwort entspricht, wie in der Anforderung angegeben.	Zeichenfolge oder Ganzzahl
UnusedParameter	Eine Warnmeldung, dass mindestens ein falscher Parameter an die API-Methode übergeben wurde und nicht verwendet wurde.	Objekt

Endpunkte anfordern

Die API verwendet drei Typen von Anforderungsendpunkten (Storage-Cluster, Storage-Cluster-Erstellung und pro Node). Sie sollten immer den neuesten Endpunkt verwenden, der von Ihrer Version der Element Software unterstützt wird.

Die drei Anforderungsendpunkte in der API sind wie folgt gekennzeichnet:

Cluster-API-Methoden

Der HTTPS-Endpunkt für Storage-Cluster-weite API-Anforderungen ist `https://<mvip>/json-rpc/<api-version>`, Wo:

- `<mvip>` Ist die Management-virtuelle IP-Adresse für das Storage-Cluster.
- `<api-version>` Ist die Version der API, die Sie verwenden.

API-Methoden für die Cluster-Erstellung und das Bootstrap

Der HTTPS-Endpunkt zum Erstellen eines Storage-Clusters und zum Zugriff auf Bootstrap-API-Anforderungen ist `https://<nodeIP>/json-rpc/<api-version>`, Wo:

- `<nodeIP>` Die IP-Adresse des Node, den Sie dem Cluster hinzufügen.
- `<api-version>` Ist die Version der API, die Sie verwenden.

API-Methoden pro Node

Der HTTPS-Endpunkt für individuelle API-Anforderungen an den Storage-Node ist `https://<nodeIP>:442/json-rpc/<api-version>`, Wo:

- `<nodeIP>` Ist die Management-IP-Adresse des Storage-Node; 442 ist der Port, auf dem der HTTPS-Server ausgeführt wird.
- `<api-version>` Ist die Version der API, die Sie verwenden.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

API-Authentifizierung

Sie können sich beim Verwenden der API mit dem System authentifizieren, indem Sie eine HTTP Basic-Authentifizierungskopfzeile mit allen API-Anforderungen verwenden. Wenn Sie keine Authentifizierungsinformationen angeben, weist das System die nicht authentifizierte Anfrage mit einer HTTP 401-Antwort zurück. Das System unterstützt die HTTP Basic-Authentifizierung über TLS.

Verwenden Sie das Cluster-Administratorkonto für die API-Authentifizierung.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Asynchrone Methoden

Einige API-Methoden sind asynchron. Dies bedeutet, dass der von ihnen vorführen Vorgang möglicherweise nicht abgeschlossen ist, wenn die Methode zurückkehrt.

Asynchrone Methoden geben ein Handle zurück, das Sie abfragen können, um den Status des Vorgangs anzuzeigen. Statusinformationen für einige Vorgänge können einen prozentualen Anteil der Fertigstellung enthalten.

Wenn Sie einen asynchronen Vorgang abfragen, kann dessen Ergebnis einer der folgenden Typen sein:

- `DriveAdd`: Das System fügt dem Cluster ein Laufwerk hinzu.
- `BulkVolume`: Das System führt einen Kopiervorgang zwischen Volumes durch, z. B. eine Sicherung oder Wiederherstellung.
- `Clone`: Das System geklont ein Volumen.
- `DriveRemoval`: Das System kopiert Daten von einem Laufwerk in Vorbereitung, um es aus dem Cluster zu entfernen.
- `RtfiPendingNode`: Das System installiert kompatible Software auf einem Knoten, bevor sie dem Cluster hinzugefügt wird.

Beachten Sie die folgenden Punkte, wenn Sie asynchrone Methoden verwenden oder den Status eines laufenden asynchronen Vorgangs erhalten:

- Asynchrone Methoden sind in der Dokumentation der einzelnen Methoden angegeben.
- Asynchrone Methoden geben eine „`Async`“ zurück, ein Griff, der durch die emittierenden API-Methode bekannt ist. Mit dem Handle können Sie den Status oder das Ergebnis des asynchronen Vorgangs abfragen.
- Sie können das Ergebnis einzelner asynchroner Methoden mit der GetAsyncResult-Methode abrufen. Wenn Sie GetAsyncResult verwenden, um einen abgeschlossenen Vorgang abzufragen, gibt das System das Ergebnis zurück und reinigt das Ergebnis automatisch vom System. Wenn Sie GetAsyncResult verwenden, um eine unvollständige Operation abzufragen, gibt das System das Ergebnis zurück, löscht es aber nicht.
- Sie können den Status und die Ergebnisse aller ausgeführten oder abgeschlossenen asynchronen Methoden mit der ListAsyncResults-Methode abrufen. In diesem Fall löscht das System die Ergebnisse für abgeschlossene Vorgänge nicht.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Merkmale

Viele API-Anfragen und -Antworten verwenden Objekte sowie einfache Typen. Objekte sind eine Sammlung von Schlüsselwert-Paaren, wobei der Wert ein einfacher Typ oder möglicherweise ein anderes Objekt ist. Attribute sind benutzerdefinierte Name-Wert-Paare, die vom Benutzer in JSON-Objekten festgelegt werden können. Mithilfe einiger Methoden können Sie beim Erstellen oder Ändern von Objekten Attribute hinzufügen.

Für codierte Attributobjekte gibt es eine Begrenzung von 1000 Byte.

Objektmitglied

Dieses Objekt enthält das folgende Mitglied:

Name	Beschreibung	Typ
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt

Anforderungsbeispiel

Das folgende Anforderungsbeispiel verwendet die AddClusterAdmin-Methode:

```
{
   "method": "AddClusterAdmin",
   "params": {
      "username": "joeadmin",
      "password": "68!5Aru268)$",
      "access": [
         "volume",
         "reporting"
      ],
      "attributes": {
         "name1": "value1",
         "name2": "value2",
         "name3": "value3"
      }
   }
}
```

Gemeinsame Objekte

Konto

Der `account` Objekt enthält Informationen zu einem Konto. Dieses Objekt enthält nur „konfigurierte“ Informationen über das Konto, keine Laufzeitinformationen oder Nutzungsinformationen.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
`accountID`	Die eindeutige Konto-ID für das Konto.	Ganzzahl

Name	Beschreibung	Typ
`attributes`	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt
`enableChap`	Gibt an, ob CHAP-Kontoanmeldeinformationen von einem Initiator für den Zugriff auf Volumes verwendet werden können.	boolesch
`initiatorSecret`	Der Initiator-CHAP-Schlüssel.	Zeichenfolge
`status`	Der aktuelle Status des Kontos. Mögliche Werte: • Aktiv: Ein aktives Konto. • Gesperrt: Ein gesperrtes Konto. • Entfernt: Ein Konto, das gelöscht und gelöscht wurde.	Zeichenfolge
`storageContainerID`	Die eindeutige ID des mit diesem Konto verknüpften Speichercontainers für virtuelle Volumes.	UUID
`targetSecret`	Der CHAP-Schlüssel des Ziels.	Zeichenfolge
`username`	Der Benutzername für das Konto.	Zeichenfolge
`volumes`	Eine Liste der Volume-IDs für Volumes, die dem Konto gehören.	Integer-Array

Weitere Informationen

- AddAccount
- GetAccountByID
- GetAccountByName
- Listenkonten

AuthSessionInfo

Der `authSessionInfo` Objekt enthält Informationen über eine auth-Sitzung.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
accessGroupList	Liste der Zugriffsgruppen für den Benutzer.	String-Array
authMethod	Der Berechtigungstyp, den der Cluster-Admin-Benutzer besitzt. Mögliche Werte: • LDAP - authentifiziert über LDAP. • Cluster - authentifiziert über einen Benutzernamen und ein Passwort in der Cluster-Datenbank gespeichert. • IDP – Authentifizierung über einen Drittanbieter.	Zeichenfolge
clusterAdminIDs	Liste der Cluster-AdminID(s), die mit dieser Sitzung verbunden sind. Bei Sitzungen im Zusammenhang mit LDAP oder einem Identitätsanbieter eines Drittanbieters (IdP) handelt es sich hierbei um eine aggregierte Liste mit übereinstimmenden Cluster-AdminIDs, die dieser Sitzung zugeordnet sind.	Integer-Array
finalTimeout	Die Zeit, zu der die Sitzung ungültig wird.Dies wird festgelegt, wenn die Sitzung erstellt wird und nicht geändert werden kann.	Zeichenfolge
idpConfigVersion	IDP-Konfigurationsversion, wenn die Sitzung erstellt wurde.	Ganzzahl
lastAccessTimeout	Der Zeitpunkt, zu dem die Sitzung aufgrund von Inaktivität ungültig wird.Es wird auf einen neuen Wert gesetzt, wenn auf die Sitzung zugegriffen wird, bis zu dem Zeitpunkt, zu dem die Sitzung ungültig wird, weil finalTimeout erreicht wird.	Zeichenfolge
sessionCreationTime	Uhrzeit, zu der die Sitzung erstellt wird.	Zeichenfolge
sessionID	UUID für diese Sitzung.	UUID

Name	Beschreibung	Typ
`username`	Der dieser Sitzung zugeordnete Benutzername. Bei Sitzungen zu LDAP wird dies der LDAP-DN des Benutzers sein. Bei Sitzungen im Zusammenhang mit IdP eines Drittanbieters handelt es sich hierbei um ein willkürliches Namenswertpaar, das für die Prüfung von Operationen innerhalb der Sitzung verwendet wird. Er entspricht nicht notwendigerweise dem Namen eines Cluster-Administrators im Cluster. Beispiel: Eine SAML-Subject-NameID, aber diese wird durch die Konfiguration des IdP und den daraus resultierenden Inhalt der SAML-Assertion vorgegeben.	Zeichenfolge

BulkVolumeJob

Der `bulkVolumeJob` Das Objekt enthält Informationen zu Lese- oder Schreibvorgängen auf dem Massenvolume, wie Klonen oder Snapshot-Erstellung.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
`attributes`	JSON-Attribut des Massenvolumenjobs.	JSON-Objekt
`bulkVolumeID`	Die interne Job-ID für das Massenvolumen.	Ganzzahl
`createTime`	Zeitstempel, der für den Massenvolumenauftrag im UTC+0-Format erstellt wurde.	ISO 8601-Datumszeichenfolge
`elapsedTime`	Die Anzahl der Sekunden seit Beginn des Jobs.	Zeichenfolge
`format`	Das Format des Massenvolumes-Vorgangs. Mögliche Werte: • Nativ • Unkomprimiert	Zeichenfolge

Name	Beschreibung	Typ
`key`	Der eindeutige Schlüssel, der von der Massenvolumensitzung erstellt wird.	Zeichenfolge
`percentComplete`	Der vom Vorgang gemeldete Prozentsatz des Abgeschlossen.	Ganzzahl
`remainingTime`	Die geschätzte verbleibende Zeit in Sekunden.	Ganzzahl
`srcVolumeID`	Die ID des Quell-Volume.	Ganzzahl
`status`	Der Status des Vorgangs. Mögliche Werte: • Vorbereitung • Wird ausgeführt • Abgeschlossen • Fehlgeschlagen	Zeichenfolge
`script`	Der Name des Skripts, falls vorhanden.	Zeichenfolge
`snapshotID`	Die ID des Snapshots, wenn sich ein Snapshot in der Quelle des Jobs mit dem Massenvolumen befindet.	Ganzzahl
`type`	Der Typ des Massenvorgangs. Mögliche Werte: • Lesen • Schreiben	Zeichenfolge

Bindung (virtuelle Volumes)

Das Bindeobjekt enthält Informationen über die Bindung für ein virtuelles Volume. Sie können eine Liste dieser Informationen für alle virtuellen Volumes mit abrufen `ListVirtualVolumeBindings` API-Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
`protocolEndpointID`	Die eindeutige ID des Protokollendpunkts.	UUID
`protocolEndpointInBandID`	Die scsiNAADeviceID des Protokollendpunkts.	Zeichenfolge
`protocolEndpointType`	Der Typ des Protokollendpunkts. SCSI ist der einzige Wert, der für den Protokollendpunkttyp zurückgegeben wird.	Zeichenfolge
`virtualVolumeBindingID`	Die eindeutige ID des Bindeobjekts für das virtuelle Volume.	Ganzzahl
`virtualVolumeHostID`	Die eindeutige ID des virtuellen Volume-Hosts.	UUID
`virtualVolumeID`	Die eindeutige ID des virtuellen Volumes.	UUID
`virtualVolumeSecondaryID`	Die sekundäre ID des virtuellen Volume.	Zeichenfolge

Weitere Informationen

- ListVirtualVolumeBindungen
- ProtocolEndpoint

ZertifikateDetails

Der `certificateDetails` Objekt enthält die decodierten Informationen über ein Sicherheitszertifikat.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
`issuer`	Der Name des Emittenten.	Zeichenfolge
`modulus`	Das Modul des öffentlichen Schlüssels.	Zeichenfolge
`notAfter`	Das Ablaufdatum des Zertifikats.	ISO 8601-Zeichenfolge

Name	Beschreibung	Typ
notBefore	Das Startdatum des Zertifikats.	ISO 8601-Zeichenfolge
serial	Die Seriennummer des Zertifikats.	Zeichenfolge
sha1Fingerprint	Der Digest der-kodierten Version des Zertifikats.	Zeichenfolge
subject	Der Name des Studienteilnehmers.	Zeichenfolge

Cluster

Das Cluster-Objekt enthält Informationen, die der Node zur Kommunikation mit dem Cluster verwendet. Sie können diese Informationen mit der GetClusterConfig-API-Methode abrufen.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Zipi	Für die Cluster-Kommunikation verwendete Netzwerkschnittstelle.	Zeichenfolge
Cluster	Eindeutiger Cluster-Name.	Zeichenfolge
VerschlüsselungBeschriftung	Gibt an, ob der Node die Laufwerkverschlüsselung unterstützt.	boolesch
Ensemble	Die Nodes, die am Cluster teilnehmen.	String-Array
FipsDriveKonfiguration	Gibt an, ob der Node FIPS 140-2-2-zertifizierte Laufwerke unterstützt.	boolesch
mipi	Die für das Node-Management verwendete Netzwerkschnittstelle.	Zeichenfolge
Name	Der Cluster-Name.	Zeichenfolge
NodeID	Die Node-ID des Node im Cluster.	Zeichenfolge

Name	Beschreibung	Typ
HängenNodeID	Die ID des ausstehenden Node im Cluster.	Ganzzahl
Rolle	Gibt die Rolle des Knotens an.	Ganzzahl
sipi	Die für Storage-Datenverkehr verwendete Netzwerkschnittstelle.	Zeichenfolge
Bundesland	Der aktuelle Status des Node. Mögliche Werte: • Verfügbar: Der Node wurde nicht mit einem Cluster-Namen konfiguriert. • Ausstehend: Der Node steht für ein bestimmtes benanntes Cluster aus und kann hinzugefügt werden. • Aktiv: Der Node ist ein aktives Mitglied eines Clusters und kann keinem anderen Cluster hinzugefügt werden. • PendingActive: Der Knoten wird derzeit an das Factory-Software-Image zurückgegeben und ist noch kein aktives Mitglied eines Clusters. Nach Abschluss wechselt es in den Status „aktiv“.	Zeichenfolge
Version	Die Version der auf dem Node ausgeführten Software.	Zeichenfolge

Mitgliedänderbarkeit und Knotenstatus

In dieser Tabelle wird angegeben, ob die Objektparameter für jeden möglichen Node-Status geändert werden können.

Parametername	Verfügbarer Status	Status „ausstehend“	Aktiver Status
Zipi	Nein	Nein	Nein
Cluster	Ja.	Ja.	Nein
VerschlüsselungBeschriftung	Nein	Nein	Nein

Ensemble	Nein	Nein	Nein
mipi	Ja.	Ja.	Nein
Name	Ja.	Ja.	Ja.
NodeID	Nein	Nein	Nein
HängenNodeID	Nein	Nein	Nein
Rolle	Nein	Nein	Nein
sipi	Nein	Nein	Nein
Bundesland	Nein	Nein	Nein
Version	Nein	Nein	Nein

Weitere Informationen

GetClusterConfig

ClusterAdmin

Das ClusterAdmin-Objekt enthält Informationen über den aktuellen Cluster-Administrator-Benutzer. Sie können Administratorbenutzerinformationen mit der GetCurrentClusterAdmin-API-Methode abrufen.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Datenzugriff	Die Methoden, die dieser Cluster-Administrator verwenden kann.	String-Array
AuthMethod	Der Berechtigungstyp, den der Cluster-Admin-Benutzer besitzt. Mögliche Werte: • LDAP • Cluster • Vor Ort	Zeichenfolge

Name	Beschreibung	Typ
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt
Cluster-AdminID	Die Cluster-Administrator-ID für diesen Cluster-Admin-Benutzer.	Ganzzahl
Benutzername	Benutzername für diesen Cluster-Administrator.	Zeichenfolge

Weitere Informationen

GetCurrentClusterAdmin

ClusterKapazität

Das ClusterCapacität Objekt enthält allgemeine Kapazitätsmessungen für das Cluster. Sie können Cluster-Kapazitätsinformationen mit der GetClusterCapacity API-Methode abrufen. Die Speicherplatzmessungen der Objektmitglieder werden in Byte berechnet.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
ActiveBlockSpace	Die Menge an Speicherplatz auf den Block-Laufwerken. Dazu gehören zusätzliche Informationen wie Metadateneinträge und Speicherplatz, der bereinigt werden kann.	Ganzzahl
ActiveSessions	Die Anzahl der aktiven iSCSI-Sitzungen, die mit dem Cluster kommunizieren.	Ganzzahl
Durchschnittlich IOPS	Der durchschnittliche IOPS für das Cluster seit Mitternacht Coordinated Universal Time (UTC).	Ganzzahl
ClusterRecentIOSize	Durchschnittliche IOPS-Größe für alle Volumes im Cluster	Ganzzahl
Aktuellen IOPS	Der durchschnittliche IOPS aller Volumes im Cluster in den letzten 5 Sekunden.	Ganzzahl

Name	Beschreibung	Typ
Maximale IOPS-Werte	Die geschätzte maximale IOPS-Kapazität des aktuellen Clusters.	Ganzzahl
MaxOverProvisionableSpace	Die maximale Menge an bereitstellbarem Speicherplatz. Dies ist ein berechneter Wert. Sie können keine neuen Volumes erstellen, wenn der aktuell bereitgestellte Speicherplatz sowie die neue Volume-Größe diese Zahl überschreiten würden. Der Wert berechnet sich wie folgt: `maxOverProvisionableSpace = maxProvisionedSpace * maxMetadataOverProvisionFactor`	Ganzzahl
Max. ProvisionedSpace	Die Gesamtmenge an bereitstellbarem Speicherplatz, wenn alle Volumes zu 100 % gefüllt sind (keine Metadaten, die über Thin Provisioning bereitgestellt wurden).	Ganzzahl
MaxUsedMetadataSpace	Die Anzahl der Bytes auf Volume-Laufwerken, die zum Speichern von Metadaten verwendet werden.	Ganzzahl
MaxUsedSpace	Die Gesamtmenge an Speicherplatz auf allen aktiven Blocklaufwerken.	Ganzzahl
NonZeroBlock	Die Gesamtzahl der 4KiB-Blöcke, die Daten enthalten, nachdem der letzte Speichervorgang abgeschlossen ist.	Ganzzahl
PeakActiveSessions	Die Spitzenzahl der iSCSI-Verbindungen seit Mitternacht UTC.	Ganzzahl
PeakIOPS	Der höchste Wert für aktuelle IOPS seit Mitternacht UTC.	Ganzzahl
ProvisionierungSpace	Der insgesamt in allen Volumes im Cluster bereitgestellte Speicherplatz.	Ganzzahl

Name	Beschreibung	Typ
Zeitstempel	Das Datum und die Uhrzeit im UTC+0-Format, für die der Beleg für die Cluster-Kapazität verwendet wurde.	ISO 8601-Zeichenfolge
TotalOps	Die Gesamtzahl der I/O-Vorgänge, die während der gesamten Nutzungsdauer des Clusters ausgeführt werden,	Ganzzahl
UniqueBlocks	Die Gesamtanzahl der auf den Blocklaufwerken gespeicherten Blöcke. Der Wert umfasst replizierte Blöcke.	Ganzzahl
UniqueBlocksUsedSpace	Die Gesamtmenge an Daten, die die uniqueBlocks auf den Blocklaufwerken aufnehmen. Weitere Informationen dazu, wie sich diese Zahl auf den Wert uniqueBlocks bezieht, finden Sie in der GetclusterCapacity-Methode.	Ganzzahl
UsedMetadataSpace	Die Gesamtzahl der Bytes auf Volume-Laufwerken, die zur Speicherung von Metadaten verwendet werden.	Ganzzahl
UsedMetadataSpaceInSnapshots	Die Anzahl der Bytes auf Volume-Laufwerken, die zum Speichern eindeutiger Daten in Snapshots verwendet werden. Diese Zahl liefert eine Schätzung der Menge an Metadaten, die wiederhergestellt werden würde, indem alle Snapshots auf dem System gelöscht werden.	Ganzzahl
UsedSpace	Der insgesamt von allen Block-Laufwerken im System genutzte Speicherplatz.	Ganzzahl
ZeroBlocks	Die Gesamtzahl der leeren 4KiB-Blöcke ohne Daten, nachdem die letzte Runde der Müllsammlung abgeschlossen ist.	Ganzzahl

Weitere Informationen

GetClusterCapacity

Cluster-Konfiguration

Der `clusterConfig` Das Objekt gibt Informationen zurück, die der Node zur Kommunikation mit dem Cluster verwendet.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
`cipi`	Für die Cluster-Kommunikation verwendete Netzwerkschnittstelle.	Zeichenfolge
`cluster`	Eindeutiger Name des Clusters.	Zeichenfolge
`encryptionCapable`	Gibt an, ob der Node die Verschlüsselung unterstützt.	boolesch
`ensemble`	Nodes, die am Cluster teilnehmen.	String-Array
`fipsDriveConfiguration`	Gibt an, ob der Node FIPS 140-2-2-zertifizierte Laufwerke unterstützt.	boolesch
`hasLocalAdmin`	Gibt an, ob der Cluster über einen lokalen Administrator verfügt.	boolesch
`mipi`	Für das Node-Management verwendete Netzwerkschnittstelle.	Zeichenfolge
`name`	Eindeutige Kennung für das Cluster	Zeichenfolge
`nodeID`	Eindeutige Kennung für den Knoten.	Ganzzahl
`pendingNodeID`	Eindeutige Kennung für den ausstehenden Node.	Ganzzahl
`role`	Gibt die Rolle des Knotens an.	Zeichenfolge
`sipi`	Für den Storage verwendete Netzwerkschnittstelle.	Zeichenfolge

Name	Beschreibung	Typ
`state`	Gibt den Status des Node an.	Zeichenfolge
`version`	Zeigt die Version des Node an.	Zeichenfolge

ClusterInfo

Das ClusterInfo-Objekt enthält Informationen, die der Node zur Kommunikation mit dem Cluster verwendet. Diese Informationen erhalten Sie mit der GetClusterInfo-API-Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt
Standardschutzschema	Das Schutzschema, das standardmäßig für neue Volumes verwendet wird, es sei denn, ein Schutzschema wird mit dem bereitgestellt CreateVolume Methodenanruf. Diese Schutzregelung muss immer in der Reihe der aktivierten Schutzmechanismen enthalten sein.	Zeichenfolge
EnabledProtectionSchemes	Eine Liste aller Sicherungsschemata, die auf diesem Storage-Cluster aktiviert wurden.	String-Array

Name	Beschreibung	Typ
VerschlüsselungAtRestState	Der Status der Funktion Verschlüsselung im Ruhezustand. Mögliche Werte: • Aktivieren: Verschlüsselung im Ruhezustand wird aktiviert. • Aktiviert: Verschlüsselung im Ruhezustand ist aktiviert. • Deaktivieren: Verschlüsselung im Ruhezustand wird deaktiviert. • Deaktiviert: Verschlüsselung im Ruhezustand ist deaktiviert.	Zeichenfolge
Ensemble	Die Nodes, die am Cluster teilnehmen.	String-Array
mvip	Die fließende (virtuelle) IP-Adresse für den Cluster im Managementnetzwerk.	Zeichenfolge
MvipInterface	Die physische Schnittstelle, die der MVIP-Adresse zugeordnet ist.	Zeichenfolge
MvipNodeID	Der Knoten, der die Master-MVIP-Adresse enthält.	Ganzzahl
MvipVlanTag	Die VLAN-ID für die MVIP-Adresse.	Zeichenfolge
Name	Der eindeutige Cluster-Name.	Zeichenfolge
RepCount	Die Anzahl der Replikate jeder Datenkomponente, die im Cluster gespeichert werden soll. Der gültige Wert ist „2“.	Ganzzahl
SoftwareverschlüsselungAtRestState	Softwarebasierte Verschlüsselung im Ruhezustand:	Zeichenfolge
UnterstützungProtectionSchemes	Eine Liste aller auf diesem Storage-Cluster unterstützten Sicherungsschemata.	String-Array
svip	Die fließende (virtuelle) IP-Adresse für den Cluster im Storage-Netzwerk (iSCSI).	Zeichenfolge

Name	Beschreibung	Typ
SvipInterface	Die physische Schnittstelle, die der Master-SVIP-Adresse zugeordnet ist.	Zeichenfolge
SvipNodeID	Der Knoten mit der Master-SVIP-Adresse.	Ganzzahl
SvipVlanTag	Die VLAN-Kennung für die Master-SVIP-Adresse.	Zeichenfolge
UniqueID	Die eindeutige ID für das Cluster.	Zeichenfolge
uuid	Die eindeutige ID für das Cluster.	UUID
VolumeLoadBalanceOnActualIops State	Der Status für den Slice-Balancing basiert auf den tatsächlichen IOPS statt auf der Funktion „Min. IOPS“. Verfügbar ab Element 12.8.	Zeichenfolge

Weitere Informationen

- "GetClusterInfo"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Cluster-Paar

Das ClusterPair-Objekt enthält Informationen über Cluster, die mit dem lokalen Cluster gekoppelt sind. Mit der ListClusterpairs-Methode können Sie eine Liste der ClusterPair-Objekte für das lokale Cluster abrufen.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
ClusterName	Der Name des anderen Clusters im Paar.	Zeichenfolge
ClusterPairID	Eine eindeutige ID, die jedem Cluster im Paar gegeben wurde.	Ganzzahl
ClusterPairUUID	Die universell eindeutige Kennung für das Cluster-Paar.	Zeichenfolge

Name	Beschreibung	Typ
UUID	Eindeutige Kennung für das Remote-Cluster im Cluster-Paar.	Ganzzahl
Latenz	Latenz in Millisekunden zwischen den Clustern.	Ganzzahl
mvip	Die IP-Adresse der Managementverbindung für gepaarte Cluster.	Zeichenfolge
Status	Der Status der Verbindung zwischen den gekoppelten Clustern. Mögliche Werte: • Nicht Konfiguriert • Verbunden • Falsch Konfiguriert • Verbindung Getrennt	Zeichenfolge
Version	Die Elementversion des anderen Clusters im Paar.	Zeichenfolge

Weitere Informationen

ListenClusterpaare

ClusterStatistik

Das clusterStats-Objekt enthält statistische Daten für ein Cluster. Viele der im Objekt enthaltenen Statistiken zum Volume werden über alle Volumes im Cluster abgemittelt. Sie können diese Informationen über die Methode GetClusterStats für einen Cluster abrufen.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Berechnung	Typ
AktualIOPS	Der aktuelle tatsächliche IOPS für den gesamten Cluster in den letzten 500 Millisekunden.	Zeitpunktgenau	Ganzzahl

Name	Beschreibung	Berechnung	Typ
MittelungIOPSize	Durchschnittliche Größe in Byte der letzten I/O-Vorgänge für den Cluster in den letzten 500 Millisekunden.	Zeitpunktgenau	Ganzzahl
ClientQueueDepth	Die Anzahl der ausstehenden Lese- und Schreibvorgänge auf dem Cluster.	1. A.	Ganzzahl
ClusterAuslastung	Der Prozentsatz der maximalen IOPS des Clusters, die derzeit genutzt werden. Dies wird als clusterUtilisation = normalizedIOPS/maxIOPS (von GetClusterCapacity) berechnet.	1. A.	Schweben
LaticyUSec	Der durchschnittliche Zeitaufwand in Mikrosekunden, um den Betrieb eines Clusters in den letzten 500 Millisekunden abzuschließen.	Zeitpunktgenau	Ganzzahl
NormalisiertIOPS	Durchschnittliche IOPS-Anzahl des gesamten Clusters in den letzten 500 Millisekunden.	Zeitpunktgenau	Ganzzahl
ReadBytes	Die insgesamt gesammelten Bytes, die vom Cluster seit der Erstellung des Clusters gelesen werden.	Monotonisch zunehmende Zahl	Ganzzahl
LesBytesLastBeispiel	Die Gesamtzahl der Bytes, die im letzten Probenzeitraum vom Cluster gelesen werden.	Zeitpunktgenau	Ganzzahl

Name	Beschreibung	Berechnung	Typ
ReadLatencyUSec	Die durchschnittliche Zeit in Mikrosekunden, um Lesevorgänge in dem Cluster in den letzten 500 Millisekunden abzuschließen.	Zeitpunktgenau	Ganzzahl
ReadLatencyUSecTotal	Die Gesamtzeit, die seit der Erstellung des Clusters für Lesevorgänge benötigt wurde.	Monotonisch zunehmende Zahl	Ganzzahl
ReadOps	Die gesamten kumulativen Lesevorgänge an dem Cluster seit der Erstellung des Clusters.	Monotonisch zunehmende Zahl	Ganzzahl
LesesOpsLastSample	Die Gesamtzahl der Leseoperationen während des letzten Probenzeitraums.	Zeitpunktgenau	Ganzzahl
SamplePeriodMSec	Die Länge des Probenzeitraums in Millisekunden.	1. A.	Ganzzahl
ServicesAnzahl	Die Anzahl der auf dem Cluster ausgeführten Services. Wenn der ServicesTotal entspricht, zeigt dies an, dass gültige Statistiken von allen Knoten erfasst wurden.	Zeitpunktgenau	Ganzzahl
ServicesSumme	Die Gesamtzahl der erwarteten Services, die auf dem Cluster ausgeführt werden	1. A.	Ganzzahl
Zeitstempel	Die aktuelle Zeit im UTC+0-Format.	1. A.	ISO 8601-Datumszeichenfolge

Name	Beschreibung	Berechnung	Typ
UnalignedReads	Die gesamten, kumulativen, nicht ausgerichteten Lesevorgänge an einem Cluster seit der Erstellung des Clusters.	Monotonisch zunehmende Zahl	Ganzzahl
UnalignedWrites	Die gesamten, kumulativen, nicht ausgerichteten Schreibvorgänge an einem Cluster seit der Erstellung des Clusters	Monotonisch zunehmende Zahl	Ganzzahl
WriteBytes	Die Summe der kumulativen Bytes, die seit der Erstellung des Clusters auf den Cluster geschrieben werden.	Monotonisch zunehmende Zahl	Ganzzahl
Write eBytesLastSample	Die Gesamtzahl der Bytes, die im letzten Probenzeitraum auf das Cluster geschrieben wurden.	Monotonisch zunehmende Zahl	Ganzzahl
Write LatencyUSec	Der durchschnittliche Zeitaufwand in Mikrosekunden, um Schreibvorgänge in einem Cluster in den letzten 500 Millisekunden abzuschließen.	Zeitpunktgenau	Ganzzahl
Write eLatencyUSecTotal	Die Gesamtzeit, die seit der Erstellung des Clusters für Schreibvorgänge verwendet wurde.	Monotonisch zunehmende Zahl	Ganzzahl
Schreiboperationen	Die gesamten, kumulativen Schreibvorgänge an den Cluster seit der Erstellung des Clusters	Monotonisch zunehmende Zahl	Ganzzahl
WriteOpsLastSample	Die Gesamtzahl der Schreibvorgänge im letzten Probenzeitraum.	Zeitpunktgenau	Ganzzahl

Weitere Informationen

GetClusterStats

ClusterStructure

Das ClusterStructure-Objekt enthält Backup-Informationen zur Clusterkonfiguration, die mit der GetClusterStructure-Methode erstellt wurden. Sie können die Methode SetClusterStructure verwenden, um diese Informationen in einem Speichercluster wiederherzustellen, den Sie neu erstellen.

Objektmitglieder verwenden

Dieses Objekt enthält die kombinierten Rückgabeinformationen aus den folgenden Methoden:

- GetClusterInfo
- Listenkonten
- ListenInitiatoren
- ListVolumes (Bei includeVirtualVolumes=false)
- ListVolumeAccessGroups
- ListStorageContainer
- ListQoSPolicies
- GetSnmpInfo
- GetNtpInfo
- ListVirtualNetworks
- ListenClusteradministratoren
- ListSchedules
- ListSnapMirrorEndpunkte
- GetFeatureStatus
- GetLdapConfiguration
- GetRemoteLoggingHosts
- GetDefaultQoS
- GetVolumeAccessGroupLunAssignments

Weitere Informationen

- GetClusterStructure
- SetClusterStructure

Laufwerk

Das Laufwerksobjekt enthält Informationen über einzelne Laufwerke in den aktiven Nodes des Clusters. Dieses Objekt enthält Details zu Laufwerken, die als Volume-Metadaten oder Block-Laufwerke hinzugefügt wurden, sowie zu Laufwerken, die noch

nicht hinzugefügt wurden und verfügbar sind. Sie können diese Informationen mit dem abrufen `ListDrives` API-Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat. Dieses Objekt ist immer Null und kann nicht geändert werden.	JSON-Objekt
Kapazität	Die Gesamtkapazität des Laufwerks in Byte.	Ganzzahl
ChassisSlot	Bei HCI-Plattformen ist dieser Wert der Node-Buchstabe und die Steckplatznummer im Server-Chassis, in dem sich dieses Laufwerk befindet. Bei Speicherplattformen ist die Steckplatznummer eine String-Darstellung der "Slot"-Ganzzahl.	Zeichenfolge
FahrausfällenDetail	Wenn der Status eines Laufwerks „ausgefallen“ lautet, enthält dieses Feld weitere Informationen darüber, warum das Laufwerk als fehlgeschlagen markiert wurde.	Zeichenfolge
DriveID	Die ID dieses Laufwerks.	Ganzzahl
SicherheitfürZufahrt FaultStason	Wenn das Aktivieren oder Deaktivieren der Laufwerksicherheit fehlgeschlagen ist, ist der Grund für dessen Fehler aufgetreten. Wenn der Wert „none“ lautet, gab es keinen Fehler.	Zeichenfolge
Schlüssel-ID	Die KeyID, die vom Schlüsselanbieter zum Abrufen des Authentifizierungsschlüssels zum Entsperren dieses Laufwerks verwendet wird.	UUID
ID von Schlüsselausweisungs-ID	Identifiziert den Provider des Authentifizierungsschlüssels zum Entsperren dieses Laufwerks.	Ganzzahl

Name	Beschreibung	Typ
NodeID	Die ID des Node, der dieses Laufwerk enthält.	Ganzzahl
SegmentFileSize	Die Segmentdateigröße des Laufwerks in Byte.	Ganzzahl
Seriell	Die Seriennummer des Laufwerks.	Zeichenfolge
Schlitz	Die Steckplatznummer im Servergehäuse, in dem sich dieses Laufwerk befindet, oder -1 wenn ein SATADimm-Gerät für das interne Metadatenlaufwerk verwendet wird.	Ganzzahl
Status	Der Status des Laufwerks. Mögliche Werte: • Verfügbar: Ein verfügbares Laufwerk. • Aktiv: Ein aktives Laufwerk. • Löschen: Ein Laufwerk ist dabei, sicher gelöscht zu werden. Alle Daten auf diesem Laufwerk werden dauerhaft entfernt. • Fehlgeschlagen: Ein Laufwerk, das ausgefallen ist. Alle Daten, die zuvor auf dem Laufwerk waren, wurden auf andere Laufwerke im Cluster migriert. • Entfernen: Ein Laufwerk wird gerade entfernt. Alle zuvor auf dem Laufwerk befindlichen Daten werden auf andere Laufwerke im Cluster migriert.	Zeichenfolge
Typ	Der Laufwerkstyp. Mögliche Werte: • Volume: Speichert Volume-Metadaten. • Block: Speichert Blockdaten. • Unbekannt: Der Laufwerkstyp ist noch nicht aktiv und muss noch ermittelt werden.	Zeichenfolge

Name	Beschreibung	Typ
UsableKapazität	Die nutzbare Kapazität des Laufwerks in Byte.	Ganzzahl

Weitere Informationen

ListenLaufwerke

Fahrstollen

Das Objekt driveStats enthält übergeordnete Aktivitätsmessungen für eine einzelne Festplatte. Mit der API-Methode können Sie Messdaten abrufen `GetDriveStats`.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
ActiveSessions	Anzahl der iSCSI-Sitzungen, die derzeit dieses Laufwerk verwenden (nur vorhanden für Metadaten-Laufwerke).	Ganzzahl
DriveID	Eindeutige ID des Laufwerks im Cluster	Ganzzahl
FailedDieCount	Anzahl der fehlerhaften Laufwerkselemente.	Ganzzahl
IosInProgress	Die Anzahl der laufenden I/O-Vorgänge für dieses Laufwerk.	Ganzzahl
LebensRemainingPercent	Anzeige der Laufwerksverschleißanzeige.	Ganzzahl
RettungszeitLesen	Insgesamt gelesene Bytes von diesem Laufwerk für die Lebensdauer des Laufwerks.	Ganzzahl
RettungsWriteBytes	Gesamtbyte, die für die Lebensdauer des Laufwerks auf dieses Laufwerk geschrieben wurden.	Ganzzahl
PowerOnHours	Anzahl der Stunden, in denen dieses Laufwerk eingeschaltet wurde.	Ganzzahl

Name	Beschreibung	Typ
Lesevorgänge	Die Anzahl der Read() Aufrufe pro Sekunde zu diesem Laufwerk.	Ganzzahl
ReadBytes	Insgesamt gelesene Bytes vom Laufwerk aufgrund von Client-Operationen.	Ganzzahl
ReadsKombiniert	Die Anzahl der Read() Aufrufe zu benachbarten Sektoren, die zu einem größeren Read kombiniert werden könnten.	Ganzzahl
ReadMsec	Die Anzahl der Millisekunden, die gelesen wurden.	Ganzzahl
ReadOps	Gesamte Lesevorgänge auf dem Laufwerk aufgrund von Client-Operationen.	Ganzzahl
Zu verlokalisierteSectors	Anzahl der fehlerhaften Sektoren, die in diesem Laufwerk ersetzt wurden.	Ganzzahl
ReservekapazitätPercent	Die verfügbare Reservekapazität des Laufwerks.	Ganzzahl
Zeitstempel	Die aktuelle Zeit im UTC+0-Format.	ISO 8601-Datumszeichenfolge
GesamtDeckkraft	Gesamtkapazität des Laufwerks in Byte.	Ganzzahl
Unkorrigierbare Error	Der gemeldete Wert nicht korrigierbarer Fehler aus dem Monitoring-System der Selbstüberwachung, der Analyse- und Berichtstechnik (SMART) im Laufwerk.	Ganzzahl
UsedKapacität	Genutzte Kapazität des Laufwerks, in Byte.	Ganzzahl
UsedMemory	Die derzeit vom Node, der dieses Laufwerk hostet, verwendete Speichermenge.	Ganzzahl
Schreibvorgänge	Die Anzahl der Write() Aufrufe pro Sekunde zu diesem Laufwerk.	Ganzzahl

Name	Beschreibung	Typ
WriteBytes	Gesamtzahl der Bytes, die aufgrund der Client-Aktivität auf das Laufwerk geschrieben wurden.	Ganzzahl
WritesKombiniert	Die Anzahl der Write() Aufrufe in benachbarte Sektoren, die zu einem größeren Schreibvorgang kombiniert werden können.	Ganzzahl
Schreibgeschwindigkeit	Die Anzahl der Millisekunden, die geschrieben wurden.	Ganzzahl
Schreiboperationen	Gesamte Schreibvorgänge auf dem Laufwerk aufgrund der Client-Aktivität.	Ganzzahl

Weitere Informationen

GetDriveStats

Fehler

Das Fehlerobjekt enthält einen Fehlercode und eine Meldung, wenn während eines Methodenaufrufs ein Fehler auftritt. Alle vom System erzeugten Fehler haben einen Fehlercode von 500.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Codieren	Der numerische Code, der zur Identifizierung des Fehlers verwendet wird. Alle vom System erzeugten Fehler geben einen Code von 500 zurück.	Ganzzahl
Name	Die eindeutige Kennung für den Fehler, der aufgetreten ist. Jede Methode gibt einen dokumentierten Satz von Fehlern zurück, obwohl Sie bereit sein sollten, nicht erkannte Fehler zu behandeln.	Zeichenfolge
Nachricht	Eine Beschreibung des Fehlers, ggf. mit weiteren Details.	Zeichenfolge

Ereignis

Das Event-Objekt enthält Details zu Ereignissen, die während eines API-Methodenaufrufs oder während des Systemvorgangs auftreten.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Details	Zusätzliche Informationen über das Ereignis.	JSON-Objekt
DriveID	Die DriveID des Laufwerks meldet den Fehler. 0, falls nicht zutreffend.	Ganzzahl
Fahrausweise	Eine Liste der Einfahrungs-IDs der Laufwerke, die den Fehler melden. Eine leere Liste, falls nicht zutreffend.	Integer-Array
EventID	Eindeutige ID, die jedem Ereignis zugeordnet ist.	Ganzzahl
EventInfoType	Die Art des Fehlers.	Zeichenfolge
Nachricht	Eine Zeichenfolge, die das Ereignis beschreibt, das aufgetreten ist.	Zeichenfolge
NodeID	Die Knoten-ID des Node, der den Fehler meldet. 0, falls nicht zutreffend.	Ganzzahl
Service-ID	Die Dienstkennung des Dienstes meldet den Fehler. 0, falls nicht zutreffend.	Ganzzahl
Schweregrad	Schweregrad: Das Ereignis meldet.	Ganzzahl
ZeitOfVeröffentlichen	Die Zeit, zu der das Ereignisprotokoll des Clusters das Ereignis empfangen hat, im UTC+0-Format.	ISO 8601-Datumszeichenfolge
UhrzeitBericht	Die Zeit, zu der das Ereignis im Cluster aufgetreten ist, im UTC+0-Format.	ISO 8601-Datumszeichenfolge

Hinweis: Es kann einen leichten Unterschied zwischen ZeitOfReport und ZeitOfPublish geben, wenn das Ereignis eingetreten ist und nicht sofort veröffentlicht werden konnte.

Ereignistypen

In der folgenden Liste werden die möglichen Ereignistypen beschrieben, die das EventInfoType-Mitglied enthalten kann:

- ApiEvent: Ereignisse, die über die API oder die Web-Benutzeroberfläche initiiert werden, um die Einstellungen zu ändern.
- BinAssignmentsEreignis: Ereignisse im Zusammenhang mit der Zuordnung von Daten zu internen Containern.
- BinSyncEvent: Ereignisse im Zusammenhang mit der Neuverteilung von Daten zwischen Blockdiensten.
- BsCheckEvent: Ereignisse im Zusammenhang mit Blockprüfungen.
- BsKillEvent: Ereignisse im Zusammenhang mit Blockabschlussstellen.
- BulkOpEvent: Ereignisse, die auf einem gesamten Volume ausgeführt werden, wie z. B. Volume-Backups, Restores, Snapshots oder Klone.
- KlonEvent: Ereignisse im Zusammenhang mit dem Klonen von Volumes
- ClusterMasterEvent: Änderungsereignisse bei der Cluster-Konfiguration, z. B. beim Hinzufügen oder Entfernen von Nodes
- Data Event: Ereignisse zum Lesen und Schreiben von Daten.
- DbEvent: Veranstaltungen im Zusammenhang mit der Ensemble-Knoten-Datenbank.
- Drive Event: Ereignisse im Zusammenhang mit dem Laufwerkbetrieb.
- VerschlüsselungAtRestEvent: Ereignisse im Zusammenhang mit der gespeicherten Datenverschlüsselung.
- EnsembleEvent: Veranstaltungen im Zusammenhang mit Ensemble Größe zu erhöhen oder verringern.
- Fiber ChannelEvent: Ereignisse im Zusammenhang mit Fibre Channel Node-Konfiguration oder -Verbindungen.
- GcEvent: Veranstaltungen im Zusammenhang mit der Müllsammlung. Diese Prozesse laufen alle 60 Minuten, um Storage auf Blocklaufwerken wieder nutzbar zu machen.
- IeEvent: Ereignisse im Zusammenhang mit internen Systemfehlern.
- Installationsereignis: Evnts bezieht sich auf automatische Softwareinstallation auf ausstehenden Speicherknoten.
- ISCSIEvent: Ereignisse im Zusammenhang mit iSCSI-Verbindungs- oder Konfigurationsproblemen.
- LimitEvent: Ereignisse im Zusammenhang mit der Anzahl von Volumes oder virtuellen Volumes in einem Konto oder im Cluster, die sich dem maximal zulässigen Wert nähern.
- NetworkEvent: Ereignisse im Zusammenhang mit virtuellen Netzwerken.
- PlattformHardware Event: Veranstaltungen im Zusammenhang mit Problemen auf Hardware-Geräten erkannt.
- RemoteClusterEvent: Ereignisse im Zusammenhang mit der Remote-Cluster-Kopplung.
- SchedulerEvent: Ereignisse im Zusammenhang mit geplanten Snapshots.
- ServiceEvent: Ereignisse im Zusammenhang mit dem Systemstatus.
- StatEvent: Ereignisse im Zusammenhang mit Systemstatistiken.
- SliceEvent: Ereignisse im Zusammenhang mit Metadaten-Speicher.

- SnmpTrapEvent: Ereignisse im Zusammenhang mit SNMP-Traps.
- TsEvent: System Transport Service Ereignisse.
- UnexpectedException: Ereignisse im Zusammenhang mit unerwarteten Fehlern.
- VasaProviderEvent: Veranstaltungen zu einem VMware VASA Provider.

Weitere Informationen

ListEvents

Fehler

Das Fehlerobjekt enthält Informationen über Fehler, die im Cluster erkannt werden. Der `ListClusterFaults` Die Methode gibt Cluster-Fehlerinformationen zurück.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
BlocksUpgrade	Der Fehler blockiert ein Upgrade. Mögliche Werte: • Wahr: Der Fehler blockiert ein Upgrade. • False: Der Fehler blockiert kein Upgrade.	boolesch
ClusterFaultID	Die eindeutige ID, die jedem Cluster-Fehler zugeordnet ist.	Ganzzahl
Codieren	Der Fehlercode für den bestimmten Fehler, der erkannt wurde. Weitere Informationen finden Sie unter Cluster-Fehlercodes.	Zeichenfolge
Daten	Zusätzliche, Fehler-spezifische Informationen.	JSON-Objekt
Datum	Die aktuelle Zeit im UTC+0-Format.	ISO 8601-Zeichenfolge
Details	Beschreibung der Störung mit weiteren Details.	Zeichenfolge

Name	Beschreibung	Typ
DriveID	Die erste Laufwerk-ID in der Liste der Einfahrten. Wenn die Liste der driveID leer ist (d. h. keine Fehler zurückgegeben wurden, die für Laufwerke erforderlich sind), ist dieser Wert 0.	Ganzzahl
Fahrausweise	Eine Liste der DriveID-Werte für die Laufwerke, auf die sich dieser Fehler bezieht. Bei Fehlern, die sich mit Laufwerken befassen, enthalten. Wenn keine, ist dies ein leeres Array.	Integer-Array
NodeHardwareFaultID	Die Kennung, die einem Hardwarefehler im Cluster zugewiesen ist.	Ganzzahl
NodeID	Die Node-ID für den Node, auf den sich dieser Fehler bezieht. Bei Node- und Laufwerksfehlern enthalten; andernfalls auf 0 gesetzt.	Ganzzahl
Behoben	Der aufgelöste Status des Fehlers. Mögliche Werte: • True: Der Fehler wird nicht mehr erkannt. • Falsch: Der Fehler ist immer noch vorhanden.	boolesch
ResolvedDate	Datum und Uhrzeit, zu der der Fehler behoben wurde.	ISO 8601-Zeichenfolge
Service-ID	Der Dienst, der dem Fehler zugeordnet ist. Dieser Wert ist „0“ (Null), wenn der Fehler nicht einem Dienst zugeordnet ist.	Ganzzahl

Name	Beschreibung	Typ
Schweregrad	Der Schweregrad des Fehlers. Mögliche Werte: • Warnung: Ein kleines Problem. Das Cluster funktioniert und Upgrades sind auf dieser Schweregrade zulässig. • Fehler: Ein Ausfall, der den Service im Allgemeinen nicht beeinträchtigen sollte (außer möglicher Performance-Abfall oder HA-Verlust). Einige Funktionen sind möglicherweise deaktiviert. • Kritisch: Ein schwerwiegender Fehler, der den Dienst beeinträchtigt. Das System kann keine API-Anfragen oder Client-I/O bedienen und besteht ein Datenverlustrisiko. • BestPractice: Fehler, die durch eine suboptimale Systemkonfiguration ausgelöst werden.	Zeichenfolge
Typ	Die Art des Fehlers. Mögliche Werte: • Node: Ein Fehler, der einen ganzen Node betrifft. • Antrieb: Ein Fehler, der einen einzelnen Antrieb betrifft. • Cluster: Ein Fehler, der das gesamte Cluster betrifft. • Service: Ein Fehler, der einen Dienst auf dem Cluster betrifft. • Volumen: Ein Fehler, der ein individuelles Volumen beeinflusst.	Zeichenfolge

Weitere Informationen

- ListenClusterstandards
- "Cluster-Fehlercodes"

Fibre Channel-Port

Das Objekt Fibre ChannelPort enthält Informationen über einzelne Ports auf einem Knoten oder für einen ganzen Knoten im Cluster. Sie können diese Informationen mithilfe von abrufen `ListNodeFibreChannelPortInfo` Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Firmware	Die Version der auf dem Fibre Channel-Port installierten Firmware.	Ganzzahl
HbaPort	Die ID des einzelnen HBA-Ports (Host Bus Adapter).	Ganzzahl
Modell	Modell des HBA am Port.	Zeichenfolge
NPortID	Die eindeutige Port-Node-ID.	Zeichenfolge
PciSlot	Der Steckplatz, der die PCI-Karte im Fibre Channel-Node-Chassis enthält.	Ganzzahl
Seriell	Die Seriennummer am Fibre Channel-Port.	Zeichenfolge
Schnell	Die Geschwindigkeit des HBA am Port.	Zeichenfolge

Name	Beschreibung	Typ
Bundesland	Mögliche Werte: • Unbekannt • NotPresent • Online • Offline • Blockiert • Umgangen • Diagnose • Linkdown • Fehler • Loopback • Gelöscht	Zeichenfolge
SwitchWwn	Der World Wide Name des Fibre Channel Switch Ports.	Zeichenfolge
wwnn	Der World Wide Node Name des HBA Node.	Zeichenfolge
wwpn	Der dem physischen Port des HBA zugewiesene World Wide Port Name.	Zeichenfolge

Weitere Informationen

ListNodeFiberChannelPortInfo

FipsErrorNodeReport

Das Objekt fipsErrorNodeReport enthält Fehlerinformationen für jeden Knoten, der nicht mit Informationen zur Unterstützung von FIPS 140-2 antwortet, wenn Sie ihn mit dem abfragen `GetFipsReport` Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
NodeID	Die ID des Node, der nicht antwortet.	Ganzzahl

Name	Beschreibung	Typ
Fehler	Ein JSON-Objekt mit Fehlerinformationen.	JSON-Objekt

FipsNodeReport

Das Objekt fipsNodeReport enthält Informationen zur Unterstützung von FIPS 140-2 für einen einzelnen Node im Storage-Cluster. Sie können diese Informationen mithilfe von abrufen `GetFipsReport` Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
NodeID	Die ID des Node, der die Informationen meldet.	Ganzzahl
FipsDrives	Gibt an, ob die FIPS 140-2-2-Laufwerkverschlüsselung für diesen Node aktiviert ist. Mögliche Werte: • Keine: Dieser Node ist nicht zur Verschlüsselung von FIPS-Laufwerken fähig. • Partiell: Node ist FIPS-Laufwerksverschlüsselung möglich, aber nicht alle vorhandenen Laufwerke sind FIPS-fähige Laufwerke. • Bereit: Node ist für FIPS-Laufwerksverschlüsselung geeignet. Dabei handelt es sich entweder um FIPS-fähige Laufwerke oder es sind keine Laufwerke vorhanden.	FipsDrivesStatusTyp
HttpsEnabled	Gibt an, ob die HTTPS-Verschlüsselung nach FIPS 140-2 für diesen Node aktiviert ist oder nicht. Mögliche Werte: • Wahr: Aktiviert • False: Deaktiviert	boolesch

FipsReport

Das Objekt fipsReport enthält Informationen zur Unterstützung von FIPS 140-2 für alle Nodes im Storage-Cluster. Sie können diese Informationen mithilfe von abrufen `GetFipsReport` Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Knoten	Ein Bericht über den Supportstatus von FIPS 140-2 für jeden Node im Storage-Cluster.	FipsNodeReport
FehlerKnoten	Fehlerinformationen für jeden Node, der nicht mit FIPS 140-2-2-Supportstatus reagiert.	FipsErrorNodeReport

GroupSnapshot

Das GroupSnapshot-Objekt enthält Informationen über einen Snapshot für eine Volume-Gruppe. Sie können das verwenden `ListGroupSnapshots` API-Methode zum Abrufen von Snapshot Informationen über Gruppen.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt
CreateTime	Der UTC+0 formatierte Tag und Uhrzeit, zu der der GruppenSnapshot erstellt wurde.	ISO 8601-Datumszeichenfolge
EnableRemoteReplication	Gibt an, ob der Snapshot für die Remote-Replikation aktiviert ist.	boolesch
GruppenSnapshotID	Die eindeutige ID des Gruppen-Snapshot.	Ganzzahl
GruppenSnapshotUUID	Die UUID des Gruppen-Snapshots.	Zeichenfolge

Name	Beschreibung	Typ
Mitglieder	Ein Array von Objekten, die Informationen zu jedem Mitglied des Gruppen-Snapshots enthalten.	snapshot Array erledigen
Name	Der Name des Gruppen-Snapshot oder, wenn keine angegeben wurde, der UTC-formatierte Tag und die Zeit, zu der der Snapshot erstellt wurde.	Zeichenfolge oder ISO 8601-Datumszeichenfolge
EntferntStatus	Ein Array, das den universellen Identifikator und den Replikationsstatus jedes Remote-Snapshots auf dem Zielcluster enthält, wie vom Quellcluster aus gesehen.	EntfernteClusterSnapshotStatus Array erledigen
Status	Aktueller Status des Snapshots. Mögliche Werte: • Unbekannt: Beim Abrufen des Status des Snapshots ist ein Fehler aufgetreten. • Vorbereiten: Dieser Snapshot wird gerade zur Verwendung vorbereitet und ist noch nicht beschreibbar. • RemoteSyncing: Dieser Snapshot wird von einem Remote-Cluster repliziert. • Fertig: Die Vorbereitung oder Replikation dieses Snapshots ist abgeschlossen und kann nun verwendet werden. • Aktiv: Dieser Snapshot ist der aktive Branch. • Klonen: Dieser Snapshot ist an einem KopierVolume-Vorgang beteiligt.	Zeichenfolge

Weitere Informationen

ListenSnapshots

HardwareInfo

Das HardwareInfo-Objekt enthält detaillierte Informationen zur Hardware und zum Status

jedes Node im Cluster. Sie können diese Informationen mit dem abrufen `GetHardwareInfo` API-Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
BoardSerial	Die Seriennummer der DMI-Platine.	Zeichenfolge
Bus	Informationen zum Hauptplatinen-Medienbus	JSON-Objekt
Chassisseriell	Die Seriennummer des Chassis.	Zeichenfolge
Fahrhardware	Eine Liste mit Informationen für jedes Laufwerk im Node.	JSON-Objekt-Array
Fibre Channel-Ports	Eine Liste der Fibre Channel-Ports auf dem Node.	Integer-Array
HardwareKonfig	Informationen zur Konfiguration der Peripheriegeräte der Hauptplatine	JSON-Objekt
KernelCrashDumpState	Die Crash Dump-Konfiguration des Betriebssystemkernels.	Zeichenfolge
Speicher	Hardware-Informationen zu Firmware und Systemspeicher.	JSON-Objekt
Netzwerk	Beschreibung der Hardware aller Netzwerkschnittstellen des Node.	JSON-Objekt
Netzwerkschnittstellen	Der Status der Netzwerkschnittstellen des Node.	JSON-Objekt
Knotenablagefach	Bei HCI-Plattformen lautet der Buchstabe „A“, „B“, „C“ oder „D“) für den Chassis-Steckplatz, in dem dieser Node befindet. Bei Storage-Plattformen ist dieser Wert Null.	Zeichenfolge
nvram	NVRAM-Statistiken für den Node.	JSON-Objekt
Ursprung	Der Anbieter der Hauptplatine.	Zeichenfolge

Name	Beschreibung	Typ
Plattform	Eine Beschreibung der Chassis-Plattform.	JSON-Objekt
Seriell	Die Seriennummer des Produkts.	Zeichenfolge
Storage	Informationen für Storage Controller.	JSON-Objekt
SystemMemory	Speichernutzung und Leistungsinformationen des Betriebssystems	JSON-Objekt
System	Der Typ des Node-Chassis.	JSON-Objekt
uuid	Die eindeutige ID des Node.	UUID

Weitere Informationen

GetHardwareInfo

Host (virtuelle Volumes)

Das Hostobjekt enthält Informationen über einen Host virtueller Volumes. Sie können das verwenden `ListVirtualVolumeHosts` Die Methode, um diese Informationen für alle Hosts des virtuellen Volumes zu erhalten.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Bindungen	Eine Liste von Objekten, die die Bindungen für den Host des virtuellen Volumes beschreiben.	Integer-Array
Cluster-ID	Die eindeutige ID des Clusters, mit dem dieser Host verknüpft ist.	UUID
HostAddress	Die IP-Adresse oder der DNS-Name des virtuellen Volume-Hosts.	Zeichenfolge
InitiatorNames	Eine Liste der Initiator-IQNs für den Host des virtuellen Volumes.	String-Array

Name	Beschreibung	Typ
VirtualVolumeHost ID	Die eindeutige ID dieses virtuellen Volume-Hosts.	UUID
VisibleProtocolEndpointIDs	Eine Liste der IDs von Protokollendpunkten, die auf diesem Host sichtbar sind.	UUID-Array

Weitere Informationen

ListVirtualVolumeHosts

IdpConfigInfo

Das idpConfigInfo-Objekt enthält Konfigurations- und Integrationsdetails für einen Identitätsanbieter (IdP) eines Drittanbieters.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Aktiviert	Gibt an, ob diese IdPkonfiguration eines Drittanbieters aktiviert ist.	boolesch
IdpKonfigurationID	UUID für die IdP-Konfiguration eines Drittanbieters.	UUID
IdpMetadaten	Metadaten für Konfigurations- und Integrationsdetails für SAML 2.0 Single Sign-On.	Zeichenfolge
IdpName	Name für das Abrufen des IdP-Providers für SAML 2.0 Single Sign-On.	Zeichenfolge
DiensteProviderzertifikat	Ein PEM-Format Base64-codiertes PKCS#10 X.509-Zertifikat zur Kommunikation mit diesem IdP.	Zeichenfolge
SpMetadataUrl	URL zum Abrufen von SP-Metadaten aus dem Cluster für die Erstellung einer Vertrauensbeziehung an das IdP.	Zeichenfolge

Initiator

Das Initiatorobjekt enthält Informationen über einen iSCSI- oder Fibre Channel-Initiator. Ein Initiator-Objekt kann IQN- oder WWPN-IDs enthalten. Sie können das verwenden `ListInitiators` Methode zum Abrufen einer Liste aller Initiatoren, die im System bekannt sind Sie verwenden Initiator-Objekte, um den Zugriff von SCSI-Initiatoren auf eine Reihe von Volumes über die Zugriffsgruppen für Volumes zu konfigurieren. Ein Initiator kann nur Mitglied einer Volume-Zugriffsgruppe gleichzeitig sein. Sie können den Initiator-Zugriff auf ein oder mehrere VLANs beschränken, indem Sie mithilfe des eine oder mehrere VirtualNetworkIDs angeben `CreateInitiators` Und `ModifyInitiators` Methoden Falls Sie keine virtuellen Netzwerke angeben, kann der Initiator auf alle Netzwerke zugreifen.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Alias	Falls vorhanden, der dem Initiator zugewiesene freundliche Name.	Zeichenfolge
Merkmale	Ein Satz von JSON-Attributen, die diesem Initiator zugewiesen sind. Leer, wenn keine Attribute zugewiesen sind.	JSON-Objekt
ChapUsername	Der eindeutige CHAP-Benutzername für diesen Initiator.	Zeichenfolge
InitiatorID	Die numerische Kennung für den Initiator.	Ganzzahl
Name des Initiators	Der Initiatorname im IQN- oder WWPN-Format.	Zeichenfolge
InitiatorSecret	Der CHAP-Schlüssel, der zur Authentifizierung des Initiators verwendet wird.	Zeichenfolge
Anforderungen	True, wenn CHAP für diesen Initiator erforderlich ist.	boolesch
TargetSecret	CHAP-Schlüssel zur Authentifizierung des Ziels (bei Verwendung der gegenseitigen CHAP-Authentifizierung).	Zeichenfolge

Name	Beschreibung	Typ
VirtualNetworkIDs	Liste der dem Initiator zugeordneten virtuellen Netzwerk-IDs. Wenn eine oder mehrere definiert sind, kann sich dieser Initiator nur bei den angegebenen virtuellen Netzwerken anmelden. Wenn keine virtuellen Netzwerke definiert sind, kann sich dieser Initiator in allen Netzwerken anmelden.	Ganzzahl
VolumeAccessGroups	Eine Liste der Volume-Zugriffsgruppen-IDs, zu denen dieser Initiator gehört.	Integer-Array

Weitere Informationen

ListenInitiatoren

ISCSIAuthentifizierung

Das iSCSI-Authentifizierungsobjekt enthält Authentifizierungsinformationen über eine ISCSI-Sitzung.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
AuthMethod	Die Authentifizierungsmethode, die bei der iSCSI-Anmeldung verwendet wird, z. B. CHAP oder None.	Zeichenfolge
Chapalgorithm	Der verwendete CHAP-Algorithmus, z. B. MD5, SHA1*, SHA-256*, Oder SHA3-256*	Zeichenfolge
ChapUsername	Der vom Initiator während einer iSCSI-Sitzungsanmeldung angegebene CHAP-Benutzername.	Zeichenfolge
Richtung	Die Authentifizierungsrichtung z. B. one-way (nur Initiator) oder Two-Way (Initiator und Ziel).	Zeichenfolge

- Verfügbar ab Element 12.7.

KeProviderKmip

Das keProviderKmip-Objekt beschreibt einen KMIP-Schlüsselanbieter (Key Management Interoperability Protocol). Ein Schlüsselanbieter ist sowohl ein Mechanismus als auch ein Speicherort zum Abrufen von Authentifizierungsschlüsseln für Cluster-Funktionen wie Verschlüsselung im Ruhezustand.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
ID von Schlüsselausweisungs-ID	Die ID des KMIP-Schlüsselanbieters. Dies ist ein eindeutiger Wert, der vom Cluster während der Erstellung des Schlüsselanbieters zugewiesen wird und der nicht geändert werden kann.	Ganzzahl
SchlüsselProviderIActive	Trifft zu, wenn der KMIP-Schlüsselanbieter aktiv ist. Ein Anbieter gilt als aktiv, wenn ausstehende Schlüssel vorhanden sind, die erstellt, aber noch nicht gelöscht wurden und daher als noch in Gebrauch gehalten werden.	boolesch
SchlüsselProvidername	Der Name des KMIP-Schlüsselanbieters.	Zeichenfolge
KeyServerIDs	Eine Schlüssel-Server-ID, die diesem Anbieter zugeordnet ist. Der Server muss hinzugefügt werden, bevor dieser Provider aktiv werden kann. Der Server kann nicht entfernt werden, während dieser Provider aktiv ist. Für jeden Provider wird nur eine Server-ID unterstützt.	Integer-Array
KmCapabilities	Den Funktionsumfang dieses KMIP-Anbieters einschließlich Details zur zugrunde liegenden Bibliothek, FIPS-Compliance, SSL-Provider usw.	Zeichenfolge

KeyServerkmip

Das keyServerkmip-Objekt beschreibt einen KMIP-Schlüsselserver (Key Management Interoperability Protocol). Dieser ist ein Speicherort zum Abrufen von Authentifizierungsschlüsseln für Cluster-Funktionen wie Encryption at Rest.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
ID von Schlüsselausweisungs-ID	Wenn dieser KMIP-Schlüsselserver einem Provider zugewiesen ist, enthält dieses Mitglied die ID des KMIP-Schlüsselanbieters, dem er zugewiesen ist. Andernfalls ist dieses Mitglied Null.	Ganzzahl
KeyServer-ID	Die ID des KMIP-Schlüsselservers. Dies ist ein eindeutiger Wert, der dem Cluster während der Erstellung eines Schlüsselservers zugewiesen wird. Dieser Wert kann nicht geändert werden.	Ganzzahl
KmipAssigneedProviderIActive	Wenn dieser KMIP-Schlüsselserver einem Provider zugewiesen ist (keyProviderID ist nicht Null), gibt dieses Mitglied an, ob dieser Provider aktiv ist (die Schlüssel angeben, die derzeit verwendet werden). Andernfalls ist dieses Mitglied Null.	boolesch
KmipCaCertificate	Das öffentliche Schlüsselzertifikat der Stammzertifizierungsstelle des externen Schlüsselservers. Mit dieser Funktion wird das vom externen Schlüsselserver in der TLS-Kommunikation präsentierte Zertifikat überprüft. Bei Schlüsselserverclustern, in denen einzelne Server unterschiedliche CAS verwenden, enthält dieses Mitglied eine verkettete Zeichenfolge der Stammzertifikate aller CAS.	Zeichenfolge

Name	Beschreibung	Typ
KmipClientZertifikat	Ein PEM-Format Base64-codiertes PKCS#10 X.509-Zertifikat, das vom Element Storage KMIP-Client verwendet wird.	Zeichenfolge
KmipKeyServerHostnames	Die diesem KMIP-Schlüsselserver zugeordneten Hostnamen oder IP-Adressen.	String-Array
KmipKeyServerName	Der Name des KMIP-Schlüsselservers. Dieser Name wird nur für Anzeigezwecke verwendet und muss nicht eindeutig sein.	Zeichenfolge
KmipKeyServerPort	Die diesem KMIP-Schlüsselserver zugeordnete Port-Nummer (in der Regel 5696).	Ganzzahl

LdapKonfiguration

Das ldapConfiguration-Objekt enthält Informationen zur LDAP-Konfiguration auf dem Speichersystem. Sie können LDAP-Informationen mit abrufen `GetLdapConfiguration` API-Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
AuthType	Gibt an, welche Benutzerauthentifizierungsmethode verwendet werden soll. Mögliche Werte: • DirectBind • SucheAndBind	Zeichenfolge
Aktiviert	Gibt an, ob das System für LDAP konfiguriert ist oder nicht. Mögliche Werte: • Richtig • Falsch	boolesch

Name	Beschreibung	Typ
GroupSearchBaseDN	Der Basis-DN des Baums, um die Gruppensuche zu starten (das System führt von hier aus eine Unterbaumsuche durch).	Zeichenfolge
GroupSearchCustomFilter	Der verwendete benutzerdefinierte Suchfilter.	Zeichenfolge
GroupSearchType	Steuert den verwendeten Standardfilter für die Gruppensuche. Mögliche Werte: • NoGroups: Keine Gruppenunterstützung. • ActiveDirectory: Verschachtelte Mitgliedschaft aller AD-Gruppen eines Benutzers. • MemberDN: MemberDN-Stilgruppen (Einzelebene).	Zeichenfolge
SuchhinBindDN	Ein vollständig qualifizierter DN zur Anmeldung bei, um eine LDAP-Suche für den Benutzer durchzuführen (Lesezugriff auf das LDAP-Verzeichnis erforderlich).	Zeichenfolge
Server-URIs	Eine kommagetrennte Liste von LDAP-Server-URIs (z. B. `ldap://1.2.3.4` Und `ldaps://1.2.3.4:123`.)	Zeichenfolge
BenutzerDNTemplatte	Eine Zeichenfolge, die zur Bildung eines vollständig qualifizierten Benutzer-DN verwendet wird.	Zeichenfolge
BenutzerSuchbaseDN	Der Basis-DN des Baums, der zur Suche verwendet wird (führt von hier aus eine Unterbaumsuche durch).	Zeichenfolge
BenutzerSuchfilter	Der verwendete LDAP-Filter.	Zeichenfolge

Weitere Informationen

GetLdapConfiguration

LoggingServer

Das loggingServer-Objekt speichert Informationen über die für den Speichercluster konfigurierten Protokollierungshosts. Verwenden `GetRemoteLoggingHosts` um die aktuellen Protokollierungshosts anzuzeigen und dann zu verwenden `SetRemoteLoggingHosts` um die gewünschte Liste aktueller und neuer Logging-Hosts festzulegen.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Host	FQDN oder IP-Adresse des Protokollservers	Zeichenfolge
Port	Portnummer, die zur Kommunikation mit dem Protokollserver verwendet wird	Ganzzahl

Verwandte Informationen

- "GetRemoteLoggingHosts"
- "SetRemoteLoggingHosts"

Netzwerk (verbundene Schnittstellen)

Das Netzwerk-Objekt (verbundene Schnittstellen) enthält Konfigurationsinformationen für verbundene Netzwerkschnittstellen auf einem Speicherknoten. Sie können das verwenden `GetConfig` Und `GetNetworkConfig` Methoden zum Abrufen dieser Informationen für einen Storage-Node

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Adresse	Die IPv4-Adresse, die dieser Schnittstelle auf dem Node zugewiesen ist.	Zeichenfolge
AdresseV6	Die der Bond1G-Schnittstelle auf dem Node zugewiesene IPv6-Managementadresse.	Zeichenfolge

Bond-Downdelay	Wartezeit in Millisekunden, bevor ein Slave deaktiviert wird, nachdem ein Verbindungsfehler erkannt wurde.	Zeichenfolge
Bond-Failover_over_mac	Die Konfiguration der MAC-Adresse der Netzwerkschnittstelle.	Zeichenfolge
Bond-miimon	Die Frequenz in Millisekunden, bei der der MII-Verbindungsstatus auf Verbindungsfehler überprüft wird.	Zeichenfolge
Bond-Modus	Der Verbindungsmodus. Mögliche Werte: • ActivePassive (Standard) • ALB • LACP (empfohlen)	Zeichenfolge
Bond-primary_Reselect	Gibt an, wann der primäre Bond-Slave als aktiver Slave ausgewählt wurde. Mögliche Werte: • Immer • Besser • Ausfall	Zeichenfolge
Bond-Slaves	Die Liste der Slave-Schnittstellen für die Verbindung.	Zeichenfolge
Bond-lacp_Rate	Wenn der Bond-Modus LACP ist, kann sich die Rate in eine der folgenden Werte ändern: • LACP schnell (Standard) • LACP langsam	Zeichenfolge
Bond-Updelay	Die Zeit, die in Millisekunden vor der Aktivierung eines Slaves gewartet wird, nachdem eine Verbindung erkannt wurde.	Zeichenfolge
dns-Nameserver	Eine Liste der für Domänennamendienste verwendeten Adressen, die durch Komma oder Leerzeichen getrennt sind.	Zeichenfolge

dns-Suche	Ein Leerzeichen oder eine kommagetrennte Liste von DNS-Suchdomänen.	Zeichenfolge
Familie	Adressfamilie, die für die Schnittstelle konfiguriert ist. Derzeit wird "inet" für IPv4 unterstützt.	Zeichenfolge
Gateway	Die IPv4-Router-Netzwerkadresse, die für das Senden von Datenverkehr aus dem lokalen Netzwerk verwendet wird.	Zeichenfolge
GatewayV6	Die IPv6-Router-Netzwerkadresse, die für das Senden von Datenverkehr aus dem lokalen Bond1G-Netzwerk verwendet wird.	Zeichenfolge
IpV6PrefixLength	Die Subnetz-Präfixlänge für statische Routen vom Typ „net“ für IPv6-Verkehr im Bond1G-Netzwerk.	Zeichenfolge
MacAddress	Die tatsächliche MAC-Adresse, die der Schnittstelle zugewiesen und vom Netzwerk beobachtet wird.	Zeichenfolge
MacAdressePermanent	Die vom Hersteller der Schnittstelle zugewiesene unveränderliche MAC-Adresse.	Zeichenfolge
Methode	Die Methode zum Konfigurieren der Schnittstelle. Mögliche Werte: • Loopback: Wird verwendet, um die IPv4-Loopback-Schnittstelle zu definieren. • Manuell: Zur Definition von Schnittstellen, die nicht automatisch konfiguriert werden. • dhcp: Kann verwendet werden, um eine IP-Adresse über DHCP zu erhalten. • Statisch: Zur Definition von Ethernet-Schnittstellen mit statisch zugewiesenen IPv4-Adressen.	Zeichenfolge

mtu	Die größte Paketgröße (in Byte), die die Schnittstelle übertragen kann. Muss größer oder gleich 1500 sein. Bis zu 9000 wird unterstützt.	Zeichenfolge
Netzmaske	Die Bitmaske, die das Subnetz für die Schnittstelle angibt.	Zeichenfolge
Netzwerk	Gibt an, wo der IP-Adressbereich basierend auf der Netzmaske beginnt.	Zeichenfolge
Routen	Kommagetrenntes Array von Routen-Strings, die auf die Routing-Tabelle angewendet werden sollen.	String-Array
Status	Der Status der Schnittstelle. Mögliche Werte: • Down: Die Schnittstelle ist inaktiv. • Up: Die Schnittstelle ist bereit, hat aber keine Verbindung. • UpAndRunning: Die Schnittstelle ist bereit und ein Link ist aufgebaut.	Zeichenfolge
SymmetricRouteRules	Die auf dem Knoten konfigurierten symmetrischen Routingregeln.	String-Array
UpAndRunning	Zeigt an, ob die Schnittstelle bereit ist und über eine Verknüpfung verfügt.	boolesch
VirtualNetworkTag	Die virtuelle Netzwerkidentifikation der Schnittstelle (VLAN-Tag).	Zeichenfolge

Mitgliedänderbarkeit und Knotenstatus

In dieser Tabelle wird angegeben, ob die Objektparameter für jeden möglichen Node-Status geändert werden können.

Mitgliedsname	Verfügbarer Status	Status „ausstehend“	Aktiver Status
Adresse	Ja.	Ja.	Nein

AdresseV6	Ja.	Ja.	Nein
Bond-Downdelay	Wird vom System konfiguriert	1. A.	1. A.
Bond-Failover_over_mac	Wird vom System konfiguriert	1. A.	1. A.
Bond-miimon	Wird vom System konfiguriert	1. A.	1. A.
Bond-Modus	Ja.	Ja.	Ja.
Bond-primary_Reselect	Wird vom System konfiguriert	1. A.	1. A.
Bond-Slaves	Wird vom System konfiguriert	1. A.	1. A.
Bond-lacp_Rate	Ja.	Ja.	Ja.
Bond-Updelay	Wird vom System konfiguriert	1. A.	1. A.
dns-Nameserver	Ja.	Ja.	Ja.
dns-Suche	Ja.	Ja.	Ja.
Familie	Nein	Nein	Nein
Gateway	Ja.	Ja.	Ja.
GatewayV6	Ja.	Ja.	Ja.
IpV6PrefixLength	Ja.	Ja.	Ja.
MacAddress	Wird vom System konfiguriert	1. A.	1. A.
MacAdressePermanent	Wird vom System konfiguriert	1. A.	1. A.
Methode	Nein	Nein	Nein
mtu	Ja.	Ja.	Ja.

Netzmaske	Ja.	Ja.	Ja.
Netzwerk	Nein	Nein	Nein
Routen	Ja.	Ja.	Ja.
Status	Ja.	Ja.	Ja.
SymmetricRouteRules	Wird vom System konfiguriert	1. A.	1. A.
UpAndRunning	Wird vom System konfiguriert	1. A.	1. A.
VirtualNetworkTag	Ja.	Ja.	Ja.

Weitere Informationen

- Getconfig
- GetNetworkConfig

Netzwerk (alle Schnittstellen)

Das Netzwerk-Objekt (alle Schnittstellen) sammelt Informationen über die Konfiguration der Netzwerkschnittstelle für einen Storage-Node. Sie können das verwenden `GetConfig` Und `GetNetworkConfig` Methoden zum Abrufen dieser Informationen für einen Storage-Node

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Bond10G	Konfigurationsinformationen für die Bond10G Bond10G Schnittstelle.	Netzwerk (verbundene Schnittstellen)
Bond1G	Konfigurationsinformationen für die Bond1G Bond1G Schnittstelle.	Netzwerk (verbundene Schnittstellen)

Eth0-5	Ein Objekt für jede Ethernet-Schnittstelle im Storage Node, das Konfigurationsinformationen für die Schnittstelle beschreibt. Diese Objekte werden mit der Nummer 0 bis 5 nummeriert, um dem Schnittstellennamen zu entsprechen.	Netzwerk (Ethernet-Schnittstellen)
lo	Konfigurationsinformationen für die Loopback-Schnittstelle.	Netzwerk (lokale Schnittstellen)

Weitere Informationen

- Getconfig
- GetNetworkConfig

Netzwerk (Ethernet-Schnittstellen)

Das Netzwerk-Objekt (Ethernet-Schnittstellen) enthält Konfigurationsinformationen für einzelne Ethernet-Schnittstellen. Sie können das verwenden `GetConfig` Und `GetNetworkConfig` Methoden zum Abrufen dieser Informationen für einen Storage-Node

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Bond-Master	Gibt an, welche gebundene Schnittstelle diese physische Schnittstelle als Bond-Slave verbunden ist.	Zeichenfolge
Familie	Adressfamilie, die für die Schnittstelle konfiguriert ist. Derzeit wird "inet" für IPv4 unterstützt.	Zeichenfolge
MacAddress	Die tatsächliche MAC-Adresse, die der Schnittstelle zugewiesen und vom Netzwerk beobachtet wird.	Zeichenfolge
MacAdressePermanent	Die vom Hersteller der Schnittstelle zugewiesene unveränderliche MAC-Adresse.	Zeichenfolge

Methode	Die Methode zum Konfigurieren der Schnittstelle. Mögliche Werte: • Loopback: Wird verwendet, um die IPv4-Loopback-Schnittstelle zu definieren. • Manuell: Zur Definition von Schnittstellen, die nicht automatisch konfiguriert werden. • dhcp: Kann verwendet werden, um eine IP-Adresse über DHCP zu erhalten. • Statisch: Zur Definition von Ethernet-Schnittstellen mit statisch zugewiesenen IPv4-Adressen.	Zeichenfolge
Status	Der Status der Schnittstelle. Mögliche Werte: • Down: Die Schnittstelle ist inaktiv. • Up: Die Schnittstelle ist bereit, hat aber keine Verbindung. • UpAndRunning: Die Schnittstelle ist bereit und ein Link ist aufgebaut.	Zeichenfolge
UpAndRunning	Zeigt an, ob die Schnittstelle bereit ist und über eine Verknüpfung verfügt.	boolesch

Mitgliedänderbarkeit und Knotenstatus

In dieser Tabelle wird angegeben, ob die Objektparameter für jeden möglichen Node-Status geändert werden können.

Parametername	Verfügbarer Status	Status „ausstehend“	Aktiver Status
Bond-Master	Nein	Nein	Nein
Familie	Nein	Nein	Nein
MacAddress	Vom System konfiguriert	1. A.	1. A.
MacAdressePermanent	Vom System konfiguriert	1. A.	1. A.

Methode	Nein	Nein	Nein
Status	Ja.	Ja.	Ja.
UpAndRunning	Vom System konfiguriert	1. A.	1. A.

Weitere Informationen

- Getconfig
- GetNetworkConfig

Netzwerk (lokale Schnittstellen)

Das Netzwerk-Objekt (lokale Schnittstellen) enthält Konfigurationsinformationen für lokale Netzwerkschnittstellen, z. B. die Loopback-Schnittstelle, auf einem Storage-Node. Sie können das verwenden `GetConfig` Und `GetNetworkConfig` Methoden zum Abrufen dieser Informationen für einen Storage-Node

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Familie	Adressfamilie, die für die Schnittstelle konfiguriert ist. Derzeit wird "inet" für IPv4 unterstützt.	Zeichenfolge
MacAddress	Die tatsächliche MAC-Adresse, die der Schnittstelle zugewiesen und vom Netzwerk beobachtet wird.	Zeichenfolge
MacAdressePermanent	Die vom Hersteller der Schnittstelle zugewiesene unveränderliche MAC-Adresse.	Zeichenfolge

Methode	Die Methode zum Konfigurieren der Schnittstelle. Mögliche Werte: • Loopback: Wird verwendet, um die IPv4-Loopback-Schnittstelle zu definieren. • Manuell: Zur Definition von Schnittstellen, die nicht automatisch konfiguriert werden. • dhcp: Kann verwendet werden, um eine IP-Adresse über DHCP zu erhalten. • Statisch: Zur Definition von Ethernet-Schnittstellen mit statisch zugewiesenen IPv4-Adressen.	Zeichenfolge
Status	Der Status der Schnittstelle. Mögliche Werte: • Down: Die Schnittstelle ist inaktiv. • Up: Die Schnittstelle ist bereit, hat aber keine Verbindung. • UpAndRunning: Die Schnittstelle ist bereit und ein Link ist aufgebaut.	Zeichenfolge
UpAndRunning	Zeigt an, ob die Schnittstelle bereit ist und über eine Verknüpfung verfügt.	boolesch

Mitgliedänderbarkeit und Knotenstatus

In dieser Tabelle wird angegeben, ob die Objektparameter für jeden möglichen Node-Status geändert werden können.

Parametername	Verfügbarer Status	Status „ausstehend“	Aktiver Status
Familie	Nein	Nein	Nein
MacAddress	Vom System konfiguriert	1. A.	1. A.
MacAdressePermanent	Vom System konfiguriert	1. A.	1. A.
Methode	Nein	Nein	Nein

Status	Ja.	Ja.	Ja.
UpAndRunning	Vom System konfiguriert	1. A.	1. A.

Weitere Informationen

- Getconfig
- GetNetworkConfig

Netzwerk (SNMP)

Das SNMP-Netzwerkobjekt enthält Informationen zur SNMP v3-Konfiguration für die Cluster-Knoten.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Datenzugriff	Der Zugriffstyp, der für SNMP-Informationsanfragen zulässig ist. Mögliche Werte: • ro: Schreibgeschützter Zugriff. • rw: Lese-Schreibzugriff. • rosys: Schreibgeschützter Zugriff auf einen eingeschränkten Satz von Systeminformationen.	Zeichenfolge
cidr	Eine CIDR-Netzwerkmaske. Diese Netzwerkmaske muss eine Ganzzahl größer oder gleich 0 und kleiner als oder gleich 32 sein. Auch darf 31 nicht entsprechen.	Ganzzahl
Community	Die SNMP-Community-Zeichenfolge.	Zeichenfolge

Netzwerk	Dieses Mitglied steuert gemeinsam mit dem cidr-Mitglied, auf welches Netzwerk der Zugriff und die Community-Zeichenfolge angewendet werden. Der Sonderwert von "default" wird verwendet, um einen Eintrag anzugeben, der für alle Netzwerke gilt. Die CIDR-Maske wird ignoriert, wenn es sich bei diesem Mitglied um einen Host-Namen oder „Standard“ handelt.	Zeichenfolge

Weitere Informationen

GetSnmpInfo

Netzwerkschnittstelle

Das Objekt NetworkInterface enthält Konfigurationsinformationen für einzelne Netzwerkschnittstellen auf einem Storage-Node.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Adresse	Die IPv4-Managementadresse der Schnittstelle.	Zeichenfolge
AdresseV6	Die IPv6-Managementadresse der Schnittstelle.	Zeichenfolge
Rundfunk	Die Broadcast-Adresse der Schnittstelle.	Zeichenfolge
MacAddress	Die MAC-Adresse der Schnittstelle.	Zeichenfolge
mtu	Die maximale Übertragungseinheit in Byte der Schnittstelle.	Ganzzahl
Name	Der Name der Schnittstelle.	Zeichenfolge
Namespace	Gibt an, ob dieser Schnittstelle ein virtueller Netzwerk-Namespace zugewiesen ist oder nicht.	boolesch

Netzmaske	Die Subnetzmaske der Schnittstelle.	Zeichenfolge
Status	Der Betriebsstatus der Schnittstelle.	Zeichenfolge
Typ	Die Art der Schnittstelle (Bond Master, Bond Slave, etc.).	Zeichenfolge
VirtualNetworkTag	Die VLAN-ID, die der Schnittstelle im virtuellen Netzwerk zugewiesen ist.	Ganzzahl

NetworkSchnittstellenStats

Das netzwerkInterface Stats-Objekt enthält Netzwerkstatistiken, die Gesamtzahl der übertragenen und empfangenen Pakete sowie Fehlerinformationen für einzelne Netzwerkschnittstellen auf einem Speicherknoten. Sie können das verwenden `ListNetworkInterfaceStats` API-Methode zum Auflisten dieser Informationen für die Netzwerkschnittstellen auf einem Storage-Node.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Kollisionen	Die Anzahl der erkannten Kollisionen.	Ganzzahl
Name	Der Name der Netzwerkschnittstelle.	Zeichenfolge
RxBytes	Die Gesamtanzahl der empfangenen Bytes.	Ganzzahl
RxCrcErrors	Die Anzahl der empfangenen Pakete, bei denen ein CRC-Fehler aufgetreten ist.	Ganzzahl
RxDrops	Die Anzahl der empfangenen Pakete, die verworfen wurden.	Ganzzahl
RxErrors	Die Anzahl der empfangenen fehlerhaften oder fehlerhaften Pakete.	Ganzzahl
RxFifoErrors	Die Anzahl der FIFO-Überlauffehler in den empfangenen Daten.	Ganzzahl
RxFrameErrors	Die Anzahl der empfangenen Pakete mit Fehler bei der Rahmenausrichtung.	Ganzzahl

Name	Beschreibung	Typ
RxLengthErrors	Die Anzahl der empfangenen Pakete mit einem Längenfehler.	Ganzzahl
RxMischerError	Die Anzahl der vom Empfänger versäumten Pakete.	Ganzzahl
RxOverErrors	Die Anzahl der Fehler beim Überlauf des Receivers-Ringpuffers für diese Schnittstelle.	Ganzzahl
RxPackets	Die Gesamtanzahl der empfangenen Pakete.	Ganzzahl
TxBytes	Die Anzahl der übertragenen Bytes.	Ganzzahl
TxCarrierErrors	Die Anzahl der Trägerfehler für die Übertragungsseite.	Ganzzahl
TxErrors	Die Anzahl der Paketübertragungsfehler.	Ganzzahl
TxFifoErrors	Die Anzahl der FIFO-Überlauffehler auf der Übertragungsseite.	Ganzzahl
TxPackets	Die Gesamtanzahl der übertragenen Pakete.	Ganzzahl

Knoten

Das Node-Objekt enthält Informationen zu jedem Node im Cluster. Sie können diese Informationen mithilfe von abrufen `ListActiveNodes` Und `ListAllNodes` Methoden

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
AssoziatedFServiceID	Die Fibre-Channel-Service-ID für den Node. „0“, wenn der Node kein Fibre Channel-Node ist.	Ganzzahl
AssoziiertMasterServiceID	Master-Service-ID für den Node.	Ganzzahl
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt
ChassisName	Eindeutig identifiziert ein Chassis, identisch für alle Nodes in einem einzelnen Chassis.	Zeichenfolge

Name	Beschreibung	Typ
cip	Die Cluster-IP-Adresse, die dem Node zugewiesen ist.	Zeichenfolge
Zipi	Für die Cluster-Kommunikation verwendete Netzwerkschnittstelle.	Zeichenfolge
KundenschutzDomainName	Identifiziert eine benutzerdefinierte Schutzdomäne eindeutig. Dieser Name ist für alle Storage-Nodes in allen Chassis einer bestimmten benutzerdefinierten Sicherungsdomäne identisch.	Zeichenfolge
Fiber ChannelTargetPortGroup	Die dem Knoten zugeordnete Zielgruppe. „Null“, wenn der Knoten kein Fibre Channel-Knoten ist.	Ganzzahl
Wartungsmodus	Zeigt an, in welchem Modus ein Node gewartet werden soll.	1. A.
mip	Die für das Node-Management verwendete IP-Adresse.	Zeichenfolge
mipi	Die für das Node-Management verwendete Netzwerkschnittstelle.	Zeichenfolge
Name	Host-Name für den Node.	Zeichenfolge
NodeID	NodeID für diesen Node.	Ganzzahl
Knotenablagefach	Bei HCI-Plattformen lautet der Buchstabe „A“, „B“, „C“ oder „D“) für den Chassis-Steckplatz, in dem dieser Node befindet. Bei Storage-Plattformen ist dieser Wert Null.	Zeichenfolge

Name	Beschreibung	Typ
PlattformInfo	Hardwareinformationen für den Node Mitglieder: • „ChassisType“: Die Hardware-Plattform des Node. • CpuModel: Das CPU-Modell der Hardware-Plattform. • NodeMemoryGB: Die Speichermenge, die in der physischen Plattform in GB installiert ist. • NodeType: Der Name des Node-Modells. • PlattformConfigVersion: Die Version der für diese Node-Hardware konfigurierten Software.	JSON-Objekt
Rolle	Die Rolle des Node im Cluster. Mögliche Werte: • Vereinfachtes • Storage • Computing • Zeuge	
sip	Die dem Node zugewiesene Storage-IP-Adresse.	Zeichenfolge
sipi	Die für Storage-Datenverkehr verwendete Netzwerkschnittstelle.	Zeichenfolge
Softwareversion	Gibt die aktuelle Version der auf dem Node ausgeführten Element-Software zurück.	Zeichenfolge
uuid	Die universell eindeutige Kennung, die diesem Knoten zugeordnet ist.	Zeichenfolge
VirtualNetworks	Objekt, das virtuelle Netzwerk-IP-Adressen und IDs enthält.	VirtualNetwork Array erledigen

Weitere Informationen

- ListenActiveNodes

- ListenAllNodes

NodeProtectionDomains

Das Objekt nodeProtectionDomains enthält Informationen über die Identifizierung eines Node und die diesem Node zugeordneten Schutzdomänen.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
NodeID	Eindeutige Kennung für den Knoten.	Ganzzahl
ProtectionDomains	Liste der Schutzdomänen, deren Mitglied der Knoten ist.	"ProtectionDomain"

KnotenStatistiken

Das Objekt nodeStats enthält allgemeine Aktivitätsmessungen für einen Knoten. Sie können das verwenden `GetNodeStats` Und `ListNodeStats` API-Methoden, um einige oder alle nodeStats-Objekte zu erhalten.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Zählen	Die Anzahl der gesamten Proben im Objekt nodeStats.	Ganzzahl
cpu	CPU-Auslastung in %.	Ganzzahl
CpuTotal	Monoton erhöhter Mehrwert der cpu-Auslastung.	Ganzzahl
CBytesIn	Byte in auf der Cluster-Schnittstelle.	Ganzzahl
CBytesOut	Byte out auf der Cluster-Schnittstelle.	Ganzzahl
SBytesIn	Byte in auf der Speicherschnittstelle.	Ganzzahl

Name	Beschreibung	Typ
SBytesOut	Bytes auf der Speicherschnittstelle entfernt.	Ganzzahl
MBytesIn	Byte in auf der Managementoberfläche.	Ganzzahl
MBytesOut	Byte out auf der Managementoberfläche.	Ganzzahl
NetworkUtilizationCluster	Auslastung der Netzwerkschnittstelle (in %) für die Cluster-Netzwerkschnittstelle.	Ganzzahl
NetworkUtilizationStorage	Auslastung der Netzwerkschnittstelle (in %) für das Speichernetzwerk-Interface.	Ganzzahl
NodeHat	Informationen zur Node-Auslastung. Verfügbar ab Element 12.8. Mitglieder: • PrimärTotalHeat: Primärer Node IOPS insgesamt/konfigurierter Node IOPS durchschnittlich über 24 Stunden • RecentPrimaryTotalHeat: IOPS pro Node, der insgesamt für den primären Node konfiguriert wurde, durchschnittlich über eine Stunde • RecentTotalHeat: IOPS pro Node, konfiguriert per Node, durchschnittlich über eine Stunde • TotalHeat: IOPS pro Node mit konfiguriertem IOPS, durchschnittlich über 24 Stunden	JSON-Objekt
ReadLatencyUSecTotal	Der monoton Mehrwert der Gesamtzeit, die für die Durchführung von Leseoperationen auf dem Node aufgewendet wurde.	Ganzzahl

Name	Beschreibung	Typ
ReadOps	Monoton erhöhter Wert von gesamten Leseoperationen auf einen Node.	Ganzzahl
SsLoadHistogramm	Histogramm-Daten zur Darstellung der Schichtdienstlast im Laufe der Zeit.	JSON-Objekt
Zeitstempel	Die aktuelle Zeit im UTC+0-Format.	ISO 8601-Datumszeichenfolge
UsedMemory	Gesamtspeicherverbrauch in Byte.	Ganzzahl
Write eLatencyUSecTotal	Der monoton Mehrwert der Gesamtzeit, die für die Durchführung von Schreibvorgängen auf den Node aufgewendet wurde.	Ganzzahl
Schreiboperationen	Monoton erhöhter Wert aller Schreibvorgänge auf einen Node.	Ganzzahl

Weitere Informationen

- GetNodeStats
- ListNodeStats

OntapVersionInfo

Das ontapVersionInfo-Objekt enthält Informationen zur API-Version des ONTAP-Clusters in einer SnapMirror-Beziehung. Die Element Web-UI verwendet das `GetOntapVersionInfo` API-Methode zum Abrufen dieser Informationen.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SnapMirrorEndpointID	Die ID des Ziel-ONTAP-Systems.	Ganzzahl
KlientAPIMajorVesion	Die vom Element API-Client verwendete Hauptversion der ONTAP API.	Zeichenfolge

Name	Beschreibung	Typ
ClientAPIMinorVesion	Die vom Element API-Client verwendete Nebenversion der ONTAP API.	Zeichenfolge
OntapAPIMajorVersion	Die aktuelle vom ONTAP System unterstützte API-Hauptversion.	Zeichenfolge
OntapAPIMinorVesion	Die vom ONTAP-System unterstützte aktuelle Version der API-Nebenversion.	Zeichenfolge
OntapVersion	Die aktuelle Softwareversion, die auf dem ONTAP-Cluster ausgeführt wird.	Zeichenfolge

HängenActiveNode

Das PendingActiveNode-Objekt enthält Informationen über einen Knoten, der sich derzeit im Status Pendingaktiv befindet, zwischen dem Status „ausstehend“ und „aktiv“. Dies sind Knoten, die derzeit an das werkseitige Softwareabbild zurückgegeben werden. Verwenden Sie die `ListPendingActiveNodes` API-Methode, um eine Liste dieser Informationen für alle hängenden aktiven Knoten zurückzugeben.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
ActiveNodeKey	Ein eindeutiger Schlüssel, mit dem der Node nach einer erfolgreichen Installation der Software automatisch zum Cluster hinzugefügt werden kann.	Zeichenfolge
ZuweisdNodeID	Die zugewiesene Node-ID für den Node.	Zeichenfolge
Asynchron	Die asynchrone Methode handle, mit der Sie den Status des Vorgangs abfragen können.	Ganzzahl
cip	Die Cluster-IP-Adresse, die dem Node zugewiesen ist.	Zeichenfolge

Name	Beschreibung	Typ
mip	Die dem Node zugewiesene Management-IP-Adresse.	Zeichenfolge
Knotenablagefach	Bei HCI-Plattformen lautet der Buchstabe „A“, „B“, „C“ oder „D“) für den Chassis-Steckplatz, in dem dieser Node befindet. Bei Storage-Plattformen ist dieser Wert Null.	Zeichenfolge
HängenActiveNodeID	Die ausstehende Node-ID des Node.	Ganzzahl
PlattformInfo	Hardwareinformationen für den Node Mitglieder: • „ChassisType“: Die Hardware-Plattform des Node. • CpuModel: Das CPU-Modell der Hardware-Plattform. • NodeMemoryGB: Die Speichermenge, die in der physischen Plattform in GB installiert ist. • NodeType: Der Name des Node-Modells. • PlattformConfigVersion: Die Version der für diese Node-Hardware konfigurierten Software.	JSON-Objekt
Rolle	Die Rolle des Node im Cluster. Mögliche Werte: • Vereinfachtes • Storage • Computing • Zeuge	
sip	Die dem Knoten zugewiesene Speicher-IP-Adresse (iSCSI).	Zeichenfolge
Softwareversion	Die aktuelle Version der auf dem Node ausgeführten Element Software.	Zeichenfolge

Weitere Informationen

ListPendingActiveNodes

Hängende Knoten

Das PendingNode-Objekt enthält Informationen zu einem Node, der einem Cluster hinzugefügt werden kann. Verwenden Sie die `ListPendingNodes` API-Methode zum Zurückgeben einer Liste dieser Informationen für alle ausstehenden Knoten. Sie können mithilfe der einen beliebigen der aufgeführten Nodes zu einem Cluster hinzufügen `AddNodes` API-Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Zipi	Die Cluster-IP-Adresse, die dem Node zugewiesen ist.	Zeichenfolge
ActiveNodeKey	Ein eindeutiger Schlüssel, mit dem der Node nach einer erfolgreichen Installation der Software automatisch zum Cluster hinzugefügt werden kann.	Zeichenfolge
ZuweisdNodeID	Die zugewiesene Node-ID für den Node.	Zeichenfolge
Asynchron	Die asynchrone Methode handle, mit der Sie den Status des Vorgangs abfragen können.	Ganzzahl
ChassisName	Eindeutig identifiziert ein Chassis, identisch für alle Nodes in einem einzelnen Chassis.	Zeichenfolge
cip	Die Cluster-IP-Adresse, die dem Node zugewiesen ist.	Zeichenfolge
mip	Die dem Node zugewiesene Management-IP-Adresse.	Zeichenfolge
Knotenablagefach	Bei HCI-Plattformen lautet der Buchstabe „A“, „B“, „C“ oder „D“) für den Chassis-Steckplatz, in dem dieser Node befindet. Bei Storage-Plattformen ist dieser Wert Null.	Zeichenfolge

Name	Beschreibung	Typ
HängenActiveNodeID	Die ausstehende Node-ID des Node.	Ganzzahl
PlattformInfo	Hardwareinformationen für den Node Mitglieder: • „ChassisType“: Die Hardware-Plattform des Node. • CpuModel: Das CPU-Modell der Hardware-Plattform. • NodeMemoryGB: Die Speichermenge, die in der physischen Plattform in GB installiert ist. • NodeType: Der Name des Node-Modells. • PlattformConfigVersion: Die Version der für diese Node-Hardware konfigurierten Software.	JSON-Objekt
Rolle	Die Rolle des Node im Cluster. Mögliche Werte: • Vereinfachtes • Storage • Computing • Zeuge	
sip	Die dem Knoten zugewiesene Speicher-IP-Adresse (iSCSI).	Zeichenfolge
Softwareversion	Die aktuelle Version der auf dem Node ausgeführten Element Software.	Zeichenfolge

Weitere Informationen

- AddNodes
- ListenPendingKnoten

ProtectionDomain

Das proteectionDomain-Objekt enthält den Namen und die Typdetails für eine Schutzdomäne.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SchutzDomainName	Der Name der Schutzdomäne.	Zeichenfolge
SchutzDomainType	Der Typ der Schutzdomäne. Mögliche Werte: • Chassis: Alle Storage-Nodes in einem einzelnen Chassis. • Kunde: Alle Storage-Nodes in einer einzelnen, vom Kunden definierten Sicherungsdomäne	Zeichenfolge

SchutzDomainLevel

Das Objekt ProtektionDomainLevel enthält Informationen zur aktuellen Toleranz und Ausfallsicherheit des Storage Clusters. Toleranzstufen geben an, dass das Cluster im Falle eines Ausfalls weiterhin Daten lesen und schreiben kann. Die Stabilitätsstufen geben an, dass das Cluster seine Fähigkeit besitzt, sich selbst bei einem oder mehreren Ausfällen seiner zugehörigen Sicherungsdomäne automatisch zu beheben.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SchutzDomainType	Der Typ der Schutz-Domain mit der entsprechenden Toleranz und Ausfallsicherheit. Mögliche Werte: • Knoten: Jeder einzelne Knoten. • Chassis: Alle einzelnen Nodes oder alle Storage-Nodes in einem einzelnen Chassis. • Kunde: Alle Storage-Nodes in einer einzelnen, vom Kunden definierten Sicherungsdomäne	Zeichenfolge
Ausfallsicherheit	Die aktuelle Ausfallsicherheit dieses Clusters aus der Perspektive dieses Schutz-Domain-Typs.	SchutzDomaininAusfallsicherheit

Name	Beschreibung	Typ
Toleranz	Die aktuelle Toleranz für diesen Cluster aus der Perspektive dieses Schutz-Domain-Typs.	SchutzDominToleranz

SchutzDomaininAusfallsicherheit

Das ProtectionDomainResiliency-Objekt enthält den Resiliency-Status dieses Storage-Clusters. Die Ausfallsicherheit zeigt an, dass sich das Storage-Cluster dank des zugehörigen Protection Domain-Typs automatisch bei einem oder mehreren Ausfällen abheilen kann. Ein Storage-Cluster gilt als geheilt, wenn es mit dem Ausfall eines einzelnen Storage-Nodes weiterhin Daten lesen und schreiben kann (Node-Toleranz).

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SchutzSchemeResilienzen	Eine Liste von Objekten (eines für jedes Schutzschema) mit Ausfallsicherheitsdaten für den zugehörigen Typ der Sicherungsdomäne.	SicherungAusfallsicherheit Array erledigen
SingleFailureThresholdBytesForBlockData	Die maximale Anzahl von Bytes, die im Storage Cluster gespeichert werden können, bevor die Funktion zur automatischen Heilung eines Node-Toleranzzustands verliert.	Ganzzahl
NachhaltigkeitForEnsemble	Die vorhergesagte Anzahl gleichzeitiger Ausfälle, die auftreten können, ohne die Fähigkeit zu verlieren, automatisch zu einem Zustand der Knotentoleranz für das Ensemble Quorum zu heilen.	Ganzzahl

SchutzDominToleranz

Der ProtectionDomainTolerance-Objekt enthält Informationen darüber, wie der Storage Cluster bei einem oder mehreren Ausfällen Daten weiterhin in einer einzelnen Sicherungsdomäne mit dem zugehörigen Protection Domain-Typ lesen und schreiben kann.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
ProtektionSchemeToleranzen	Eine Liste von Objekten (eines für jedes Schutzschema) mit Ausfalltoleranz-Informationen für den zugehörigen Typ der Schutzdomäne.	SchutzSchemeToleranz Array erledigen
NachhaltigkeitForEnsemble	Die Anzahl gleichzeitiger Ausfälle innerhalb der entsprechenden Schutzdomäne, die ohne Verlust des Ensemblegorums auftreten können.	Ganzzahl

SicherungAusfallsicherheit

Das Schutzobjekt SchemeResiliency enthält Informationen darüber, ob sich ein Storage-Cluster für ein bestimmtes Schutzschema automatisch vor einem oder mehreren Ausfällen seiner verbundenen SchutzDomainType beheben kann. Ein Storage-Cluster gilt als geheilt, wenn es mit dem Ausfall eines einzelnen Storage-Nodes weiterhin Daten lesen und schreiben kann (Node-Toleranz).

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Schutzschema	Das derzeitige Sicherungsschema dieses Storage Clusters. Der einzige mögliche Wert ist zweifelleHelix.	Zeichenfolge
NachhaltigkeitForBlockData	Die prognostizierte Anzahl an gleichzeitigen Ausfällen kann auftreten, ohne dass die Fähigkeit zur automatischen Heilung eines Status von Node-Toleranz für Daten verloren geht.	Ganzzahl
NachhaltigkeitMetadaten	Die prognostizierte Anzahl an gleichzeitigen Ausfällen kann auftreten, ohne dass die Fähigkeit nicht beeinträchtigt wird, automatisch mit einer Node-Toleranz für Metadaten zu heilen.	Ganzzahl

SchutzSchemeToleranz

Das Protektionsobjekt SchemeTolerance enthält Informationen darüber, ob ein Storage-Cluster für ein bestimmtes Sicherungsschema weiterhin Daten nach Ausfällen lesen und schreiben kann.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Schutzschema	Das derzeitige Sicherungsschema dieses Storage Clusters. Der einzige mögliche Wert ist zweifelleHelix.	Zeichenfolge
NachhaltigkeitForBlockData	Die aktuelle Anzahl gleichzeitiger Ausfälle, die ohne Verlust der Verfügbarkeit der Blockdaten im entsprechenden Sicherungsschema auftreten können.	Ganzzahl
NachhaltigkeitMetadaten	Die aktuelle Anzahl gleichzeitiger Ausfälle, die ohne Verlust der Metadaten-Verfügbarkeit für das zugehörige Schutzschema auftreten können.	Ganzzahl

ProtocolEndpoint

Das Objekt ProtocolEndpoint enthält die Attribute eines Protokollendpunkts. Sie können diese Informationen für alle Protokollendpunkte im Cluster mithilfe von abrufen `ListProtocolEndpoints` API-Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
PrimärProviderID	Die ID des Objekts vom Endpunkt des primären Protokolls für den Protokollendpunkt.	Ganzzahl
Protokoll-EndpointID	Die eindeutige ID des Protokollendpunkts.	UUID

Name	Beschreibung	Typ
Protokoll EndpointState	Der Status des Protokollendpunkts. Mögliche Werte: • Aktiv: Der Protokollendpunkt wird verwendet. • Start: Der Protokollendpunkt wird gestartet. • Failover: Der Protokollendpunkt ist ein Failover aufgetreten. • Reserviert: Der Protokollendpunkt ist reserviert.	Zeichenfolge
Anbietertyp	Der Typ des Provider des Protokollendpunkts. Mögliche Werte: • Primär • Sekundär	Zeichenfolge
ScsiNAADeviceID	Die weltweit eindeutige SCSI-Gerätekennung für den Protokollendpunkt im NAA IEEE Registered Extended Format.	Zeichenfolge
Zweiter ProviderID	Die ID des Objekts vom Endpunkt des sekundären Protokolls für den Protokollendpunkt.	Ganzzahl

Weitere Informationen

ListProtocolEndpunkte

QoS

Das QoS-Objekt enthält Informationen zu QoS-Einstellungen (Quality of Service) für Volumes. Volumes, die ohne angegebene QoS-Werte erstellt wurden, werden mit den Standardwerten erstellt. Standardwerte finden Sie mit der `GetDefaultQoS` Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
IOPS	Maximal 4 KB IOPS mit Spitzenauslastung über kurze Zeiträume zulässig. Ermöglicht Spitzen von I/O-Aktivitäten über den normalen IOPS-Wert max.	Ganzzahl
Brennzeit	Die Länge des Zeitaufwands für BurstIOPS ist zulässig. Der zurückgegebene Wert wird in Sekunden dargestellt. Dieser Wert wird vom System auf Basis der für QoS eingestellten IOPS berechnet.	Ganzzahl
Kurve	Die Kurve ist ein Satz von Schlüsselwert-Paaren. Die Schlüssel sind E/A-Größen in Bytes. Die Werte stellen die Kosten für die Performance eines IOP bei einer bestimmten I/O-Größe dar. Die Kurve wird relativ zu einem 4096-Byte-Vorgang berechnet, der auf 100 IOPS eingestellt ist.	JSON-Objekt
Maximale IOPS-Werte	Die gewünschten maximal 4-KB-IOPS konnten über einen längeren Zeitraum hinweg verwendet werden.	Ganzzahl
IOPS-Minimum	Das gewünschte Mindestwert von 4 KB IOPS zu garantieren. Die zulässigen IOPS sinken nur unter dieses Niveau, wenn alle Volumes auf ihren MinIOPS-Wert begrenzt wurden und es weiterhin eine unzureichende Performance-Kapazität gibt.	Ganzzahl

Weitere Informationen

GetDefaultQoS

QoSPolicy

Das Objekt QoSPolicy enthält Informationen über eine QoS-Richtlinie auf einem Storage-Cluster, auf dem die Element Software ausgeführt wird.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
QosPolicyID	Eine eindeutige ganzzahlige Kennung für die QoSPolicy, die vom Storage-Cluster automatisch zugewiesen wird.	Ganzzahl
Name	Der Name der QoS-Richtlinie Zum Beispiel: Gold, Platin oder Silber.	Zeichenfolge
qos	Die QoS-Einstellungen, für die diese Richtlinie gilt.	QoS
VolumeIDs	Eine Liste der Volumes, die dieser Richtlinie zugeordnet sind.	Integer-Array

Weitere Informationen

GetQoSPolicy

EntfernteClusterSnapshotStatus

Der `remoteClusterSnapshotStatus` Objekt enthält die UUID und den Status eines Snapshots, der auf einem Remote-Storage-Cluster gespeichert ist. Sie können diese Informationen mit erhalten `ListSnapshots` Oder `ListGroupSnapshots` API-Methoden

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
EntferntStatus	Der Replikationsstatus des Remote-Snapshots auf dem Zielcluster, wie vom Quellcluster aus gesehen. Mögliche Werte: • Vorhanden: Der Snapshot ist auf einem Remote-Cluster vorhanden. • NotPresent: Der Snapshot ist nicht auf einem Remote-Cluster vorhanden. • Synchronisierung: Es handelt sich um ein Ziel-Cluster, in dem der Snapshot repliziert wird. • Gelöscht: Dies ist ein Ziel-Cluster. Der Snapshot wurde gelöscht und ist weiterhin auf der Quelle vorhanden.	Zeichenfolge
VolumePairUUID	Die universelle Kennung des Volume-Paares.	UUID

Zeitplan

Das Schedule-Objekt enthält Informationen zu einem Zeitplan, der erstellt wurde, um einen Snapshot eines Volumes autonom zu erstellen. Sie können Terminplaninformationen für alle Zeitpläne mit abrufen `ListSchedules` API-Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Merkmale	Gibt die Häufigkeit des Zeitplaneintretens an. Mögliche Werte: • Wochentag • Tag des Monats • Zeitintervall	JSON-Objekt

Name	Beschreibung	Typ
HasFehler	Zeigt an, ob der Zeitplan Fehler enthält. Mögliche Werte: • Richtig • Falsch	boolesch
Stunden	Zeigt die Stunden an, die vergehen, bevor der nächste Snapshot erstellt wird. Mögliche Werte sind 0 bis 24.	Ganzzahl
LastRunStatus	Zeigt den Status des letzten geplanten Snapshots an. Mögliche Werte: • Erfolg • Fehlgeschlagen	Zeichenfolge
LastRunTimeStart	Zeigt das letzte Mal an, zu dem der Zeitplan gestartet wurde.	ISO 8601-Datumszeichenfolge
Minuten	Zeigt die Minuten an, die vergehen werden, bevor der nächste Snapshot erstellt wird. Mögliche Werte sind 0 bis 59.	Ganzzahl
Monthdays	Gibt die Tage des Monats an, an denen ein Snapshot erstellt wird.	Array erledigen
Angehalten	Gibt an, ob der Zeitplan angehalten wurde oder nicht. Mögliche Werte: • Richtig • Falsch	boolesch
Wiederkehrend	Gibt an, ob der Zeitplan wiederholt ist oder nicht. Mögliche Werte: • Richtig • Falsch	boolesch

Name	Beschreibung	Typ
RunNextInterval	Gibt an, ob der Zeitplan das nächste Mal ausgeführt wird, wenn der Planer aktiv ist. Wenn wahr, wird der Zeitplan das nächste Mal ausgeführt, wenn der Planer aktiv ist und dieser Wert auf false gesetzt wird. Mögliche Werte: • Richtig • Falsch	boolesch
ScheduleID	Die eindeutige ID des Zeitplans.	Ganzzahl

Name	Beschreibung	Typ
ScheduleInfo	Enthält den eindeutigen Namen des Zeitplans, den Aufbewahrungszeitraum für den erstellten Snapshot und die Volume-ID des Volumes, aus dem der Snapshot erstellt wurde. Gültige Werte: • `enableRemoteReplication`: Gibt an, ob der Snapshot in die Remote-Replikation aufgenommen werden soll. (boolesch) • `ensureSerialCreation`: Legt fest, ob eine neue Snapshot-Erstellung zulässig sein soll, wenn eine vorherige Snapshot-Replikation ausgeführt wird. (boolesch) • `name`: Der zu verwendenden Snapshot-Name. (Zeichenfolge) • `retention`: Die Zeit, die der Snapshot aufbewahrt wird. Je nach Uhrzeit wird es in einem der folgenden Formate angezeigt: ◦ `fifo`: Der Snapshot wird auf First-in-First-Out-Basis (FIFO) beibehalten. Wenn leer, wird der Snapshot für immer aufbewahrt. (Zeichenfolge) ◦ HH:mm:ss • `volumeID`: Die ID des Volumens, das in den Schnappschuss aufgenommen werden soll. (Ganze Zahl) • `volumes`: Eine Liste der Volume-IDs, die in den Gruppen-Snapshot aufgenommen werden sollen. (Ganzzahliges Array)	JSON-Objekt
Planname	Der dem Zeitplan zugewiesene eindeutige Name.	Zeichenfolge

Name	Beschreibung	Typ
Planungstyp	Derzeit werden nur Zeitplantypen von Snapshots unterstützt.	Zeichenfolge
SnapMirror Label	Das SnapMirrorLabel, das auf den erstellten Snapshot oder Gruppen-Snapshot angewendet wird, der im ScheduleInfo enthalten ist. Wenn nicht festgelegt, ist dieser Wert Null.	Zeichenfolge
Startdatum	Gibt das Datum an, an dem der Zeitplan zum ersten Mal gestartet wurde oder beginnt; formatiert in UTC-Zeit.	ISO 8601-Datumszeichenfolge
ToBeDeleted	Gibt an, ob der Zeitplan zum Löschen markiert ist. Mögliche Werte: • Richtig • Falsch	boolesch
Wochentage	Gibt die Tage der Woche an, an denen ein Snapshot erstellt wird.	Array erledigen

Weitere Informationen

ListSchedules

Sitzung (Fibre Channel)

Das Sitzungsobjekt enthält Informationen zu jeder Fibre-Channel-Sitzung, die für das Cluster sichtbar ist und auf welchen Zielports es angezeigt wird. Sie können diese Informationen mit dem abrufen `ListFibreChannelSessions` API-Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
InitiatorWWPN	Der World Wide Port Name (WWPN) des Initiators, der im Ziel-Port angemeldet ist.	Zeichenfolge
NodeID	Der Knoten, der die Fibre Channel-Sitzung besitzt.	Ganzzahl

Name	Beschreibung	Typ
Initiator	Informationen über den Server-Initiator dieser Fibre Channel-Sitzung. Mitglieder: • Alias: Der dem Initiator zugewiesene Anzeigename. • Attribute: Die Attribute dieses Initiators. • InitiatorID: Die ID dieses Initiators. • Initiatorname: Der Name dieses Initiators. • VolumeAccessGroups: Eine Liste der Volume-Zugriffsgruppen, die diesem Initiator zugeordnet sind.	JSON-Objekt
Service-ID	Die Service-ID des an dieser Sitzung beteiligten Zielports.	Ganzzahl
TargetWWPN	Der WWPN des an dieser Sitzung beteiligten Zielports.	Zeichenfolge
VolumeAccessGroupID	Die ID der Volume Access Group, zu der der initiatorWWPN gehört. Wenn es sich nicht um eine Volume Access Group handelt, ist dieser Wert Null.	Ganzzahl

Weitere Informationen

ListFiberChannelSessions

Sitzung (iSCSI)

Das iSCSI-Objekt (Session) enthält detaillierte Informationen über die iSCSI-Sitzung jedes Volumes. Sie können iSCSI-Sitzungsdaten mit dem abrufen `ListISCSISessions` API-Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
AccountID	Die Konto-ID des Kontos, das für die CHAP-Authentifizierung verwendet wird, falls vorhanden.	Ganzzahl
AccountName	Der Name des für die CHAP-Authentifizierung verwendeten Kontos, falls vorhanden.	Zeichenfolge
Authentifizierung	Authentifizierungsinformationen für diese iSCSI-Sitzung.	ISCSIAuthentifizierung
CreateTime	Der Zeitpunkt der Erstellung der iSCSI-Sitzung im UTC+0-Format.	ISO 8601-Datumszeichenfolge
DriveID	Die DriveID, die mit dem Transportdienst verknüpft ist, der die Sitzung hostet.	Ganzzahl
Fahrausweise	Eine Liste der Einfahrungs-IDs der Laufwerke, die den Fehler melden. Eine leere Liste, falls nicht zutreffend.	Integer-Array
Initiator	Informationen über den Server-Initiator dieser iSCSI-Sitzung. Mitglieder: • Alias: Der dem Initiator zugewiesene Anzeigename. • Attribute: Die Attribute dieses Initiators. • InitiatorID: Die ID dieses Initiators. • Initiatorname: Der Name dieses Initiators. • VolumeAccessGroups: Eine Liste der Volume-Zugriffsgruppen, die diesem Initiator zugeordnet sind.	JSON-Objekt
InitiatorIP	Die IP-Adresse und die Portnummer des iSCSI-Server-Initiators.	Zeichenfolge
Name des Initiators	Der iSCSI Qualified Name (IQN) des iSCSI-Server-Initiators.	Zeichenfolge

Name	Beschreibung	Typ
InitiatorPortName	Der initiatorname kombiniert mit der initiatorSessionID; identifiziert den Initiator-Port.	Zeichenfolge
InitiatorSitzungs-ID	Eine 48-Bit-ID des Initiators, die die iSCSI-Sitzung zu diesem Initiator gehört.	Ganzzahl
MsSinceLastIscsiPDU	Die Zeit in Millisekunden seit der letzten iSCSI-PDU für diese Sitzung empfangen wurde.	Ganzzahl
MsSinceLastScsiCommand	Die Zeit in Millisekunden seit dem letzten SCSI-Befehl für diese Sitzung empfangen wurde.	Ganzzahl
NodeID	Die NodeID, die mit dem Transportdienst verknüpft ist, der die Sitzung hostet.	Ganzzahl
Service-ID	Die DiensteID des Transportdienstes, der die Sitzung hostet.	Ganzzahl
Sessionid	Die iSCSI-Sitzungs-ID.	Ganzzahl
TargetIP	Die IP-Adresse und die Portnummer des iSCSI-Speicherziels.	Zeichenfolge
Name des Targetnamens	Der IQN des iSCSI-Ziels.	Zeichenfolge
TargetPortName	Der TargetName kombiniert mit dem Gruppen-Tag des Zielportals; identifiziert den Zielport.	Zeichenfolge
VirtualNetworkID	Die virtuelle Netzwerk-ID, die der Sitzung zugeordnet ist.	Ganzzahl
VolumeID	Falls vorhanden, die VolumeID des Volumes, das der Sitzung zugeordnet ist.	Ganzzahl
VolumePosition	Identifiziert gegebenenfalls das Volume-Objekt, das der iSCSI-Sitzung zugeordnet ist.	Ganzzahl

Weitere Informationen

ListISSessions

SnapMirror Aggregat

Das SnapMirrorAggregat enthält Informationen zu den verfügbaren ONTAP Aggregaten, bei denen es sich um Sammlungen von Festplatten handelt, die Volumes als Storage zur Verfügung gestellt werden. Sie können diese Informationen mit der ListSnapMirrorAggregates API-Methode erhalten.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SnapMirrorEndpointID	Die ID des Ziel-ONTAP-Systems.	Ganzzahl
AggregateName	Der Name des Aggregats.	Zeichenfolge
NodeName	Der Name des ONTAP Node, der zu diesem Aggregat gehört.	Zeichenfolge
GrößeVerfügbar	Die Anzahl der im Aggregat verbleibenden verfügbaren Bytes.	Ganzzahl
GrößeGesamt	Die Gesamtgröße (in Bytes) des Aggregats.	Ganzzahl
%Usedacacity	Der Prozentsatz des derzeit verwendeten Speicherplatzes.	Ganzzahl
VolumeAnzahl	Anzahl der Volumes im Aggregat.	Ganzzahl

SnapMirror Clusteridentität

Das SnapMirrorClusterIdentitäts-Objekt enthält Identifikationsinformationen über den Remote-ONTAP-Cluster in einer SnapMirror Beziehung.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SnapMirrorEndpointID	Die ID des Ziel-ONTAP-Systems.	Ganzzahl

Name	Beschreibung	Typ
ClusterName	Der Name des Ziel-ONTAP-Clusters.	Zeichenfolge
ClusterUUID	Die 128-Bit Universally-Unique Identifier des Ziel-ONTAP-Clusters.	Zeichenfolge
ClusterSerialNummer	Die Seriennummer des Ziel-ONTAP-Clusters.	Zeichenfolge

SnapMirror Endpoint

Das SnapMirrorEndpoint Objekt enthält Informationen zu den Remote-SnapMirror-Storage-Systemen, die mit dem Element Storage-Cluster kommunizieren. Sie können diese Informationen mit der ListSnapMirrorEndpoints API-Methode abrufen.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SnapMirrorEndpointID	Die eindeutige ID für das Objekt im lokalen Cluster.	Ganzzahl
Management IP	Die Cluster-Management-IP-Adresse des Endpunkts.	Zeichenfolge
ClusterName	Der ONTAP Cluster-Name. Dieser Wert wird automatisch mit dem Wert „`clusterName`“ aus dem SnapMirrorClusterIdentity-Objekt gefüllt.	Zeichenfolge
Benutzername	Der Management-Benutzername für das ONTAP System.	Zeichenfolge
IpAddresses	Liste der Cluster-übergreifenden Storage IP-Adressen für alle Nodes im Cluster. Diese IP-Adressen können Sie mit der Methode ListSnapMirrorNetworkInterfaces erhalten.	String-Array
Verbindung hergestellt	Der Konnektivitätsstatus der Kontrollverbindung zum ONTAP-Cluster.	boolesch

SnapMirrorJobeCronInfo

Das SnapMirrorJobeCronZeitplanInfo-Objekt enthält Informationen über einen Cron-Job-Zeitplan auf dem ONTAP-System.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SnapMirrorEndpointID	Die ID des Ziel-ONTAP-Systems.	Ganzzahl
ZeitplanName	Der Name des Jobplans.	Zeichenfolge
JobplananlaufBeschreibung	Eine automatisch generierte, vom Menschen lesbare Zusammenfassung des Zeitplans.	Zeichenfolge

SnapMirrorLunInfo

Das SnapMirrorLunInfo-Objekt enthält Informationen zum ONTAP-LUN-Objekt.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SnapMirrorEndpointID	Die ID des Ziel-ONTAP-Systems.	Ganzzahl
CreationZeitstempel	Die Erstellungszeit der LUN.	ISO 8601-Datumszeichenfolge
LunName	Der Name der LUN.	Zeichenfolge
Pfad	Der Pfad der LUN.	Zeichenfolge
Größe	Die Größe der LUN in Byte.	Ganzzahl
SizeUsed	Die Anzahl der von der LUN verwendeten Bytes.	Ganzzahl

Name	Beschreibung	Typ
Bundesland	Der aktuelle Zugriffsstatus der LUN. Mögliche Werte: • Online • Offline • Foreign_lun_Fehler • NV-Fehler • Space_error	Zeichenfolge
Datenmenge	Der Name des Volume, das die LUN enthält.	Zeichenfolge
vserver	Der Vserver, der die LUN enthält.	Zeichenfolge

SnapMirror Netzwerkschnittstelle

Das SnapMirrorNetworkInterface-Objekt enthält Informationen zu den Cluster-logischen Schnittstellen (LIFs).

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
AdministrativeStatus	Gibt an, ob die logische Schnittstelle (LIF) administrativ aktiviert oder deaktiviert ist. Mögliche Werte: • Hoch • Runter	Zeichenfolge
SnapMirrorEndpointID	Die ID des Ziel-ONTAP-Systems.	Ganzzahl
SchnittstellenName	Der LIF-Name.	Zeichenfolge
Netzwerkadresse	Die IP-Adresse des LIF.	Zeichenfolge
Netzwerkmaske	Die Netzwerkmaske des LIF.	Zeichenfolge

Name	Beschreibung	Typ
OberflächeRole	Die Rolle des LIF. Mögliche Werte: • Entf • Cluster • Daten • Node-Management • Intercluster • Cluster_Management	Zeichenfolge
OperationalStatus	Der Betriebsstatus der logischen Schnittstelle (unabhängig davon, ob sie eine erfolgreiche Verbindung gebildet hat). Dieser Status kann vom Administrationsstatus abweichen, wenn ein Netzwerkproblem vorliegt, das die Funktionsweise der Schnittstelle verhindert. Mögliche Werte: • Hoch • Runter	Zeichenfolge
VserverName	Der Name des Vserver.	Zeichenfolge

SnapMirror Node

Das SnapMirrorNode-Objekt enthält Informationen zu den Nodes des Ziel-ONTAP Clusters in einer SnapMirror Beziehung.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SnapMirrorEndpointID	Die ID des Ziel-ONTAP-Systems.	Ganzzahl
Name	Der Name des ONTAP Node.	Zeichenfolge
Modell	Das Modell des ONTAP Nodes.	Zeichenfolge
Seriennummer	Die Seriennummer des ONTAP-Node.	Zeichenfolge
Produktversion	Die Produktversion von ONTAP.	Zeichenfolge

Name	Beschreibung	Typ
Es ist nicht heilishealthy	Der Systemzustand eines Node im ONTAP Cluster. Mögliche Werte: • Richtig • Falsch	Zeichenfolge
Voraussetzungen	Gibt an, ob der Node zur Teilnahme an einem ONTAP Cluster berechtigt ist oder nicht. Mögliche Werte: • Richtig • Falsch	Zeichenfolge

SnapMirror Richtlinie

Das SnapMirrorPolicy-Objekt enthält Informationen zu einer SnapMirror-Richtlinie, die auf einem ONTAP System gespeichert ist.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SnapMirrorEndpointID	Die ID des Ziel-ONTAP-Systems.	Ganzzahl
PolicyName	Der der Richtlinie zugewiesene eindeutige Name.	Zeichenfolge
Richtlinientyp	Der Typ der Richtlinie. Mögliche Werte: • Async_Mirror • Mirror_Vault	Zeichenfolge
Kommentar	Eine von Menschen lesbare Beschreibung im Zusammenhang mit der SnapMirror-Richtlinie	Zeichenfolge

Name	Beschreibung	Typ
Transferpriorität	Die Priorität, bei der eine SnapMirror Übertragung ausgeführt wird. Mögliche Werte: • Normal: Die Standardpriorität. Diese Transfers werden vor Transfers mit höchster Priorität geplant. • Niedrig: Diese Transfers haben die niedrigste Priorität und werden nach den meisten normalen Prioritätstransfers geplant.	Zeichenfolge
Richtlinie	Eine Liste von Objekten, die die Richtlinienregeln beschreiben	SnapMirror PolicyRule Array erledigen
TotalKeepCount	Die Gesamtzahl der Aufbewahrung für alle Regeln in der Richtlinie.	Ganzzahl
TotalRegeln	Die Gesamtzahl der Regeln in der Richtlinie.	Ganzzahl
VserverName	Der Name des Vserver für die SnapMirror Richtlinie	Zeichenfolge

SnapMirror PolicyRule

Das Objekt SnapMirror PolicyRule enthält Informationen zu den Regeln in einer SnapMirror-Richtlinie.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SnapMirror Label	Das Label für Snapshot Kopien, das zur Auswahl von Snapshot Kopien in erweiterten Datensicherungsbeziehungen verwendet wird.	Zeichenfolge
KeepCount	Gibt die maximale Anzahl an Snapshot Kopien an, die im SnapMirror Ziel-Volume für eine Regel beibehalten werden.	Ganzzahl

SnapMirror Beziehung

Das SnapMirrorRelationship-Objekt enthält Informationen zu einer SnapMirror Beziehung zwischen einem Element Volume und einem ONTAP Volume.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SnapMirrorEndpointID	Die ID des Ziel-ONTAP-Systems.	Ganzzahl
SnapMirrorRelationshipID	Die eindeutige Kennung für jedes SnapMirror-Relationship-Objekt in einem Array wie in ListSnapMirrorRelationships zurückgegeben wird. Diese UUID wird erstellt und vom ONTAP System zurückgegeben.	Zeichenfolge
QuelleVolume	Ein Objekt, das das Quell-Volume beschreibt.	SnapMirrorVolumeInfo
Zielvolumen	Ein Objekt, das das Ziel-Volume beschreibt.	SnapMirrorVolumeInfo
CurrentMaxTransferRate	Die aktuelle maximale Übertragungsrate zwischen Quell- und Ziel-Volumes in Kilobyte pro Sekunde.	Ganzzahl
Ist heidhy	Ob die Beziehung gesund ist oder nicht. Mögliche Werte: • Wahr: Die Beziehung ist gesund. • Falsch: Die Beziehung ist nicht gesund. Dies kann durch ein fehlendes manuelles oder geplantes Update oder durch einen Abbruch der letzten geplanten Aktualisierung verursacht werden.	boolesch
Lagtime	Die Zeit in Sekunden, in der die Daten auf dem Ziel-Volume hinter den Daten auf dem Quell-Volume abliegen.	Ganzzahl

Name	Beschreibung	Typ
LastTransferDauer	Die Zeit in Sekunden, die für die letzte Übertragung benötigt wurde.	Ganzzahl
LastTransferFehler	Eine Nachricht, in der die Ursache des letzten Übertragungsfehlers beschrieben wird.	Zeichenfolge
LastTransferGröße	Die Gesamtanzahl der während der letzten Übertragung übertragenen Bytes.	Ganzzahl
LastTransferEndZeitstempel	Der Zeitstempel des Endes der letzten Übertragung.	ISO 8601-Datumszeichenfolge
LastTransferTyp	Die Art des vorherigen Transfers in der Beziehung.	Zeichenfolge
Maximale Transferrate	Gibt die maximale Datentransferrate zwischen den Volumes in Kilobyte pro Sekunde an. Der Standardwert 0 ist unbegrenzt und erlaubt der SnapMirror Beziehung, die verfügbare Netzwerkbandbreite voll zu nutzen.	Ganzzahl
MirrorState	Der Mirror-Status der SnapMirror Beziehung. Mögliche Werte: • Nicht initialisiert: Das Ziel-Volume wurde nicht initialisiert. • Snapmirrored: Das Ziel-Volume wurde initialisiert und ist bereit, SnapMirror Updates zu erhalten. • Broken-off: Der Zieldatenträger ist Lesen-Schreiben und Schnappschüsse sind vorhanden.	Zeichenfolge
Neuer Snapshot	Der Name der neuesten Snapshot Kopie auf dem Ziel-Volume.	Zeichenfolge

Name	Beschreibung	Typ
PolicyName	Gibt den Namen der ONTAP SnapMirror Richtlinie für die Beziehung an. Eine Liste der verfügbaren Richtlinien kann mit ListSnapMirrorPolicies abgerufen werden. Beispielwerte sind “MirrorLatest” und “MirrorAndVault”.	Zeichenfolge
Richtlinientyp	Typ der ONTAP SnapMirror-Richtlinie für die Verbindung. Siehe ListSnapMirrorPolicies. Beispiele sind: „`async_mirror`“ oder „`mmirror_Vault`“.	Zeichenfolge
BeziehungProgress	Die Gesamtzahl der bisher für die aktuelle Aktivität der im Beziehungsstatus zurückgegebenen Bytes. Diese Einstellung wird nur dann festgelegt, wenn das Mitglied „RelationshipStatus“ darauf hinweist, dass eine Aktivität gerade läuft.	Ganzzahl
Beziehungsstatus	Der Status der SnapMirror Beziehung. Mögliche Werte: • Leerlauf • Übertragung • Prüfen • Wird stillgelegt • Stillgelegt • Warteschlange • Vorbereitung • Abschließen • Wird abgebrochen • Breaking	Zeichenfolge
Beziehungstyp	Der Typ der SnapMirror-Beziehung. Auf Storage-Clustern, auf denen die Element Software ausgeführt wird, ist dieser Wert immer „`Extended_Data_Protection`“.	Zeichenfolge

Name	Beschreibung	Typ
Planname	Der Name des vorbestehenden cron-Zeitplans auf dem ONTAP-System, das zum Aktualisieren der SnapMirror-Beziehung verwendet wird. Eine Liste der verfügbaren Zeitpläne kann mit ListSnapMirrorSchedules abgerufen werden.	Zeichenfolge
UnshealtyReasone	Der Grund, warum die Beziehung nicht gesund ist.	Zeichenfolge

SnapMirror Volume

Das SnapMirrorVolume-Objekt enthält Informationen zu einem ONTAP Volume.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SnapMirrorEndpointID	Die ID des Ziel-ONTAP-Systems.	Ganzzahl
Name	Der Name des Volume.	Zeichenfolge
Typ	Der Volume-Typ. Mögliche Werte: • rw: Volumen für Lese- und Schreibvorgänge • ls: Volumen der Lastverteilung • datensicherung: Datensicherungs-Volume	Zeichenfolge
vserver	Der Name des Vserver, dem dieses Volume gehört.	Zeichenfolge
AggrName	Der mit Aggregatname.	Zeichenfolge

Name	Beschreibung	Typ
Bundesland	Der Status des Volume. Mögliche Werte: • Online • Eingeschränkt • Offline • Gemischt	Zeichenfolge
Größe	Die Gesamtgröße des Dateisystems (in Bytes) des Volumes.	Zeichenfolge
Verfügbare Größe	Die Größe (in Byte) des verfügbaren Speicherplatzes im Volume.	Zeichenfolge

SnapMirrorVolumeInfo

Das SnapMirrorVolumeInfo-Objekt enthält Informationen zu einem Speicherort eines Volumes in einer SnapMirror-Beziehung, z. B. Name und Typ.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Typ	Der Volume-Typ. Mögliche Werte: • SolidFire: Das Volume befindet sich auf einem Storage-Cluster, auf dem die Element Software ausgeführt wird. • ONTAP: Das Volume befindet sich auf einem Remote-ONTAP-Cluster.	Zeichenfolge
VolumeID	Die ID des Volume. Nur gültig, wenn „Typ“ SolidFire ist.	Ganzzahl
vserver	Der Name des Vserver, dem dieses Volume gehört. Nur gültig, wenn „Typ“ ONTAP ist.	Zeichenfolge
Name	Der Name des Volume.	Zeichenfolge

SnapMirrorVServer

Das SnapMirrorVServer-Objekt enthält Informationen zu Storage Virtual Machines (oder Vservern) im Ziel-ONTAP Cluster.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
SnapMirrorEndpointID	Die ID des Ziel-ONTAP-Systems.	Ganzzahl
VserverName	Der Name des Vserver.	Zeichenfolge
VserverType	Der Vserver Typ. Mögliche Werte: • Daten • Admin • System • Knoten	Zeichenfolge
VserverSubtyp	Der Untertyp des Vserver. Mögliche Werte: • Standard • dv-Destination • Daten • Sync_Source • Sync_Destination	Zeichenfolge
Wurzelvolumen	Das Root Volume des vServers.	Zeichenfolge
RootVolumeaggregate	Das Aggregat, auf dem das Root-Volume erstellt wird.	Zeichenfolge
VserveraggregateInfo	Eine Reihe von SnapMirrorVserverAggregateInfo-Objekten.	JSON-Objekt

Name	Beschreibung	Typ
AdminStaat	Der detaillierte Administrationsstatus des vServers. Mögliche Werte: • Wird ausgeführt • Angehalten • Wird gestartet • Wird angehalten • Initialisierung • Löschen	Zeichenfolge
OperationalState	Der grundlegende Betriebsstatus des vServers. Mögliche Werte: • Wird ausgeführt • Angehalten	Zeichenfolge

SnapMirrorVserveraggregateInfo

Das SnapMirrorVserverAggregateInfo Objekt enthält Informationen zu den verfügbaren Storage Virtual Machines (auch Vserver genannt) auf dem Ziel-ONTAP Cluster.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
AggrName	Der Name des Aggregats, das einem Vserver zugewiesen ist.	Zeichenfolge
AggrVerfügbare Größe	Die verfügbare Größe des zugewiesenen Aggregats.	Ganzzahl

snapshot

Das Snapshot-Objekt enthält Informationen über einen Snapshot, der für ein Volume erstellt wurde. Sie können das verwenden `ListSnapshots` API-Methode zum Abrufen einer Liste von Snapshot-Informationen für ein Volume oder für alle Volumen. Das Objekt enthält Informationen über den aktiven Snapshot sowie jeden für ein Volume erstellten Snapshot.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt
Prüfsumme	Eine kleine Zeichenfolgendarstellung der Daten im gespeicherten Snapshot. Diese Prüfsumme kann später verwendet werden, um andere Snapshots zu vergleichen, um Fehler in den Daten zu erkennen.	Zeichenfolge
CreateTime	Die UTC+0-formatierte Zeit, zu der der Snapshot erstellt wurde.	ISO 8601-Datumszeichenfolge
EnableRemoteReplication	Gibt an, ob Snapshot für die Remote-Replikation aktiviert ist.	boolesch
AusweiseLeason	Gibt an, wie der Snapshot-Ablauf festgelegt wurde. Mögliche Werte: • API: Die Ablaufzeit wird mithilfe der API festgelegt. • Keine: Keine Ablaufzeit festgelegt. • Test: Die Ablaufzeit ist für Tests eingestellt. • fifo: Ablauf erfolgt auf einer First-in-First-Out-Basis.	Zeichenfolge
Zeit für AufwandsZeit	Der Zeitpunkt, zu dem dieser Snapshot abläuft und aus dem Cluster gelöscht wird	ISO 8601-Datumszeichenfolge
Gruppen-ID	Die Gruppen-ID, wenn der Snapshot Mitglied eines Gruppen-Snapshots ist.	Ganzzahl
GroupsnapshotUUID	Enthält Informationen zu den einzelnen Snapshots der Gruppe. Jeder dieser Mitglieder verfügt über einen UUID-Parameter für die UUID des Snapshots.	Zeichenfolge

Name	Beschreibung	Typ
InstanceCreateTime	Die Zeit, zu der der Snapshot auf dem lokalen Cluster erstellt wurde.	ISO 8601-Datumszeichenfolge
Snapshot UUID erstellen	Die universell eindeutige ID des Snapshots auf dem lokalen Cluster. Diese ID wird nicht auf andere Cluster repliziert.	Zeichenfolge
Name	Der eindeutige Name, der dem Snapshot zugewiesen wurde. Wenn kein Name angegeben wird, ist der Name der Zeitstempel im UTC+0-Format des Erstellungszeitpunkt des Snapshots.	Zeichenfolge
EntferntStatus	Ein Array, das den universellen Identifikator und den Replikationsstatus jedes Remote-Snapshots auf dem Zielcluster enthält, wie vom Quellcluster aus gesehen.	EntfernteClusterSnapshotStatus Array erledigen
SnapMirror Label	Das von der SnapMirror Software verwendete Etikett, um die Richtlinie zur Snapshot-Aufbewahrung auf SnapMirror Endpunkten festzulegen. Wenn nicht festgelegt, ist dieser Wert Null.	Zeichenfolge
Snapshot-ID	Die eindeutige ID eines vorhandenen Snapshots.	Zeichenfolge
SnapshotUUID	Die universell eindeutige ID eines vorhandenen Snapshots. Wenn der Snapshot über Cluster hinweg repliziert wird, wird diese ID zusammen mit ihm repliziert und zur Identifizierung des Snapshots über Cluster verwendet.	Zeichenfolge

Name	Beschreibung	Typ
Status	Aktueller Status des Snapshots. Mögliche Werte: • Unbekannt: Beim Abrufen des Status des Snapshots ist ein Fehler aufgetreten. • Vorbereiten: Dieser Snapshot wird gerade zur Verwendung vorbereitet und ist noch nicht beschreibbar. • RemoteSyncing: Dieser Snapshot wird von einem Remote-Cluster repliziert. • Fertig: Die Vorbereitung oder Replikation dieses Snapshots ist abgeschlossen und kann nun verwendet werden. • Aktiv: Dieser Snapshot ist der aktive Branch. • Klonen: Dieser Snapshot ist an einem KopierVolume-Vorgang beteiligt.	Zeichenfolge
Summengröße	Die Gesamtgröße in Byte des Snapshots.	Ganzzahl
VirtualVolumeID	Die ID des virtuellen Volumes, das diesem Snapshot zugeordnet ist.	UUID
VolumeID	Die ID des Datenträgers, aus dem der Snapshot erstellt wurde.	Ganzzahl
VolumeName	Der Name des Volumes zum Zeitpunkt der Erstellung des Snapshots.	Zeichenfolge

Weitere Informationen

ListenSnapshots

SnmpTrapEmpfänger

Das snmpTrapEmpfänger-Objekt enthält Informationen über einen Host, der so konfiguriert ist, dass vom Storage-Cluster generierte SNMP-Traps empfangen werden. Sie können das verwenden `GetSnmpTrapInfo` API-Methode zum Abrufen einer Liste von Hosts, die für den Empfang von SNMP-Traps konfiguriert sind.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Host	Die IP-Adresse oder der Hostname des Ziel-Hosts.	Zeichenfolge
Port	Die UDP-Portnummer auf dem Host, an dem der Trap gesendet werden soll. Gültiger Bereich: 1 bis 65535. 0 (null) ist keine gültige Portnummer. Der Standardport ist 162.	Ganzzahl
Community	SNMP-Community-String.	Zeichenfolge

Storage Container

Das storageContainer-Objekt enthält die Attribute eines virtuellen Volume-Storage-Containers. Sie können diese Informationen für jeden Storage-Container im Cluster mithilfe von abrufen `ListStorageContainers` API-Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
AccountID	Die ID des Speichersystemkontos, das mit dem Speichercontainer verknüpft ist.	Ganzzahl
InitiatorSecret	Der CHAP-Authentifizierungsschlüssel für den Initiator, der dem Speichercontainer zugeordnet ist.	Zeichenfolge
Name	Der Name des Speichercontainers.	Zeichenfolge
Protokoll EndpointType	Der Endpunkt-Typ des Storage-Containers. SCSI ist der einzige gültige Wert.	Zeichenfolge

Name	Beschreibung	Typ
Status	Der Status des Speichercontainers. Mögliche Werte: • Aktiv: Der Speicherbehälter wird verwendet. • Gesperrt: Der Speicherbehälter ist gesperrt.	Zeichenfolge
SpeicherkontainerID	Die eindeutige ID des Speicherbehälters.	UUID
TargetSecret	Der CHAP-Authentifizierungsschlüssel für das Ziel, das dem Speichercontainer zugeordnet ist.	Zeichenfolge
VirtuellesVolumes	Eine Liste der IDs der virtuellen Volumes, die dem Speichercontainer zugeordnet sind.	UUID-Array

Weitere Informationen

ListStorageContainer

SyncJob

Das syncJob-Objekt enthält Informationen zu Klon-, Remote-Replikation- oder Slice-Synchronisierungsjobs, die auf einem Cluster ausgeführt werden.

Sie können Synchronisierungsinformationen mit dem abrufen `ListSyncJobs` API-Methode.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
BlockenPerSecond	Die Anzahl der Datenblöcke, die pro Sekunde vom Quell-Cluster zum Ziel-Cluster übertragen werden. Nur vorhanden, wenn das Typmitglied auf Remote gesetzt ist.	Ganzzahl

Name	Beschreibung	Typ
BranchType	Dieser Wert wird nur für Synchronisierungsaufträge mit Remote-Replikation zurückgegeben. Mögliche Werte: • snapshot • Datenmenge	Zeichenfolge
Von: Persezweite	Die Anzahl der Bytes, die der Klon pro Sekunde verarbeitet. Nur vorhanden, wenn das Typenelement auf Klonen oder Slice eingestellt ist.	Schweben
KlonID	Die ID des Klonvorgangs, der gerade ausgeführt wird. Nur vorhanden, wenn das Typmitglied auf Klon gesetzt ist.	Ganzzahl
CurrentBytes	Die Anzahl der Bytes, die der Klon im Quell-Volume verarbeitet hat. Nur vorhanden, wenn das Typenelement auf Klonen oder Slice eingestellt ist.	Ganzzahl
DstService-ID	Die Service-ID, die das primäre Replikat für das Volume hostet. Nur vorhanden, wenn das Typmitglied auf Remote gesetzt ist.	Ganzzahl
DstVolumeID	Die Ziel-Volume-ID. Nur vorhanden, wenn das Typmitglied auf Clone oder Remote gesetzt ist.	Ganzzahl
Verstrichene Zeit	Die verstrichene Zeit in Sekunden seit dem Start des Synchronisierungsjobs.	Float oder Integer abhängig von der Art des Synchronisierungsvorgangs
GroupCloneID	Die ID des Gruppenklonvorgangs, der gerade ausgeführt wird.	Ganzzahl
NodeID	Gibt den Node an, auf dem der Klon ausgeführt wird. Nur vorhanden, wenn das Typmitglied auf Klon gesetzt ist.	Ganzzahl

Name	Beschreibung	Typ
%Kompletete	Der Prozentsatz des Synchronisierungsauftrags.	Float oder Integer abhängig von der Art des Synchronisierungsvorgangs
RestiningTime	Die geschätzte Zeit in Sekunden, um den Vorgang abzuschließen.	Schweben
SliceID	Die ID des zu synchronisierenden Slice-Laufwerks.	Ganzzahl
Stufe	Nur vorhanden, wenn das Typmitglied auf Remote oder Clone eingestellt ist. Mögliche Werte: • Metadaten: Die Replizierung bestimmt gerade, welche Daten an das Remote-Cluster übertragen werden müssen. Für diese Phase des Replikationsprozesses wird kein Status gemeldet. • Daten: Bei der Replizierung wird der Großteil der Daten auf das Remote-Cluster übertragen. • Ganz: Zeigt die Abwärtskompatibilität des Slice für Slice-Sync-Jobs an.	Zeichenfolge
Snapshot-ID	Die ID des Snapshot, aus dem der Klon erstellt wurde. Nur vorhanden, wenn das Typmitglied auf Klon gesetzt ist.	Ganzzahl
SrcService-ID	Die Quell-Service-ID.	Ganzzahl
SrcVolumeID	Die ID des Quell-Volume.	Ganzzahl
Insgesamt Bytes	Die Gesamtzahl der Bytes des Klons. Nur vorhanden, wenn das Typenelement auf Klonen oder Slice eingestellt ist.	Ganzzahl

Name	Beschreibung	Typ
Typ	Typ des Synchronisierungsvorgangs. Mögliche Werte: • Klon • Schneiden • Block-Storage • Remote	Zeichenfolge

Weitere Informationen

ListSyncJobs

Aufgabe (virtuelle Volumes)

Das Task-Objekt enthält Informationen über eine Aufgabe, die derzeit ausgeführt oder abgeschlossen ist, eines virtuellen Volumes im System. Sie können das verwenden `ListVirtualVolumeTasks` Methode zum Abrufen dieser Informationen für alle Aufgaben des virtuellen Volumes.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Storniert	Gibt an, ob die Aufgabe abgebrochen wurde oder nicht. Mögliche Werte: • Richtig • Falsch	boolesch
KlonVirtualVolumeID	Die eindeutige virtuelle Volume-ID des zu klonenden virtuellen Volumes (für Klonaufgaben).	UUID
ParentMetadaten	Ein Objekt mit Metadaten des übergeordneten Objekts für Aufgaben, die Snapshots eines virtuellen Volumes klonen oder erstellen.	JSON-Objekt

Name	Beschreibung	Typ
ParentTotalSize	Der insgesamt verfügbare Speicherplatz (in Byte) auf dem übergeordneten Objekt für Klon- oder Snapshot-Aufgaben.	Ganzzahl
ParentNutzungGröße	Der verwendete Speicherplatz des übergeordneten Objekts (in Byte) für Klon- oder Snapshot-Aufgaben.	Ganzzahl
Betrieb	Die Art der Operation, die die Aufgabe ausführt. Mögliche Werte: • Unbekannt: Der Task-Vorgang ist unbekannt. • Vorbereitung: Die Aufgabe bereitet ein virtuelles Volume vor. • snapshot: Die Aufgabe ist, einen Snapshot eines virtuellen Volumes zu erstellen. • Rollback: Die Aufgabe erstellt ein Rollback eines virtuellen Volumes auf einen Snapshot. • Klon: Die Aufgabe ist es, einen Klon des virtuellen Volumes zu erstellen. • FastClone: Die Aufgabe ist die Erstellung eines schnellen Klons eines virtuellen Volumes. • CopyDiffs: Die Aufgabe kopiert unterschiedliche Blöcke in ein virtuelles Volume.	Zeichenfolge
Status	Der aktuelle Status der Aufgabe für das virtuelle Volume. Mögliche Werte: • Fehler: Die Aufgabe ist fehlgeschlagen und gibt einen Fehler zurück. • Warteschlange: Die Aufgabe wartet auf die Ausführung. • Wird ausgeführt: Die Aufgabe wird gerade ausgeführt. • Erfolgreich: Die Aufgabe wurde erfolgreich abgeschlossen.	Zeichenfolge

Name	Beschreibung	Typ
VirtualVolumeHost ID	Die eindeutige ID des Hosts, der die Aufgabe gestartet hat.	UUID
VirtualVolumeID	Die neue, eindeutige ID des virtuellen Volumes (für Aufgaben, die ein neues virtuelles Volume erstellen).	UUID
VirtualVolumeTaskID	Die eindeutige ID der Aufgabe.	UUID

Weitere Informationen

ListVirtualVolumeTasks

UsmUser

Sie können das SNMP usmUser-Objekt mit dem verwenden `SetSnmpInfo` API-Methode zum Konfigurieren von SNMP auf dem Storage-Cluster.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Datenzugriff	Der Typ des SNMP-Zugriffs für diesen Benutzer. Mögliche Werte: • Rouser: Schreibgeschützter Zugriff. • Rwuser: Lese-Schreib-Zugriff. Alle Element Software MIB-Objekte sind schreibgeschützt.	Zeichenfolge
Name	Der Name des Benutzers.	Zeichenfolge
Passwort	Das Kennwort des Benutzers.	Zeichenfolge
Passphrase	Die Passphrase des Benutzers.	Zeichenfolge

Name	Beschreibung	Typ
SecLevel	Der für diesen Benutzer erforderliche Benutzeranmeldungstyp. Mögliche Werte: • Hinweis: Es ist kein Passwort oder eine Passphrase erforderlich. • Auth: Für den Benutzerzugriff ist ein Passwort erforderlich. • priv: Für den Benutzerzugriff sind ein Passwort und eine Passphrase erforderlich.	Zeichenfolge

Weitere Informationen

SetSnmpInfo

VirtualNetwork

Das VirtualNetwork-Objekt enthält Informationen über ein bestimmtes virtuelles Netzwerk. Sie können das verwenden `ListVirtualNetworks` API-Methode zum Abrufen einer Liste dieser Informationen für alle virtuellen Netzwerke im System.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
AdressenSperren	Der Bereich der Adressblöcke, die derzeit dem virtuellen Netzwerk zugewiesen sind. Mitglieder: • Verfügbar: Binäre Zeichenfolge in "1"s und "0"s. „1“ bedeutet, dass die IP-Adresse verfügbar ist und „0“ bedeutet, dass die IP nicht verfügbar ist. Die Zeichenfolge wird von rechts nach links gelesen, wobei die Ziffer ganz rechts die erste IP-Adresse in der Liste der Adressblöcke ist. • Größe: Die Größe dieses Adressblocks. • Start: Die erste IP-Adresse im Block.	JSON-Objekt-Array

Name	Beschreibung	Typ
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt
Name	Der Name, der dem virtuellen Netzwerk zugewiesen ist.	Zeichenfolge
Netzmaske	Die IP-Adresse der Netzmaske für das virtuelle Netzwerk.	Zeichenfolge
svip	Die Speicher-IP-Adresse für das virtuelle Netzwerk.	Zeichenfolge
Gateway	Das Gateway, das für das virtuelle Netzwerk verwendet wird.	Zeichenfolge
VirtualNetworkID	Die eindeutige Kennung für ein virtuelles Netzwerk.	Ganzzahl
VirtualNetworkTag	Die VLAN-Tag-ID.	Ganzzahl

Weitere Informationen

ListVirtualNetworks

VirtualVolume

Das virtualVolume-Objekt enthält Konfigurationsinformationen über ein virtuelles Volume sowie Informationen über Snapshots des virtuellen Volumes. Sie enthält keine Laufzeit- oder Nutzungsinformationen. Sie können das verwenden `ListVirtualVolumes` Methode zum Abrufen dieser Informationen für ein Cluster.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Bindungen	Eine Liste der Binding-IDs für dieses virtuelle Volume.	UUID-Array
Kinder	Eine Liste der virtuellen Volume-UUIDs, die Kinder dieses virtuellen Volumes sind.	UUID-Array

Name	Beschreibung	Typ
Nachfahren	Wenn Sie rekursive: True zur Methode ListVirtualVolumes übergeben, enthält eine Liste der UIDs des virtuellen Volumes, die Nachfahren dieses virtuellen Volumes sind.	UUID-Array
Metadaten	Schlüsselwertpaare der Metadaten des virtuellen Volume, wie z. B. der Typ des virtuellen Volume, der Typ des Gast-Betriebssystems usw.	JSON-Objekt
ParentVirtualVolumeID	Die ID des virtuellen Volume des übergeordneten virtuellen Volumes. Wenn die ID null ist, ist dies ein unabhängiges virtuelles Volume ohne Link zu einem übergeordneten Volume.	UUID
Snapshot-ID	Die ID des zugrunde liegenden Volume-Snapshots. Dieser Wert ist „0“, wenn das virtuelle Volume keinen Snapshot darstellt.	Ganzzahl
SnapshotInfo	Das Snapshot-Objekt für den zugeordneten Snapshot (Null, wenn nicht ixestent).	snapshot
Status	Aktueller Status des virtuellen Volume. Mögliche Werte: • Klonen: Das virtuelle Volume wird als Antwort auf einen Klon- oder Snapshot-Vorgang verarbeitet. • Warten: Das virtuelle Volume wartet auf den Abschluss eines Snapshot-Vorgangs. • Bereit: Das virtuelle Volume ist für den allgemeinen Gebrauch bereit.	Zeichenfolge
Storage Container	Ein Objekt, das den Storage-Container beschreibt, der Eigentümer dieses virtuellen Volume ist.	Storage Container

Name	Beschreibung	Typ
VirtualVolumeID	Die eindeutige ID des virtuellen Volumes.	UUID
VirtualVolumeType	Der Typ des virtuellen Volume.	Zeichenfolge
VolumeID	Die ID des zugrunde liegenden Volumes.	Ganzzahl
VolumeInfo	Wenn Sie Details übergeben: Wahr zur ListVirtualVolumes-Methode, ist dieses Mitglied ein Objekt, das das Volume beschreibt.	Datenmenge

Weitere Informationen

- ListVirtualVolumes
- snapshot
- Storage Container
- Datenmenge

Datenmenge

Das Volume-Objekt enthält Konfigurationsinformationen über nicht gepaarte oder gepaarte Volumes. Sie enthält keine Laufzeitinformationen oder Nutzungsinformationen und enthält keine Informationen über virtuelle Volumes.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Datenzugriff	Der für das Volume zulässige Zugriffstyp. Mögliche Werte: • `readOnly`: Nur Leseoperationen sind erlaubt. • `readWrite`: Lesen und Schreiben sind erlaubt. • `locked`: Es sind keine Lese- oder Schreibvorgänge zulässig. • `replicationTarget`: Als Zielvolumen in einem replizierten Volume-Paar bestimmt.	Zeichenfolge

Name	Beschreibung	Typ
AccountID	Die AccountID des Kontos, der das Volumen enthält.	Ganzzahl
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt
Blocksize	Die Größe von Blöcken auf dem Volume.	Ganzzahl
CreateTime	Die UTC+0-formatierte Zeit, zu der das Volume erstellt wurde.	ISO 8601-Zeichenfolge
AktuellenSchutzschema	Das Schutzschema, das für dieses Volumen verwendet wird. Wenn ein Volumen von einem Schutzschema in ein anderes konvertiert wird, spiegelt dieses Mitglied das Schutzschema wider, in das das Volumen konvertiert wird.	Zeichenfolge
DeleteTime	Die UTC+0-formatierte Zeit, zu der das Volume gelöscht wurde.	ISO 8601-Zeichenfolge
Able512e	Wenn auf „true“ gesetzt ist, bietet das Volume 512-Byte-Sektoremulation.	boolesch
AbleSnapMirrorReplication	Gibt an, ob das Volume für die Replizierung mit SnapMirror Endpunkten verwendet werden kann.	boolesch
FifoGröße	Gibt die maximale Anzahl der Snapshots des zu pflegenden Volumes an, wenn der First-in-First-Out (FIFO)-Snapshot-Aufbewahrungsmodus verwendet wird.	Ganzzahl
iqn	Der qualifizierte iSCSI-Name des Volumes.	Zeichenfolge
LastAccessTime	Das letzte Mal, wenn ein Zugriff (einschließlich I/O) auf das Volume auftrat (formatiert als UTC+0). Wenn die letzte Zugriffszeit nicht bekannt ist, ist dieser Wert Null.	ISO 8601-Zeichenfolge

Name	Beschreibung	Typ
LastAccessTimeIO	Das letzte Mal, wenn ein I/O zum Volume aufgetreten ist (formatiert als UTC+0). Wenn die letzte Zugriffszeit nicht bekannt ist, ist dieser Wert Null.	ISO 8601-Zeichenfolge
Min50 Größe	Gibt die Mindestanzahl der FIFO-Snapshot-Steckplätze an, die gleichzeitig vom Volume reserviert wurden, wenn der FIFO-Modus (First in First-Out) für die Snapshot-Aufbewahrung verwendet wird.	Ganzzahl
Name	Der Name des Volumes, der bei der Erstellung angegeben wurde.	Zeichenfolge
Zurückgewinnungsschema	Wenn ein Volumen von einem Schutzschema in ein anderes konvertiert wird, spiegelt dieses Mitglied das Schutzschema wider, aus dem das Volumen konvertiert wird. Dieses Mitglied ändert sich erst, wenn eine Konvertierung gestartet wird. Wenn ein Volume noch nie konvertiert wurde, ist dieses Mitglied null.	Zeichenfolge
PurgeTime	Die UTC+0-formatierte Zeit, zu der das Volume aus dem System gelöscht wurde.	ISO 8601-Zeichenfolge
qos	Die Quality-of-Service-Einstellungen für dieses Volume.	QoS
QosPolicyID	Die dem Volume zugeordnete QoS-Richtlinien-ID. Der Wert ist null, wenn das Volume nicht einer Richtlinie zugeordnet ist.	Ganzzahl
ScsiEUIDeviceID	Weltweit eindeutige SCSI-Gerätekennung für das Volume im 16-Byte-Format auf Basis von EUI-64.	Zeichenfolge
ScsiNAADeviceID	Weltweit eindeutige SCSI-Gerätekennung für das Volume im NAA IEEE-Registered Extended-Format.	Zeichenfolge

Name	Beschreibung	Typ
SliceCount	Die Anzahl der Schichten auf dem Volumen. Dieser Wert ist immer „1“.	Ganzzahl
Status	Der aktuelle Status des Volumes. Mögliche Werte: • Init: Ein Volume, das initialisiert wird und nicht für Verbindungen bereit ist. • Aktiv: Ein aktives Volume, das für Verbindungen bereit ist. • Gelöscht: Ein Volume, das zum Löschen markiert, aber noch nicht gelöscht wurde.	Zeichenfolge
Summengröße	Die bereitgestellten Gesamtbyte Kapazität.	Ganzzahl
VirtualVolumeID	Die eindeutige ID des virtuellen Volumes, die dem Volume zugeordnet ist, falls vorhanden.	UUID
VolumeAccessGroups	Liste der IDs Pf Volume Zugriffsgruppen, zu denen ein Volume gehört. Dieser Wert ist eine leere Liste, wenn ein Volume keiner Volume-Zugriffsgruppe angehört.	Integer-Array
VolumeConsistencyGroupUUID	Die universell eindeutige ID der Volume-Konsistenzgruppe, deren Mitglied das Volume ist.	UUID
VolumeID	Spezielle VolumeID für das Volume	Ganzzahl
Volumepaar	Informationen zu einem gepaarten Volume. Nur sichtbar, wenn ein Volume gekoppelt ist. Dieser Wert ist eine leere Liste, wenn das Volume nicht gekoppelt ist.	Volumepaar Array erledigen
VolumeUUID	Die universell eindeutige ID des Volumens.	UUID

Weitere Informationen

- ListeActiveVolumes

- ListDeletedVolumes
- ListVolumes
- ListVolumesForAccount
- QoS

VolumeAccessGroup

Das Volume AccessGroup-Objekt enthält Informationen über eine bestimmte Volume-Zugriffsgruppe. Mit der API-Methode können Sie eine Liste dieser Informationen für alle Zugriffsgruppen abrufen `ListVolumeAccessGroups`.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt
DeletedVolumes	Array von Volumes, die aus der Zugriffsgruppe des Volumes gelöscht wurden, die noch nicht aus dem System gelöscht wurden.	Integer-Array
InitiatorIDs	Eine Liste der IDs von Initiatoren, die der Volume-Zugriffsgruppe zugeordnet sind.	Integer-Array
Initiatoren	Array eindeutiger IQN/WWPN-Initiatoren, die der Volume-Zugriffsgruppe zugeordnet sind.	String-Array
Name	Name der Zugriffsgruppe für Volumes.	Zeichenfolge
VolumeAccessGroupID	Eindeutige VolumeAccessGroupID-ID für die Volume Access Group.	Ganzzahl
Volumes	Eine Liste der VolumeIDs, die zur Zugriffsgruppe des Volumes gehören.	Integer-Array

Weitere Informationen

ListVolumeAccessGroups

Volumepaar

Das VolumePair Objekt enthält Informationen zu einem Volume, das mit einem anderen Volume in einem anderen Cluster kombiniert wird. Wenn das Volume nicht gekoppelt ist, ist dieses Objekt leer. Sie können das verwenden `ListActivePairedVolumes` Und `ListActiveVolumes` API-Methoden zur Rückgabe von Informationen über gepaarte Volumes.

Objektmitglieder verwenden

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Typ
ClusterPairID	Den Cluster, auf dem das Volume gekoppelt ist.	Ganzzahl
RemoteReplication	Details zur Volume-Replizierung. Mitglieder: • Modus: (String) einer von "Async", "Sync" oder "SnapshotsOnly". • PauseLimit: (Integer) nur für den internen Gebrauch. • EntfernungServiceID: (Integer) die Service-ID der Remote-Schicht. • ResumeDetails: (String) reserviert für zukünftige Verwendung. • Snapshot Replication (JSON-Objekt) ◦ Status: (String) der Status der laufenden Snapshot-Replikation, wenn einer gerade läuft. ◦ StatusDetails: (String) reserviert für zukünftige Verwendung. • Status: (String) der Status der Volume-Replikation. • StatusDetails: (String) reserviert für zukünftige Verwendung.	JSON-Objekt
EntfernungSliceID	Die Cluster-definierte Slice-ID im Remote-Cluster.	Ganzzahl

Name	Beschreibung	Typ
EntferntVolumeID	Die ID des Volumes auf dem Remote-Cluster, mit dem das lokale Volume gekoppelt ist.	Ganzzahl
Remote VolumeName	Der Name des Remote-Volumes.	Zeichenfolge
VolumePairUUID	Eine universell eindeutige, Cluster-definierte Kennung für diese Paarung im kanonischen Format.	Zeichenfolge

Weitere Informationen

- ListeActivePairedVolumes
- ListeActiveVolumes

VolumeStatistik

Das VolumeStats-Objekt enthält statistische Daten eines einzelnen Volumes.

Objektmitglieder verwenden

Mithilfe der folgenden Methoden können Sie VolumeStats-Objekte für einige oder alle Volumes abrufen:

- GetVolumeStats
- ListVolumeStatsByKonto
- ListVolumeStatsByVolume
- ListVolumeStatsByVolumeAccessGroup

Dieses Objekt enthält die folgenden Mitglieder:

Name	Beschreibung	Berechnung	Typ
AccountID	Die ID des Kontos des Volume-Inhabers.	1. A.	Ganzzahl
AktualIOPS	Der aktuelle tatsächliche IOPS für das Volume in den letzten 500 Millisekunden.	Zeitpunktgenau	Ganzzahl
Asynchron	Die Zeitspanne, seit das Volume zuletzt mit dem Remote-Cluster synchronisiert wurde. Wenn das Volume nicht gekoppelt ist, ist dieser Wert Null. **Hinweis:** Ein Zielvolumen in einem aktiven Replikationszustand hat immer einen Async von 0 (Null). Ziel-Volumes erkennen sich während der Replizierung systemorientiert und angenommen, dass Async Delay zu jeder Zeit korrekt ist.	1. A.	ISO 8601 Duration String oder Null

Name	Beschreibung	Berechnung	Typ
MittelungIOPSize	Die durchschnittliche Größe in Byte der letzten I/O-Vorgänge für das Volume in den letzten 500 Millisekunden.	Zeitpunktgenau	Ganzzahl
BurstIOPSCredit	Die Gesamtanzahl der IOP-Gutschriften, die dem Benutzer zur Verfügung stehen. Wenn Volumes nicht bis zu dem konfigurierten IOPS-Maxima nutzen, werden Gutschriften angesammelt.	1. A.	Ganzzahl
ClientQueueDepth	Die Anzahl der ausstehenden Lese- und Schreibvorgänge auf dem Volume.	1. A.	Ganzzahl
DesiredMetadataHosts	Die Metadaten-Services (Slice), auf die migriert werden, wenn die Volume-Metadaten zwischen den Metadaten-Services migriert werden. Ein Wert von „null“ bedeutet, dass das Volume nicht migriert wird.	1. A.	JSON-Objekt
LaticyUSec	Der durchschnittliche Zeitaufwand in Mikrosekunden, um den Betrieb des Volumes in den letzten 500 Millisekunden abzuschließen. Ein Wert von „0“ (Null) bedeutet, dass kein I/O für das Volume vorhanden ist.	Zeitpunktgenau	Ganzzahl
MetadataHosts	Die Metadaten-Services (Slice), auf denen sich die Volume-Metadaten befinden. Mögliche Werte: • Primär: Die primären Metadaten-Services, die das Volume hosten • Zweitens: Sekundäre Metadaten-Services, die sich derzeit in einem „live“ Zustand befinden. • Zweiergebiete: Sekundäre Metadaten-Dienste, die sich in einem toten Zustand befinden.	1. A.	JSON-Objekt
NormalisiertIOPS	Durchschnittliche IOPS-Anzahl des gesamten Clusters in den letzten 500 Millisekunden.	Zeitpunktgenau	Ganzzahl
Nicht ZeroBlocks	Die Gesamtzahl der 4KiB-Blöcke, die Daten enthalten, nachdem der letzte Speichervorgang abgeschlossen ist.	1. A.	Ganzzahl
ReadBytes	Die insgesamt angesammelten Bytes, die vom Volume seit der Erstellung des Volumes gelesen werden.	Monotonisch zunehmende Zahl	Ganzzahl
LesBytesLastBeispiel	Die Gesamtzahl der Bytes, die während des letzten Probenzeitraums aus dem Volumen gelesen wurden.	Zeitpunktgenau	Ganzzahl

Name	Beschreibung	Berechnung	Typ
ReadLatencyUSec	Die durchschnittliche Zeit in Mikrosekunden, um Lesevorgänge in dem Volume in den letzten 500 Millisekunden abzuschließen.	Zeitpunktgenau	Ganzzahl
ReadLatencyUSecTotal	Die Gesamtzeit, die für die Durchführung von Leseoperationen vom Volume aufgewendet wurde.	Monotonisch zunehmende Zahl	Ganzzahl
ReadOps	Die gesamten Lesevorgänge auf dem Volume seit der Erstellung des Volumes.	Monotonisch zunehmende Zahl	Ganzzahl
LesesOpsLastSample	Die Gesamtzahl der Leseoperationen während des letzten Probenzeitraums.	Zeitpunktgenau	Ganzzahl
SamplePeriodMSec	Die Länge des Probenzeitraums in Millisekunden.	1. A.	Ganzzahl

Name	Beschreibung	Berechnung	Typ
SliceIopsStats	Die Statistiken zur I/O-Nutzung für ein Volume. Verfügbar ab Element 12.8. Mögliche Werte für sliceIopsStats: • LargeStatistics: Die I/O-Statistiken für das Volumen, die über einen längeren Zeitraum gemessen werden, in der Regel die letzten 24 Stunden. • SmallStatistics: Die I/O-Statistiken für das Volumen, die über einen kürzeren Zeitraum gemessen werden, in der Regel in der letzten Stunde. Mögliche Werte für largeStatistics und smallStatistics: • AverageReadIops: Die durchschnittlichen Lese-IOPS für das Volume. • AverageTotalIops: Die durchschnittliche Summe (lesen + schreiben) IOPS für das Volume. • AverageWriteIops: Die durchschnittlichen Schreib-IOPS für das Volume. • NSamples: Die Anzahl der Proben, die in der statistischen Berechnung enthalten sind. • PeakReadIops: Die maximale Lese-IOPS, die über ein statistisches Intervall beobachtet werden. • PeakTotalIops: Die maximale Summe der über ein statistisches Intervall beobachteten IOPS. • PeakWriteIops: Die maximale Anzahl der über ein statistisches Intervall beobachteten Schreib-IOPS. • SliceID: Volume-ID oder Slice-ID	Zeitpunktgenau	JSON-Objekt
Drosselklappe	Ein schwebender Wert zwischen 0 und 1, der zeigt, wie viel das System die Clients unter ihre IOPS-Maxime drosselt, da Daten, transiente Fehler und erzeugte Snapshots neu repliziert werden.	1. A.	Schweben
Zeitstempel	Die aktuelle Zeit im UTC+0-Format.	1. A.	ISO 8601-Datumszeichenfolge
UnalignedReads	Die gesamten, kumulativen, nicht ausgerichteten Lesevorgänge an einem Volume seit der Erstellung des Volumes.	Monotonisch zunehmende Zahl	Ganzzahl

Name	Beschreibung	Berechnung	Typ
UnalignedWrites	Die insgesamt kumulativen, nicht ausgerichteten Schreibvorgänge werden seit der Erstellung des Volumes durchgeführt.	Monotonisch zunehmende Zahl	Ganzzahl
VolumeAccessGroups	Liste der IDs der Volume-Zugriffsgruppen, der ein Volume angehört.	1. A.	Integer-Array
VolumeID	Die ID des Volume.	1. A.	Ganzzahl
Volume-Größe	Insgesamt bereitgestellte Kapazität in Byte.	1. A.	Ganzzahl
VolumeUtilisation	Ein Gleitkommwert, der beschreibt, wie vollständig der Client die ein-/Ausgabe-Funktionen des Volume im Vergleich zur maxIOPS QoS-Einstellung für dieses Volume nutzt. Mögliche Werte: • 0: Der Client verwendet das Volume nicht. • 0.01 zu 0.99: Der Client nutzt die IOPS-Fähigkeiten des Volumes nicht vollständig. • 1.00: Der Client nutzt das Volume bis zu dem IOPS-Limit, das durch die Einstellung von maxIOPS festgelegt wird. • > 1.00: Der Client nutzt mehr als das von maxIOPS festgelegte Limit. Dies ist möglich, wenn die QoS-Einstellung burstIOPS über dem Wert für max. IOPS festgelegt wird. Wenn beispielsweise „maxIOPS“ auf 1000 festgelegt und dann „burstIOPS“ auf 2000 festgelegt ist, wird das angezeigt `volumeUtilization` Der Wert wäre 2.00, wenn der Client das Volume voll nutzt.	1. A.	Schweben
WriteBytes	Die Gesamtmenge an kumulativen Bytes, die seit der Erstellung des Volumes auf das Volume geschrieben wurden.	Monotonisch zunehmende Zahl	Ganzzahl
WriteBytesLastSample	Die Gesamtzahl der Bytes, die im letzten Probenzeitraum auf das Volumen geschrieben wurden.	Monotonisch zunehmende Zahl	Ganzzahl
Write LatencyUSec	Der durchschnittliche Zeitaufwand in Mikrosekunden, um Schreibvorgänge in einem Volume in den letzten 500 Millisekunden abzuschließen.	Zeitpunktgenau	Ganzzahl
WriteLatencyUSecTotal	Die Gesamtzeit, die für die Durchführung von Schreibvorgängen auf das Volume aufgewendet wurde.	Monotonisch zunehmende Zahl	Ganzzahl

Name	Beschreibung	Berechnung	Typ
Schreiboperationen	Die kumulierten Schreibvorgänge insgesamt auf das Volume seit der Erstellung des Volumes.	Monotonisch zunehmende Zahl	Ganzzahl
WriteOpsLastSample	Die Gesamtzahl der Schreibvorgänge im letzten Probenzeitraum.	Zeitpunktgenau	Ganzzahl
ZeroBlocks	Die Gesamtzahl der leeren 4KiB-Blöcke ohne Daten, nachdem die letzte Runde der Müllsammlung abgeschlossen ist.	Zeitpunktgenau	Ganzzahl

Gängige Methoden

GetAPI

Sie können das verwenden `GetAPI` Methode zum Abrufen einer Liste aller API-Methoden und unterstützten API-Endpunkte, die im System verwendet werden können.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
<Version>	Eine Liste aller unterstützten API-Methoden für diese Softwareversion, wobei <Version> die aktuelle Softwareversion ist, auf der dieses System ausgeführt wird.	String-Array
CurrentVersion	Die aktuelle Version der Storage-Cluster-Software.	Zeichenfolge
UnterstützungVersions	Eine Liste aller vom System unterstützten API-Endpunkte.	String-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetAPI",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"id": 1,
    "result": {
        "12.0": [
            "AbortSnapMirrorRelationship",
            "AddAccount",
            "AddClusterAdmin",
            "AddDrives",
            "AddIdpClusterAdmin",
            "AddInitiatorsToVolumeAccessGroup",
            "AddKeyServerToProviderKmip",
            "AddLdapClusterAdmin",
            "AddNodes",
            "AddVirtualNetwork",
            "AddVolumesToVolumeAccessGroup",
            "BreakSnapMirrorRelationship",
            "BreakSnapMirrorVolume",
            "CancelClone",
            "CancelGroupClone",
            "CheckPingOnVlan",
            "CheckProposedCluster",
            "CheckProposedNodeAdditions",
            "ClearClusterFaults",
            "CloneMultipleVolumes",
            "CloneVolume",
            "CompleteClusterPairing",
            "CompleteVolumePairing",
            "CopyVolume",
            "CreateBackupTarget",
            "CreateClusterInterfacePreference",
            "CreateClusterSupportBundle",
            "CreateGroupSnapshot",
            "CreateIdpConfiguration",
            "CreateInitiators",
            "CreateKeyProviderKmip",
```

```
            "CreateKeyServerKmip",
            "CreatePublicPrivateKeyPair",
            "CreateQoSPolicy",
            "CreateSchedule",
            "CreateSnapMirrorEndpoint",
            "CreateSnapMirrorEndpointUnmanaged",
            "CreateSnapMirrorRelationship",
            "CreateSnapMirrorVolume",
            "CreateSnapshot",
            "CreateStorageContainer",
            "CreateSupportBundle",
            "CreateVolume",
            "CreateVolumeAccessGroup",
            "DeleteAllSupportBundles",
            "DeleteAuthSession",
            "DeleteAuthSessionsByClusterAdmin",
            "DeleteAuthSessionsByUsername",
            "DeleteClusterInterfacePreference",
            "DeleteGroupSnapshot",
            "DeleteIdpConfiguration",
            "DeleteInitiators",
            "DeleteKeyProviderKmip",
            "DeleteKeyServerKmip",
            "DeleteQoSPolicy",
            "DeleteSnapMirrorEndpoints",
            "DeleteSnapMirrorRelationships",
            "DeleteSnapshot",
            "DeleteStorageContainers",
            "DeleteVolume",
            "DeleteVolumeAccessGroup",
            "DeleteVolumes",
            "DisableAutoip",
            "DisableBmcColdReset",
            "DisableClusterSsh",
            "DisableEncryptionAtRest",
            "DisableIdpAuthentication",
            "DisableLdapAuthentication",
            "DisableSnmp",
            "EnableAutoip",
            "EnableBmcColdReset",
            "EnableClusterSsh",
            "EnableEncryptionAtRest",
            "EnableFeature",
            "EnableIdpAuthentication",
            "EnableLdapAuthentication",
            "EnableSnmp",
```

```
            "GetAccountByID",
            "GetAccountByName",
            "GetAccountEfficiency",
            "GetActiveTlsCiphers",
            "GetAsyncResult",
            "GetBackupTarget",
            "GetBinAssignmentProperties",
            "GetClientCertificateSignRequest",
            "GetClusterCapacity",
            "GetClusterConfig",
            "GetClusterFullThreshold",
            "GetClusterHardwareInfo",
            "GetClusterInfo",
            "GetClusterInterfacePreference",
            "GetClusterMasterNodeID",
            "GetClusterSshInfo",
            "GetClusterState",
            "GetClusterStats",
            "GetClusterStructure",
            "GetClusterVersionInfo",
            "GetCompleteStats",
            "GetConfig",
            "GetCurrentClusterAdmin",
            "GetDefaultQoS",
            "GetDriveHardwareInfo",
            "GetDriveStats",
            "GetFeatureStatus",
            "GetFipsReport",
            "GetHardwareConfig",
            "GetHardwareInfo",
            "GetIdpAuthenticationState",
            "GetIpmiConfig",
            "GetIpmiInfo",
            "GetKeyProviderKmip",
            "GetKeyServerKmip",
            "GetLdapConfiguration",
            "GetLimits",
            "GetLldpInfo",
            "GetLoginBanner",
            "GetLoginSessionInfo",
            "GetNetworkConfig",
            "GetNetworkInterface",
            "GetNodeFipsDrivesReport",
            "GetNodeHardwareInfo",
            "GetNodeStats",
            "GetNtpInfo",
```

```
            "GetNvramInfo",
            "GetOntapVersionInfo",
            "GetOrigin",
            "GetPendingOperation",
            "GetProtectionDomainLayout",
            "GetQoSPolicy",
            "GetRawStats",
            "GetRemoteLoggingHosts",
            "GetSSLCertificate",
            "GetSchedule",
            "GetSnapMirrorClusterIdentity",
            "GetSnmpACL",
            "GetSnmpInfo",
            "GetSnmpState",
            "GetSnmpTrapInfo",
            "GetStorageContainerEfficiency",
            "GetSupportedTlsCiphers",
            "GetSystemStatus",
            "GetVirtualVolumeCount",
            "GetVolumeAccessGroupEfficiency",
            "GetVolumeAccessGroupLunAssignments",
            "GetVolumeCount",
            "GetVolumeEfficiency",
            "GetVolumeStats",
            "InitializeSnapMirrorRelationship",
            "ListAccounts",
            "ListActiveAuthSessions",
            "ListActiveNodes",
            "ListActivePairedVolumes",
            "ListActiveVolumes",
            "ListAllNodes",
            "ListAsyncResults",
            "ListAuthSessionsByClusterAdmin",
            "ListAuthSessionsByUsername",
            "ListBackupTargets",
            "ListBulkVolumeJobs",
            "ListClusterAdmins",
            "ListClusterFaults",
            "ListClusterInterfacePreferences",
            "ListClusterPairs",
            "ListDeletedVolumes",
            "ListDriveHardware",
            "ListDriveStats",
            "ListDrives",
            "ListEvents",
            "ListFibreChannelPortInfo",
```

```
            "ListFibreChannelSessions",
            "ListGroupSnapshots",
            "ListISCSISessions",
            "ListIdpConfigurations",
            "ListInitiators",
            "ListKeyProvidersKmip",
            "ListKeyServersKmip",
            "ListNetworkInterfaces",
            "ListNodeFibreChannelPortInfo",
            "ListNodeStats",
            "ListPendingActiveNodes",
            "ListPendingNodes",
            "ListProtectionDomainLevels",
            "ListProtocolEndpoints",
            "ListQoSPolicies",
            "ListSchedules",
            "ListServices",
            "ListSnapMirrorAggregates",
            "ListSnapMirrorEndpoints",
            "ListSnapMirrorLuns",
            "ListSnapMirrorNetworkInterfaces",
            "ListSnapMirrorNodes",
            "ListSnapMirrorPolicies",
            "ListSnapMirrorRelationships",
            "ListSnapMirrorSchedules",
            "ListSnapMirrorVolumes",
            "ListSnapMirrorVservers",
            "ListSnapshots",
            "ListStorageContainers",
            "ListSyncJobs",
            "ListTests",
            "ListUtilities",
            "ListVirtualNetworks",
            "ListVirtualVolumeBindings",
            "ListVirtualVolumeHosts",
            "ListVirtualVolumeTasks",
            "ListVirtualVolumes",
            "ListVolumeAccessGroups",
            "ListVolumeStats",
            "ListVolumeStatsByAccount",
            "ListVolumeStatsByVirtualVolume",
            "ListVolumeStatsByVolume",
            "ListVolumeStatsByVolumeAccessGroup",
            "ListVolumes",
            "ListVolumesForAccount",
            "ModifyAccount",
```

```
            "ModifyBackupTarget",
            "ModifyClusterAdmin",
            "ModifyClusterFullThreshold",
            "ModifyClusterInterfacePreference",
            "ModifyGroupSnapshot",
            "ModifyInitiators",
            "ModifyKeyServerKmip",
            "ModifyQoSPolicy",
            "ModifySchedule",
            "ModifySnapMirrorEndpoint",
            "ModifySnapMirrorEndpointUnmanaged",
            "ModifySnapMirrorRelationship",
            "ModifySnapshot",
            "ModifyStorageContainer",
            "ModifyVirtualNetwork",
            "ModifyVolume",
            "ModifyVolumeAccessGroup",
            "ModifyVolumeAccessGroupLunAssignments",
            "ModifyVolumePair",
            "ModifyVolumes",
            "PurgeDeletedVolume",
            "PurgeDeletedVolumes",
            "QuiesceSnapMirrorRelationship",
            "RemoveAccount",
            "RemoveBackupTarget",
            "RemoveClusterAdmin",
            "RemoveClusterPair",
            "RemoveDrives",
            "RemoveInitiatorsFromVolumeAccessGroup",
            "RemoveKeyServerFromProviderKmip",
            "RemoveNodes",
            "RemoveSSLCertificate",
            "RemoveVirtualNetwork",
            "RemoveVolumePair",
            "RemoveVolumesFromVolumeAccessGroup",
            "ResetDrives",
            "ResetNetworkConfig",
            "ResetNode",
            "ResetSupplementalTlsCiphers",
            "RestartNetworking",
            "RestartServices",
            "RestoreDeletedVolume",
            "ResumeSnapMirrorRelationship",
            "ResyncSnapMirrorRelationship",
            "RollbackToGroupSnapshot",
            "RollbackToSnapshot",
```

```
            "SecureEraseDrives",
            "SetClusterConfig",
            "SetClusterStructure",
            "SetConfig",
            "SetDefaultQoS",
            "SetLoginBanner",
            "SetLoginSessionInfo",
            "SetNetworkConfig",
            "SetNtpInfo",
            "SetProtectionDomainLayout",
            "SetRemoteLoggingHosts",
            "SetSSLCertificate",
            "SetSnmpACL",
            "SetSnmpInfo",
            "SetSnmpTrapInfo",
            "SetSupplementalTlsCiphers",
            "Shutdown",
            "SnmpSendTestTraps",
            "StartBulkVolumeRead",
            "StartBulkVolumeWrite",
            "StartClusterPairing",
            "StartVolumePairing",
            "TestAddressAvailability",
            "TestConnectEnsemble",
            "TestConnectMvip",
            "TestConnectSvip",
            "TestDrives",
            "TestHardwareConfig",
            "TestKeyProviderKmip",
            "TestKeyServerKmip",
            "TestLdapAuthentication",
            "TestLocalConnectivity",
            "TestLocateCluster",
            "TestNetworkConfig",
            "TestPing",
            "TestRemoteConnectivity",
            "UpdateBulkVolumeStatus",
            "UpdateIdpConfiguration",
            "UpdateSnapMirrorRelationship"
        ],
        "currentVersion": "12.0",
        "supportedVersions": [
            "1.0",
            "2.0",
            "3.0",
            "4.0",
```

```
            "5.0",
            "5.1",
            "6.0",
            "7.0",
            "7.1",
            "7.2",
            "7.3",
            "7.4",
            "8.0",
            "8.1",
            "8.2",
            "8.3",
            "8.4",
            "8.5",
            "8.6",
            "8.7",
            "9.0",
            "9.1",
            "9.2",
            "9.3",
            "9.4",
            "9.5",
            "9.6",
            "10.0",
            "10.1",
            "10.2",
            "10.3",
            "10.4",
            "10.5",
            "10.6",
            "10.7",
            "11.0",
            "11.1",
            "11.3",
            "11.5",
            "11.7",
            "11.8",
            "12.0"
        ]
    }
}
```


GetAsyncResult

Verwenden Sie können `GetAsyncResult` Zum Abrufen des Ergebnisses von Asynchronous-Method-Anrufen. Manche Methodenaufrufe benötigen eine gewisse Zeit,

und sind möglicherweise nicht beendet, wenn das System die erste Antwort sendet. Um den Status oder das Ergebnis des Methodenaufrufs zu erhalten, verwenden Sie `GetAsyncResult` Um den asynchronen Handle-Wert zu erzeugen, der von der Methode zurückgegeben wird.

`GetAsyncResult` Gibt den Gesamtstatus des Vorgangs (in Bearbeitung, Abgeschlossen oder Fehler) standardmäßig zurück, aber die tatsächlich zurückgegebenen Daten für den Vorgang hängen vom ursprünglichen Methodenaufruf ab und die Rückgabedaten werden mit jeder Methode dokumentiert.

Wenn der Parameter keepResult fehlt oder falsch ist, wird Async bei der Rückgabe des Ergebnisses inaktiv und versucht später, eine Abfrage zu erstellen, die Async Handle einen Fehler zurückgibt. Sie können die Async-Handle für zukünftige Abfragen aktiv halten, indem Sie den keepResult-Parameter auf „true“ setzen.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Asynchron	Ein Wert, der vom ursprünglichen Aufruf der asynchronen Methode zurückgegeben wurde.	Ganzzahl	Keine	Ja.
KeepResult	Wenn „true“, entfernt GetAsyncResult das asynchrone Ergebnis nach der Rückgabe nicht, sodass zukünftige Anfragen an diese Async Handle möglich sind.	boolesch	Falsch	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Status	Status des Aufrufs der asynchronen Methode. Mögliche Werte: • Läuft: Die Methode läuft noch. • Abgeschlossen: Die Methode ist abgeschlossen und das Ergebnis oder der Fehler ist verfügbar.	Zeichenfolge
Ergebnis	Wenn die asynchrone Methode erfolgreich abgeschlossen wurde, ist dies das Ergebnis des asynchronen Vorgangs. Wenn der asynchrone Vorgang fehlgeschlagen ist, ist dieses Mitglied nicht vorhanden.	Zeichenfolge
Fehler	Wenn der Status abgeschlossen ist und die asynchrone Methode fehlgeschlagen ist, enthält dieses Mitglied die Fehlerdetails. Wenn der asynchrone Vorgang erfolgreich war, ist dieses Mitglied nicht vorhanden.	Zeichenfolge
Typ	Die Art des Vorgangs, den der asynchrone Methodenaufruf ausführt, ist oder wurde ausgeführt.	Zeichenfolge
Details	Wenn der Status ausgeführt wird, enthält dieses Mitglied Informationen, die für den aktuellen Vorgang der Methode relevant sind. Wenn die asynchrone Methode nicht ausgeführt wird, ist dieses Mitglied nicht vorhanden.	JSON-Objekt
CreateTime	Die Zeit, zu der die asynchrone Methode aufgerufen wurde, im UTC+0-Format.	ISO 8601-Datumszeichenfolge
LastUpdateTime	Die Zeit, zu der der Status der asynchronen Methode zuletzt im UTC+0-Format aktualisiert wurde.	ISO 8601-Datumszeichenfolge

Hinweis: der Rückgabewert von GetAsyncResult ist im Wesentlichen eine verschachtelte Version der Standard-JSON-Antwort mit einem zusätzlichen Statusfeld.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetAsyncResult",
  "params": {
      "asyncHandle" : 389
},
"id" : 1
}
```

Antwortbeispiel: Methodenfehler

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "error": {
      "code": 500,
      "message": "DBClient operation requested on a non-existent path at
[/asyncresults/1]",
      "name": "xDBNoSuchPath"
   },
   "id": 1
}
```

Wenn "Response" das JSON-Antwortobjekt aus dem GetAsyncResult-Aufruf wäre, dann würde "response.error" einem Fehler mit der GetAsyncResult-Methode selbst entsprechen (z.B. Abfrage eines nicht vorhandenen Async-Handle).

Beispiel für eine Antwort: Asynchronous Task error

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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"
   }
}
```

Die “response.result.error” würde einem Fehlerergebnis aus dem ursprünglichen Methodenaufruf entsprechen.

Antwortbeispiel: Asynchrone Aufgabe erfolgreich

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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"
   }
}
```

Die “response.result.result” ist der Rückgabewert für den ursprünglichen Methodenaufruf, wenn der Anruf erfolgreich abgeschlossen wurde.

Neu seit Version

9.6

GetCompleteStats

NetApp Engineering verwendet das `GetCompleteStats` API-Methode zum Testen neuer Funktionen. Die von zurückgegebenen Daten `GetCompleteStats` Wird nicht dokumentiert, häufig geändert und ist nicht garantiert korrekt. Sie sollten nicht verwenden `GetCompleteStats` Zum Erfassen von Performance-Daten oder anderer Managementintegration in einen Storage-Cluster mit Element Software.

Verwenden Sie die folgenden unterstützten API-Methoden, um statistische Informationen abzurufen:

- GetVolumeStats
- GetClusterStats
- GetNodeStats
- GetDriveStats

Neu seit Version

9.6

GetLimits

Sie können das verwenden `GetLimits` Methode zum Abrufen der von der API festgelegten Grenzwerte. Diese Werte können sich zwischen Versionen von Element ändern, ändern sich aber nicht ohne ein Update des Systems. Das Wissen über die von der API festgelegten Grenzwerte kann nützlich sein, wenn API-Skripte für Tools für Benutzer geschrieben werden.

Der `GetLimits` Die Methode gibt unabhängig von der zum Bestehen der Methode verwendeten API-Endpunktversion die Grenzwerte für die aktuelle Softwareversion zurück.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode gibt ein JSON-Objekt mit Name-Wert-Paaren zurück, die die API-Grenzwerte enthalten.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetLimits",
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:


```
{
    "id": 1,
    "result": {
        "accountCountMax": 5000,
        "accountNameLengthMax": 64,
        "accountNameLengthMin": 1,
        "backupTargetNameLengthMax": 64,
        "backupTargetNameLengthMin": 1,
        "bulkVolumeJobsPerNodeMax": 8,
        "bulkVolumeJobsPerVolumeMax": 2,
        "chapCredentialsCountMax": 15000,
        "cloneJobsPerNodeMax": 8,
        "cloneJobsPerVirtualVolumeMax": 8,
        "cloneJobsPerVolumeMax": 2,
        "clusterAdminAccountMax": 5000,
        "clusterAdminInfoNameLengthMax": 1024,
        "clusterAdminInfoNameLengthMin": 1,
        "clusterPairsCountMax": 4,
        "fibreChannelVolumeAccessMax": 16384,
        "initiatorAliasLengthMax": 224,
        "initiatorCountMax": 10000,
        "initiatorNameLengthMax": 224,
        "initiatorsPerVolumeAccessGroupCountMax": 128,
        "iscsiSessionsFromFibreChannelNodesMax": 4096,
        "maxAuthSessionsForCluster": 1024,
        "maxAuthSessionsPerUser": 1024,
        "nodesPerClusterCountMax": 100,
        "nodesPerClusterCountMin": 3,
        "qosPolicyCountMax": 500,
        "qosPolicyNameLengthMax": 64,
        "qosPolicyNameLengthMin": 1,
        "scheduleNameLengthMax": 244,
        "secretLengthMax": 16,
        "secretLengthMin": 12,
        "snapMirrorEndpointIPAddressesCountMax": 64,
        "snapMirrorEndpointsCountMax": 4,
        "snapMirrorLabelLengthMax": 31,
        "snapMirrorObjectAttributeValueInfoCountMax": 9900000,
        "snapshotNameLengthMax": 255,
        "snapshotsPerVolumeMax": 32,
        "storageNodesPerClusterCountMin": 2,
        "virtualVolumeCountMax": 8000,
```

```
        "virtualVolumesPerAccountCountMax": 10000,
        "volumeAccessGroupCountMax": 1000,
        "volumeAccessGroupLunMax": 16383,
        "volumeAccessGroupNameLengthMax": 64,
        "volumeAccessGroupNameLengthMin": 1,
        "volumeAccessGroupsPerInitiatorCountMax": 1,
        "volumeAccessGroupsPerVolumeCountMax": 64,
        "volumeBurstIOPSMax": 200000,
        "volumeBurstIOPSMin": 100,
        "volumeCountMax": 4000,
        "volumeMaxIOPSMax": 200000,
        "volumeMaxIOPSMin": 100,
        "volumeMinIOPSMax": 15000,
        "volumeMinIOPSMin": 50,
        "volumeNameLengthMax": 64,
        "volumeNameLengthMin": 1,
        "volumeSizeMax": 17592186044416,
        "volumeSizeMin": 1000000000,
        "volumesPerAccountCountMax": 2000,
        "volumesPerGroupSnapshotMax": 32,
        "volumesPerVolumeAccessGroupCountMax": 2000,
        "witnessNodesPerClusterCountMax": 4
    }
}
```


Neu seit Version

9.6

GetOrigin

Sie können das verwenden `GetOrigin` Methode zum Abrufen des Ursprungs-Zertifikats, für den der Knoten erstellt wurde.

Parameter

Bei dieser Methode wird „Null“ zurückgegeben, wenn keine Ausgangszertifizierung vorliegt.

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Auf diese Weise werden die Zertifizierungsinformationen des Anbieters zurückgegeben.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
 "method": "GetOrigin",
 "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "integrator": "SolidFire",
  "<signature>": {
    "pubkey": [public key info],
    "version": 1,
    "data": [signature info]
  },
   "contract-id": "none",
   "location": "Boulder, CO",
   "organization": "Engineering",
   "type": "element-x"
  }
 ]
}
```

Neu seit Version

9.6

GetRawStats

NetApp Engineering verwendet das `GetRawStats` API-Methode zum Testen neuer Funktionen. Die von zurückgegebenen Daten `GetRawStats` Wird nicht dokumentiert, häufig geändert und ist nicht garantiert korrekt. Sie sollten nicht verwenden `GetRawStats` Zum Erfassen von Performance-Daten oder anderer Managementintegration in einen Storage-Cluster mit Element Software.

Verwenden Sie die folgenden unterstützten API-Methoden, um statistische Informationen abzurufen:

- GetVolumeStats
- GetClusterStats
- GetNodeStats
- GetDriveStats

Neu seit Version

9.6

ListeAsyncResults

Verwenden Sie können `ListAsyncResults` Liste der Ergebnisse aller aktuell ausgeführten und abgeschlossenen asynchronen Methoden im System. Abfragen asynchroner Ergebnisse mit `ListAsyncResults` Läuft nicht vollständig Async ab, sondern Sie können es verwenden `GetAsyncResult` Um eine der von zurückgegebenen asynchronen Handles abzufragen `ListAsyncResults`.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Async	Eine optionale Liste der Ergebnistypen. Sie können diese Liste verwenden, um die Ergebnisse nur auf diese Arten von Operationen zu beschränken. Mögliche Werte: • DriveAdd: Operationen, bei denen das System ein Laufwerk zum Cluster fügt. • BulkVolume: Kopiervorgänge zwischen Volumes wie Backups oder Restores. • Klon: Klonvorgänge für Volumes • DriveRemoval: Vorgänge mit dem System, das Daten von einem Laufwerk kopiert, um sie aus dem Cluster zu entfernen. • RtfiPendingNode: Operationen, bei denen das System die kompatible Software auf einem Knoten installiert, bevor sie dem Cluster hinzugefügt wird.	String-Array	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Asynchrone Handles	Eine Reihe serialisierter asynchroner Methodenergebnisse.	JSON-Objekt-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListAsyncResults",
   "params": {
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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
      },
      ...]
   }
}
```

Neu seit Version

9.6

Weitere Informationen

GetAsyncResult

Account-API-Methoden

AddAccount

Verwenden Sie können `AddAccount` Um dem System ein neues Konto hinzuzufügen. Sie können diese Methode auch verwenden, um unter dem neuen Konto neue Volumes zu erstellen, während das Konto erstellt wird. Die für das Konto angegebenen CHAP-Einstellungen (Challenge-Handshake Authentication Protocol) gelten für alle Volumes, die dem Konto gehören.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`attributes`	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
`enableChap`	Gibt an, ob CHAP-Kontoanmeldeinformationen von einem Initiator für den Zugriff auf Volumes verwendet werden können.	boolesch	Richtig	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`initiatorSecret`	Der CHAP-Schlüssel, der für den Initiator verwendet werden soll. Dieses Geheimnis muss 12 bis 16 Zeichen lang sein und undurchdringlich sein. Der Initiator-CHAP-Schlüssel muss eindeutig sein und darf nicht mit dem Ziel-CHAP-Schlüssel übereinstimmen. Wenn nicht angegeben, wird ein zufälliges Geheimnis erstellt.	Zeichenfolge	Keine	Nein
`targetSecret`	Der CHAP-Schlüssel, der für das Ziel verwendet werden soll (gegenseitige CHAP-Authentifizierung). Dieses Geheimnis muss 12 bis 16 Zeichen lang sein und undurchdringlich sein. Der Ziel-CHAP-Schlüssel muss eindeutig sein und darf nicht mit dem CHAP-Schlüssel des Initiators übereinstimmen. Wenn nicht angegeben, wird ein zufälliges Geheimnis erstellt.	Zeichenfolge	Keine	Nein
`username`	Der eindeutige Benutzername für dieses Konto. (Muss 1 bis 64 Zeichen lang sein).	Zeichenfolge	Keine	Ja.

Rückgabewert

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Konto	Ein Objekt, das Informationen zum neu erstellten Konto enthält.	Konto
AccountID	Die ID des neu erstellten Kontoobjekts.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "AddAccount",
    "params": {
     "username"  : "bobsmith",
     "initiatorSecret" : "168[#5A757ru268)",
     "targetSecret" : "tlt&lt;,8TUYa7bC",
     "attributes" : {
       "billingcode" : 2345
     }
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
  }
}
```


Neu seit Version

9.6

GetAccountByID

Verwenden Sie können `GetAccountByID` Um Details zu einem bestimmten Konto zu erhalten, mit der Rechnungs-ID.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
AccountID	Die Konto-ID des Kontos, für das Informationen erhalten werden sollen.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Konto	Kontodetails:	Konto

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetAccountByID",
   "params": {
     "accountID"  : 3
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "account": {
        "attributes": {},
        "username": "account3",
        "targetSecret": "targetsecret",
        "volumes": [],
        "enableChap": true,
        "status": "active",
        "accountID": 3,
        "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
        "initiatorSecret": "initiatorsecret"
    }
}
```

Neu seit Version

9.6

GetAccountByName

Verwenden Sie können `GetAccountByName` Um Details zu einem bestimmten Konto zu erhalten, geben Sie den Benutzernamen an.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Benutzername	Benutzername für das Konto.	Zeichenfolge	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Konto	Kontodetails:	Konto

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetAccountByName",
   "params": {
     "username"  : "jimmyd"
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "account": {
        "attributes": {},
        "username": "jimmyd",
        "targetSecret": "targetsecret",
        "volumes": [],
        "enableChap": true,
        "status": "active",
        "accountID": 1,
        "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
        "initiatorSecret": "initiatorsecret"
    }
}
```

Neu seit Version

9.6

GetAccountEffizienz

Verwenden Sie können `GetAccountEfficiency` Um Effizienzstatistiken zu einem Volume-Konto zu erhalten. Diese Methode gibt nur Effizienzinformationen für das Konto zurück, das Sie als Parameter angeben.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
AccountID	Gibt das Volume-Konto an, für das Effizienzstatistiken zurückgegeben werden.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Komprimierung	Die Menge an Speicherplatz, der durch die Datenkomprimierung für alle Volumes im Konto eingespart wird Als Verhältnis angegeben, in dem ein Wert von „1“ bedeutet, dass Daten ohne Komprimierung gespeichert wurden.	Schweben
Deduplizierung	Die Menge an gespeichertem Speicherplatz, indem keine Daten für alle Volumes im Konto dupliziert werden. Als Verhältnis angegeben.	Schweben
MisingVolumes	Die Volumes, die nicht nach Effizienzdaten abgefragt werden konnten. Fehlende Volumes können durch den GC-Zyklus (Garbage Collection) verursacht werden, der weniger als eine Stunde alt ist, vorübergehend keine Netzwerkverbindung mehr besteht oder Services seit dem GC-Zyklus neu gestartet werden.	Integer-Array

Name	Beschreibung	Typ
Thin Provisioning	Das Verhältnis des belegten Speicherplatzes zum zugewiesenen Speicherplatz zum Speichern von Daten. Als Verhältnis angegeben.	Schweben
Zeitstempel	Die letzten Effizienzdaten wurden nach der Garbage Collection (GC) im UTC+0-Format erfasst.	ISO 8601-Datumszeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetAccountEfficiency",
   "params": {
     "accountID": 3
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {
       "compression": 2.020468042933262,
       "deduplication": 2.042488619119879,
       "missingVolumes": [],
       "thinProvisioning": 1.010087163391013,
       "timestamp": "2014-03-10T14:06:02Z"
   }
}
```

Neu seit Version

9.6

Listenkonten

Verwenden Sie können `ListAccounts` Um die vollständige Liste der Storage-

Mandantenkonten zu erhalten, mit optionalem Paging-Support. Element Konten ermöglichen den Zugriff auf Volumes.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
IncludeStorageContainer	Virtuelle Volume-Storage-Container sind in der Antwort standardmäßig enthalten. Wenn Sie Speichercontainer ausschließen möchten, setzen Sie auf false.	boolesch	Richtig	Nein
StartAccountID	Die AccountID wird gestartet, um die Rückgabe zu starten. Wenn mit dieser AccountID kein Konto vorhanden ist, wird das nächste Konto nach AccountID-Auftrag als Beginn der Liste verwendet. Um durch die Liste zu blättern, übergeben Sie die AccountID des letzten Kontos in der vorherigen Antwort + 1.	Ganzzahl	Keine	Nein
Grenze	Maximale Anzahl der zurückzukehrenden Kontoobjekte.	Ganzzahl	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Konten	Die Liste der Accounts.	Konto Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListAccounts",
   "params": {
     "startAccountID"  : 0,
     "limit" : 1000
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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"
    }
  ]
}
}
```

Neu seit Version

9.6

ModifyAccount

Sie können das verwenden `ModifyAccount` Methode zum Ändern eines vorhandenen Kontos.

Wenn Sie ein Konto sperren, werden alle vorhandenen Verbindungen dieses Kontos sofort beendet. Wenn Sie die CHAP-Einstellungen eines Kontos ändern, bleiben alle vorhandenen Verbindungen aktiv, und die neuen CHAP-Einstellungen werden für nachfolgende Verbindungen oder erneute Verbindungen verwendet. Um die Attribute eines Kontos zu löschen, geben Sie {} für den Attributparameter an.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
AccountID	AccountID für das zu ändernde Konto.	Ganzzahl	Keine	Ja.
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
AbleableAbtlg	Gibt an, ob CHAP-Kontoanmeldeinformationen von einem Initiator für den Zugriff auf Volumes verwendet werden können.	boolesch	Keine	Nein
InitiatorSecret	Der CHAP-Schlüssel, der für den Initiator verwendet werden soll. Dieses Geheimnis muss 12-16 Zeichen lang sein und undurchdringlich sein. Der Initiator-CHAP-Schlüssel muss eindeutig sein und darf nicht mit dem Ziel-CHAP-Schlüssel übereinstimmen.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Status	Status des Kontos. Mögliche Werte: • Aktiv: Konto ist aktiv und Verbindungen sind zulässig. • Gesperrt: Konto ist gesperrt und Verbindungen werden abgelehnt.	Zeichenfolge	Keine	Nein
TargetSecret	Der CHAP-Schlüssel, der für das Ziel verwendet werden soll (gegenseitige CHAP-Authentifizierung). Dieses Geheimnis muss 12-16 Zeichen lang sein und undurchdringlich sein. Der Ziel-CHAP-Schlüssel muss eindeutig sein und darf nicht mit dem CHAP-Schlüssel des Initiators übereinstimmen.	Zeichenfolge	Keine	Nein
Benutzername	Wird verwendet, um den mit dem Konto verknüpften Benutzernamen zu ändern. (Muss 1 bis 64 Zeichen lang sein).	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Konto	Ein Objekt, das Informationen über das geänderte Konto enthält.	Konto

Anforderungsbeispiel

Anforderungen für diese Methode sind dem folgenden Beispiel ähnlich. In diesem Beispiel werden die Attribute gelöscht, indem {} für sie angegeben wird:

```
{
   "method": "ModifyAccount",
   "params": {
     "accountID"  : 25,
     "status"   : "locked",
     "attributes" : {}
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "account": {
        "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
        "username": "user1",
        "accountID": 1,
        "volumes": [
        ],
        "enableChap": true,
        "initiatorSecret": "txz123456q890",
        "attributes": {
        },
        "status": active",
        "targetSecret": "rxe123b567890"
    }
}
```

Neu seit Version

9.6

RemoveAccount

Sie können das verwenden `RemoveAccount` Methode zum Entfernen eines vorhandenen Kontos. Sie müssen alle Volumes löschen und löschen, die dem Konto zugeordnet sind, indem Sie verwenden `DeleteVolume` Bevor Sie das Konto entfernen können. Wenn Volumes im Konto noch nicht gelöscht werden müssen, können Sie nicht

verwenden `RemoveAccount` Um das Konto zu entfernen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
AccountID	Die ID des zu entfernenden Kontos.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind dem folgenden Beispiel ähnlich.

```
{
   "method": "RemoveAccount",
   "params": {
     "accountID"  : 25
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
 "id" : 1,
 "result" : { }
}
```

Neu seit Version

9.6

Weitere Informationen

DeleteVolume

Administrator-API-Methoden

AddClusterAdmin

Sie können das verwenden `AddClusterAdmin` Methode zum Hinzufügen eines neuen Cluster-Administratorkontos. Ein Cluster-Administrator kann das Cluster mithilfe der API und der Managementtools managen. Cluster-Administratoren sind völlig getrennt und haben nichts mit standardmäßigen Mandantenkonten zu tun.

Jeder Cluster-Administrator kann auf einen Teil der API beschränkt sein. Sie sollten mehrere Cluster-Administratorkonten für verschiedene Benutzer und Applikationen verwenden. Als Best Practice empfiehlt es sich, jedem Cluster-Administrator die erforderlichen minimalen Berechtigungen zuzuweisen, wodurch sich die potenziellen Auswirkungen von Kompromissbereitschaft für Zugangsdaten verringern lassen.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Datenzugriff	Steuert, welche Methoden der Cluster Admin verwenden kann.	String-Array	Keine	Ja.
Akzepteula	Akzeptieren Sie die Endnutzer-Lizenzvereinbarung. Setzen Sie auf „true“, um dem System ein Cluster-Administratorkonto hinzuzufügen. Wenn keine Angabe erfolgt oder auf FALSE gesetzt wird, schlägt der Methodenaufruf fehl.	boolesch	Keine	Ja.
Merkmale	Liste von Name/Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
Passwort	Passwort, das für die Authentifizierung dieses Clusteradministrators verwendet wird.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Benutzername	Eindeutiger Benutzername für diesen Cluster-Administrator. Muss zwischen 1 und 1024 Zeichen lang sein.	Zeichenfolge	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Cluster-AdminID	ClusterAdminID für den neu erstellten Cluster-Administrator.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "AddClusterAdmin",
  "params": {
    "username": "joeadmin",
    "password": "68!5Aru268)$",
    "attributes": {},
    "acceptEula": true,
    "access": ["volumes", "reporting", "read"]
  },
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id":1,
  "result" : {
    "clusterAdminID": 2
   }
}
```

Neu seit Version

9.6

Weitere Informationen

Zugriffssteuerung

GetCurrentClusterAdmin

Sie können das verwenden `GetCurrentClusterAdmin` Methode zur Rückgabe von Informationen für den aktuellen primären Cluster Admin Der primäre Cluster Admin wurde beim Erstellen des Clusters erstellt.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
ClusterAdmin	Informationen über den Cluster-Administrator.	ClusterAdmin

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method": "GetCurrentClusterAdmin",
"id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"id": 1,
"result": {
    "clusterAdmin":
        "access": [
           "administrator"
        ],
         "attributes": null,
         "authMethod": "Cluster"
         "clusterAdminID": 1,
         "username": "admin"
     }
   }
}
```

Neu seit Version

10.0

GetLoginBanner

Sie können das verwenden `GetLoginBanner` Methode, um das aktuell aktive Banner für Nutzungsbedingungen zu erhalten, das Benutzer sehen, wenn sie sich bei der Element Web-Schnittstelle anmelden.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Banner	Der aktuelle Text der Nutzungsbedingungen Banner. Dieser Wert kann auch dann Text enthalten, wenn das Banner deaktiviert ist.	Zeichenfolge

Name	Beschreibung	Typ
Aktiviert	Der Status der Nutzungsbedingungen Banner. Mögliche Werte: • True: Das Banner für Nutzungsbedingungen wird bei der Anmeldung auf der Web-Schnittstelle angezeigt. • False: Das Banner für Nutzungsbedingungen wird bei der Anmeldung über das Web-Interface nicht angezeigt.	boolesch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 3411,
  "method": "GetLoginBanner",
  "params": {}
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 3411,
  "result": {
    "loginBanner": {
      "banner": "Welcome to NetApp!",
      "enabled": false
    }
  }
}
```

Neu seit Version

10.0

ListenClusteradministratoren

Sie können das verwenden `ListClusterAdmins` Die Methode, um die Liste aller

Cluster-Administratoren für den Cluster zurückzugeben.

Es können mehrere Cluster-Administratorkonten mit unterschiedlichen Berechtigungsebenen vorhanden sein. Im System kann nur ein primärer Cluster-Administrator vorhanden sein. Der primäre Clusteradministrator ist der Administrator, der beim Erstellen des Clusters erstellt wurde. LDAP-Administratoren können auch beim Einrichten eines LDAP-Systems auf dem Cluster erstellt werden.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ShowHidden	Zeigt verborgene Cluster-Administrator-Benutzer, z. B. SNMP-Admin.	boolesch	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Clusteradministratoren	Informationen zu allen Cluster- und LDAP-Administratoren, die für ein Cluster vorhanden sind	ClusterAdmin Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListClusterAdmins",
   "params": {},
    "showHidden": true
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"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"
       }
     ]
   }
}
```


Neu seit Version

9.6

ModifyClusterAdmin

Sie können das verwenden `ModifyClusterAdmin` Methode zum Ändern der Einstellungen für Cluster-Admin, LDAP-Cluster-Administrator oder IdP-Clusteradministrator (Identity Provider) von Drittanbietern. Sie können den Zugriff für das Administratorcluster-Administratorkonto nicht ändern.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Datenzugriff	Steuert, welche Methoden dieser Cluster-Administrator verwenden kann.	String-Array	Keine	Nein
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
Cluster-AdminID	ClusterAdminID für den Cluster-Administrator, den LDAP-Cluster-Administrator oder den IdP-Cluster-Administrator zum Ändern.	Ganzzahl	Keine	Ja.
Passwort	Passwort, das für die Authentifizierung dieses Clusteradministrators verwendet wird. Dieser Parameter gilt nicht für einen LDAP- oder IdP-Clusteradministrator.	Zeichenfolge	Keine	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ModifyClusterAdmin",
   "params": {
     "clusterAdminID"  : 2,
     "password"    : "7925Brc429a"
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
 "id" : 1
 "result" : { }
}
```

Neu seit Version

9.6

Weitere Informationen

Zugriffssteuerung

RemoveClusterAdmin

Sie können das verwenden `RemoveClusterAdmin` Methode zum Entfernen eines Clusteradministrators, eines LDAP-Clusteradministrators oder eines IdP-Clusteradministrators (Identity Provider) eines Drittanbieters. Sie können das „admin“-Cluster-Administratorkonto nicht entfernen.

Parameter

Wenn ein IdP-Cluster-Administrator entfernt wird, bei dem authentifizierte Sitzungen zu einem IdP-IdP eines Drittanbieters verknüpft sind, werden diese Sitzungen entweder aberkannt oder es besteht möglicherweise ein Verlust von Zugriffsrechten innerhalb der aktuellen Sitzung. Der Verlust von Zugriffsrechten hängt davon ab, ob der entfernte IdP-Cluster-Administrator einem von mehreren IdP-Cluster-Administratoren aus den SAML-Attributen eines bestimmten Benutzers zugeordnet hat. Die verbleibende Gruppe passender IdP-Cluster-Administratoren führt zu einer reduzierten Anzahl von aggregierten Zugriffsrechten. Andere Cluster-Admin-Benutzertypen werden abgemeldet, wenn ihre Cluster-Administratoren entfernt werden.

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Cluster-AdminID	ClusterAdminID für den Cluster-Admin zum Entfernen.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "RemoveClusterAdmin",
   "params": {
     "clusterAdminID"  : 2
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
 "id" : 1
 "result" : { }
}
```

Neu seit Version

9.6

SetLoginBanner

Sie können das verwenden `SetLoginBanner` Methode zum Konfigurieren des Banners für Nutzungsbedingungen, das Benutzer sehen, wenn sie sich bei der Element-Webschnittstelle anmelden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Banner	Der gewünschte Text des Banner für Nutzungsbedingungen. Die maximal zulässige Länge beträgt 4,096 Zeichen.	Zeichenfolge	Keine	Nein
Aktiviert	Der Status der Nutzungsbedingungen Banner. Mögliche Werte: • `true`: Die Nutzungsbedingungen Banner wird bei Web-Interface-Login angezeigt. • `false`: Die Nutzungsbedingungen Banner wird nicht bei Web-Interface-Login angezeigt.	boolesch	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Banner	Der aktuelle Text der Nutzungsbedingungen Banner. Dieser Wert kann auch dann Text enthalten, wenn das Banner deaktiviert ist.	Zeichenfolge

Name	Beschreibung	Typ
Aktiviert	Der Status der Nutzungsbedingungen Banner. Mögliche Werte: • True: Das Banner für Nutzungsbedingungen wird bei der Anmeldung auf der Web-Schnittstelle angezeigt. • False: Das Banner für Nutzungsbedingungen wird bei der Anmeldung über das Web-Interface nicht angezeigt.	boolesch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 3920,
  "method": "SetLoginBanner",
  "params": {
    "banner": "Welcome to NetApp!",
    "enabled": true
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 3920,
  "result": {
    "loginBanner": {
      "banner": "Welcome to NetApp!",
      "enabled": true
    }
  }
}
```

Neu seit Version

10.0

Cluster-API-Methoden

AddNodes

Sie können das verwenden `AddNodes` Methode zum Hinzufügen eines oder mehrerer neuer Nodes zu einem Cluster

Wenn beim ersten Start eines Node, der nicht konfiguriert ist, werden Sie aufgefordert, den Node zu konfigurieren. Sobald Sie den Node konfiguriert haben, wird dieser bei dem Cluster als „ausstehender Node“ registriert. Storage-Cluster, die Element Software ausführen, erstellen automatisch ein Node zur Version auf dem Cluster. Wenn Sie einen ausstehenden Node hinzufügen, enthält die Methodenantwort einen asynchronen Wert, den Sie mit der verwenden können `GetAsyncResult` Methode zum Abfragen des Status des automatischen Bildgebungsprozesses.

Der Vorgang, bei dem ein Fibre-Channel-Node hinzugefügt wird, entspricht dem Hinzufügen des Elements iSCSI-Storage-Nodes zu einem Cluster. Fibre Channel-Knoten sind im System mit einer NodeID registriert. Wenn sie zugänglich werden, werden sie in den Status „ausstehender Knoten“ versetzt. Der `ListAllNodes` Die Methode gibt die hängende NodeID für iSCSI-Knoten sowie alle Fibre-Channel-Knoten zurück, die dem Cluster hinzugefügt werden können.

Wenn Sie einem Cluster einen Knoten hinzufügen, den Sie für ein virtuelles Netzwerk konfiguriert haben, benötigt das System eine ausreichende Anzahl an virtuellen Speicher-IP-Adressen, um dem neuen Knoten eine virtuelle IP zuzuweisen. Wenn für den neuen Knoten keine virtuellen IP-Adressen verfügbar sind, wird das angezeigt `AddNode` Der Vorgang schlägt fehl. Verwenden Sie die `ModifyVirtualNetwork` Methode zum Hinzufügen weiterer Speicher-IP-Adressen zu Ihrem virtuellen Netzwerk.

Sobald Sie einen Node hinzufügen, werden alle Laufwerke des Nodes verfügbar gemacht und können über die hinzugefügt werden `AddDrives` Methode zum Erhöhen der Speicherkapazität des Clusters.

> Es kann einige Sekunden dauern, nachdem ein neuer Knoten hinzugefügt wurde, damit er gestartet und seine Laufwerke so registriert werden können, wie verfügbar.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Automatische Installation	Wenn wahr, wird beim Hinzufügen eine Rückkehr zum werkseitigen Image (RTFI) auf dem Knoten durchgeführt. Das Standardverhalten ist die Ausführung von RTFI. Wenn der `cEnableAutoInstall` Die Cluster-Konstante ist falsch, sie hat Priorität gegenüber diesem Parameter. Wenn ein Upgrade ausgeführt wird, erfolgt der RTFI-Prozess unabhängig vom Wert für diesen Parameter nicht.	boolesch	Keine	Nein
Hängende Knoten	Ausstehende NodeIDs für die Nodes, die hinzugefügt werden sollen. Sie können alle ausstehenden Knoten mit der Methode ListPendingNodes auflisten.	Integer-Array	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Automatische Installation	Gibt an, ob die hinzugefügten Nodes an das werkseitige Image zurückgegeben werden.	boolesch

Knoten	Eine Reihe von Objekten, die die vorherige „PendingNodeID“ der „nodeID“ zuordnen. Wenn Sie einen ausstehenden Node hinzufügen, auf dem eine inkompatible Softwareversion ausgeführt wird, enthält dieses Array einen Async-Handle-Wert, den Sie mit der GetAsyncResult-Methode verwenden können, um den Status des automatischen Bildgebungsprozesses abzufragen.	JSON-Objekt-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "AddNodes",
   "params": {
     "autoInstall" : true,
     "pendingNodes" : [1]
   },
   "id":1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  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"
      }
    ]
  }
}
```


Neu seit Version

9.6

Weitere Informationen

- AddDrives
- GetAsyncResult
- ListenAllNodes
- ModifyVirtualNetwork

ClearClusterStandards

Sie können das verwenden `ClearClusterFaults` Methode zum Löschen von Informationen über aktuelle und zuvor erkannte Fehler. Sowohl behobene als auch ungelöste Fehler können behoben werden.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Fehlertypen	Bestimmt die Art der zu beseitigen Fehler. Mögliche Werte: • Aktuell: Fehler, die derzeit erkannt und nicht behoben wurden. • Behoben: Fehler, die zuvor entdeckt und behoben wurden. • Alles: Sowohl aktuelle als auch gelöste Fehler. Der Fehlerstatus kann durch das Feld „`reSolved`“ des Fehlerobjekts bestimmt werden.	Zeichenfolge	Behoben	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ClearClusterFaults",
   "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
    "result" : {}
}
```

Neu seit Version

9.6

CreateClusterSchnittstellenPräferenz

Der `CreateClusterInterfacePreference` Die Methode ermöglicht in Storage-Cluster integrierte Systeme mit Element Software, um beliebige Informationen auf dem Storage-Cluster zu erstellen und zu speichern. Diese Methode ist für den internen Gebrauch bestimmt.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Name	Der Name der bevorzugten Cluster-Schnittstelle.	Zeichenfolge	Keine	Ja.
Wert	Der Wert der bevorzugten Cluster-Schnittstelle.	Zeichenfolge	Keine	Ja.

Rückgabewert

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
        "method": "CreateClusterInterfacePreference",
        "params": {
            "name": "prefname",
            "value": "testvalue"
        },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {}
}
```

Neu seit Version

11.0

DeleteClusterSchnittstellenPräferenz

Der `DeleteClusterInterfacePreference` „Method“ ermöglicht die in Storage-Cluster, auf denen Element Software ausgeführt wird, integrierte Systeme, um eine vorhandene Cluster-Schnittstellenpräferenz zu löschen. Diese Methode ist für den internen Gebrauch bestimmt.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Name	Der Name der zu löschenden Cluster-Schnittstelle.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "DeleteClusterInterfacePreference",
    "params": {
        "name": "prefname"
        },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {}
}
```

Neu seit Version

11.0

DisableFeature

Sie können die Methode verwenden `DisableFeature`, um die Funktion zu deaktivieren `VolumeLoadBalanceOnActualIOPS`. `VolumeLoadBalanceOnActualIOPS` Ist standardmäßig deaktiviert.

Wenn Sie versuchen, eine andere Funktion, z. B. VVols, zu deaktivieren, wird die folgende Fehlermeldung angezeigt:

```
{"error":{"code":500,"message":"VolumeLoadBalanceOnActualIOPS is the only feature that can be disabled","name":"xAPINotPermitted"},"id":null}
```

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Merkmal	Deaktivieren einer Cluster-Funktion. Möglicher Wert: • `VolumeLoadBalanceOnActualIOPS`: Deaktivieren Sie den Slice-Balancing auf tatsächlichen IOPS statt auf Min IOPS.	Zeichenfolge	Keine	Ja.

Rückgabewert

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DisableFeature",
    "params": {
        "feature" : "VolumeLoadBalanceOnActualIOPS"
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {}
}
```

Neu seit Version

12,8

EnableFeature

Sie können das verwenden `EnableFeature` Methode zum Aktivieren von Cluster-Funktionen wie VVols, die standardmäßig deaktiviert sind

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter.

> Bei Systemen mit Element Software 11.x funktioniert die Funktion virtueller Volumes vor oder nach dem Festlegen der Schutzdomäne-Überwachung nur auf Node-Ebene.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Merkmal	Aktivieren einer Cluster-Funktion Mögliche Werte: • `fips`: Aktivierung von FIPS 140-2-2-zertifizierter Verschlüsselung für HTTPS-Kommunikation. • `FipsDrives`: Aktivierung der FIPS 140-2-Laufwerksunterstützung für den Speicher-Cluster. • `SnapMirror`: Aktivieren Sie die SnapMirror Replikation-Cluster-Funktion. • `VolumeLoadBalanceOnActualIOPS`: Aktivieren Sie den Slice-Balancing auf tatsächlichen IOPS statt auf Min IOPS. Verfügbar ab Element 12.8. • `vvols`: Aktivieren Sie die Element Software VVols Cluster Feature.	Zeichenfolge	Keine	Ja.

Rückgabewert

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "vvols"
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {}
}
```

Neu seit Version

9.6

GetClusterCapacity

Sie können das verwenden `GetClusterCapacity` Zur Rückgabe von allgemeinen Kapazitätsmessungen für ein gesamtes Storage Cluster. Diese Methode gibt Felder zurück, mit denen Sie die Effizienzraten berechnen können, die in der Element Web UI angezeigt werden. Die Effizienzberechnungen in Skripten können verwendet werden, um die Effizienzraten für Thin Provisioning, Deduplizierung, Komprimierung und Gesamteffizienz wiederzukommen.

Effizienzberechnungen

Berechnen Sie Thin Provisioning, Deduplizierung und Komprimierung mit den folgenden Gleichungen. Diese Gleichungen gelten für Element 8.2 und höher.

- DünnProvisioningFactor = (nonZeroBlocks + NeroBlocks) / nonZeroBlocks
- DeDuplicationFactor = (nonZeroBlocks + snapshotNonZeroBlocks) / uniqueBlocks
- KompressionFactor = (uniqueBlocks * 4096) / (uniqueBlocksUsedSpace * 0.93)

Gesamteffizienzrate Berechnung

Mithilfe der folgenden Gleichung berechnen Sie die Cluster-Effizienz insgesamt anhand der Ergebnisse der Effizienzberechnungen mit Thin Provisioning, Deduplizierung und Komprimierung.

- Effizienzfaktor = thinProvisioningFactor * deDuplicationFactor * Komprimierungfaktor

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
ClusterKapazität	Kapazitätsmessungen für das Storage-Cluster	ClusterKapazität

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetClusterCapacity",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
    }
  }
}
```

Neu seit Version

9.6

GetClusterFullThreshold

Sie können das verwenden `GetClusterFullThreshold` Methode zum Anzeigen der für Cluster-Auslastungsebenen eingestellten Phasen. Bei dieser Methode werden alle Auslastungsmetriken für den Cluster angezeigt.

> Wenn ein Cluster die Error-Phase der Block-Cluster-Fülle erreicht, werden die maximalen IOPS auf allen Volumes linear auf die minimale IOPS des Volumes reduziert, wenn der Cluster der kritischen Phase nähert. So verhindert, dass der Cluster die kritische Phase der Block-Cluster-Fülle erreicht.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Blockfullness	Die aktuell berechnete Blockebene der Blockfülle des Clusters • Stage1Happy: Keine Warnungen oder Fehlerbedingungen. Entspricht dem **gesunden**-Status in der Web-UI. • Stage2Aware: Keine Warnungen oder Fehlerbedingungen. Entspricht dem **gesunden**-Status in der Web-UI. • Stage3Low: Das System kann nicht vor zwei nicht gleichzeitigen Node-Ausfällen redundante Daten schützen. Entspricht dem Status **Warnung** in der Web-Benutzeroberfläche. Sie können diesen Level in der Web-Benutzeroberfläche konfigurieren (standardmäßig löst das System diese Warnung mit einer Kapazität von 3 % unter dem Fehlerzustand aus). • Stage4kritisch: Das System kann nicht redundante Datensicherung bei einem Single Node-Ausfall bieten. Es können keine neuen Volumes oder Klone erstellt werden. Entspricht dem Status **Error** in der Element UI. • Stage5CompletelyVerbrauch: Vollständig verbraucht. Das Cluster ist schreibgeschützt und iSCSI-Verbindungen bleiben erhalten, alle Schreibvorgänge werden jedoch ausgesetzt. Entspricht dem **kritischen**-Status in der Element-UI.	Zeichenfolge
Fülle	Spiegelt die höchste Ebene der Fülle zwischen "BlockFullness" und "MetadaFullness" wider.	Zeichenfolge

Name	Beschreibung	Typ
MaxMetadaÜberProvisionFaktor	Ein Wert, der repräsentativ für die Anzahl der Zeiten ist, für die Metadaten im Verhältnis zum verfügbaren Speicherplatz überprovisioniert werden können. Wenn beispielsweise genügend Metadatenspeicherplatz vorhanden war, um 100 tib Volumes zu speichern, und diese Zahl auf 5 gesetzt wurde, könnten dann 500 tib an Volumes erstellt werden.	Ganzzahl

Name	Beschreibung	Typ
MetadataFullness	Die aktuell berechnete Metadatenfülle des Clusters. • Stage1Happy: Keine Warnungen oder Fehlerbedingungen. Entspricht dem **gesunden**-Status in der Web-UI. • Stage2Aware: Keine Warnungen oder Fehlerbedingungen. Entspricht dem **gesunden**-Status in der Web-UI. • Stage3Low: Das System kann nicht vor zwei nicht gleichzeitigen Node-Ausfällen redundante Daten schützen. Entspricht dem Status **Warnung** in der Web-Benutzeroberfläche. Sie können diesen Level in der Web-Benutzeroberfläche konfigurieren (standardmäßig löst das System diese Warnung mit einer Kapazität von 3 % unter dem Fehlerzustand aus). • Stage4kritisch: Das System kann nicht redundante Datensicherung bei einem Single Node-Ausfall bieten. Es können keine neuen Volumes oder Klone erstellt werden. Entspricht dem Status **Error** in der Element UI. • Stage5CompletelyVerbrauch: Vollständig verbraucht. Das Cluster ist schreibgeschützt und iSCSI-Verbindungen bleiben erhalten, alle Schreibvorgänge werden jedoch ausgesetzt. Entspricht dem **kritischen**-Status in der Element-UI.	Zeichenfolge
SliceReserveUsedThresholdPunkt	Fehlerbedingung. Eine Systemwarnung wird ausgelöst, wenn die reservierte Schichtauslastung größer als dieser Wert ist.	Ganzzahl

Name	Beschreibung	Typ
Stage2AwareThreshold	Bewusstseinszustand. Der für die Stufe 2 des Cluster-Schwellenwerts festgelegte Wert.	Ganzzahl
Stage2BlockThresholdBytes	Die Anzahl der Bytes, die vom Cluster verwendet werden, auf dem eine Phase 2-Bedingung bestehen soll.	Ganzzahl
Stage2MetadataThresholdBytes	Die Anzahl der Metadaten-Bytes, die vom Cluster verwendet werden, auf dem eine Bedingung für die Fülle von Phase 2 vorhanden ist.	
Stage3BlockThresholdBytes	Die Anzahl der Storage Bytes, die vom Cluster verwendet werden, an dem eine Bedingung für die Fülle von Phase 3 vorhanden sein wird.	Ganzzahl
Stage3BlockThresholdPercent	Der Prozentwert, der für Phase 3 festgelegt wurde. Bei diesem Prozentsatz wird eine Warnung im Alarmprotokoll ausgegeben.	Ganzzahl
Stage3LowThreshold	Fehlerbedingung. Der Schwellenwert, bei dem eine Systemwarnung aufgrund einer geringen Kapazität in einem Cluster erstellt wird.	Ganzzahl
Stage3MetadataThresholdBytes	Die Anzahl der Metadaten-Bytes, die vom Cluster verwendet werden, auf dem eine Bedingung für die Phase 3 der Fülle vorhanden ist.	Ganzzahl
Stage3MetadataThresholdPercent	Der Prozentwert, der für die Metadaten-Fülle von „stage3“ festgelegt wurde. Bei diesem Prozentsatz wird eine Warnung im Alarmprotokoll veröffentlicht.	Ganzzahl
Stage4BlockThresholdBytes	Die Anzahl der Storage Bytes, die vom Cluster verwendet werden, an dem eine Bedingung für die Fülle von Phase 4 vorhanden sein wird.	Ganzzahl

Name	Beschreibung	Typ
Stage4CriticalThreshold	Fehlerbedingung. Der Schwellenwert, bei dem eine Systemwarnung erstellt wird, um über eine kritisch niedrige Kapazität auf einem Cluster zu warnen.	Ganzzahl
Stage4MetadataThresholdBytes	Die Anzahl der Metadaten-Bytes, die vom Cluster verwendet werden, auf dem eine Bedingung für die Phase 4 der Fülle vorhanden ist.	Ganzzahl
Stage5BlockThresholdBytes	Die Anzahl der Speicherbyte, die vom Cluster verwendet wird, an dem eine Bedingung für die Phase 5-Fülle vorhanden sein soll.	Ganzzahl
Stage5MetadataThresholdBytes	Die Anzahl der Metadaten-Bytes, die vom Cluster verwendet werden, auf dem eine Bedingung für die Phase 5 der Fülle vorhanden ist.	Ganzzahl
Summe ClusterBytes	Die physische Kapazität des Clusters, gemessen in Byte.	Ganzzahl
SumTotalMetadaClusterBytes	Der gesamte Speicherplatz, der zum Speichern von Metadaten verwendet werden kann.	Ganzzahl
Summe - ClusterBytes	Die Anzahl der im Cluster verwendeten Storage Bytes.	Ganzzahl
SuumUseMetadataClusterBytes	Der Speicherplatz, der auf Volume-Laufwerken zum Speichern von Metadaten verwendet wird.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method" : "GetClusterFullThreshold",
   "params" : {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:


```
{
  "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
  }
}
```


Neu seit Version

9.6

Weitere Informationen

ModifyClusterFullThreshold

GetClusterHardware-Informationen

Sie können das verwenden `GetClusterHardwareInfo` Methode zum Abrufen des Hardware-Status und der Informationen für alle Fibre Channel-Knoten, iSCSI-Knoten und -Laufwerke im Cluster. Dazu gehören im Allgemeinen Hersteller, Anbieter, Versionen und weitere zugehörige Hardware-Identifikationsinformationen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Typ	Geben Sie nur eine der folgenden Arten von Hardwareinformationen in die Antwort ein. Mögliche Werte: • Laufwerke: Listet nur Laufwerksinformationen in der Antwort auf. • Knoten: Listet nur Node-Informationen in der Antwort auf. • Alle: Enthält sowohl Laufwerks- als auch Node-Informationen in der Antwort. Wenn dieser Parameter nicht angegeben wird, wird als Typ von allen angenommen.	Zeichenfolge	Alle	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
ClusterHardwareInfo	Hardwareinformationen für alle Nodes und Laufwerke im Cluster Jedes Objekt in dieser Ausgabe ist mit der Node-ID des angegebenen Node gekennzeichnet.	HardwareInfo

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetClusterHardwareInfo",
    "params": {
        "type": "all"
    },
    "id": 1
}
```

Antwortbeispiel

Aufgrund der Länge dieses Antwortbeispiels wird es in einem ergänzenden Thema dokumentiert.

Neu seit Version

9.6

Weitere Informationen

GetClusterHardware-Informationen

GetClusterInfo

Sie können das verwenden `GetClusterInfo` „Methode“, um Konfigurationsinformationen über das Cluster zurückzugeben

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
ClusterInfo	Cluster-Informationen	ClusterInfo

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetClusterInfo",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:


```
{
    "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"
        }
    }
}
```


Neu seit Version

9.6

GetClusterSchnittstellenPräferenz

Der `GetClusterInterfacePreference` „Method“ ermöglicht in Storage-Cluster, auf denen Element Software ausgeführt wird, integrierte Systeme, um Informationen über eine vorhandene Cluster-Schnittstelle zu erhalten. Diese Methode ist für den internen Gebrauch bestimmt.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Name	Der Name der bevorzugten Cluster-Schnittstelle.	Zeichenfolge	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Präferenz	Name und Wert der gewünschten Cluster-Schnittstelle.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "GetClusterInterfacePreference",
    "params": {
        "name": "prefname"
        },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "preference": {
            "name": "prefname",
            "value": "testvalue"
        }
    }
}
```

Neu seit Version

11.0

GetClusterMasterNodeID

Sie können das verwenden `GetClusterMasterNodeID` Methode zum Abrufen der ID des Node, der clusterweite Administrationsaufgaben ausführt und die virtuelle IP-Adresse (Storage Virtual IP Address, SVIP) und die virtuelle Management-IP-Adresse (MVIP) enthält.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
NodeID	ID des Hauptknotens.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetClusterMasterNodeID",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1
  "result": {
    "nodeID": 1
   }
}
```

Neu seit Version

9.6

GetClusterStats

Sie können das verwenden `GetClusterStats` Methode zum Abrufen von allgemeinen Aktivitätsmessungen für das Cluster Der zurückgegebene Wert wird durch die Erstellung des Clusters kumulativ erfasst.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
ClusterStatistik	Informationen zur Cluster-Aktivität	ClusterStatistik

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetClusterStats",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
    }
  }
}
```


Neu seit Version

9.6

GetClusterVersionInfo

Sie können das verwenden `GetClusterVersionInfo` Methode zum Abrufen von Informationen über die auf jedem Node im Cluster ausgeführte Element Softwareversion. Diese Methode gibt auch Informationen zu Nodes zurück, die sich derzeit beim Aktualisieren der Software befinden.

Cluster-Version Info-Objektmitglieder

Diese Methode verfügt über die folgenden Objektmitglieder:

Name	Beschreibung	Typ
NodeID	ID des Node.	Ganzzahl
NodeInternalRevision	Interne Softwareversion des Node.	Zeichenfolge
Knotenversion	Softwareversion des Node.	Zeichenfolge

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
ClusterAPIVersion	Die aktuelle API-Version auf dem Cluster.	Zeichenfolge
ClusterVersion	Version der Element Software, die derzeit auf dem Cluster ausgeführt wird.	Zeichenfolge
Cluster-VersionInfo	Liste der Nodes im Cluster mit Versionsinformationen für jeden Node	JSON-Objekt-Array
HängenClusterVersion	Ist diese Version vorhanden, wird die Cluster-Software derzeit aktualisiert oder auf zurückgesetzt.	Zeichenfolge

Name	Beschreibung	Typ
SoftwareVersionInfo	Der Status eines Upgrades. Objektmitglieder: • StromstärkeVersion: Die aktuelle Softwareversion auf einem Node. • NodeID: ID des Node, der von CurrentVersion auf PendingVersion aktualisiert wird. Dieses Feld ist 0 (Null), wenn keine Aktualisierung durchgeführt wird. • Paketname: Name des Softwarepakets, das installiert wird. • PendingVersion: Die Version der installierten Software. • StartZeit: Datum und Uhrzeit der Installation im UTC+0-Format.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetClusterVersionInfo",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
 "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": ""
    }
  }
}
```

Neu seit Version

9.6

GetFeatureStatus

Sie können das verwenden `GetFeatureStatus` Methode zum Abrufen des Status einer Cluster-Funktion.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Merkmal	Der Status einer Cluster-Funktion. Wenn kein Wert angegeben wird, gibt das System den Status aller Funktionen zurück. Mögliche Werte: • `Vvols`: Status der VVols Cluster-Funktion abrufen. • `SnapMirror`: Status der SnapMirror-Replikationscluster-Funktion abrufen. • `Fips`: Status der Verschlüsselung nach FIPS 140-2 für HTTPS-Kommunikation abrufen. • `FipsDrives`: Status der FIPS 140-2-Laufwerksverschlüsselung abrufen. • `VolumeLoadBalanceOnActualIOPS`: Status für den Slice-Balancing auf tatsächlichen IOPS statt auf Min IOPS-Funktion abrufen. Verfügbar ab Element 12.8.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Funktionen	Ein Array von Feature-Objekten, das den Funktionsnamen und seinen Status angibt. Objektmitglieder: • Feature: (String) der Name des Features. • Aktiviert: (boolesch) ob die Funktion aktiviert ist oder nicht.	JSON-Objekt-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetFeatureStatus",
    "params": {
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "features": [
            {
                "enabled": true,
                "feature": "Vvols"
            },
            {
                "enabled": true,
                "feature": "SnapMirror"
            },
            {
                "enabled": true,
                "feature": "Fips"
            },
            {
                "enabled": true,
                "feature": "FipsDrives"
            },
            {
                "enabled": true,
                "feature": "VolumeLoadBalanceOnActualIOPS"
            }
        ]
    }
}
```


Neu seit Version

9.6

GetLoginSessionInfo

Sie können das verwenden `GetLoginSessionInfo` Methode zur Rückgabe des Zeitraums, in dem eine Anmelde-Authentifizierungssitzung gültig ist, sowohl für Login-Shells als auch für die TUI.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
LoginSessionInfo	Ein Objekt, das den Gültigkeitszeitraum der Authentifizierung enthält. Mögliche zurückgegebene Objekte: • Zeitüberschreitung: Die Zeit in Minuten, zu der diese Sitzung abgelaufen ist. Formatiert in H:mm:ss Beispiel: 1:30:00, 20:00, 5:00. Alle führenden Nullen und Doppelpunkte werden unabhängig vom eingegebenen Format entfernt.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetLoginSessionInfo",
    "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"id": 1,
  "result" : {
    "loginSessionInfo" : {
      "timeout" : "30:00"
    }
  }
}
```

Neu seit Version

9.6

GetNodeHardwareInfo

Sie können das verwenden `GetNodeHardwareInfo` Methode zum Zurückgeben aller Hardwareinformationen und -Status für den angegebenen Node. Dazu gehören im Allgemeinen Hersteller, Anbieter, Versionen und weitere zugehörige Hardware-Identifikationsinformationen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
NodeID	Die ID des Node, für den Hardwareinformationen angefordert werden. Informationen über einen Fibre Channel-Node werden zurückgegeben, wenn ein Fibre Channel-Node angegeben wird.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
NodeHardwareInfo	Hardwareinformationen für die angegebene NodeID. Jedes Objekt in dieser Ausgabe ist mit der Node-ID des angegebenen Node gekennzeichnet.	HardwareInfo

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetNodeHardwareInfo",
   "params": {
     "nodeID": 1
   },
"id" : 1
}
```

Antwortbeispiel

Aufgrund der Länge dieses Antwortbeispiels wird es in einem ergänzenden Thema dokumentiert.

Neu seit Version

9.6

Weitere Informationen

GetNodeHardwareInfo (Ausgabe für Fibre Channel Nodes)

GetNodeHardwareInfo (Ausgabe für iSCSI)

GetNodeStats

Sie können das verwenden `GetNodeStats` Methode zum Abrufen der allgemeinen Aktivitätsmessungen für einen einzelnen Knoten.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
NodeID	Gibt die ID des Node an, für den Statistiken zurückgegeben werden sollen.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
KnotenStatistiken	Informationen zu Node-Aktivitäten	KnotenStatistiken

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetNodeStats",
   "params": {
     "nodeID": 5
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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
     }
   }
}
```


Neu seit Version

9.6

ListenActiveNodes

Sie können das verwenden `ListActiveNodes` Die Methode zum Zurückgeben der Liste der derzeit aktiven Nodes, die sich im Cluster befinden.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Knoten	Liste der aktiven Nodes im Cluster.	Knoten Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListActiveNodes",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Aufgrund der Länge dieses Antwortbeispiels wird es in einem ergänzenden Thema dokumentiert.

Neu seit Version

9.6

Weitere Informationen

ListenActiveNodes

ListenAllNodes

Sie können das verwenden `ListAllNodes` „Methode“ zum Auflisten von aktiven und ausstehenden Nodes im Cluster.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Knoten	Liste von Objekten, die aktive Nodes im Cluster beschreiben	Knoten
Hängende ActiveNodes	Liste von Objekten, die ausstehende aktive Nodes für das Cluster beschreiben.	HängenActiveNode Array erledigen
Hängende Knoten	Liste von Objekten, die ausstehende Nodes für das Cluster beschreiben	Hängende Knoten Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListAllNodes",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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": []
    }
}
```


Neu seit Version

9.6

ListenClusterstandards

Sie können das verwenden `ListClusterFaults` Methode zum Auflisten von Informationen zu Fehlern, die im Cluster erkannt wurden. Mit dieser Methode können Sie sowohl aktuelle Fehler als auch Fehler auflisten, die behoben wurden. Das System

speichert Fehler alle 30 Sekunden im Cache.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Bestpractices	Schließen Sie Fehler ein, die durch eine suboptimale Systemkonfiguration ausgelöst werden. Mögliche Werte: • Richtig • Falsch	boolesch	Keine	Nein
Fehlertypen	Bestimmt die Art der zurückgegebenen Fehler. Mögliche Werte: • Aktuell: Liste der aktiven, nicht behobenen Fehler. • Behoben: Listen Sie Fehler auf, die zuvor erkannt und behoben wurden. • Alle: Listen Sie sowohl aktuelle als auch aufgelöste Fehler auf. Sie können den Fehlerstatus im „`reSolved`“-Mitglied des Fehlerobjekts sehen.	Zeichenfolge	Alle	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ

Fehler	Ein Objekt, das die angeforderten Cluster-Fehler beschreibt.	Fehler

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListClusterFaults",
    "params": {
      "faultTypes": "current",
      "bestPractices": true
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
      }
    ]
  }
}
```

Neu seit Version

9.6

ListenClusterSchnittstelleneinstellungen

Der `ListClusterInterfacePreference` Die Methode ermöglicht in Storage-Cluster integrierte Systeme, auf denen Element Software ausgeführt wird, um die im System gespeicherten Voreinstellungen für die Cluster-Schnittstelle aufzulisten. Diese Methode ist für den internen Gebrauch bestimmt.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Einstellungen	Eine Liste der aktuell im Storage-Cluster gespeicherten Cluster-Schnittstellenobjekte, die jeweils den Namen und den Wert der Voreinstellungen enthalten.	JSON-Objekt-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "ListClusterInterfacePreferences",
    "params": {
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "preferences": [
            {
                "name": "prefname",
                "value": "testvalue"
            }
        ]
    }
}
```

Neu seit Version

11.0

ListEvents

Sie können das verwenden `ListEvents` Methode zum Auflisten von Ereignissen, die auf dem Cluster erkannt wurden, sortiert von älteste bis neueste.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
DriveID	Gibt an, dass nur Ereignisse mit dieser Laufwerk-ID zurückgegeben werden.	Ganzzahl	0	Nein
EndEventID	Identifiziert das Ende eines Bereichs von Ereignis-IDs, die zurückgegeben werden sollen.	Ganzzahl	(Unbegrenzt)	Nein
EndPublishTime	Gibt an, dass nur Ereignisse, die früher als dieses Mal veröffentlicht wurden, zurückgegeben werden.	Zeichenfolge	0	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
EndReportTime	Gibt an, dass nur Ereignisse, die früher als dieses Mal gemeldet wurden, zurückgegeben werden.	Zeichenfolge	0	Nein
EventType	Gibt den Typ der zurückkehrenden Ereignisse an. Siehe Ereignis Für mögliche Ereignistypen.	Zeichenfolge	0	Nein
Max Events	Gibt die maximale Anzahl von Ereignissen an, die zurückgegeben werden sollen.	Ganzzahl	(Unbegrenzt)	Nein
NodeID	Gibt an, dass nur Ereignisse mit dieser Node-ID zurückgegeben werden.	Ganzzahl		
Service-ID	Gibt an, dass nur Ereignisse mit dieser Service-ID zurückgegeben werden.			
StartEventID	Gibt den Beginn einer Reihe von Ereignissen an, die zurückgegeben werden sollen.	Ganzzahl	0	Nein
StartPublishTime	Gibt an, dass nur nach diesem Zeitpunkt veröffentlichte Ereignisse zurückgegeben werden.	Zeichenfolge	0	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
StartBerichtUhrzeit	Gibt an, dass nur nach diesem Zeitpunkt gemeldete Ereignisse zurückgegeben werden.	Zeichenfolge	0	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Veranstaltungen	Liste der Ereignisse.	Ereignis Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListEvents",
   "params": {
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
       }
     ]
   }
}
```


Neu seit Version

9.6

ListNodeStats

Sie können das verwenden `ListNodeStats` Methode zur Anzeige der allgemeinen Aktivitätsmessungen für alle Storage-Nodes in einem Storage-Cluster

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
KnotenStatistiken	Aktivitätsinformationen zu Storage-Nodes	KnotenStatistiken

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListNodeStats",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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
         }
       ]
     }
 }
```

Neu seit Version

9.6

ListISSessions

Sie können das verwenden `ListISCSISessions` „Methode“ zum Auflisten der iSCSI-Verbindungsinformationen für Volumes im Cluster.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Sitzungen	Informationen zu den einzelnen iSCSI-Sitzungen.	Session

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListISCSISessions",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
 {
  "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
      }
     ...
    ]
  }
}
```


Neu seit Version

9.6

ListServices

Sie können das verwenden `ListServices` Die Methode führt Serviceinformationen für Nodes, Laufwerke, aktuelle Software und andere Dienste auf, die auf dem Cluster ausgeführt werden.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Services	Services, die auf Laufwerken und Nodes ausgeführt werden.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListServices",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
"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"
            }
        }
    ]
}
```

Neu seit Version

9.6

ListenPendingKnoten

Sie können das verwenden `ListPendingNodes` Methode zum Auflisten der ausstehenden Storage-Nodes im System. Ausstehende Knoten sind Speicherknoten, die ausgeführt und konfiguriert sind, um dem Speicher-Cluster beizutreten, aber noch nicht mit der AddNodes API Methode hinzugefügt wurden.

IPv4- und IPv6-Managementadressen

Beachten Sie das `ListPendingNodes` Listet nicht ausstehende Knoten auf, die unterschiedliche Adresstypen für die Management-IP-Adresse (MIP) und die virtuelle Management-IP-Adresse (MVIP) haben. Wenn z. B. ein ausstehender Node über einen IPv6 MVIP und eine IPv4 MIP verfügt, `ListPendingNodes` Berücksichtigt den Node nicht im Ergebnis.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Hängende Knoten	Liste der ausstehenden Nodes im Cluster.	Hängende Knoten Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListPendingNodes",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
      }
    ]
  }
}
```


Neu seit Version

9.6

Weitere Informationen

AddNodes

ListPendingActiveNodes

Sie können das verwenden `ListPendingActiveNodes` Methode zum Auflisten von Nodes im Cluster, die sich im Status „PendingActive“ befinden, zwischen dem Status „Ausstehend“ und „aktiv“. Knoten in diesem Status werden an das Werkseinstellungen zurückgegeben.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Hängende ActiveNodes	Liste der Objekte mit Informationen zu allen PendingActive Nodes im System.	HängenActiveNode Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListPendingActiveNodes",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  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"
    }
    ]
  }
}
```

Neu seit Version

9.6

ModifyClusterFullThreshold

Sie können das verwenden `ModifyClusterFullThreshold` Methode zum Ändern des Levels, auf dem das System ein Ereignis generiert, wenn der Storage-Cluster einer bestimmten Kapazitätsauslastung nähert. Mithilfe der Schwellenwerteinstellung können Sie den zulässigen Umfang des genutzten Blockspeichers angeben, bevor das System eine Warnung erzeugt.

Wenn Sie zum Beispiel benachrichtigt werden möchten, wenn das System 3 % unter der Blockspeichernutzung auf „Error“-Ebene liegt, geben Sie einen Wert von „3“ für den Parameter stage3BlockThresholdPercent ein. Wenn diese Ebene erreicht wird, sendet das System eine Warnmeldung an das Ereignisprotokoll in der Cluster-Management-Konsole.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Sie müssen mindestens einen Parameter auswählen.

Name	Beschreibung	Typ	Standardwert	Erforderlich
MaxMetadaÜberProvisionFaktor	Ein Wert, der repräsentativ für die Anzahl der Zeiten ist, für die Metadaten im Verhältnis zum verfügbaren Speicherplatz überprovisioniert werden können. Wenn beispielsweise genügend Metadatenspeicherplatz vorhanden war, um 100 tib Volumes zu speichern, und diese Zahl auf 5 gesetzt wurde, könnten dann 500 tib an Volumes erstellt werden.	Ganzzahl	5	Nein
Stage2AwareThreshold	Die Anzahl der im Cluster verbliebenen Nodes an Kapazität, bevor das System eine Kapazitätsbenachrichtigung auslöst.	Ganzzahl	Keine	Nein
Stage3BlockThresholdPercent	Der Prozentsatz der Storage-Auslastung unter dem Schwellenwert für „Fehler“, der dazu führt, dass das System eine Cluster-Warnmeldung auslöst.	Ganzzahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Stage3MetadataThresholdPercent	Der Prozentsatz der Metadaten-Storage-Auslastung unter dem Schwellenwert „`Fehler`“, durch den das System eine Cluster-Warnmeldung „`Warnung`“ auslöst	Ganzzahl	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ

Blockfullness	Die aktuell berechnete Blockebene der Blockfülle des Clusters • Stage1Happy: Keine Warnungen oder Fehlerbedingungen. Entspricht dem **gesunden**-Status in der Web-UI. • Stage2Aware: Keine Warnungen oder Fehlerbedingungen. Entspricht dem **gesunden**-Status in der Web-UI. • Stage3Low: Das System kann nicht vor zwei nicht gleichzeitigen Node-Ausfällen redundante Daten schützen. Entspricht dem Status **Warnung** in der Web-Benutzeroberfläche. Sie können diesen Level in der Web-Benutzeroberfläche konfigurieren (standardmäßig löst das System diese Warnung mit einer Kapazität von 3 % unter dem Fehlerzustand aus). • Stage4kritisch: Das System kann nicht redundante Datensicherung bei einem Single Node-Ausfall bieten. Es können keine neuen Volumes oder Klone erstellt werden. Entspricht dem Status **Error** in der Element UI. • Stage5CompletelyVerbrauch: Vollständig verbraucht. Das Cluster ist schreibgeschützt und iSCSI-Verbindungen bleiben erhalten, alle Schreibvorgänge werden jedoch ausgesetzt. Entspricht dem **kritischen**-Status in der Element-UI.	Zeichenfolge
Fülle	Spiegelt die höchste Ebene der Fülle zwischen "BlockFullness" und "MetadaFullness" wider.	Zeichenfolge

MaxMetadaÜberProvisionFaktor	Ein Wert, der repräsentativ für die Anzahl der Zeiten ist, für die Metadaten im Verhältnis zum verfügbaren Speicherplatz überprovisioniert werden können. Wenn beispielsweise genügend Metadatenspeicherplatz vorhanden war, um 100 tib Volumes zu speichern, und diese Zahl auf 5 gesetzt wurde, könnten dann 500 tib an Volumes erstellt werden.	Ganzzahl

MetadataFullness	Die aktuell berechnete Metadatenfülle des Clusters. • Stage1Happy: Keine Warnungen oder Fehlerbedingungen. Entspricht dem **gesunden**-Status in der Web-UI. • Stage2Aware: Keine Warnungen oder Fehlerbedingungen. Entspricht dem **gesunden**-Status in der Web-UI. • Stage3Low: Das System kann nicht vor zwei nicht gleichzeitigen Node-Ausfällen redundante Daten schützen. Entspricht dem Status **Warnung** in der Web-Benutzeroberfläche. Sie können diesen Level in der Web-Benutzeroberfläche konfigurieren (standardmäßig löst das System diese Warnung mit einer Kapazität von 3 % unter dem Fehlerzustand aus). • Stage4kritisch: Das System kann nicht redundante Datensicherung bei einem Single Node-Ausfall bieten. Es können keine neuen Volumes oder Klone erstellt werden. Entspricht dem Status **Error** in der Element UI. • Stage5CompletelyVerbrauch: Vollständig verbraucht. Das Cluster ist schreibgeschützt und iSCSI-Verbindungen bleiben erhalten, alle Schreibvorgänge werden jedoch ausgesetzt. Entspricht dem **kritischen**-Status in der Element-UI.	Zeichenfolge
SliceReserveUsedThresholdPunkt	Fehlerbedingung. Eine Systemwarnung wird ausgelöst, wenn die reservierte Schichtauslastung größer ist als der zurückgegebene sliceReserveUsedThresholdPct-Wert.	Ganzzahl

Stage2AwareThreshold	Bewusstseinszustand. Der für den „Phase 2“-Cluster-Schwellenwert festgelegte Wert.	Ganzzahl
Stage2BlockThresholdBytes	Die Anzahl der Bytes, die vom Cluster verwendet werden, an dem eine Bedingung für die Fülle von Phase 2 vorhanden ist.	Ganzzahl
Stage2MetadataThresholdBytes	Die Anzahl der Metadaten-Bytes, die vom Cluster verwendet werden, auf dem eine Bedingung für die Fülle von Phase 2 vorhanden ist.	
Stage3BlockThresholdBytes	Die Anzahl der Storage Bytes, die vom Cluster verwendet werden, an dem eine Bedingung für die Fülle von Phase 3 vorhanden sein wird.	Ganzzahl
Stage3BlockThresholdPercent	Der Prozentwert, der für Phase 3 festgelegt wurde. Bei diesem Prozentsatz wird eine Warnung im Alarmprotokoll ausgegeben.	Ganzzahl
Stage3LowThreshold	Fehlerbedingung. Der Schwellenwert, bei dem eine Systemwarnung aufgrund einer geringen Kapazität in einem Cluster erstellt wird.	Ganzzahl
Stage3MetadataThresholdBytes	Die Anzahl der Metadaten-Bytes, die vom Cluster verwendet werden, auf dem eine Bedingung für die Phase 3 der Fülle vorhanden ist.	
Stage4BlockThresholdBytes	Die Anzahl der Storage Bytes, die vom Cluster verwendet werden, an dem eine Bedingung für die Fülle von Phase 4 vorhanden sein wird.	Ganzzahl
Stage4CriticalThreshold	Fehlerbedingung. Der Schwellenwert, bei dem eine Systemwarnung erstellt wird, um über eine kritisch niedrige Kapazität auf einem Cluster zu warnen.	Ganzzahl

Stage4MetadataThresholdBytes	Die Anzahl der Metadaten-Bytes, die vom Cluster verwendet werden, auf dem eine Bedingung für die Phase 4 der Fülle vorhanden ist.	
Stage5BlockThresholdBytes	Die Anzahl der Speicherbyte, die vom Cluster verwendet wird, an dem eine Bedingung für die Phase 5-Fülle vorhanden sein soll.	Ganzzahl
Stage5MetadataThresholdBytes	Die Anzahl der Metadaten-Bytes, die vom Cluster verwendet werden, auf dem eine Bedingung für die Phase 5 der Fülle vorhanden ist.	
Summe ClusterBytes	Die physische Kapazität des Clusters, gemessen in Byte.	Ganzzahl
SumTotalMetadaClusterBytes	Der gesamte Speicherplatz, der zum Speichern von Metadaten verwendet werden kann.	Ganzzahl
Summe - ClusterBytes	Die Anzahl der im Cluster verwendeten Storage Bytes.	Ganzzahl
SuumUseMetadataClusterBytes	Der Speicherplatz, der auf Volume-Laufwerken zum Speichern von Metadaten verwendet wird.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method" : "ModifyClusterFullThreshold",
   "params" : {
               "stage3BlockThresholdPercent" : 3
               },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
  }
}
```


Neu seit Version

9.6

ModifyClusterSchnittstellenPräferenz

Der `ModifyClusterInterfacePreference` „Method“ ermöglicht die Integration von Systemen in Storage Cluster, auf denen Element Software ausgeführt wird, die Änderung einer bestehenden Cluster-Schnittstelle. Diese Methode ist für den internen Gebrauch bestimmt.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Name	Der Name der zu ändernden Cluster-Schnittstelle.	Zeichenfolge	Keine	Ja.

Wert	Der neue Wert der bevorzugten Cluster-Schnittstelle.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "ModifyClusterInterfacePreference",
    "params": {
    "name": "testname",
    "value": "newvalue"
},
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {}
}
```

Neu seit Version

11.0

RemoveNodes

Verwenden Sie können `RemoveNodes` Einen oder mehrere Nodes entfernen, die nicht mehr am Cluster teilnehmen sollen.

Vor dem Entfernen eines Node müssen Sie alle Laufwerke entfernen, die der Node mit enthält `RemoveDrives` Methode. Sie können den Node bis zum nicht entfernen `RemoveDrives` Der Prozess ist abgeschlossen, und alle Daten wurden vom Node migriert. Nachdem Sie einen Knoten entfernt haben, wird er sich als ausstehender Knoten registriert. Sie können den Node erneut hinzufügen oder ihn herunterfahren (durch das Herunterfahren des Node wird er aus der Liste der ausstehenden Node entfernt).

Entfernen des Cluster Master Node

Wenn Sie verwenden `RemoveNodes` Zum Entfernen des Cluster-Master-Node weist die Methode möglicherweise eine außerhalb auf, bevor eine Antwort zurückgegeben wird. Wenn der Methodenaufruf den Knoten nicht entfernt, führen Sie den Methodenaufruf erneut aus. Wenn Sie den Cluster-Master-Node zusammen mit anderen Nodes entfernen, sollten Sie einen separaten Aufruf verwenden, um den Cluster-Master-Node eigenständig zu entfernen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
IgnoreEnsembleToleranceWechsel	Änderungen an der Ausfalltoleranz des Knotens des Ensembles ignorieren, wenn Knoten entfernt werden. Wenn das Storage Cluster Datensicherungsschemata verwendet, die Ausfälle mehrerer Nodes tolerieren und durch das Entfernen der Nodes die Ausfalltoleranz des Ensembles verringern würden, schlägt das Entfernen des Node normalerweise mit einem Fehler fehl. Sie können diesen Parameter auf true setzen, um die Prüfung der Ensembletoleranz zu deaktivieren, damit die Knotenentfernung erfolgreich ist.	boolesch	Falsch	Nein
Knoten	Liste der NodeIDs für die zu entfernenden Nodes	Integer-Array	Keine	Ja.

Rückgabewert

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "RemoveNodes",
   "params": {
     "nodes"  : [3,4,5]
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1
  "result" : {},
}
```

Neu seit Version

9.6

SetLoginSessionInfo

Sie können das verwenden `SetLoginSessionInfo` Methode zum Festlegen des Zeitraumes, für den eine Anmeldeauthentifizierung für eine Sitzung gültig ist. Nachdem die Anmeldezeit ohne Aktivität auf dem System abgelaufen ist, läuft die Authentifizierung ab. Nach Ablauf des Anmeldezeitraums sind neue Anmeldedaten erforderlich, um weiterhin auf das Cluster zugreifen zu können.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Zeitüberschreitung	Ablaufdatum der Cluster-Authentifizierung. Formatiert in HH:mm:ss Zum Beispiel: 01:30:00, 00:90:00 und 00:00:5400 können alle verwendet werden, um eine 90-Minuten-Timeout-Zeitraum. Der minimale Timeout-Wert beträgt 1 Minute. Wenn ein Wert nicht angegeben wird oder auf Null gesetzt ist, hat die Anmeldesitzung keinen Timeout-Wert.	Zeichenfolge	30 Minuten	Nein

Rückgabewert

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "SetLoginSessionInfo",
  "params": {
    "timeout" : "01:30:00"
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {}
}
```

Neu seit Version

9.6

Herunterfahren

Sie können das verwenden `Shutdown` Methode zum Neustart oder Herunterfahren der Nodes in einem Cluster. Sie können über diese Methode einen einzelnen Node, mehrere Nodes oder alle Nodes im Cluster herunterfahren.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Knoten	Liste der NodeIDs für die Nodes, die neu gestartet oder heruntergefahren werden sollen.	Integer-Array	Keine	Ja.
Option	Aktion, die für den Cluster ausgeführt wird. Mögliche Werte: • Neustart: Startet das Cluster neu. • Stop: Führt eine vollständige Abschaltung durch.	Zeichenfolge	Neustart	Nein

Rückgabewert

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "Shutdown",
   "params": {
     "nodes": [
       2,
       3,
       4
     ],
     "option": "halt"
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {
     "failed": [],
     "successful": [
          6
      [
   }
}
```

Neu seit Version

9.6

API-Methoden zur Clustererstellung

CheckeAngebot für Cluster

Sie können das verwenden `CheckProposedCluster` Methode zum Testen einer Reihe von Storage-Nodes vor der Erstellung eines Storage-Clusters mit ihnen zur Identifizierung der möglichen Fehler oder Fehler, die bei dem Versuch auftreten würden, z. B. unsymmetrische Funktionen für gemischte Nodes oder Node-Typen, die für Storage Cluster mit zwei Nodes nicht unterstützt werden.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Knoten	Eine Liste der Speicher-IP-Adressen der ursprünglichen Gruppe von Speicher-Nodes, aus denen das Storage-Cluster besteht.	String-Array	Keine	Ja.
Erzwingen	Auf „true“ setzen, um auf allen Storage-Nodes im Storage-Cluster ausgeführt zu werden.	boolesch	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Antragsteller ClusterValid	Gibt an, ob die vorgeschlagenen Storage-Nodes ein gültiges Storage-Cluster bilden oder nicht. Mögliche Werte: • Richtig • Falsch	boolesch
Antragsteller ClusterErrors	Fehler, die auftreten würden, wenn ein Storage-Cluster mit den vorgeschlagenen Storage-Nodes erstellt würde.	String-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "CheckProposedCluster",
    "params": {
    "nodes": [
        "192.168.1.11",
        "192.168.1.12",
        "192.168.1.13",
        "192.168.1.14"
    ]
},
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "proposedClusterValid": true,
        "proposedClusterErrors": [ ]
    }
}
```

Neu seit Version

11.0

CreateCluster erstellen

Sie können das verwenden `CreateCluster` Methode zum Initialisieren des Knotens in einem Cluster, der Eigentümer der Adressen „mvip“ und „svip“ ist. Jedes neue Cluster wird mit der Management-IP (MIP) des ersten Node im Cluster initialisiert. Bei dieser Methode werden auch automatisch alle Nodes hinzugefügt, die im Cluster konfiguriert wurden. Sie müssen diese Methode nur einmal verwenden, wenn ein neues Cluster initialisiert wird.

> Nachdem Sie sich beim Master-Node für das Cluster angemeldet und den ausgeführt haben GetBootStrapConfig Methode um die IP-Adressen für die restlichen Nodes, die Sie in den Cluster aufnehmen möchten, zu erhalten, können Sie die CreateCluster-Methode gegen den Master-Knoten für den Cluster ausführen.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Akzepteula	Geben Sie an, dass Sie die Endnutzer-Lizenzvereinbarung akzeptieren, wenn Sie dieses Cluster erstellen. Um die EULA zu akzeptieren, setzen Sie diesen Parameter auf „true“.	boolesch	Keine	Ja.
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
EnableSoftwareVerschlüsselungAtest	Aktivieren Sie diesen Parameter, um eine softwarebasierte Verschlüsselung im Ruhezustand zu verwenden. Bei allen Clustern ist der Standardwert FALSE. Nach Aktivierung der Softwareverschlüsselung im Ruhezustand kann sie nicht auf dem Cluster deaktiviert werden.	boolesch	Richtig	Nein
mvip	Fließende (virtuelle) IP-Adresse für den Cluster im Managementnetzwerk.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Knoten	CIP/SIP-Adressen der ersten Knotengruppe, die den Cluster einrichten. Die IP-Adresse dieses Node muss in der Liste enthalten sein.	String-Array	Keine	Ja.
Auftragsnummer	Alphanumerische Auftragsnummer. Erforderlich auf softwarebasierten Plattformen	Zeichenfolge	Keine	Nein (hardwarebasierte Plattformen) Ja (softwarebasierte Plattformen)
Passwort	Anfängliches Passwort für das Cluster-Administratorkonto.	Zeichenfolge	Keine	Ja.
Seriennummer	Neunstellige alphanumerische Seriennummer. Möglicherweise auf softwarebasierten Plattformen erforderlich	Zeichenfolge	Keine	Nein (hardwarebasierte Plattformen) Ja (softwarebasierte Plattformen)
svip	Fließende (virtuelle) IP-Adresse für den Cluster im Storage-Netzwerk (iSCSI).	Zeichenfolge	Keine	Ja.
Benutzername	Benutzername für den Cluster-Administrator.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "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
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"id" : 1,
"result" : {}
}
```

Neu seit Version

9.6

Weitere Informationen

- "GetBootstrapConfig"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

GetBootstrapConfig

Sie können das verwenden `GetBootstrapConfig` Methode zum Abrufen von Cluster- und Node-Informationen aus der Bootstrap-Konfigurationsdatei Verwenden Sie diese API-Methode auf einem einzelnen Knoten, bevor er mit einem Cluster verbunden wurde.

Die Informationen, die diese Methode zurückgibt, werden beim Erstellen eines Clusters in der Cluster-Konfigurationsschnittstelle verwendet.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
ClusterName	Der Name des Clusters.	Zeichenfolge
mvip	Cluster-MVIP-Adresse. Leer, wenn der Node nicht Teil eines Clusters ist.	Zeichenfolge
NodeName	Der Name des Node.	Zeichenfolge
Knoten	Liste der Informationen über die einzelnen Nodes, die aktiv auf das Cluster warten Mögliche Werte: • ChassisType: (String) Hardware-Plattform des Node. • cip: (String) Cluster-IP-Adresse des Knotens. • Kompatibel: (boolean) gibt an, ob der Knoten mit dem Knoten kompatibel ist, für den der API-Aufruf ausgeführt wurde. • Hostname: (Zeichenfolge) Hostname des Knotens. • mip: (String) die IPv4-Management-IP-Adresse des Knotens. • MipV6: (String) die IPv6-Management-IP-Adresse des Knotens. • NodeType: (String)Modellname des Knotens. • Version: (String)Version der auf dem Knoten installierten Software.	JSON-Objekt-Array

Name	Beschreibung	Typ
svip	Cluster SVIP-Adresse. Null, wenn der Node nicht Teil eines Clusters ist.	Zeichenfolge
Version	Die Version der derzeit auf dem Node installierten Element-Software, die mit dieser API-Methode aufgerufen wurde.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetBootstrapConfig",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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"
    }
}
```

Neu seit Version

9.6

Weitere Informationen

CreateCluster erstellen

Drive-API-Methoden

AddDrives

Sie können das verwenden `AddDrives` Methode zum Hinzufügen eines oder mehrerer verfügbarer Laufwerke zum Cluster, wodurch die Laufwerke einen Teil der Daten für das Cluster hosten können.

Wenn Sie dem Cluster einen Speicherknoten hinzufügen oder neue Laufwerke in einem bestehenden Knoten installieren, sind die neuen Laufwerke als verfügbar gekennzeichnet und müssen über AddDrives hinzugefügt werden, bevor sie verwendet werden können. Verwenden Sie die ListenLaufwerke Methode zum Anzeigen von Laufwerken, die hinzugefügt werden können. Wenn Sie ein Laufwerk hinzufügen, bestimmt das System automatisch den Laufwerkstyp.

Die Methode ist asynchron und gibt sie zurück, sobald die Prozesse zur Ausbalancierung der Laufwerke im Cluster gestartet werden. Es kann jedoch mehr Zeit dauern, bis die Daten im Cluster mit den neu hinzugefügten Laufwerken neu ausgeglichen werden; die Neuverteilung wird auch nach Abschluss des Aufruf der AddDrives-Methode fortgesetzt. Sie können das verwenden GetAsyncResult Methode zum Abfragen der zurückgegebenen Methode Async. Nachdem die AddDrives-Methode zurückkehrt, können Sie die verwenden ListSyncJobs Methode zum Anzeigen des Fortschritts der Datenumverteilung mit den neuen Laufwerken.

> Wenn Sie mehrere Laufwerke hinzufügen, ist es effizienter, sie in einem einzigen AddDrives-Methodenaufruf hinzuzufügen, anstatt mehrere einzelne Methoden mit jeweils einem einzigen Laufwerk zu verwenden. Dies reduziert die Menge an Datenausgleich, die zur Stabilisierung der Storage-Last im Cluster erfolgen muss.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Laufwerke	Informationen über die einzelnen Laufwerke, die dem Cluster hinzugefügt werden sollen. Mögliche Werte: • DriveID: Die ID des Laufwerks, das hinzugefügt werden soll (Integer). • Typ: Der Typ des hinzufügenden Laufwerks (String). Gültige Werte sind „Slice“, „Block“ oder „Volume“. Wenn keine Angabe erfolgt, weist das System den korrekten Typ zu.	JSON-Objekt-Array	Keine	Ja (Typ ist optional)

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Asynchron	Handle-Wert, der zum Abrufen des Operationsergebnisses verwendet wird.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 1,
  "method": "AddDrives",
  "params": {
    "drives": [
      {
        "driveID": 1,
        "type": "slice"
      },
      {
        "driveID": 2,
        "type": "block"
      },
      {
        "driveID": 3,
        "type": "block"
      }
    ]
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result" : {
    "asyncHandle": 1
  }
}
```

Neu seit Version

9.6

Weitere Informationen

- GetAsyncResult
- ListenLaufwerke
- ListSyncJobs

GetDriveHardwareInfo

Sie können das verwenden `GetDriveHardwareInfo` Methode, um alle Hardware-

Informationen für das angegebene Laufwerk zu erhalten. Dazu gehören im Allgemeinen Hersteller, Anbieter, Versionen und weitere zugehörige Hardware-Identifikationsinformationen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
DriveID	ID des Laufwerks für den Antrag.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Ergebnis	Hardwareinformationen für die angegebene DriveID wurden zurückgegeben.	HardwareInfo

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetDriveHardwareInfo",
   "params": {
     "driveID": 5
   },
   "id" : 100
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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"
     }
   }
}
```


Neu seit Version

9.6

Weitere Informationen

ListenLaufwerke

GetDriveStats

Sie können das verwenden `GetDriveStats` Methode, um allgemeine Aktivitätsmessungen für eine einzelne Festplatte zu erhalten. Die Werte werden durch das Hinzufügen des Laufwerks zum Cluster kumulativ erfasst. Einige Werte sind spezifisch für Blocklaufwerke. Statistische Daten werden entweder für Block- oder Metadaten-Laufwerkstypen zurückgegeben, wenn Sie diese Methode ausführen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
DriveID	ID des Laufwerks für den Antrag.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Fahrstollen	Informationen zur Laufwerkaktivität für die angegebene DriveID.	Fahrstollen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetDriveStats",
   "params": {
     "driveID": 3
   },
   "id" : 1
}
```

Beispiel für Antwort (Blocklaufwerk)

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel für ein Blocklaufwerk entspricht:

```
{
  "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
    }
  }
}
```


Antwortbeispiel (Volume Metadatenlaufwerk)

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel für ein Volume-Metadatenlaufwerk ähnelt:

```
{
  "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
    }
  }
}
```


Neu seit Version

9.6

Weitere Informationen

ListenLaufwerke

ListenLaufwerke

Sie können das verwenden `ListDrives` Methode zum Auflisten der Laufwerke, die in den aktiven Nodes des Clusters vorhanden sind. Diese Methode liefert Laufwerke, die als Volume-Metadaten oder Blocklaufwerke hinzugefügt wurden, sowie Laufwerke, die nicht hinzugefügt wurden und verfügbar sind.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Laufwerke	Liste der Laufwerke im Cluster.	Laufwerk Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListDrives",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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"
       }
     }
   ]
}
```


Neu seit Version

9.6

ListDriveStats

Sie können das verwenden `ListDriveStats` Methode zur Auflistung grundlegender Aktivitätsmessungen für mehrere Laufwerke im Cluster. Bei dieser Methode werden standardmäßig Statistiken für alle Laufwerke im Cluster angezeigt. Die Messungen werden durch das Hinzufügen des Laufwerks zum Cluster kumulativ durchgeführt. Einige Werte, die diese Methode zurückgibt, sind speziell für Blocklaufwerke und einige für Metadaten-Laufwerke spezifisch.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Laufwerke	Liste der Laufwerk-IDs (DriveID), für die Laufwerksstatistiken zurückgegeben werden sollen. Wenn Sie diesen Parameter nicht angeben, werden die Messungen für alle Laufwerke zurückgegeben.	Integer-Array	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Fahrstollen	Liste der Informationen zur Laufwerkaktivität für jedes Laufwerk	Fahrstollen Array erledigen
Fehler	Diese Liste enthält die DriveID und die zugehörige Fehlermeldung. Es ist immer vorhanden und leer, wenn keine Fehler vorhanden sind.	JSON-Objekt-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 1,
  "method": "ListDriveStats",
  "params": {
    "drives":[22,23]
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
        }
      }
    ]
  }
}
```


Neu seit Version

9.6

Weitere Informationen

GetDriveStats

RemoveDrives

Sie können das verwenden `RemoveDrives` Methode zum proaktiven Entfernen von

Laufwerken, die Teil des Clusters sind Sie können diese Methode verwenden, wenn Sie die Cluster-Kapazität verringern oder Laufwerke ersetzen möchten, die sich dem Ende ihrer Lebensdauer nähern. `RemoveDrives` Erstellt eine dritte Kopie der Blockdaten auf den anderen Nodes im Cluster und wartet auf den Abschluss der Synchronisierung, bevor die Laufwerke in die Liste „verfügbar“ verschoben werden. Laufwerke in der Liste „verfügbar“ werden vollständig aus dem System entfernt und verfügen nicht über laufende Dienste oder aktive Daten.

`RemoveDrives` Ist eine asynchrone Methode. Abhängig von der Gesamtkapazität der entfernten Laufwerke kann es einige Minuten dauern, bis alle Daten migriert sind.

Verwenden Sie beim Entfernen mehrerer Laufwerke nur ein einziges `RemoveDrives` Methodenaufruf statt mehreren einzelnen Methoden mit jeweils einem einzigen Laufwerk. Hierdurch wird die Menge an Daten reduziert, die stattfinden muss, um die Storage-Last im Cluster gleichmäßig zu stabilisieren.

Sie können auch Laufwerke mit dem Status „Fehlgeschlagen“ entfernen `RemoveDrives`. Wenn Sie ein Laufwerk mit dem Status „ausgefallen“ entfernen, wird das Laufwerk nicht in den Status „verfügbar“ oder „`aktiv`“ zurückgeführt. Das Laufwerk ist nicht zur Verwendung im Cluster verfügbar.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Laufwerke	Liste der aus dem Cluster zu entfernenden Auffahrungen.	Integer-Array	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Asynchron	Handle-Wert, der zum Abrufen des Operationsergebnisses verwendet wird.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "RemoveDrives",
   "params": {
      "drives"  : [3, 4, 5]
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result" : {
     "asyncHandle": 1
   }
}
```

Neu seit Version

9.6

Weitere Informationen

- GetAsyncResult
- ListenLaufwerke

SecureEraseDrives

Sie können das verwenden `SecureEraseDrives` Methode zum Entfernen von Restdaten von Laufwerken mit dem Status „verfügbar“. Sie können diese Methode verwenden, wenn Sie ein Laufwerk ersetzen, das sich dem Ende seiner Lebensdauer nähert, und das sensible Daten enthielt. Bei dieser Methode wird mit dem Befehl Security Erase Unit ein vorbestimmtes Muster auf das Laufwerk geschrieben und der Verschlüsselungsschlüssel auf dem Laufwerk zurückgesetzt. Diese asynchrone Methode kann mehrere Minuten in Anspruch nehmen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Laufwerke	Liste der Laufwerk-IDs zum sicheren Löschen.	Integer-Array	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Asynchron	Handle-Wert, der zum Abrufen des Operationsergebnisses verwendet wird.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "SecureEraseDrives",
   "params": {
     "drives"  : [3, 4, 5]
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1
   "result" : {
     "asyncHandle" : 1
   }
}
```

Neu seit Version

9.6

Weitere Informationen

- GetAsyncResult

- ListenLaufwerke

Fibre Channel-API-Methoden

GetVolumeAccessGroupLunAssignments

Sie können das verwenden `GetVolumeAccessGroupLunAssignments` Methode zum Abrufen von Details in LUN-Zuordnungen einer angegebenen Volume-Zugriffsgruppe.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeAccessGroupID	Eine eindeutige Zugriffsgruppen-ID für Volumes, mit der Informationen zurückgegeben werden.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeAccessGroupLunAssignments	Eine Liste aller physischen Fibre-Channel-Ports oder ein Port für einen einzelnen Node.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetVolumeAccessGroupLunAssignments",
   "params": {
      "volumeAccessGroupID": 5
    },
  "id" : 1
   }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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}
       ]
    }
  }
}
```

Neu seit Version

9.6

ListFiberChannelPortInfo

Sie können das verwenden `ListFibreChannelPortInfo` „Methode“ zum Auflisten von Informationen zu den Fibre Channel-Ports.

Diese API-Methode ist für die Verwendung auf einzelnen Knoten bestimmt. Für den Zugriff auf einzelne Fibre Channel-Knoten sind eine Benutzer-ID und ein Passwort erforderlich. Diese Methode kann jedoch im Cluster verwendet werden, wenn der Kraft-Parameter auf „true“ gesetzt ist. Wenn Sie auf dem Cluster verwendet werden, werden alle Fibre-Channel-Schnittstellen aufgeführt.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Erzwingen	Auf „true“ setzen, um auf allen Nodes im Cluster ausgeführt zu werden.	boolesch	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Fibre Channel-Ports	Eine Liste aller physischen Fibre-Channel-Ports oder ein Port für einen einzelnen Node.	Fibre Channel-Port Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListFibreChannelPortInfo",
    "params": {},
    "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
          }
        ]
      }
    }
  }
 }
}
```

Neu seit Version

9.6

ListFiberChannelSessions

Sie können das verwenden `ListFibreChannelSessions` „Methode“, um Informationen zu den Fibre Channel-Sitzungen auf einem Cluster aufzulisten.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Sitzungen	Eine Liste von Objekten, die aktive Fibre Channel-Sitzungen auf dem Cluster beschreiben.	Session Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListFibreChannelSessions",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
    }
    ]
  }
}
```

Neu seit Version

9.6

ListNodeFiberChannelPortInfo

Sie können das verwenden `ListNodeFibreChannelPortInfo` „Methode“, um Informationen zu den Fibre Channel-Ports auf einem Node aufzulisten.

Diese API-Methode ist für die Verwendung auf einzelnen Knoten bestimmt. Für den Zugriff auf einzelne Fibre Channel-Knoten sind eine Benutzer-ID und ein Passwort erforderlich. Wenn Sie auf dem Cluster verwendet werden, werden alle Fibre-Channel-Schnittstellen aufgeführt.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Fibre Channel-Ports	Eine Liste aller physischen Fibre-Channel-Ports oder ein Port für einen einzelnen Node.	Fibre Channel-Port Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListNodeFibreChannelPortInfo",
   "params": {
       "nodeID": 5,
       "force": true
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
       }
     ]
   }
}
```


Neu seit Version

9.6

ModifyVolumeAccessGroupLunAssignments

Sie können das verwenden `ModifyVolumeAccessGroupLunAssignments` Methode zum Definieren benutzerdefinierter LUN-Zuweisungen für bestimmte Volumes

Diese Methode ändert nur die LUN-Werte, die im Parameter „lunAssignments“ in der Zugriffsgruppe „Volume“ festgelegt sind. Alle anderen LUN-Zuweisungen bleiben unverändert.

Die LUN-Zuweisungswerte müssen für Volumes in einer Volume-Zugriffsgruppe eindeutig sein. Sie können keine doppelten LUN-Werte innerhalb einer Volume-Zugriffsgruppe definieren. Sie können jedoch dieselben LUN-Werte auch in verschiedenen Volume-Zugriffsgruppen wieder verwenden.

Gültige LUN-Werte sind 0 bis 16383. Das System generiert eine Ausnahme, wenn Sie einen LUN-Wert außerhalb dieses Bereichs übergeben. Wenn eine Ausnahme besteht, werden keine der angegebenen LUN-Zuweisungen geändert.

ACHTUNG:

Wenn Sie eine LUN-Zuweisung für ein Volume mit aktiver I/O ändern, kann der I/O unterbrochen werden. Sie sollten die Serverkonfiguration ändern, bevor Sie die Volume-LUN-Zuweisungen ändern.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeAccessGroupID	Eindeutige Zugriffsgruppen-ID des Volumes, für die die LUN-Zuweisungen geändert werden.	Ganzzahl	Keine	Ja.
LunAssignments	Die Volume-IDs mit den neuen zugewiesenen LUN-Werten.	Integer-Array	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeAccessGroupLunAssignments	Ein Objekt, das Details zu den geänderten LUN-Zuordnungen der Zugriffsgruppe für Volumes enthält.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ModifyVolumeAccessGroupLunAssignments",
   "params": {
       "volumeAccessGroupID" : 218,
       "lunAssignments" : [
           {"volumeID" : 832, "lun" : 0},
           {"volumeID" : 834, "lun" : 1}
        ]
    },
    "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
    "volumeAccessGroupLunAssignments": {
      "deletedLunAssignments": [],
      "lunAssignments": [
        {
          "lun": 0,
          "volumeID": 832
        },
        {
          "lun": 1,
          "volumeID": 834
        }
      ],
      "volumeAccessGroupID": 218
    }
  }
}
```

Neu seit Version

9.6

Initiator-API-Methoden

CreateInitiatoren

Verwenden Sie können `CreateInitiators` Um mehrere neue Initiator-IQNs oder World Wide Port Names (WWPNs) zu erstellen und optional Aliase und Attribute zuzuweisen. Wenn Sie verwenden `CreateInitiators` Zum Erstellen neuer Initiatoren können Sie sie auch zu Volume-Zugriffsgruppen hinzufügen.

Wenn der Vorgang einen der im Parameter angegebenen Initiatoren nicht erstellt, gibt die Methode einen Fehler aus und erstellt keine Initiatoren (ein partieller Abschluss ist nicht möglich).

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Initiatoren	Eine Liste von Objekten, die die Eigenschaften der einzelnen neuen Initiatoren enthalten. Objekte: • `alias`: (Optional) der freundliche Name, der diesem Initiator zugewiesen werden soll. (Zeichenfolge) • `attributes`: (Optional) ein Satz von JSON-Attributen, die diesem Initiator zugewiesen werden sollen. (JSON-Objekt) • `chapUsername`: (Optional) der eindeutige CHAP-Benutzername für diesen Initiator. Setzt den Initiatornamen (IQN) standardmäßig ein, wenn er während der Erstellung nicht angegeben wurde und requiredChap wahr ist. (Zeichenfolge) • `initiatorSecret`: (Optional) der CHAP-Schlüssel, der zur Authentifizierung des Initiators verwendet wird. Die Standardeinstellung ist ein zufällig generiertes	JSON-Objekt-Array	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Initiatoren	Liste von Objekten, die die neu erstellten Initiatoren beschreiben	Initiator Array erledigen

Fehler

Mit dieser Methode kann der folgende Fehler zurückgegeben werden:

Name	Beschreibung
XInitiatorExists	Dieser Wert wird zurückgegeben, wenn der ausgewählte Name des Initiators bereits vorhanden ist.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "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"
      }
    ]
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

Geheimnis, wenn es wahr ist. (Zeichenfolge)

- `name`: (Erforderlich) der Name des zu

(Optional) true, wenn CHAP während der Sitzungsanmeld ung für diesen während der Erstellung nicht angegeben wurde und requiredChap wahr ist. (Zeichenfolge)

- `virtualNetwo rkIDs`: (Optional) die Liste der virtuellen

```
{
  "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": []
      }
    ]
  }
}
```


Neu seit Version	(Optional) die ID der Volume Access Group, der dieser neu erstellte Initiator hinzugefügt wird. (Ganze Zahl)
9.6	
Weitere Informationen	
ListenInitiatoren	

DeleteInitiatoren

Verwenden Sie können `DeleteInitiators` So löschen Sie einen oder mehrere Initiatoren aus dem System (und aus allen zugehörigen Volumes oder Volume-Zugriffsgruppen):

Wenn `DeleteInitiators` Löscht einen der im Parameter angegebenen Initiatoren nicht, gibt das System einen Fehler aus und löscht keine Initiatoren (kein partieller Abschluss möglich).

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Initiatoren	Ein Array mit IDs von zu löschenden Initiatoren.	Integer-Array	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Fehler

Mit dieser Methode kann der folgende Fehler zurückgegeben werden:

Name	Beschreibung
XInitiatorDoesNotExist	Dieser Wert wird zurückgegeben, wenn der gewählte Initiatorname nicht vorhanden ist.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 5101,
  "method": "DeleteInitiators",
  "params": {
    "initiators": [
      145,
      147
    ]
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 5101,
  "result": {}
}
```

Neu seit Version

9.6

ListenInitiatoren

Sie können das verwenden `ListInitiators` Methode zum Abrufen der Liste von Initiator-IQNs oder World Wide Port Names (WWPNs).

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Initiatoren	Eine Liste der abzurufenden Initiator-IDs. Sie können diesen Parameter oder den StartInitiatorID-Parameter angeben, aber nicht beides.	Integer-Array	Keine	Nein
StartInitiatorID	Die Initiator-ID, bei der die Aufnahme gestartet werden soll. Sie können diesen Parameter oder den Parameter der Initiatoren angeben, aber nicht beides.	Ganzzahl	0	Nein
Grenze	Die maximale Anzahl der zurückzukehrenden Initiator-Objekte.	Ganzzahl	(Unbegrenzt)	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Initiatoren	Liste der Initiator-Informationen.	Initiator Array erledigen

Ausnahmen

Diese Methode kann die folgende Ausnahme haben:

Name	Beschreibung

XInvalidParameter	Wird angezeigt, wenn Sie sowohl die StartInitiatorID als auch die Initiatoren-Parameter in den gleichen Methodenaufruf einbeziehen.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListInitiators",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
    "initiators": [
      {
        "alias": "",
        "attributes": {},
        "initiatorID": 2,
        "initiatorName": "iqn.1993-08.org.debian:01:c84ffd71216",
        "volumeAccessGroups": [
          1
        ]
      }
    ]
  }
}
```

Neu seit Version

9.6

ModifyInitiatoren

Sie können das verwenden `ModifyInitiators` Methode zum Ändern der Attribute eines oder mehrerer vorhandener Initiatoren.

Sie können den Namen eines vorhandenen Initiators nicht ändern. Wenn Sie den Namen eines Initiators

ändern müssen, löschen Sie diesen zunächst mit der DeleteInitiatoren Methode und erstellen Sie mit dem eine neue Methode CreateInitiatoren Methode.

Wenn ModityInitiatoren einen der im Parameter angegebenen Initiatoren nicht ändern können, gibt die Methode einen Fehler zurück und ändert keine Initiatoren (kein Teilabschluss möglich).

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich

Initiatoren	Eine Liste der Objekte, die die Merkmale der einzelnen zu ändernden Initiatoren enthalten. Mögliche Objekte: • `alias`: (Optional) ein neuer Anzeigename, der dem Initiator zugewiesen werden soll. (Zeichenfolge) • `attributes`: (Optional) ein neuer Satz von JSON-Attributen, die dem Initiator zugewiesen werden sollen. (JSON-Objekt) • `chapUsername`: (Optional) ein neuer eindeutiger CHAP-Benutzername für diesen Initiator. (Zeichenfolge) • `forceDuringUpgrade`: Abschließen der Initiator-Änderung während einer Aktualisierung. • `initiatorID`: (Erforderlich) die ID des zu ändernden Initiators. (Ganze Zahl) • `initiatorSecret`: (Optional) Ein neuer CHAP-Schlüssel zur Authentifizierung des Initiators. (Zeichenfolge)	JSON-Objekt-Array	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Initiatoren	Liste von Objekten, die die neu geänderten Initiatoren beschreiben	Initiator Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 6683,
  "method": "ModifyInitiators",
  "params": {
    "initiators": [
      {
        "initiatorID": 2,
        "alias": "alias1",
        "volumeAccessGroupID": null
      },
      {
        "initiatorID": 3,
        "alias": "alias2",
        "volumeAccessGroupID": 1
      }
    ]
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

- `requireChap`: (Optional) true wenn CHAP für
- neuer CHAP-Schlüssel zur Authentifizierung des Ziels (bei Verwendung der
- anmelden. Wenn Sie keine virtuellen Netzwerke definieren, kann sich dieser Initiator bei allen Netzwerken anmelden.
- `volumeAccessGroupID`: (Optional) die ID der Volume Access Group, der der Initiator hinzugefügt werden soll. Wenn der Initiator zuvor in einer anderen Volume-

```
{
  "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
        ]
      }
    ]
  }
}
```


Neu seit Version

9.6

Weitere Informationen

- CreateInitiatoren
- DeleteInitiatoren

LDAP-API-Methoden

AddLdapClusterAdmin

Sie können das verwenden `AddLdapClusterAdmin` So fügen Sie einen neuen LDAP-Cluster-Administratorbenutzer hinzu: Ein LDAP-Clusteradministrator kann den Cluster mithilfe der API und Managementtools verwalten. LDAP-Cluster-Administratorkonten sind vollständig getrennt und stehen in keinem Zusammenhang mit standardmäßigen Mandantenkonten.

Parameter

Mit dieser Methode können Sie auch eine in Active Directory® definierte LDAP-Gruppe hinzufügen. Die Zugriffsebene, die der Gruppe zugewiesen wird, wird an die einzelnen Benutzer in der LDAP-Gruppe übergeben.

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Datenzugriff	Steuert, welche Methoden dieser Cluster-Administrator verwenden kann.	String-Array	Keine	Ja.
Akzepteula	Akzeptieren Sie die Endnutzer-Lizenzvereinbarung. Setzen Sie auf „true“, um dem System ein Cluster-Administratorkonto hinzuzufügen. Wenn keine Angabe erfolgt oder auf FALSE gesetzt wird, schlägt der Methodenaufruf fehl.	boolesch	Keine	Ja.
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
Benutzername	Der Distinguished Benutzername für den neuen LDAP-Cluster Admin.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "AddLdapClusterAdmin",
  "params": {"username":"cn=mike
jones,ou=ptusers,dc=prodtest,dc=solidfire,dc=net",
    "access": ["administrator", "read"
    ]
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
 "id": 1,
 "result": {}
}
```

Neu seit Version

9.6

Weitere Informationen

Zugriffssteuerung

EnableLdapAuthentifizierung

Sie können das verwenden `EnableLdapAuthentication` Methode zum Konfigurieren einer LDAP-Verzeichnisverbindung für die LDAP-Authentifizierung in einem Cluster. Benutzer, die Mitglieder des LDAP-Verzeichnisses sind, können sich dann mithilfe ihrer LDAP-Anmeldedaten am Speichersystem anmelden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
AuthType	Gibt an, welche Benutzerauthentifizierungsmethode verwendet werden soll. Mögliche Werte: • `DirectBind` • `SearchAndBind`	Zeichenfolge	SucheAndBind	Nein
GroupSearchBaseDN	Der Basis-DN des Baums, um die Unterstruktursuche zu starten.	Zeichenfolge	Keine	Nein
GroupSearchType	Steuert den verwendeten Standardfilter für die Gruppensuche. Mögliche Werte: • NoGroups: Keine Gruppenunterstützung. • ActiveDirectory: Verschachtelte Mitgliedschaft aller Active Directory-Gruppen eines Benutzers. • MemberDN: MemberDN-Stilgruppen (einzelne Ebene).	Zeichenfolge	ActiveDirectory	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Server-URIs	Eine kommagetrennte Liste von LDAP- oder LDAPS-Server-URIs. Sie können einen benutzerdefinierten Port am Ende eines LDAP- oder LDAPS-URI hinzufügen, indem Sie einen Doppelpunkt gefolgt von der Portnummer verwenden. Der URI „ldap://1.2.3.4“ verwendet beispielsweise den Standardport und der URI „ldaps://1.2.3.4:123“ verwendet den benutzerdefinierten Port 123.	String-Array	Keine	Ja.
BenutzerSuchbaseDN	Der Basis-DN des Baums, um die Unterbaumsuche zu starten. Dieser Parameter ist erforderlich, wenn Sie einen AuthType von SearchAndBind verwenden.	Zeichenfolge	Keine	Nein
SuchhinBindDN	Ein vollständig qualifizierter DN zur Anmeldung bei, um eine LDAP-Suche für den Benutzer durchzuführen. Der DN benötigt Lesezugriff auf das LDAP-Verzeichnis. Dieser Parameter ist erforderlich, wenn Sie einen AuthType von SearchAndBind verwenden.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
SucheBindPasswort	Das Kennwort für das SuchBindDN-Konto, das für die Suche verwendet wurde. Dieser Parameter ist erforderlich, wenn Sie einen AuthType von SearchAndBind verwenden.	Zeichenfolge	Keine	Ja.
BenutzerSuchfilter	Der LDAP-Suchfilter, der beim Abfragen des LDAP-Servers verwendet werden soll. Die Zeichenfolge sollte den Platzhaltertext „%USERNAME%“ haben, der durch den Benutzernamen des authentifizierenden Benutzers ersetzt wird. Zum Beispiel verwendet (&(objectClass=Person)(sAMAccountName=%USERNAME%) das Feld sAMAccountName in Active Directory, um mit dem bei der Cluster-Anmeldung eingegebenen Benutzernamen überein. Dieser Parameter ist erforderlich, wenn Sie einen AuthType von SearchAndBind verwenden.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
BenutzerDNTemplate	Eine Zeichenkettenvorlage, mit der ein Muster zum Erstellen eines vollständigen, vom Benutzer bestimmten Namens (DN) definiert wird. Die Zeichenfolge sollte den Platzhaltertext „%USERNAME%“ haben, der durch den Benutzernamen des authentifizierenden Benutzers ersetzt wird. Dieser Parameter ist erforderlich, wenn Sie einen AuthType von DirectBind verwenden.	Zeichenfolge	Keine	Ja.
GroupSearchCustomFilter	Für die Verwendung mit dem CustomFilter-Suchtyp, ein LDAP-Filter, mit dem der DNS von Benutzergruppen zurückgegeben werden kann. Der Platzhalter-Text von %USERNAME% und %USDN% kann bei Bedarf durch ihren Benutzernamen und vollständigen Benutzer-DN ersetzt werden.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "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
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"id": 1,
"result": {
  }
}
```

Neu seit Version

9.6

DisableLdapAuthentifizierung

Sie können das verwenden `DisableLdapAuthentication` Methode zum Deaktivieren der LDAP-Authentifizierung und Entfernen aller LDAP-Konfigurationseinstellungen. Bei dieser Methode werden keine konfigurierten Cluster-Administratorkonten für Benutzer oder Gruppen entfernt. Nachdem die LDAP-Authentifizierung deaktiviert wurde, können Clusteradministratoren, die für die LDAP-Authentifizierung konfiguriert sind, nicht mehr auf das Cluster zugreifen.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DisableLdapAuthentication",
  "params": {},
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"id": 1,
"result": {}
}
```

Neu seit Version

9.6

GetLdapConfiguration

Sie können das verwenden `GetLdapConfiguration` Methode zum Abrufen der derzeit aktiven LDAP-Konfiguration auf dem Cluster.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert.

Name	Beschreibung	Typ
LdapKonfiguration	Liste der aktuellen LDAP-Konfigurationseinstellungen. Dieser API-Aufruf gibt nicht den Klartext des Suchkontenpassworts zurück. **Hinweis:** Wenn die LDAP-Authentifizierung derzeit deaktiviert ist, sind alle zurückgegebenen Einstellungen mit Ausnahme von "AuthType" und "groupSearchType" leer, die auf "SearchAndBind" bzw. "ActiveDirectory" gesetzt sind.	LdapKonfiguration

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetLdapConfiguration",
  "params": {},
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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%))"
     }
   }
}
```

Neu seit Version

9.6

TestLdapAuthentifizierung

Sie können das verwenden `TestLdapAuthentication` Methode zum Validieren der derzeit aktivierten LDAP-Authentifizierungseinstellungen. Wenn die Konfiguration korrekt ist, gibt der API-Aufruf die Gruppenmitgliedschaft des getesteten Benutzers zurück.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Benutzername	Der zu testenden Benutzername.	Zeichenfolge	Keine	Ja.
Passwort	Das Kennwort für den zu testenden Benutzernamen.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
LdapKonfiguration	Ein ldapConfiguration Objekt, das getestet werden soll. Wenn Sie diesen Parameter angeben, testet das System die angegebene Konfiguration, auch wenn die LDAP-Authentifizierung derzeit deaktiviert ist.	LdapKonfiguration	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Gruppen	Liste der LDAP-Gruppen, die den getesteten Benutzer als Mitglied enthalten.	Array erledigen
Benutzer-DN	Der vollständige LDAP Distinguished Name des geprüften Benutzers.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method": "TestLdapAuthentication",
"params": {"username":"admin1",
           "password":"admin1PASS"
      },
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
 "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"
  }
}
```

Neu seit Version

9.6

Multi-Faktor-Authentifizierungs-API-Methoden

AddIdpClusterAdmin

Sie können das verwenden `AddIpdClusterAdmin` Methode zum Hinzufügen eines Clusteradministratorbenutzers, der von einem Drittanbieter-Identitäts-Provider (IdP) authentifiziert wurde. IDP-Cluster-Administratorkonten werden basierend auf den Informationen zu SAML-Attributwerten konfiguriert, die in der SAML-Assertion des IdP bereitgestellt wurden, die mit dem Benutzer verknüpft ist. Wenn ein Benutzer erfolgreich mit dem IdP authentifiziert und SAML-Attributerklärungen innerhalb der SAML-Assertion besitzt, die mehreren IdP-Cluster-Administratorkonten entsprechen, verfügt der Benutzer über die kombinierte Zugriffsebene der entsprechenden IdP-Cluster-Administratorkonten.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Datenzugriff	Steuert, welche Methoden dieser IdP-Clusteradministrator verwenden kann.	String-Array	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Akzepteula	Akzeptieren Sie die Endnutzer-Lizenzvereinbarung. Setzen Sie auf „true“, um dem System ein Cluster-Administratorkonto hinzuzufügen. Wenn keine Angabe erfolgt oder auf FALSE gesetzt wird, schlägt der Methodenaufruf fehl.	boolesch	Keine	Ja.
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
Benutzername	Eine Zuordnung von SAML-Attributwerten zu einem IdP-Cluster-Administrator (z. B. E-Mail=test@example.com). Dies kann mit einem bestimmten SAML-Subjekt definiert werden `NameID` Oder als Eintrag in der SAML-Attributanweisung, z. B. `eduPersonAffiliation`.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Cluster-AdminID	Eindeutige Kennung für den neu erstellten Cluster-Administrator	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "AddIdpClusterAdmin",
    "params": {
        "username": "email=test@example.com",
        "acceptEula": true,
        "access": ["administrator"]
    }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "result": {
        "clusterAdminID": 13
    }
}
```

Neu seit Version

12.0

CreateIdpConfiguration

Sie können das verwenden `CreateIpdConfiguration` Methode zum Erstellen einer potenziellen Vertrauensbeziehung für die Authentifizierung mit einem Drittanbieter-Identitätsanbieter (IdP) für den Cluster. Für die IdP-Kommunikation ist ein SAML-Service-Provider-Zertifikat erforderlich. Dieses Zertifikat wird bei Bedarf generiert und von diesem API-Aufruf zurückgegeben.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
IdpMetadaten	IDP-Metadaten zu speichern.	Zeichenfolge	Keine	Ja.
IdpName	Name, der zur Identifizierung eines IdP-Providers für die Single-Sign-On SAML 2.0 verwendet wird.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
IdpConfigInfo	Informationen zur IdP-Konfiguration (Identity Provider) eines Drittanbieters.	"IdpConfigInfo"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "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"
    },
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "result": {
        "idpConfigInfo": {
        "enabled": false,
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n
        <EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n
        xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n
        xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n
        xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n
        ... </Organization>\r\n
        </EntityDescriptor>",
        "idpName": "https://privider.name.url.com",
        "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
        MIID...SlBHi\n
        -----END CERTIFICATE-----\n",
        "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
        }
    }
}
```


Neu seit Version

12.0

DeleteAuthSession

Sie können das verwenden `DeleteAuthSession` Methode zum Löschen einer einzelnen Benutzerauthentifizierungssitzung. Wenn sich der aufrufende Benutzer nicht in der ClusterAdmins / Administrator-Zugriffsgruppe befindet, kann nur die Authentifizierungssitzung des aufrufenden Benutzers gelöscht werden.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Sessionid	Eindeutige Kennung für die zu löschende auth-Sitzung.	UUID	Keine	Ja.

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Session	Sitzungsinformationen für die Löschsitzung.	"AuthSessionInfo"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "DeleteAuthSession",
    "params": {
        "sessionID": "a862a8bb-2c5b-4774-a592-2148e2304713"
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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"
        }
    }
}
```

Neu seit Version

12.0

DeleteAuthSessionByClusterAdmin

Sie können das verwenden `DeleteAuthSessionsByClusterAdmin` Methode zum Löschen aller mit dem angegebenen verknüpften Authentifizierungssitzungen `ClusterAdminID`. Wenn die angegebene ClusterAdminID einer Gruppe von Benutzern zugeordnet ist, werden alle Authentifizierungs-Sessions für alle Mitglieder dieser Gruppe gelöscht. Um eine Liste von Sitzungen zum möglichen Löschen anzuzeigen, verwenden Sie die Methode ListAuthSessionsByClusterAdmin mit dem `ClusterAdminID` Parameter.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Cluster-AdminID	Eindeutige Kennung für den Cluster-Administrator	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Sitzungen	Sitzungsinformationen für die gelöschten Authentifizierungssitzungen.	"AuthSessionInfo"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DeleteAuthSessionsByClusterAdmin",
  "params": {
    "clusterAdminID": 1
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"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"
      }
    ]
}
```


Neu seit Version

12.0

DeleteAuthSessionsByUsername

Sie können das verwenden `DeleteAuthSessionsByUsername` Methode zum Löschen aller Authentifizierungssitzungen für einen bestimmten Benutzer. Ein nicht in der Zugriffsgruppe ClusterAdmins/Administrator kann nur seine eigenen Sitzungen löschen. Ein Anrufer mit ClusterAdmins/Administratorrechten kann Sitzungen löschen, die einem beliebigen Benutzer angehören. Um die Liste der zu löschenden Sitzungen anzuzeigen, verwenden Sie `ListAuthSessionsByUsername` Mit den gleichen Parametern. Um eine Liste von Sitzungen zum möglichen Löschen anzuzeigen, verwenden Sie den `ListAuthSessionsByUsername` Methode mit dem gleichen Parameter.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
AuthMethod	Authentifizierungsmethode der zu löschenden Benutzersitzungen. Dieser Parameter kann nur von einem Anrufer in der ClusterAdmins/Administrator-Zugriffsgruppe angegeben werden. Mögliche Werte sind: • **AutMethod=Cluster** gibt den ClusterAdmin-Benutzernamen an. • **AuthMethod=LDAP** gibt den LDAP-DN des Benutzers an. • **AutMethod=IDP** gibt entweder die IdP UUID oder die NameID des Benutzers an. Wenn das IdP nicht so konfiguriert ist, dass es eine Option zurückgibt, gibt dies eine zufällige UUID an, die beim Erstellen der Sitzung ausgegeben wurde.	AuthMethod	Keine	Nein
Benutzername	Eindeutige Kennung für den Benutzer.	Zeichenfolge	Keine	Nein

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Sitzungen	Sitzungsinformationen für die gelöschten Authentifizierungssitzungen.	"AuthSessionInfo"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DeleteAuthSessionsByUsername",
  "params": {
    "authMethod": "Cluster",
    "username": "admin"
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"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"
      }
    ]
}
```

Neu seit Version

12.0

DeleteIdpKonfiguration

Sie können das verwenden `DeleteIdpConfiguration` Methode zum Löschen einer vorhandenen Konfiguration eines Drittanbieter-IdP für das Cluster. Durch Löschen der letzten IdP-Konfiguration wird das SAML-Service-Provider-Zertifikat aus dem Cluster entfernt.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
IdpKonfigurationID	UUID für die IdP-Konfiguration eines Drittanbieters.	UUID	Keine	Nein
IdpName	Name, der zum Identifizieren und Abrufen eines IdP-Providers für SAML 2.0 Single Sign-On verwendet wird.	Zeichenfolge	Keine	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DeleteIdpConfiguration",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
    "idpName": "https://provider.name.url.com"
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "result":{}
}
```

Neu seit Version

12.0

DisableIdpAuthentifizierung

Sie können das verwenden `DisableIdpAuthentication` Methode zum Deaktivieren der Unterstützung für die Authentifizierung mithilfe von Drittanbieter-IDPs für das Cluster. Nach der Deaktivierung können Benutzer, die von IDPs von Drittanbietern authentifiziert wurden, nicht mehr auf das Cluster zugreifen und alle aktiven authentifizierten Sitzungen werden nicht validiert/getrennt. LDAP- und Cluster-Administratoren können über unterstützte UIs auf das Cluster zugreifen.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DisableIdpAuthentication",
  "params": {}
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"result": {}
}
```

Neu seit Version

12.0

EnableIdpAuthentifizierung

Sie können das verwenden `EnableIdpAuthentication` Methode, um die Unterstützung für die Authentifizierung mithilfe von Drittanbieter-IDPs für den Cluster zu aktivieren. Sobald die IdP-Authentifizierung aktiviert ist, können LDAP- und Cluster-

Administratoren über unterstützte UIs nicht mehr auf das Cluster zugreifen und alle aktiven authentifizierten Sitzungen werden nicht validiert/getrennt. Nur durch Drittanbieter-IDPs authentifizierte Benutzer können über unterstützte UIs auf das Cluster zugreifen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
IdpKonfigurationID	UUID für die IdP-Konfiguration eines Drittanbieters. Wenn nur eine IdP-Konfiguration vorhanden ist, wird diese Konfiguration standardmäßig aktiviert. Wenn Sie nur über eine einzige IdpConfiguration verfügen, müssen Sie den Parameter idpConfiguration ID nicht angeben.	UUID	Keine	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "EnableIdpAuthentication",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"result": {}
}
```

Neu seit Version

12.0

GetIdpAuthenticationState

Sie können das verwenden `GetIdpAuthenticationState` Methode zur Rückgabe von Informationen zum Authentifizierungsstatus mithilfe von IDPs von Drittanbietern.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Aktiviert	Gibt an, ob die IdP-Authentifizierung eines Drittanbieters aktiviert ist.	boolesch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetIdpAuthenticationState"
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "result": {"enabled": true}
}
```

Neu seit Version

12.0

ListActiveAuthSessions

Sie können das verwenden `ListActiveAuthSessions` Methode zum Auflisten aller aktiven authentifizierten Sitzungen. Diese Methode kann nur von Benutzern mit Administratorrechten verwendet werden.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Sitzungen	Sitzungsinformationen für die Authentifizierungssitzungen.	"AuthSessionInfo"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListActiveAuthSessions"
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"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"
      }
    ]
}
```


Neu seit Version

12.0

ListIdpConfigurations

Sie können das verwenden `ListIdpConfigurations` Methode zum Auflisten von Konfigurationen für IDPs von Drittanbietern. Optional können Sie entweder die angeben `enabledOnly` Flag zum Abrufen der derzeit aktivierten IdP-Konfiguration oder einer IdP-Metadaten-UUID oder IdP-Namen, um Informationen für eine bestimmte IdP-Konfiguration abzufragen.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Barbardnur	Filtert das Ergebnis, um die aktuell aktivierte IdP-Konfiguration zurückzugeben.	boolesch	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
IdpKonfigurationID	UUID für die IdP-Konfiguration eines Drittanbieters.	UUID	Keine	Nein
IdpName	Ruft IdP-Konfigurationsinformationen für einen bestimmten IdP-Namen ab.	Zeichenfolge	Keine	Nein

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
IdpConfigInfos	Informationen zu den IdP-Konfigurationen von Drittanbietern.	"IdpConfigInfo" Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListIdpConfigurations",
  "params": {}
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "result": {
        "idpConfigInfo": {
        "enabled": true,
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n
        <EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n
        xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n
        xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n
        xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n
        ...</Organization>\r\n
        </EntityDescriptor>",
        "idpName": "https://privider.name.url.com",
        "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
        MI...BHi\n
        -----END CERTIFICATE-----\n",
        "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
        }
    }
}
```


Neu seit Version

12.0

UpdateIdpKonfiguration

Sie können das verwenden `UpdateIdpConfiguration` Methode zum Aktualisieren einer vorhandenen Konfiguration mit einem IdP eines Drittanbieters für das Cluster.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
GenerateNewCertificate	Wenn True angegeben wird, wird ein neuer SAML-Schlüssel und ein neues Zertifikat generiert und das vorhandene Paar ersetzt. Hinweis: Durch das Ersetzen des vorhandenen Zertifikats wird das etablierte Vertrauen zwischen dem Cluster und dem IdP unterbrochen, bis die Metadaten des Clusters am IdP neu geladen sind. Wenn nicht angegeben oder auf false gesetzt, bleiben SAML-Zertifikat und -Schlüssel unverändert.	boolesch	Keine	Nein
IdpKonfigurationID	UUID für die IdP-Konfiguration eines Drittanbieters.	UUID	Keine	Nein
IdpMetadaten	IDP-Metadaten für Konfigurations- und Integrationsdetails für SAML 2.0 Single Sign-On.	Zeichenfolge	Keine	Nein
IdpName	Name, der zum Identifizieren und Abrufen eines IdP-Providers für SAML 2.0 Single Sign-On verwendet wird.	Zeichenfolge	Keine	Nein
NewIdpName	Wenn angegeben, ersetzt dieser Name den alten IdP-Namen.	Zeichenfolge	Keine	Nein

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
IdpConfigInfo	Informationen rund um die IdP-Konfiguration von Drittanbietern.	"IdpConfigInfo"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method": "UpdateIdpConfiguration",
"params": {
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "generateNewCertificate": true
    }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "result": {
        "idpConfigInfo": {
        "enabled": true,
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n
        <EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n
        xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n
        xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n
        xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n
        ...</Organization>\r\n
        </EntityDescriptor>",
        "idpName": "https://privider.name.url.com",
        "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
        MI...BHi\n
        -----END CERTIFICATE-----\n",
        "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
        }
    }
}
```


Neu seit Version

12.0

API-Methoden für die Sitzungsauthentifizierung

ListAuthSessionByClusterAdmin

Sie können das verwenden `ListAuthSessionsByClusterAdmin` Methode zum Auflisten aller mit dem angegebenen verknüpften auth-Sitzungen `ClusterAdminID`. Wenn der angegebene `ClusterAdminID` Karten zu einer Gruppe von Benutzern werden alle Auth-Sitzungen für alle Mitglieder dieser Gruppe aufgelistet.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Cluster-AdminID	Eindeutige Kennung für den Cluster-Administrator	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Sitzungen	Liste der Sitzungsinformationen für die auth Sessions.	"AuthSessionInfo"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "ListAuthSessionsByClusterAdmin",
    "clusterAdminID": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"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"
      }
    ]
}
```

Neu seit Version

12.0

ListAuthSessionsByBenutzername

Sie können das verwenden `ListAuthSessionsByUsername` Methode zum Auflisten aller Auth-Sitzungen für den angegebenen Benutzer. Ein Anrufer, der nicht in der Zugriffsgruppe enthalten ist ClusterAdmins/Administratorrechte dürfen nur seine eigenen Sitzungen auflisten. Ein Anrufer mit ClusterAdmins/Administratorrechten kann Sitzungen eines beliebigen Benutzers auflisten.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
AuthMethod	Authentifizierungsmethode der zu aufgelistenden Benutzersitzungen. Dieser Parameter kann nur von einem Anrufer in der ClusterAdmins/Administrator-Zugriffsgruppe angegeben werden. Mögliche Werte sind: • **AutMethod=Cluster** gibt den ClusterAdmin-Benutzernamen an. • **AuthMethod=LDAP** gibt den LDAP-DN des Benutzers an. • **AutMethod=IDP** gibt entweder die IdP UUID oder die NameID des Benutzers an. Wenn das IdP nicht so konfiguriert ist, dass es eine Option zurückgibt, gibt dies eine zufällige UUID an, die beim Erstellen der Sitzung ausgegeben wurde.	AuthMethod	Keine	Ja.
Benutzername	Eindeutige Kennung für den Benutzer.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Sitzungen	Liste der Sitzungsinformationen für die auth Sessions.	"AuthSessionInfo"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "ListAuthSessionsByUsername",
    "authMethod": "Cluster",
    "username": "admin"
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"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"
      }
    ]
}
```

Neu seit Version

12.0

Node-API-Methoden

CheckPingOnVlan

Sie können das verwenden `CheckPingOnVlan` Methode zum Testen der Netzwerkverbindung auf einem temporären VLAN bei der Durchführung der Netzwerkvalidierung vor der Bereitstellung. `CheckPingOnVlan` Erstellt eine temporäre VLAN-Schnittstelle, sendet ICMP-Pakete mithilfe der VLAN-Schnittstelle an alle Knoten im Speicher-Cluster und entfernt dann die Schnittstelle.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Versuche	Gibt an, wie oft das System den Ping-Test wiederholen soll.	Ganzzahl	5	Nein
Hosts	Gibt eine kommagetrennte Liste von Adressen oder Hostnamen von Geräten an, die Ping verwenden sollen.	Zeichenfolge	Die Nodes im Cluster	Nein
Schnittstelle	Die bestehende (Basis-)Schnittstelle, von der die Pings gesendet werden sollen. Mögliche Werte: • Bond10G: Sendet Pings von der Bond10G-Schnittstelle. • Bond1G: Senden von Pings von der Bond1G-Schnittstelle.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
PacketSize	Gibt die Anzahl der Bytes an, die in das ICMP-Paket gesendet werden sollen, das an jede IP gesendet wird. Die Anzahl der Bytes muss kleiner sein als die in der Netzwerkkonfiguration angegebene maximale MTU.	Ganzzahl	Keine	Nein
PingTimeoutMsec	Gibt die Anzahl der Millisekunden an, die für jede einzelne Ping-Antwort warten soll.	Ganzzahl	500 ms	Nein
Verbot der Fragmentierung	Aktiviert das DF-Flag (Do Not Fragment) für die ICMP-Pakete.	boolesch	Falsch	Nein
SourceAddressV4	Die IPv4-Quelladresse, die in den ICMP-Ping-Paketen verwendet werden soll.	Zeichenfolge	Keine	Ja.
SourceAddressV6	Die IPv6-Quelladresse, die in den ICMP-Ping-Paketen verwendet werden soll.	Zeichenfolge	Keine	Ja.
TotalTimeoutSec	Gibt die Zeit in Sekunden an, die der Ping auf eine Systemantwort warten soll, bevor er den nächsten Ping-Versuch ausgibt oder den Prozess beendet.	Ganzzahl	5	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
VirtualNetworkTag	Die VLAN-ID, die beim Senden der Ping-Pakete verwendet wird.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Ergebnis	Liste jeder IP der Knoten konnte mit und Ping-Antwortstatistiken kommunizieren.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "CheckPingOnVlan",
    "params": {
        "interface": "Bond10G",
        "virtualNetworkTag": 4001,
        "sourceAddressV4": "192.168.41.4",
        "hosts": "192.168.41.2"
},
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
    }
  }
}
```


Neu seit Version

11.1

CheckeAngebot NodeAdditions

Sie können das verwenden `CheckProposedNodeAdditions` Methode zum Testen einer Reihe von Storage-Nodes, um zu ermitteln, ob Sie diese einem Storage Cluster ohne Fehler oder Verstöße gegen die Best Practices hinzufügen können.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Knoten	Eine Liste der Storage-IP-Adressen von Storage-Nodes, die einem Storage-Cluster hinzugefügt werden können	String-Array	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Antragsteller ClusterValid	Gibt an, ob die vorgeschlagenen Storage-Nodes ein gültiges Storage-Cluster bilden oder nicht. Mögliche Werte: • Richtig • Falsch	boolesch

Antragsteller ClusterErrors	Fehler, die auftreten würden, wenn ein Storage-Cluster mit den vorgeschlagenen Storage-Nodes erstellt würde. Mögliche Fehlercodes: • `nodesNoCapacity`: Knoten hatten keine nutzbare Kapazität. • `nodesTooLarge`: Knoten stellen für das aktive Schutzschema einen zu großen Teil der Clusterkapazität dar. • `nodesConnectFailed`: Verbindung zu Knoten konnte nicht hergestellt werden, um die Hardwarekonfiguration abzufragen. • `nodesQueryFailed`: Knoten konnten nicht nach Hardware-Konfiguration abgefragt werden. • `nodesClusterMember`: IP-Adressen für Knoten werden bereits im Cluster verwendet. • `nonFipsNodeCapable`: Es ist nicht möglich, einen nicht FIPS-fähigen Knoten zum Speicher-Cluster hinzuzufügen, während die Verschlüsselungsfunktion für FIPS 140-2-Laufwerke aktiviert ist. • `nonFipsDrivesCapable`: Es ist nicht möglich, einen Knoten mit nicht FIPS-fähigen Laufwerken zum Cluster hinzuzufügen, während die FIPS 140-2 Laufwerksverschlüsselungsfunktion aktiviert ist.	String-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "CheckProposedNodeAdditions",
    "params": {
    "nodes": [
        "192.168.1.11",
        "192.168.1.12",
        "192.168.1.13",
        "192.168.1.14"
    ]
},
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "proposedClusterValid": true,
        "proposedClusterErrors": [ ]
    }
}
```

Neu seit Version

11.0

CreateClusterSupportBundle

Sie können das verwenden `CreateClusterSupportBundle` Auf dem Management-Node, um Support-Bundles von allen Nodes eines Clusters zu erfassen. Die unterstützten Bundles der einzelnen Nodes werden als tar.gz Dateien komprimiert. Das Cluster-Support-Bundle ist eine tar-Datei mit den Knoten-Support-Bundles. Sie können diese Methode nur auf einem Management-Node ausführen. Dies funktioniert nicht, wenn Sie auf einem Storage-Node ausgeführt werden.

Parameter

Sie müssen diese Methode für den Management-Node anrufen. Beispiel:

```
https://<management node IP>:442/json-rpc/10.0
```

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
NachlassVervollständigung	Ermöglicht die Ausführung des Skripts, wenn Pakete nicht von einem oder mehreren Knoten gesammelt werden können.	boolesch	Keine	Nein
Beetname	Eindeutiger Name für jedes erstellte Supportpaket. Wenn kein Name angegeben wird, werden „Supportbundle“ und der Node-Name als Dateiname verwendet	Zeichenfolge	Keine	Nein
mvip	Das MVIP des Clusters. Bundles werden von allen Nodes im Cluster gesammelt. Dieser Parameter ist erforderlich, wenn der Node-Parameter nicht angegeben ist.	Zeichenfolge	Keine	Ja.
Knoten	Die IP-Adressen der Nodes, aus denen Pakete gesammelt werden sollen. Verwenden Sie entweder Knoten oder mvip, jedoch nicht beides, um die Knoten anzugeben, von denen Pakete gesammelt werden sollen. Dieser Parameter ist erforderlich, wenn mvip nicht angegeben wird.	String-Array	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Passwort	Das Cluster-Admin-Passwort. **Hinweis:** Dieses Passwort ist als Text bei Eingabe sichtbar.	Zeichenfolge	Keine	Ja.
Benutzername	Der Benutzername des Cluster-Admin-Benutzers.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method": "CreateClusterSupportBundle",
"params": {
          "bundlename": "clusterbundle",
          "mvip": "132.119.120.100"
     }
   },
 "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
    }
}
```


Neu seit Version

9.6

CreateSupportBundle

Verwenden Sie können `CreateSupportBundle` Um eine Support Bundle-Datei unter dem Verzeichnis des Node zu erstellen. Nach der Erstellung wird das Bundle als tar-Datei auf dem Knoten gespeichert (die Option gz-Komprimierung ist über den Parameter extraArgs verfügbar.)

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Beetname	Eindeutiger Name für das Support-Bundle. Wenn kein Name angegeben wird, werden „Supportbundle“ und der Node-Name als Dateiname verwendet.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
ExtraArgs	Verwenden Sie '--compress gz', um das Support-Paket als tar.gz-Datei zu erstellen.	Zeichenfolge	Keine	Nein
TimeoutSec	Die Anzahl der Sekunden, die das Skript für das Support-Bundle ausgeführt wird.	Ganzzahl	1500	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Details	Details zum Support-Bundle. Mögliche Werte: • BundleName: Der in der CreateSupportBundleAPI-Methode angegebene Name. Falls kein Name angegeben wurde, wird „Supportbundle“ verwendet. • ExtraArgs: Die Argumente wurden mit dieser Methode bestanden. • Dateien: Eine Liste der vom System erstellten Support Bundle-Dateien. • Ausgabe: Die Kommandozeilenausgabe aus dem Skript, das das Supportpaket erstellt hat. • TimeoutSec: Die Anzahl der Sekunden, die das Skript des Support-Bundles vor dem Anhalten ausgeführt wird. • url: URL zum erstellten Support-Paket.	JSON-Objekt

Dauer	Die Zeit, die zum Erstellen des Support-Bundles im Format HH:MM:SS.ssssss verwendet wurde.	Zeichenfolge
Ergebnis	Erfolg oder Misserfolg des Support-Bundle-Vorgangs.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
 "method": "CreateSupportBundle",
"params": {
  "extraArgs": "--compress gz"
 },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"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"
  }
}
```


Neu seit Version

9.6

DeleteAllSupportBundles

Sie können das verwenden `DeleteAllSupportBundles` Methode zum Löschen aller mit dem erstellten Support-Bundles `CreateSupportBundle` API-Methode.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "DeleteAllSupportBundles",
   "params": {}
  },
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {}
 }
}
```

Neu seit Version

9.6

Instandhaltungmodus

Sie können das verwenden `DisableMaintenanceMode` Methode, um den Wartungsmodus eines Storage-Node zu beenden. Nachdem Sie die Wartung abgeschlossen haben und der Node online ist, sollten Sie den Wartungsmodus nur deaktivieren.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Knoten	Liste der Storage-Node-IDs, die den Wartungsmodus nicht verlassen sollen	Integer-Array	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ

Asynchron	Sie können die Methode GetAsyncResult verwenden, um diese Async Handle abzurufen und zu bestimmen, wann die Transition des Wartungsmodus abgeschlossen ist.	Ganzzahl
Stromstärkemodus	Der aktuelle Status des Wartungsmodus des Node. Mögliche Werte: • Deaktiviert: Es wurde keine Wartung angefordert. • FailedToRecover: Der Knoten konnte nicht aus dem Wartungsmodus wiederherstellen. • Unerwartete: Der Node wurde offline gefunden, war aber im deaktivierten Modus. • RecoveringFromMaintenance: Der Knoten wird gerade vom Wartungsmodus wiederhergestellt. • VorbereitungForMaintenance: Es werden Maßnahmen ergriffen, um einen Knoten vorzubereiten, der gewartet werden soll. • ReadyForMaintenance: Der Knoten ist zur Durchführung der Wartung bereit.	Wartungsmodus (String)

Anforderungsmodus	Der angeforderte Wartungsmodus des Node. Mögliche Werte: • Deaktiviert: Es wurde keine Wartung angefordert. • FailedToRecover: Der Knoten konnte nicht aus dem Wartungsmodus wiederherstellen. • Unerwartete: Der Node wurde offline gefunden, war aber im deaktivierten Modus. • RecoveringFromMaintenance: Der Knoten wird gerade vom Wartungsmodus wiederhergestellt. • VorbereitungForMaintenance: Es werden Maßnahmen ergriffen, um einen Knoten vorzubereiten, der gewartet werden soll. • ReadyForMaintenance: Der Knoten ist zur Durchführung der Wartung bereit.	Wartungsmodus (String)

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DisableMaintenanceMode",
  "params": {
    "nodes": [6]
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {
        "requestedMode": "Disabled",
        "asyncHandle": 1,
        "currentMode": "Enabled"
     }
}
```

Neu seit Version

12.2

Weitere Informationen

"Konzepte des NetApp HCI Storage-Wartungsmodus"

DisableSsh

Sie können das verwenden `DisableSsh` Methode zum Deaktivieren des SSH-Service für einen einzelnen Storage-Node Diese Methode hat keine Auswirkungen auf die Dauer der Zeitüberschreitung des Cluster-weiten SSH-Service.

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Aktiviert	Der Status des SSH-Service für diesen Node.	boolesch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DisableSsh",
  "params": {
      },
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {"enabled": false}
}
```

Instandhaltungmodus

Sie können das verwenden `EnableMaintenanceMode` Methode zum Vorbereiten eines Storage-Nodes für Wartungsarbeiten. Wartungsszenarien beinhalten alle Aufgaben, die das Ausschalten oder Neustarten des Node erfordern.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ErwegeUnresolvedForcards	Aktivierung des Wartungsmodus für diesen Node erzwingen, selbst wenn Cluster-Fehler blockiert sind.	boolesch	Falsch	Nein
Knoten	Die Liste der Node-IDs, die in den Wartungsmodus versetzt werden sollen. Es wird nur jeweils ein Node unterstützt.	Integer-Array	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
PerMinutePrimarySwapLimit	Die Anzahl der primären Schichten, die pro Minute ausgetauscht werden sollen. Wenn nicht angegeben, werden alle primären Schichten gleichzeitig ausgetauscht.	Ganzzahl	Keine	Nein
Zeitüberschreitung	Gibt an, wie lange der Wartungsmodus aktiviert bleiben soll, bevor er automatisch deaktiviert wird. Formatiert als Zeitzeichenfolge (z. B. HH:mm:ss). Wenn nicht angegeben, bleibt der Wartungsmodus aktiviert, bis er explizit deaktiviert ist.	Zeichenfolge	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Asynchron	Sie können die Methode GetAsyncResult verwenden, um diese Async Handle abzurufen und zu bestimmen, wann die Transition des Wartungsmodus abgeschlossen ist.	Ganzzahl

Stromstärkemodus	Der aktuelle Status des Wartungsmodus des Node. Mögliche Werte: • Deaktiviert: Es wurde keine Wartung angefordert. • FailedToRecover: Der Knoten konnte nicht aus dem Wartungsmodus wiederherstellen. • RecoveringFromMaintenance: Der Knoten wird gerade vom Wartungsmodus wiederhergestellt. • VorbereitungForMaintenance: Es werden Maßnahmen ergriffen, um einen Knoten vorzubereiten, der gewartet werden soll. • ReadyForMaintenance: Der Knoten ist zur Durchführung der Wartung bereit.	Wartungsmodus (String)
Anforderungsmodus	Der angeforderte Wartungsmodus des Node. Mögliche Werte: • Deaktiviert: Es wurde keine Wartung angefordert. • FailedToRecover: Der Knoten konnte nicht aus dem Wartungsmodus wiederherstellen. • RecoveringFromMaintenance: Der Knoten wird gerade vom Wartungsmodus wiederhergestellt. • VorbereitungForMaintenance: Es werden Maßnahmen ergriffen, um einen Knoten vorzubereiten, der gewartet werden soll. • ReadyForMaintenance: Der Knoten ist zur Durchführung der Wartung bereit.	Wartungsmodus (String)

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "EnableMaintenanceMode",
  "params": {
    "forceWithUnresolvedFaults": False,
    "nodes": [6],
    "perMinutePrimarySwapLimit" : 40,
    "timeout" : "01:00:05"
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {
        "requestedMode": "ReadyForMaintenance",
        "asyncHandle": 1,
        "currentMode": "Disabled"
     }
}
```

Neu seit Version

12.2

Weitere Informationen

"Konzepte des NetApp HCI Storage-Wartungsmodus"

EnableSsh

Sie können das verwenden `EnableSsh` Methode zum Aktivieren des SSH-Dienstes (Secure Shell) für einen einzelnen Node. Diese Methode wirkt sich nicht auf die Cluster-weite SSH-Zeitüberschreitungsdauer aus und befreit den Node nicht davon, SSH durch das globale SSH-Timeout deaktiviert zu haben.

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Aktiviert	Der Status des SSH-Service für diesen Node.	boolesch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "EnableSsh",
  "params": {
     },
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {"enabled": true}
}
```

GetClusterConfig

Sie können das verwenden `GetClusterConfig` API-Methode zur Rückgabe von Informationen über die Cluster-Konfiguration verwendet der Node zur Kommunikation mit seinem Cluster.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Cluster	Informationen zur Cluster-Konfiguration, die der Node zur Kommunikation mit dem Cluster verwendet.	Cluster

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetClusterConfig",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
    }
  }
}
```

Neu seit Version

9.6

GetClusterStatus

Sie können das verwenden `GetClusterState` API-Methode zur Angabe, ob ein Node Teil eines Clusters ist oder nicht.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Cluster	Der Name des Clusters.	Zeichenfolge
Bundesland	• Verfügbar: Der Node wurde nicht mit einem Cluster-Namen konfiguriert. • Ausstehend: Node steht für ein bestimmtes benanntes Cluster aus und kann hinzugefügt werden. • Aktiv: Node ist ein aktives Mitglied eines Clusters und kann keinem anderen Cluster hinzugefügt werden.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetClusterState",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1,
   "result" :
      "cluster" :  "Cluster101"
      "state" : "Active"
}
```

Neu seit Version

9.6

Getconfig

Sie können das verwenden `GetConfig` API-Methode zum Abrufen aller Konfigurationsinformationen für einen Node. Diese API-Methode enthält die gleichen Informationen, die in beiden verfügbar sind `GetClusterConfig` Und `GetNetworkConfig` API-Methoden

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Konfigurations	Die Konfigurationsdetails des Clusters. Dieses Objekt enthält: • Cluster: Cluster-Informationen, die erkennen, wie der Storage-Node mit dem Storage-Cluster kommuniziert, mit dem er verknüpft ist. • Netzwerk (alle Schnittstellen): Netzwerkverbindungstypen und aktuelle Einstellungen für jede Netzwerkschnittstelle des Knotens.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetConfig",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Aufgrund der Länge dieses Antwortbeispiels wird es in einem ergänzenden Thema dokumentiert.

Neu seit Version

9.6

Weitere Informationen

- GetClusterConfig
- GetNetworkConfig
- Getconfig

GetDriveConfig

Sie können das verwenden `GetDriveConfig` Methode zum Abrufen von Laufwerksinformationen für die erwartete Anzahl von Slices und Blocklaufwerken sowie die Anzahl der Schichten und Blocklaufwerke, die derzeit mit dem Node verbunden sind.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Auffahrt Konfiguration	Informationen zu den Laufwerken, die mit dem Node verbunden sind.	Laufwerk

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetDriveConfig",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Die Antworten für diese Methode sind dem folgenden Beispiel ähnlich. Aufgrund der Länge enthält die Antwort nur Informationen für ein Laufwerk eines Storage-Node.

```
{
    "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
            }
    }
}
```

VMware HardwareConfig

Sie können das verwenden `GetHardwareConfig` Methode zum Abrufen der Hardware-Konfigurationsinformationen für einen Node. Diese Konfigurationsdaten sind für den internen Gebrauch bestimmt. Verwenden Sie den, um eine nützliche Live-Bestandsaufnahme der Systemhardwarekomponenten zu erhalten `GetHardwareInfo` Methode.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
HardwareKonfig	Liste der Hardwareinformationen und aktuellen Einstellungen	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetHardwareConfig",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Die Antworten für diese Methode sind dem folgenden Beispiel ähnlich.

```
{
    "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
            }
        }
    }
}
```


Neu seit Version

9.6

GetHardwareInfo

Sie können das verwenden `GetHardwareInfo` Methode zum Abrufen von Live-Hardware-Informationen und -Status für einen einzelnen Node Hardwareinformationen umfassen im Allgemeinen Hersteller, Anbieter, Versionen, Laufwerke und andere damit verbundene Identifikationsinformationen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Erzwingen	Setzen Sie diesen Parameter „Force“ auf „true“, um auf allen Nodes im Cluster ausgeführt zu werden.	boolesch	Falsch	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
HardwareInfo	Hardwareinformationen für den Node	HardwareInfo

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetHardwareInfo",
   "params": {
   },
"id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
        },
      ...
      ]
    }
  }
}
```


Neu seit Version

9.6

GetIpmiConfig

Sie können das verwenden `GetIpmiConfig` Methode zum Abrufen von Hardware-Sensorinformationen von Sensoren, die sich im Node befinden.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ
Chassistyp	Wird verwendet, um Informationen für jeden Node-Chassis-Typ anzuzeigen. Mögliche Werte: • Alle: Gibt für jeden Chassis-Typ Sensorinformationen zurück. • {Chassis-Typ}: Liefert Sensorinformationen für einen angegebenen Chassis-Typ.	Zeichenfolge

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Sensorname	Name des gefundenen Sensors.	Zeichenfolge
UniqueSensorID	Eindeutige Kennung für den Sensor.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetIpmiConfig",
  "params": {
     "chassisType"; "all"
     },
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
 "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"
```

```
                    }
                ],
            }
```

Neu seit Version

9.6

GetIpmiInfo

Sie können das verwenden `GetIpmiInfo` Methode zur Anzeige einer detaillierten Meldung von Sensoren (Objekten) für Knotenlüfter, ein- und Auspufftemperaturen sowie von dem System überwachte Netzteile.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Sensoren	Detaillierte Informationen von jedem Sensor innerhalb eines Node	JSON-Objekt-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetIpmiInfo",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Aufgrund der Länge der zurückgegebenen Antwort für diese API-Methode wurden Teile der Antwort absichtlich aus diesem Dokument entfernt. Enthalten sind die Bestandteile der Hardwareinformationen, die das System überwacht, um sicherzustellen, dass der Knoten mit optimaler Leistung ausgeführt wird.

```
{
  "id": 1,
    "result": {
```

```
    "ipmiInfo": {
        "sensors": [
          {
            "entityID": "7.1 (System Board)",
            "sensorID": "0x72",
            "sensorName": "SEL",
            "sensorType": "Event Logging Disabled",
            "uniqueSensorID": "7.1:0x72"
          },
          {
            "assertionsEnabled": [ "General Chassis intrusion" ],
            "deassertionsEnabled": [ "General Chassis intrusion" ],
            "entityID": "7.1 (System Board)", "sensorID": "0x73",
            "sensorName": "Intrusion",
            "sensorType": "Physical Security",
            "uniqueSensorID": "7.1:0x73"
          },
          {THIS ENTIRE SECTION IS REPEATED FOR EACH FAN IN THE SYSTEM
            "assertionEvents": [],
            "assertionsEnabled": [],
            "deassertionsEnabled": [],
            "entityID": "7.1 (System Board)",
            "eventMessageControl": "Per-threshold",
            "lowerCritical": "720.000",
            "lowerNonCritical": "840.000",
            "maximumSensorRange": "Unspecified",
            "minimumSensorRange": "Unspecified",
            "negativeHysteresis": "600.000",
            "nominalReading": "10080.000",
            "normalMaximum": "23640.000",
            "normalMinimum": "16680.000",
            "positiveHysteresis": "600.000",
            "readableThresholds": "lcr lnc",
            "sensorID": "0x30",
            "sensorName": "Fan1A RPM",
            "sensorReading": "4440 (+/- 120) RPM",
            "sensorType": "Fan",
            "settableThresholds": "",
            "status": "ok",
            "thresholdReadMask": "lcr lnc",
            "uniqueSensorID": "7.1:0x30"
          },
          .
          .
          .
          {THIS ENTIRE SECTION IS REPEATED FOR THE EXHAUST TEMPERATURE
```

```
OF EACH NODE
              "assertionEvents": [],
              "assertionsEnabled": [],
              "entityID": "7.1 (System Board)",
              "eventMessageControl": "Per-threshold",
              "lowerCritical": "3.000",
              "lowerNonCritical": "8.000",
              "maximumSensorRange": "Unspecified",
              "minimumSensorRange": "Unspecified",
              "negativeHysteresis": "1.000",
              "nominalReading": "23.000",
              "normalMaximum": "69.000",
              "normalMinimum": "11.000",
              "positiveHysteresis": "1.000",
              "readableThresholds": "lcr lnc unc ucr",
              "sensorID": "0x1",
              "sensorName": "Exhaust Temp",
              "sensorReading": "44 (+/- 1) degrees C",
              "sensorType": "Temperature",
              "settableThresholds": "",
              "status": "ok",
              "uniqueSensorID": "7.1:0x1",
              "upperCritical": "75.000",
              "upperNonCritical": "70.000"
            },
            {THIS ENTIRE SECTION IS REPEATED FOR THE INLET TEMPERATURE OF
EACH NODE
              "assertionEvents": [],
              "assertionsEnabled": [],
              "deassertionsEnabled": [],
              "entityID": "7.1 (System Board)",
              "eventMessageControl": "Per-threshold",
              "lowerCritical": "-7.000",
              "lowerNonCritical": "3.000",
              "maximumSensorRange": "Unspecified",
              "minimumSensorRange": "Unspecified",
              "negativeHysteresis": "1.000",
              "nominalReading": "23.000",
              "normalMaximum": "69.000",
              "normalMinimum": "11.000",
              "positiveHysteresis": "1.000",
              "readableThresholds": "lcr lnc unc ucr",
              "sensorID": "0x4",
              "sensorName": "Inlet Temp",
              "sensorReading": "20 (+/- 1) degrees C",
              "sensorType": "Temperature",
```

```
              "settableThresholds": "lcr lnc unc ucr",
              "status": "ok",
              "thresholdReadMask": "lcr lnc unc ucr",
              "uniqueSensorID": "7.1:0x4",
              "upperCritical": "47.000",
              "upperNonCritical": "42.000"
            },
            {THIS ENTIRE SECTION IS REPEATED FOR EACH POWER SUPPLY ON EACH
NODE
              "assertionEvents": [],
              "assertionsEnabled": [],
              "entityID": "10.2 (Power Supply)",
              "eventMessageControl": "Per-threshold",
"maximumSensorRange": "Unspecified",
              "minimumSensorRange": "Unspecified",
              "negativeHysteresis": "Unspecified",
              "nominalReading": "0.000",
              "normalMaximum": "0.000",
              "positiveHysteresis": "Unspecified",
              "readableThresholds": "No Thresholds",
              "sensorID": "0x6d",
              "sensorName": "Voltage 2",
              "sensorReading": "118 (+/- 0) Volts",
              "sensorType": "Voltage",
              "settableThresholds": "No Thresholds", "status": "ok",
"uniqueSensorID": "10.2:0x6d"
            },
              .
              .
              .
            }
          ]
        }
      }
    }
```


Neu seit Version

9.6

GetNetworkConfig

Sie können das verwenden `GetNetworkConfig` Methode zum Anzeigen der Netzwerkkonfigurationsinformationen für einen Node.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Netzwerk	Verbindungstypen und aktuelle Einstellungen für jede Netzwerkschnittstelle des Nodes.	Netzwerk (alle Schnittstellen)

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetNetworkConfig",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Aufgrund der Länge dieses Antwortbeispiels wird es in einem ergänzenden Thema dokumentiert.

Neu seit Version

9.6

Weitere Informationen

GetNetworkConfig

GetNetworkInterface

Sie können das verwenden `GetNetworkInterface` Methode zum Abrufen von Informationen über eine Netzwerkschnittstelle auf einem Node.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Schnittstelle	Der Name der Schnittstelle, über die Informationen für den einzelnen Node angezeigt werden sollen. Mögliche Werte: • Bond1G • Bond10G	Zeichenfolge	Keine	Nein
Erzwingen	Setzen Sie diesen Parameter auf „true“, um auf allen Nodes im Cluster ausgeführt zu werden.	boolesch	Falsch	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Knoten	Ein Array von Objekten, die die Schnittstelle für die einzelnen Storage-Nodes im Storage-Cluster beschreiben Jedes Objekt im Array enthält die folgenden Elemente: • NodeID: (Integer) die ID des Speicherknoten im Speicher-Cluster die Schnittstelleninformationen gelten für. • Ergebnis: (Netzwerkschnittstelle) Schnittstellenkonfigurationsinformationen für diesen Speicherknoten.	JSON-Objekt-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "GetNetworkInterface",
    "params": {
        "interface": "Bond1G",
        "force": true
        },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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
                }
            }
        }
    ]
}
```

```
}
```

Neu seit Version

9.6

GetNodeActiveTlsCiphers

Sie können das verwenden `GetNodeActiveTlsCiphers` Methode auf einem einzelnen Knoten, um eine Liste der TLS-Chiffren zu erhalten, die derzeit auf diesem Knoten akzeptiert werden. Sie können diese Methode auf Management- und Storage-Nodes verwenden.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
MandatoryCiphers	Liste der obligatorischen TLS-Chiffren-Suites für den Knoten. Dies sind Chiffren, die auf dem Knoten immer aktiv sind.	Zeichenfolge
SupplementalCiphers	Liste der zusätzlichen TLS-Chiffren-Suites für den Knoten.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetNodeActiveTlsCiphers",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
      "id" : 1,
      "result" : {
        "mandatoryCiphers": [
            "DHE-RSA-AES256-SHA256",
            "DHE-RSA-AES256-GCM-SHA384",
            "ECDHE-RSA-AES256-SHA384",
            "ECDHE-RSA-AES256-GCM-SHA384"
        ],
        "supplementalCiphers": [
            "DHE-RSA-AES128-SHA256",
            "DHE-RSA-AES128-GCM-SHA256",
            "ECDHE-RSA-AES128-SHA256",
            "ECDHE-RSA-AES128-GCM-SHA256"
        ]
    }
}
```

GetNodeFipsDrivesReport

Sie können das verwenden `GetNodeFipsDrivesReport` Methode zur Überprüfung des FIPS 140-2 Laufwerksverschlüsselungsstatus eines einzelnen Node im Storage Cluster. Sie müssen diese Methode für einen einzelnen Storage-Node ausführen.

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
FipsDrives	Ein JSON-Objekt, das den Status der Unterstützung von FIPS 140-2-Funktionen für diesen Node enthält. Mögliche Werte: • Keine: Node ist nicht FIPS-fähig. • Partiell: Node ist FIPS-fähig, nicht alle Laufwerke im Node sind FIPS-Laufwerke. • Bereit: Node ist FIPS-fähig und alle Laufwerke im Node sind FIPS-Laufwerke (oder es sind keine Laufwerke vorhanden).	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetNodeFipsDrivesReport",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "fipsDrives": "None"
    }
}
```

Neu seit Version

11.5

GetNodeSSLZertifikat

Sie können das verwenden `GetNodeSSLCertificate` Methode zum Abrufen des SSL-Zertifikats, das derzeit auf dem Management-Node aktiv ist.

Parameter

Sie müssen diese Methode für den Management-Node anrufen. Beispiel:

```
https://<management node IP>:442/json-rpc/10.0
```

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Zertifikat	Der vollständige PEM-codierte Text des Zertifikats.	Zeichenfolge
Details	Die decodierten Informationen des Zertifikats.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method" : "GetNodeSSLCertificate",
    "params" : {},
    "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "certificate": "-----BEGIN CERTIFICATE-----
\nMIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSIb3DQEBBQUAMIGDMQswCQYD\nVQQGEw
JVUzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\nA1UEChMYV2hhdC
BIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBFh53\naGF0aGFwcGVuc0B2ZWdhc3
N0YXlzaW4udmVnYXMwHhcNMTcwMzA4MjI1MDI2WhcN\nMjcwMzA2MjI1MDI2WjCBgzELMAkGA1
UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYD\nVQQHFAxWZWdhcywgQmFieSExITAfBgNVBAoTGF
doYXQgSGFwcGVucyBpbiBWZWdh\ncy4uLjEtMCsGCSqGSIb3DQEJARYed2hhdGhhcHBlbnNAdm
VnYXNzdGF5c2luLnZl\nZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f
```

```
nLKQNWEWMR\n6akeDKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH
P4\nt6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nmrgp
GZQF3iOSIcBHtLKE5186JVT6j5dg6yjUGQO352ylc9HXHcn6lb/jyl0DmVNU\nZ0caQwAmIS3J
moyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K6lS\n7dg9cyXu4afXcgKy14Ji
NBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzxF+AC\nq+itawIDAQABo4HrMIHoMB0GA1Ud
DgQWBBRvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYDVQQHFAxW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbiBWZWdhcy4uLjEtMCsGCSqG
SIb3DQEJARYe\nd2hhdGhhcHBlbnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjjf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s71mQPECwVLfiE/ndtIbnpe\nMq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7JyfS37l4rRolFpX6N\niebEgAaE5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dHOlQ+WYnoO/eIMy0coT26JBl5H\nDEwvdl+DwkxnS1cx1v
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAjJDg
l0QoQDWNDoTeRBsz80nwiouA==\n-----END CERTIFICATE-----\n",
        "details": {
            "issuer":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org",
            "modulus":
"F14FB6F1F9CB290356116311E9A91E0CAB9E852A52EFDA1D2C68A0235F2A94257F0146396
4B8EAB138C1BD325546FE38CA809380DAF1DFA53B1473F8B7A3FF4A2D1A62BE28BF1979C03
A44337432CB924F07B25E94E07A003EDF9A24F078FDB41D162966F63E533ECB6041429AB82
9199405DE239221C047B4B284E75F3A2554FA8F9760EB28D41903B7E76CA573D1D71DC9FA9
5BFE3CA5D0399535467471A430026212DC99A8CB1FB38FF61AE162AAFB64AA4C05FB6D7D05
DF01C77D79D99479CCF1F113E4DFFD03E2BA952EDD83D7325EEE1A7D77202B2D78262341BE
A6C18E1809B44EFAC80CBAAD31EED313378E376471BF58F2688DCF117E002ABE8AD6B",
            "notAfter": "2027-03-06T22:50:26Z",
            "notBefore": "2017-03-08T22:50:26Z",
            "serial": "CC1B221598E37FF3",
            "sha1Fingerprint":
"1D:70:7A:6F:18:8A:CD:29:50:C7:95:B1:DD:5E:63:21:F4:FA:6E:21",
            "subject":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org"
        }
    }
}
```


GetNodeSupportedTlsCiphers

Sie können das verwenden `GetNodeSupportedTlsCiphers` Methode auf einem einzelnen Knoten, um eine Liste der TLS-Chiffren zu erhalten, die derzeit auf diesem Knoten unterstützt werden. Sie können diese Methode auf Management- und Storage-Nodes verwenden.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
MandatoryCiphers	Liste der obligatorischen TLS-Chiffren-Suites für den Knoten. Dies sind Chiffren, die auf dem Knoten immer aktiv sind.	Zeichenfolge
StandardSupplementalCiphers	Liste der standardmäßigen zusätzlichen TLS-Chiffren-Suites für den Knoten. Die zusätzlichen Chiffren werden auf dieser Liste wiederhergestellt, wenn Sie die ResetNodeSupplementalTlsCiphers API-Methode ausführen.	Zeichenfolge
SupportErgänzungErgänzungCiphers	Liste der verfügbaren zusätzlichen TLS-Chiffre-Suites, die Sie mit der SetNodeSupplementalTlsCiphers API-Methode konfigurieren können.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetNodeSupportedTlsCiphers",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {
    "defaultSupplementalCiphers": [
        "DHE-RSA-AES128-SHA256",
        "DHE-RSA-AES128-GCM-SHA256",
        "ECDHE-RSA-AES128-SHA256",
        "ECDHE-RSA-AES128-GCM-SHA256"
    ],
    "mandatoryCiphers": [
        "DHE-RSA-AES256-SHA256",
        "DHE-RSA-AES256-GCM-SHA384",
        "ECDHE-RSA-AES256-SHA384",
        "ECDHE-RSA-AES256-GCM-SHA384"
    ],
    "supportedSupplementalCiphers": [
        "DHE-RSA-AES128-SHA256",
        "DHE-RSA-AES128-GCM-SHA256",
        "ECDHE-RSA-AES128-SHA256",
        "ECDHE-RSA-AES128-GCM-SHA256",
        "DHE-RSA-AES256-SHA",
        "ECDHE-RSA-AES256-SHA",
        "DHE-RSA-CAMELLIA256-SHA",
        "DHE-RSA-AES128-SHA",
        "ECDHE-RSA-AES128-SHA",
        "DHE-RSA-CAMELLIA128-SHA"
    ]
}
}
```

GetPatchInfo

Sie können das verwenden `GetPatchInfo` Methode zum Abrufen von Informationen über auf einem Storage-Node installierte Element Software Patches

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`force`	Erzwingen der Ausführung auf allen Nodes im Storage Cluster. Sie brauchen dies nur, wenn Sie die API einer Cluster-IP-Adresse anstelle eines einzelnen Node ausgeben. Mögliche Werte: • `true` • `false`	boolesch	`false`	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Patches	Objekt mit Informationen zu den auf diesem Node installierten Patches	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetPatchInfo",
   "params": {
      "force": false,
      },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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"
          ]
          }
        }
    }
}
```

Neu seit Version

12.3

GetPendingOperation

Sie können das verwenden `GetPendingOperation` Methode zum Erkennen eines Vorgangs auf einem Knoten, der derzeit ausgeführt wird. Diese Methode kann auch verwendet werden, um einen Bericht zu erstellen, wenn eine Operation abgeschlossen ist.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Ausstehend	Mögliche Werte: • Wahr: Die Operation läuft noch. • Falsch: Der Vorgang läuft nicht mehr.	boolesch
Betrieb	Name des Vorgangs, der gerade ausgeführt wird oder abgeschlossen ist.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetPendingOperation",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1,
   "result" : {
      "pendingOperation" : {
         "pending" : "true",
         "operation" : "TestDrivesInternal",
      }
   }
}
```

Neu seit Version

9.6

GetSshInfo

Sie können das verwenden `GetSshInfo` Methode zum Abfragen des Status des SSH-Dienstes auf einem einzelnen Node.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Ergebnis	Der Status des SSH-Service für diesen Node.	boolesch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method" : "GetSshInfo",
    "params" : {},
    "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "enabled": false
    }
}
```

ListDriveHardware

Sie können das verwenden `ListDriveHardware` Methode zum Auflisten aller Laufwerke, die mit einem Node verbunden sind. Bei der Verwendung auf einzelnen Nodes werden mit dieser Methode Informationen zur Laufwerk-Hardware zurückgegeben. Bei Verwendung auf dem Cluster-Master-Knoten MVIP gibt diese Methode Informationen für alle Laufwerke auf allen Knoten zurück.

Parameter

Die "securitySupped": Wahre Zeile der Methodenantwort bedeutet nicht, dass die Laufwerke in der Lage sind zu verschlüsseln; nur dass der Sicherheitsstatus abgefragt werden kann. Wenn Sie über einen Node-Typ mit einer Modellnummer verfügen, die in „-NE“ endet, schlagen Befehle zur Aktivierung der Sicherheitsfunktionen auf diesen Laufwerken fehl.

Diese Methode verfügt über den folgenden Parameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Erzwingen	Setzen Sie auf true, um diese Methode auf allen Knoten auszuführen.	boolesch	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Fahrhardware	Zurückgegeben werden die Informationen über die Laufwerk-Hardware für den Node.	JSON-Objekt-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method": "ListDriveHardware",
"params": {},
"id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
      }
    ]
}
```


Neu seit Version

9.6

Weitere Informationen

EnableVerschlüsselungAtZiel

ListNetworkInterfaces

Sie können das verwenden `ListNetworkInterfaces` Methode zum Auflisten von Informationen zu jeder Netzwerkschnittstelle auf einem Node. Diese API-Methode ist für die Verwendung auf einzelnen Nodes gedacht. Für den Zugriff auf einzelne Nodes ist eine Benutzer-ID und Passwort-Authentifizierung erforderlich. Sie können diese Methode jedoch im Cluster verwenden, wenn der Parameter Force im Methodenaufruf den Wert „true“ angegeben hat. Wenn der Parameter auf dem Cluster verwendet wird, werden alle Schnittstellen aufgeführt.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Erzwingen	Mögliche Werte: • True: Informationen zu allen Netzwerkschnittstellen im Cluster werden zurückgegeben. • False: Es werden keine Informationen zurückgegeben.	boolesch	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Schnittstellen	Eine Liste der Konfigurationsinformationen für jede Netzwerkschnittstelle des Storage-Nodes (oder des gesamten Storage-Clusters, falls Force =) `true`).	Netzwerkschnittstelle Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method": "ListNetworkInterfaces",
"params": {},
"id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "nodes": [
            {
                "nodeID": 1,
                "result": {
                    "interfaces": [
                        {
                            "address": "10.117.80.32",
                            "addressV6": "::",
                            "broadcast": "10.117.95.255",
                            "macAddress": "90:b1:1c:42:e0:1a",
                            "mtu": 9000,
                            "name": "Bond10G",
                            "namespace": false,
                            "netmask": "255.255.240.0",
                            "status": "UpAndRunning",
                            "type": "BondMaster",
                            "virtualNetworkTag": 0
                        },
                        {
                            "address": "10.117.64.32",
                            "addressV6": "::",
                            "broadcast": "10.117.79.255",
                            "macAddress": "90:b1:1c:42:e0:1e",
                            "mtu": 1500,
                            "name": "Bond1G",
                            "namespace": false,
                            "netmask": "255.255.240.0",
                            "status": "UpAndRunning",
                            "type": "BondMaster",
                            "virtualNetworkTag": 0
                        },
                        {
```

```
                            "address": "0.0.0.0",
                            "addressV6": "::",
                            "broadcast": "0.0.0.0",
                            "macAddress": "90:b1:1c:42:e0:1a",
                            "mtu": 9000,
                            "name": "eth0",
                            "namespace": false,
                            "netmask": "0.0.0.0",
                            "status": "UpAndRunning",
                            "type": "BondSlave",
                            "virtualNetworkTag": 0
                        },
                        {
                            "address": "127.0.0.1",
                            "addressV6": "::",
                            "broadcast": "0.0.0.0",
                            "macAddress": "00:00:00:00:00:00",
                            "mtu": 0,
                            "name": "lo",
                            "namespace": false,
                            "netmask": "0.0.0.0",
                            "status": "UpAndRunning",
                            "type": "Loopback",
                            "virtualNetworkTag": 0
                        }
                    ]
                }
            }
        ]
    }
}
```


Neu seit Version

9.6

ListNetworkSchnittstellenStats

Sie können das verwenden `ListNetworkInterfaceStats` Methode zum Auflisten von Statistiken, wie z. B. die Anzahl der heruntergelassenen Pakete und verschiedene Arten von Fehlern für jede Netzwerkschnittstelle auf einem Node. Diese API-Methode ist für die Verwendung auf einzelnen Nodes gedacht. Für den Zugriff auf einzelne Nodes ist eine Benutzer-ID und Passwort-Authentifizierung erforderlich. Sie können diese Methode jedoch im Cluster verwenden, wenn der Parameter Force im Methodenaufruf den Wert „true“ angegeben hat. Wenn der Parameter auf dem Cluster verwendet wird, werden die Netzwerkstatistiken für alle Schnittstellen aufgeführt.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
NetworkSchnittstellenStats	Eine Liste der Netzwerkstatistiken, wie z. B. die Anzahl der heruntergelassenen Pakete und verschiedene Arten von Netzwerkfehlern für jede Netzwerkschnittstelle eines Storage-Nodes.	NetworkSchnittstellenStats Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method": "ListNetworkInterfaceStats",
"params": {},
"id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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
        }
    ]
}
```


Neu seit Version

12.3

ListTruhen

Sie können das verwenden `ListTests` Methode zum Auflisten der Tests, die für die Ausführung auf einem Knoten verfügbar sind.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Testen	Liste der Tests, die auf dem Knoten durchgeführt werden können	String-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListTests",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
   "tests": [
              "TestConnectEnsemble",
              "TestConnectMvip",
              "TestConnectSvip",
              "TestDrives",
              "TestHardwareConfig",
              "TestLocateCluster",
              "TestPing",
              "TestLocalConnectivity",
              "TestRemoteConnectivity",
              "TestNetworkConfig"
            ]
      }
}
```

Neu seit Version

9.6

ListenUtilities

Sie können das verwenden `ListUtilities` Methode zum Auflisten der Vorgänge, die auf einem Knoten ausgeführt werden können.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Versorgungsunternehmen	Liste der derzeit auf dem Knoten verfügbaren Dienstprogramme.	String-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListUtilities",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
    "utilities": [
      "ResetDrives",
      "ResetNode",
      "RestartNetworking",
      "RestartServices",
      "CreateSupportBundle",
      "DeleteAllSupportBundles",
      "CreateClusterSupportBundle"
    ]
  }
}
```

Neu seit Version

9.6

RemoveNodeSSLZertifikat

Sie können das verwenden `RemoveNodeSSLCertificate` Methode zum Entfernen des Benutzer-SSL-Zertifikats und des privaten Schlüssels für den Management-Node.

Nachdem das Zertifikat und der private Schlüssel entfernt wurden, wird der Management-Node so konfiguriert, dass er das Standardzertifikat und den privaten Schlüssel verwendet.

Parameter

Sie müssen diese Methode für den Management-Node anrufen. Beispiel:

```
https://<management node IP>:442/json-rpc/10.0
```

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method" : "RemoveNodeSSLCertificate",
    "params" : {},
    "id" : 3
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id" : 3,
    "result" : {}
}
```

Erneutes Ansetzen von Laufwerken

Sie können das verwenden `ResetDrives` Methode zum proaktiven Initialisieren von Laufwerken und Entfernen aller derzeit auf einem Laufwerk befindlichen Daten. Das Laufwerk kann dann in einem vorhandenen Node wiederverwendet oder in einem aktualisierten Node verwendet werden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Laufwerke	Liste der zu rücksetzenden Gerätenamen (keine Fahrerkennungen).	Zeichenfolge	Keine	Ja.
Erzwingen	Setzen Sie auf true, um das Laufwerk zurückzusetzen.	boolesch	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Details	Details zu Laufwerken, die zurückgesetzt werden.	JSON-Objekt-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ResetDrives",
   "params": {
      "drives" : "slot3",
      "force" : true
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
  }
}
```


Neu seit Version

9.6

ResetNode neu

Sie können das verwenden `ResetNode` Methode zum Zurücksetzen eines Knotens auf die Werkseinstellungen. Alle Daten, Pakete (Software-Upgrades usw.), Konfigurationen und Protokolldateien werden vom Knoten gelöscht, wenn Sie diese Methode aufrufen. Während dieses Vorgangs werden jedoch die Netzwerkeinstellungen für den Node beibehalten. Nodes, die an einem Cluster beteiligt sind, können nicht auf die Werkseinstellungen zurückgesetzt werden.

Parameter

Die ResetNode-API kann nur für Knoten verwendet werden, die sich im Status „verfügbar“ befinden. Er kann nicht für Nodes verwendet werden, die in einem Cluster „aktiv“ oder sich in einem „Ausstehend“ befinden.

ACHTUNG:

Bei dieser Methode werden alle Kundendaten auf dem Node gelöscht.

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Entwickeln	Wird verwendet, um die URL auf ein Remote Element Software-Image anzugeben, auf das der Knoten zurückgesetzt wird.	URL	Keine	Nein
Erzwingen	Setzen Sie auf „true“, um den Node zurückzusetzen.	boolesch	Keine	Ja.
Optionen	Zur Eingabe von Spezifikationen für die Ausführung der Reset-Vorgänge. Details werden vom NetApp Support zur Verfügung gestellt, falls erforderlich.	JSON-Objekt	Keine	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ResetNode",
   "params": {
      "build" : "file:///sf/rtfi/image/filesystem.squashfs",
      "force" : true
              },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
    }
  }
}
```

Neu seit Version

9.6

ResetNodeErgänzungTlsCiphers

Sie können das verwenden `ResetNodeSupplementalTlsCiphers` Methode zur Wiederherstellung der Liste der zusätzlichen TLS-Chiffren auf der Standardvorgabe. Sie können diesen Befehl für Management-Nodes verwenden.

Parameter

Sie müssen diese Methode für den Management-Node anrufen. Beispiel:

```
https://<management node IP>:442/json-rpc/10.0
```

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ResetNodeSupplementalTlsCiphers",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {}
}
```

Netzwerk neu starten

Sie können das verwenden `RestartNetworking` Methode zum Neustart der Netzwerkdienste auf einem Knoten.

ACHTUNG:

Mit dieser Methode werden alle Netzwerkdienste auf einem Node neu gestartet, was zu einem vorübergehenden Verlust der Netzwerkverbindung führt.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Erzwingen	Auf „true“ gesetzt, um Netzwerkdienste auf einem Knoten neu zu starten.	boolesch	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "RestartNetworking",
   "params": {
              "force" : true
             },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{ "id" : 1,
  "result" : {}
}
```

Neu seit Version

9.6

RestartServices neu starten

Sie können das verwenden `RestartServices` Methode zum Neustart der Dienste auf einem Knoten.

Parameter

ACHTUNG:

Diese Methode führt zu einer vorübergehenden Unterbrechung von Node-Services.

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Erzwingen	Auf „true“ gesetzt, um Dienste auf einem Knoten neu zu starten.	boolesch	Keine	Ja.
Service	Dienstname, der neu gestartet werden soll.	Zeichenfolge	Keine	Nein
Aktion	Aktion für den Dienst (Start, Stopp, Neustart).	Zeichenfolge	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Details	Die Ausgabe des Service-Neustarts, einschließlich Fehler (falls vorhanden).	JSON-Objekt
Dauer	Die Zeit dauerte, in Sekunden die Dienste des Node neu zu starten.	Zeichenfolge
Ergebnis	Ergebnisse des Neustarts.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "RestartServices",
   "params": {
              "force" : true
              "action" : restart,
             }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
    "details": "solidfire stop/waiting\nsolidfire start/running, process
7284\n",
    "duration": "00:00:02.541594",
    "result": "Passed"
  }
}
```

Neu seit Version

9.6

SetClusterConfig

Sie können das verwenden `SetClusterConfig` Methode zum Festlegen der Konfiguration, die ein Node zur Kommunikation mit dem ihm zugeordneten Cluster verwendet. Führen Sie zum Anzeigen der aktuellen Einstellungen für die Cluster-Schnittstelle für einen Node die aus `GetClusterConfig` API-Methode.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Cluster	Konfigurationsattribute, die während dieses Methodenaufrufs geändert werden sollten. Nur die Felder, die geändert werden sollen, müssen dieser Methode als Mitglieder in diesem Parameter hinzugefügt werden.	Cluster	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Cluster	Konfigurationsinformationen, über die der Node mit dem Cluster kommunizieren kann.	Cluster

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "SetClusterConfig",
   "params": {
      "cluster": {
         "name": "myhost",
         "mipi": "Bond10G"
      },
    "id" : 1
   }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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"
      }
   }
}
```

Neu seit Version

9.6

SetConfig

Sie können das verwenden `SetConfig` Methode zum Festlegen der Netzwerk- und Cluster-Informationen für den Node. Diese Methode umfasst die gleichen Einstellungen in einer einzelnen API-Methode, die mit beiden zur Verfügung stehen `SetClusterConfig` Und `SetNetworkConfig` Methoden Nur die Felder, die geändert werden sollen, müssen mit dieser Methode enthalten sein.

Parameter

ACHTUNG:

Wenn der Bond-Modus auf einem Node geändert wird, kann dies zu einem vorübergehenden Verlust der Netzwerkverbindung führen.

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Cluster	Cluster-Informationen, die erkennen, wie der Storage-Node mit dem Storage-Cluster kommuniziert, dem er zugeordnet ist.	Cluster	Keine	Nein
Netzwerk	Verbindungstypen und aktuelle Einstellungen für jede Netzwerkschnittstelle des Nodes.	Netzwerk (alle Schnittstellen)	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Konfigurations	Die neue und aktuelle Konfiguration des Node. Dieses Objekt enthält: • Cluster: Cluster-Informationen, die erkennen, wie der Storage-Node mit dem Storage-Cluster kommuniziert, mit dem er verknüpft ist. • Netzwerk (alle Schnittstellen): Netzwerkverbindungstypen und aktuelle Einstellungen für jede Netzwerkschnittstelle des Knotens.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "SetConfig",
    "params": {
        "cluster": {
            "name": "MyHostname"
        },
        "network": {
            "Bond10G": {
                "bond-mode": "ALB"
            }
        }
    }
}
```

Antwortbeispiel

Die Antwort von dieser Methode ist die gleiche wie die Rückkehr für die getconfig Methode. Bei Verwendung von SetConfig werden alle Felder für die Objektanzeige und die aktualisierten Werte angezeigt.

Neu seit Version

9.6

Weitere Informationen

- SetClusterConfig
- SetNetworkConfig
- Getconfig

SetNetworkConfig

Sie können das verwenden `SetNetworkConfig` Methode zum Festlegen der Netzwerkkonfiguration für einen Knoten. Um die aktuellen Netzwerkeinstellungen für einen Node anzuzeigen, führen Sie den aus `GetNetworkConfig` API-Methode.

Parameter

ACHTUNG:

Wenn der Bond-Modus auf einem Node geändert wird, kann dies zu einem vorübergehenden Verlust der Netzwerkverbindung führen.

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Netzwerk	Ein Objekt, das die zu ändernden Node-Netzwerkeinstellungen enthält. In diesem Parameter müssen Sie nur die Felder hinzufügen, die Sie in diese Methode als Attribute geändert haben möchten.	Netzwerk (alle Schnittstellen)	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Netzwerk	Die neue und aktuelle Netzwerkkonfiguration für den Node.	Netzwerk (alle Schnittstellen)

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "SetNetworkConfig",
        "params": {
            "network": {
                "Bond10G": {
                    "bond-mode": "ALB"
                },
                "Bond1G": {
                    "netmask": "255.255.224.0"
                },
                "eth0": {
                    "method": "bond"
                },
                "lo": {
                    "method": "loopback"
                }
            }
        }
}
```

Antwortbeispiel

Die Antwort dieser Methode entspricht der Antwort der Methode GetNetworkConfig. Die Methode zeigt alle Mitglieder für jedes Objekt an und enthält die neuen Werte für alle geänderten Mitglieder.

Neu seit Version

9.6

Weitere Informationen

- GetNetworkConfig
- GetNetworkConfig

SetNodeSSLZertifikat

Sie können das verwenden `SetNodeSSLCertificate` Methode zum Festlegen eines Benutzer-SSL-Zertifikats und eines privaten Schlüssels für den Management-Node.

Nach Verwendung der API müssen Sie den Management-Node neu booten.

Parameter

Sie müssen diese Methode für den Management-Node anrufen. Beispiel:

```
https://<management node IP>:442/json-rpc/10.0
```

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Zertifikat	Die PEM-kodierte Textversion des Zertifikats.**Hinweis:** beim Festlegen eines Node- oder Cluster-Zertifikats muss das Zertifikat die Erweiterung DECDKeyUsage für serverAuth enthalten. Mit dieser Erweiterung kann das Zertifikat ohne Fehler auf gängigen Betriebssystemen und Browsern verwendet werden. Wenn die Erweiterung nicht vorhanden ist, weist die API das Zertifikat als ungültig zurück.	Zeichenfolge	Keine	Ja.
PrivateKey	Die PEM-codierte Textversion des privaten Schlüssels.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method" : "SetNodeSSLCertificate",
    "params" : {
        "privateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEA8U+28fnLKQNWEWMR6akeDKuehSpS79odLGigI18qlCV/AUY5\nZLjqsT
jBvTJVRv44yoCTgNrx36U7FHP4t6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7Je\nlOB6AD7fmiTweP
20HRYpZvY+Uz7LYEFCmrgpGZQF3iOSIcBHtLKE5186JVT6j5dg\n6yjUGQO352ylc9HXHcn6lb
/jyl0DmVNUZ0caQwAmIS3Jmoyx+zj/Ya4WKq+2SqTA\nX7bX0F3wHHfXnZlHnM8fET5N/9A+K6
lS7dg9cyXu4afXcgKy14JiNBvqbBjhgJtE\n76yAy6rTHu0xM3jjdkcb9Y8miNzxF+ACq+itaw
IDAQABAoIBAH1jlIZr6/sltqVW\nO0qVC/49dyNu+KWVSq92ti9rFe7hBPueh9gklh78hP9Qli
tLkir3YK4GFsTFUMux\n7z1NRCxA/4LrmLSkAjW2kRXDfVl2bwZq0ua9NefGw92O8D2OZvbuOx
k7Put2p6se\nfgNzSjf2SI5DIX3UMe5dDN5FByu52CJ9mI4U16ngbWln2wc4nsxJg0aAEkzB7w
nq\nt+Am5/Vu1LI6rGiG6oHEW0oGSuHl1esIyXXa2hqkU+1+iF2iGRMTiXac4C8d11NU\nWGIR
```

```
CXFJAmsAQ+hQm7pmtsKdEqumj/PIoGXf0BoFVEWaIJIMEgnfuLZp8IelJQXn\nSFJbk2ECgYEA
+d5ooU4thZXylWHUZqomaxyzOruA1T53UeH69HiFTrLjvfwuaiqj\nlHzPlhms6hxexwz1dzAp
gog/NOM+2bAc0rn0dqvtV4doejtlDZKRqrNCf/cuN2QX\njaCJClCWau3sEHCckLOhWeY4HaPS
oWq0GKLmKkKDChB4nWUYg3gSWQkCgYEA9zuN\nHW8GPS+yjixeKXmkKO0x/vvxzR+J5HH5znaI
Hss48THyhzXpLr+v30Hy2h0yAlBS\nny5Ja6wsomb0mVe4NxVtVawg2E9vVvTa1UC+TNmFBBuL
RPfjcnjDerrSuQ5lYY+M\nC9MJtXGfhp//G0bzwsRzZxOBsUJb15tppaZIs9MCgYAJricpkKjM
0xlZ1jdvXsos\nPilnbho4qLngrzuUuxKXEPEnzBxUOqCpwQgdzZLYYw788TCVVIVXLEYem2s0
7dDA\nDTo+WrzQNkvC6IgqtXH1RgqegIoG1VbgQsbsYmDhdaQ+os4+AOeQXw3vgAhJ/qNJ\njQ
4Ttw3ylt7FYkRH26ACWQKBgQC74Zmf4JuRLAo5WSZFxpcmMvtnlvdutqUH4kXA\nzPssy6t+QE
La1fFbAXkZ5Pg1ITK752aiaX6KQNG6qRsA3VS1J6drD9/2AofOQU17\n+jOkGzmmoXf49Zj3iS
akwg0ZbQNGXNxEsCAUr0BYAobPp9/fB4PbtUs99fvtocFr\njS562QKBgCb+JMDP5q7jpUuspj
0obd/ZS+MsomE+gFAMBJ71KFQ7KuoNezNFO+ZE\n3rnR8AqAm4VMzqRahs2PWNe2Hl4J4hKu96
qNpNHbsW1NjXdAL9P7oqQIrhGLVdhX\nInDXvTgXMdMoet4BKnftelrXFKHgGqXJoczq4JWzGS
IHNgvkrH60\n-----END RSA PRIVATE KEY-----\n",
        "certificate": "-----BEGIN CERTIFICATE-----
\nMIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSIb3DQEBBQUAMIGDMQswCQYD\nVQQGEw
JVUzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\nA1UEChMYV2hhdC
BIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBFh53\naGF0aGFwcGVuc0B2ZWdhc3
N0YXlzaW4udmVnYXMwHhcNMTcwMzA4MjI1MDI2WhcN\nMjcwMzA2MjI1MDI2WjCBgzELMAkGA1
UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYD\nVQQHFAxWZWdhcywgQmFieSExITAfBgNVBAoTGF
doYXQgSGFwcGVucyBpbiBWZWdh\ncy4uLjEtMCsGCSqGSIb3DQEJARYed2hhdGhhcHBlbnNAdm
VnYXNzdGF5c2luLnZl\nZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f
nLKQNWEWMR\n6akeDKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH
P4\nt6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nmrgp
GZQF3iOSIcBHtLKE5186JVT6j5dg6yjUGQO352ylc9HXHcn6lb/jyl0DmVNU\nZ0caQwAmIS3J
moyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K6lS\n7dg9cyXu4afXcgKy14Ji
NBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzxF+AC\nq+itawIDAQABo4HrMIHoMB0GA1Ud
DgQWBBRvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYDVQQHFAxW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbiBWZWdhcy4uLjEtMCsGCSqG
SIb3DQEJARYe\nd2hhdGhhcHBlbnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjjf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s71mQPECwVLfiE/ndtIbnpe\nMq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7JyfS37l4rRolFpX6N\niebEgAaE5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dHOlQ+WYnoO/eIMy0coT26JBl5H\nDEwvdl+DwkxnS1cx1v
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAjJDg
l0QoQDWNDoTeRBsz80nwiouA==\n-----END CERTIFICATE-----\n"
    },
    "id" : 2
}
```


Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id" : 2,
    "result" : {}
}
```

SetNodeSupplementalTlsCiphers

Sie können das verwenden `SetNodeSupplementalTlsCiphers` Methode zur Angabe der Liste der zusätzlichen TLS-Chiffren. Sie können diesen Befehl für Management-Nodes verwenden.

Parameter

Sie müssen diese Methode für den Management-Node anrufen. Beispiel:

```
https://<management node IP>:442/json-rpc/10.0
```

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SupplementalCiphers	Die zusätzlichen Namen der Chiffre-Suite unter Verwendung des OpenSSL-Benennungsschemas. Die Groß-/Kleinschreibung wird nicht berücksichtigt.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
MandatoryCiphers	Liste der obligatorischen TLS-Chiffren-Suites für den Knoten. Dies sind Chiffren, die auf dem Knoten immer aktiv sind.	Zeichenfolge
SupplementalCiphers	Liste der zusätzlichen TLS-Chiffren-Suites für den Knoten.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "SetNodeSupplementalTlsCiphers",
   "params": {
        "supplementalCiphers": [
            "DHE-RSA-AES128-SHA256",
            "DHE-RSA-AES128-GCM-SHA256",
            "ECDHE-RSA-AES128-SHA256",
            "ECDHE-RSA-AES128-GCM-SHA256"
        ]
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
        ]
    }
}
```

Herunterfahren

Sie können das verwenden `Shutdown` Methode zum Neustart oder Herunterfahren der Nodes in einem Cluster. Sie können über diese Methode einen einzelnen Node, mehrere Nodes oder alle Nodes im Cluster herunterfahren.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Knoten	Liste der NodeIDs für die Nodes, die neu gestartet oder heruntergefahren werden sollen.	Integer-Array	Keine	Ja.
Option	Aktion, die für den Cluster ausgeführt wird. Mögliche Werte: • Neustart: Startet das Cluster neu. • Stop: Führt eine vollständige Abschaltung durch.	Zeichenfolge	Neustart	Nein

Rückgabewert

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "Shutdown",
   "params": {
     "nodes": [
       2,
       3,
       4
     ],
     "option": "halt"
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {
     "failed": [],
     "successful": [
          6
      [
   }
}
```

Neu seit Version

9.6

TestConnectEnsemble

Sie können das verwenden `TestConnectEnsemble` Methode zum Überprüfen der Konnektivität mit einem bestimmten Datenbankensemble. Standardmäßig verwendet es das Ensemble für den Cluster, dem der Knoten zugeordnet ist. Alternativ können Sie auch ein anderes Ensemble zur Prüfung der Konnektivität bereitstellen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Ensemble	Eine kommagetrennte Liste von Ensemble Node Cluster IP-Adressen für Verbindungstests.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Details	Zurückgegebene Objekte: • `nodes`: (Objekt) eine Liste der einzelnen Ensembleknoten im Test und die Ergebnisse der Tests. • `duration`: (String) die Zeit, die zum Ausführen des Tests benötigt wird. • `result`: (String) die Ergebnisse des gesamten Tests.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "TestConnectEnsemble",
  "params": {},
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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"
   }
}
```

Neu seit Version

9.6

TestConnectMvip

Sie können das verwenden `TestConnectMvip` Methode zum Testen der Managementverbindung zum Storage-Cluster. Der Test pingt den MVIP an und führt eine einfache API-Methode zur Überprüfung der Konnektivität durch.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
mvip	Sie können diesen Wert übergeben, um die Verwaltungsverbindung eines anderen MVIP zu testen. Sie müssen diesen Wert nicht verwenden, wenn Sie die Verbindung zum Ziel-Cluster testen.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Details	Informationen zum Testverfahren (JSON-Objekt): • `connected`: Gibt an, ob der Test eine Verbindung zum MVIP herstellen könnte (boolescher Wert) • `mvip`: Die MVIP getestet gegen (String) • `pingBytes`: Einzelheiten der Ping-Tests mit 56 Bytes und 1500 Bytes (Objekt) ◦ `56`: Ergebnisse des 56 Byte Ping Tests (JSON Objekt): ▪ `individualResponseTimes`: Liste der Reaktionszeiten von jedem Ensemble-Knoten (String-Array) ▪ `individualStatus`: Liste des Ping-Status von jedem Ensemble-Knoten (boolescher Array) ▪ `responseTime`: Durchschnittliche Ping-Antwortzeit (String) ▪ `successful`: Gibt an, ob der Ping-Test erfolgreich war (boolesch) ◦ `1500`: Ergebnisse des 1500-Byte-Ping-Tests (JSON-Objekt): ▪ `individualResponseTimes`: Liste der Reaktionszeiten von jedem Ensemble-Knoten (String-Array) ▪ `individualStatus`: Liste des Ping-Status von jedem Ensemble-Knoten (boolescher Array) ▪ `responseTime`: Durchschnittliche Ping-Antwortzeit (String) `successful`: Ob der Ping-Test erfolgreich war (boolesch)	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

- `duration`: Dauer für die Durchführung des Tests

```
{
   "method": "TestConnectMvip",
   "params": {
       "mvip" : "172.27.62.50"
       },
    "id":1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
  }
}
```


Neu seit Version

9.6

TestConnectSvip

Sie können das verwenden `TestConnectSvip` Methode zum Testen der Storage-Verbindung zum Storage-Cluster. Der Test pingt den SVIP mithilfe von ICMP-Paketen an und stellt, wenn er erfolgreich war, eine Verbindung als iSCSI-Initiator her.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
svip	Sie können diesen Wert übergeben, um die Verwaltungsverbindung eines anderen SVIP zu testen. Sie müssen diesen Wert nicht verwenden, wenn Sie die Verbindung zum Ziel-Cluster testen.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Details	Informationen zum Testverfahren (JSON-Objekt): • `connected`: Gibt an, ob der Test eine Verbindung zum SVIP herstellen kann (boolescher Wert). • `svip`: Der SVIP geprüft gegen (String) • `pingBytes`: Einzelheiten der Ping-Tests mit 56 Bytes und 9000 Bytes (Objekt) ◦ `56`: Ergebnisse des 56-Byte-Ping-Tests (JSON-Objekt): ▪ `individualResponseTimes`: Liste der Reaktionszeiten von jedem Ensemble-Knoten (String-Array) ▪ `individualStatus`: Liste des Ping-Status von jedem Ensemble-Knoten (boolescher Array) ▪ `responseTime`: Durchschnittliche Ping-Antwortzeit (String) ▪ `successful`: Gibt an, ob der Ping-Test erfolgreich war (boolesch) ◦ `9000`: Ergebnisse des 9000 Byte Ping Tests (JSON Objekt): ▪ `individualResponseTimes`: Liste der Reaktionszeiten von jedem Ensemble-Knoten (String-Array) ▪ `individualStatus`: Liste des Ping-Status von jedem Ensemble-Knoten (boolescher Array) ▪ `responseTime`: Durchschnittliche Ping-Antwortzeit (String)	Zeichenfolge
	`successful`: Gibt an, ob der Ping-Test	

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "TestConnectSvip",
   "params": {
      "svip" : "172.27.62.50"
      },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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",
```

- erfolgreich war (boolesch)

```
                    "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"
    }
}
```


Neu seit Version

9.6

TestDrives

Sie können das verwenden `TestDrives` Methode zum Ausführen einer Hardwarevalidierung auf allen Laufwerken auf dem Knoten. Bei dieser Methode werden Hardwareausfälle auf den Laufwerken erkannt und die Ergebnisse der Validierungstests angezeigt.

Parameter

Sie können nur die verwenden `TestDrives` Methode auf Nodes, die in einem Cluster nicht „aktiv“ sind

Dieser Test dauert etwa 10 Minuten.

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Erzwingen	Setzen Sie auf „true“, um die Laufwerke auf dem Node zu testen.	boolesch	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Minuten	Gibt die Anzahl der Minuten für den auszuführenden Test an.	Ganzzahl	10	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Details	Informationen über den Testvorgang erfolgreich oder fehlgeschlagen.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "TestDrives",
   "params": {
              "force": true,
              "minutes" : 10
             },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Tabelle mit den Testergebnissen für jedes Laufwerk im Node zurück.

Neu seit Version

9.6

TestHardwareConfig

Sie können das verwenden `TestHardwareConfig` Methode zum Durchführen von Hardwaretests auf einem Knoten. Die Testoptionen umfassen die Überprüfung der Hardware-Konfigurationen, Firmware-Versionen und der Tatsache, dass alle Laufwerke vorhanden sind.

Parameter

Diese Tests dienen nicht zur Erkennung von Hardwarefehlern.

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Sauber	Startet den Hardware-Konfigurationstest mit einem sauberen Cache. Mögliche Werte: • True: Löscht die Datei mit den gecachten Testergebnissen und führt die Tests erneut aus. • False: Ruft zwischengespeicherte Testergebnisse ab.	boolesch	Falsch	Nein
Erzwingen	Der Force-Parameter muss in diese Methode aufgenommen werden, um den Knoten erfolgreich zurückzusetzen.	boolesch	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Details	Details zur Hardwarekonfiguration.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "TestHardwareConfig",
   "params": {
      "force": true
     },
   "id" : 1
}
```

Antwortbeispiel

Aufgrund der Länge dieses Antwortbeispiels wird es in einem ergänzenden Thema dokumentiert.

Neu seit Version

9.6

Weitere Informationen

TestHardwareConfig

TestLocateCluster

Sie können das verwenden `TestLocateCluster` Methode zum Überprüfen, ob der Node den in der Cluster-Konfiguration angegebenen Cluster finden kann. Die Ausgabe bestätigt, dass der Cluster erstellt wurde, und listet die Knoten im Cluster-Ensemble auf.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Details	Informationen über den Testvorgang erfolgreich oder fehlgeschlagen.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "TestLocateCluster",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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"
   }
}
```

Neu seit Version

9.6

TestLocalConnectivity

Sie können das verwenden `TestLocalConnectivity` Methode zum Ping der Cluster-

IP (CIP) jedes Knotens in einem aktiven Cluster.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Details	Individuelle Ping-Reaktionszeiten für jeden Node im lokalen, aktiven Cluster.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "TestLocalConnectivity",
   "params": {},
   "id": 1
}
```

Antwortbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "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"
  }
}
```

Neu seit Version

9.6

TestNetworkConfig

Sie können das verwenden `TestNetworkConfig` Methode zum Testen, dass die konfigurierten Netzwerkeinstellungen mit den im System verwendeten Netzwerkeinstellungen übereinstimmen.

Parameter

Wenn Sie einen Knoten mit der Methode SetNetworkConfig in der UI oder TUI konfigurieren, wird die Konfiguration validiert und gespeichert. Der Test der TestNetworkConfig API verwendet die gespeicherte Konfiguration für die Logik nach der Validierung. Wenn beispielsweise ein Stromausfall oder ein Netzwerkfehler auftritt, können Sie diese API-Methode verwenden, um sicherzustellen, dass ein Node mit der derzeit am meisten gespeicherten Netzwerkkonfiguration ausgeführt wird. Dadurch wird überprüft, dass bei der Konfiguration keine Fehler auftreten und dass die aktuelle Konfiguration verwendet wird.

Dieser Test ist darauf ausgelegt, nur Fehler in der Antwortausgabe anzuzeigen. Wenn keine Fehler auftreten, gibt dieser Test keine Ausgabe zurück. Sehen Sie sich die folgenden Antwortbeispiele an.

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Details	Enthält alle Fehler, die bei der Validierung der aktuell gespeicherten Netzwerkeinstellungen mit der laufenden Netzwerkkonfiguration gefunden wurden.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "TestNetworkConfig",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel 1

Wenn keine Fehler erkannt werden, werden keine Antworten zurückgegeben.

```
{
   "id" : 1,
   "result": {
   "details": {
   "network": {...}
  },
   "duration": "00:00:00.144514",
   "result": "Passed"
  }
}
```

Antwortbeispiel 2

Beispiel für eine MTU-Übereinstimmung.

```
{
  "id" : 1,
  "result":
  {
     "details" :
     {
        "error":
        {
           "message" : "Network configuration mismatch on Bond10G:
Incorrect MTU expectedMTU=[1500]  actualMTU=[9600]", name:
"xAssertionFailure"
        }
     },
     "duration": "0.125213sec",
     "result": "Failed"
  }
}
```

Antwortbeispiel 3

Beispiel für eine fehlende statische Route.

```
{
  "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"
  }
}
```

Neu seit Version

9.6

Weitere Informationen

SetNetworkConfig

TestPing

Sie können das verwenden `TestPing` Methode zum Testen der Netzwerkkonnektivität zu allen Knoten im Cluster auf 1G- und 10G-Schnittstellen mithilfe von ICMP-Paketen. Der Test verwendet die entsprechenden MTU-Größen für jedes Paket basierend auf den MTU-Einstellungen in der Netzwerkkonfiguration. `TestPing` Keine temporäre VLAN-Schnittstelle erstellt.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Versuche	Gibt an, wie oft das System den Ping-Test wiederholen soll.	Ganzzahl	5	Nein
Hosts	Gibt eine kommagetrennte Liste von Adressen oder Hostnamen von Geräten an, die Ping verwenden sollen. Wenn keine Hosts angegeben werden, pingt die Methode die Hosts im Storage-Cluster an.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Schnittstelle	Die bestehende (Basis-)Schnittstelle, von der die Pings gesendet werden sollen. Mögliche Werte: • `Bond10G`: Senden von Pings von der Bond10G-Schnittstelle. • `Bond1G`: Senden von Pings von der Bond1G-Schnittstelle.	Zeichenfolge	Keine	Nein
PacketSize	Gibt die Anzahl der Bytes an, die in das ICMP-Paket gesendet werden sollen, das an jede IP gesendet wird. Die Anzahl der Bytes muss kleiner sein als die in der Netzwerkkonfiguration angegebene maximale MTU.	Ganzzahl	Keine	Nein
PingTimeoutMsec	Gibt die Anzahl der Millisekunden an, die für jede einzelne Ping-Antwort warten soll.	Ganzzahl	500 Millisekunden	Nein
Verbot der Fragmentierung	Aktiviert das DF-Flag (Do Not Fragment) für die ICMP-Pakete.	boolesch	Falsch	Nein
SourceAddressV4	Die IPv4-Quelladresse, die in den ICMP-Ping-Paketen verwendet werden soll.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
SourceAddressV6	Die IPv6-Quelladresse, die in den ICMP-Ping-Paketen verwendet werden soll.	Zeichenfolge	Keine	Nein
TotalTimeoutSec	Gibt die Zeit in Sekunden an, die der Ping auf eine Systemantwort warten soll, bevor er den nächsten Ping-Versuch ausgibt oder den Prozess beendet.	Ganzzahl	5	Nein
VirtualNetworkTag	Die VLAN-ID, die beim Senden der Ping-Pakete verwendet wird.	Ganzzahl	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Details	Liste jeder IP der Knoten konnte mit und Ping-Antwortstatistiken kommunizieren.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "TestPing",
    "params": {
        "interface": "Bond1G",
        "hosts": "192.168.0.1"
    },
    "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:


```
{
  "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"
  }
}
```


Neu seit Version

5.0

TestRemoteConnectivity

Verwenden Sie können `TestRemoteConnectivity` Methode, um jeden Knoten des Remote-Clusters anzupingen und die Remote-Ensemble-Datenbankverbindung zu prüfen. Cluster müssen gekoppelt werden, um nützliche Ergebnisse mit dieser Methode zu liefern. Wenn die Remote-Datenbankverbindung fehlschlägt, werden die Ausnahmen in der Antwort des Systems aufgelistet.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Details	Individuelle Ping-Reaktionszeiten für jeden Knoten.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "TestRemoteConnectivity",
    "params": {
      "force": "true"
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
  }
}
```


Neu seit Version

9.6

Replizierungs-API-Methoden

Reihenfolge der Vorgänge für die Cluster-Paarung

Sie müssen eine Verbindung zwischen einem Storage-Cluster-Paar mit Element Software herstellen, bevor die Remote-Replizierung verwendet werden kann.

Verwenden Sie die folgenden API-Methoden, um eine Cluster-Verbindung herzustellen:

- StartClusterPairing:

  Mit dieser API-Methode wird ein Kopplungsschlüssel erstellt und zurückgegeben, der zum Aufbau eines

Cluster-Paares verwendet wird. Der Schlüssel ist kodiert und enthält Informationen, die für die Kommunikation zwischen Clustern verwendet werden. Ein einzelnes Cluster kann mit bis zu vier anderen Clustern gekoppelt werden. Jedoch muss für jede Cluster-Paarung ein neuer Schlüssel generiert werden. Der StartClusterPairing Methode generiert bei jedem Mal, wenn die Methode aufgerufen wird, einen neuen Schlüssel. Verwenden Sie jeden eindeutigen Schlüssel mit dem CompleteClusterPairing Methode, um jeden zusätzlichen Cluster zu koppeln.

> Aus Sicherheitsgründen darf der Kopplungsschlüssel nicht per E-Mail an andere Benutzer gesendet werden. Der Schlüssel enthält einen Benutzernamen und ein Passwort.

- CompleteClusterPairing:

  Bei dieser Methode wird der mit dem erstellte Kopplschlüssel verwendet StartClusterPairing API-Methode zum Erstellen eines Cluster-Paares. Stellen Sie das aus CompleteClusterPairing API-Methode mit dem clusterPairingKey-Parameter zum Ziel. Der Ursprung des Clusters ist das Cluster, das den Schlüssel erstellt hat.

Weitere Informationen

- StartClusterPairing
- CompleteClusterPairing

Reihenfolge der Vorgänge für die Volume-Kopplung

Sie müssen ein Cluster-Paar zwischen zwei entsprechenden Clustern erstellen, bevor Volumes gekoppelt werden können.

Verwenden Sie die folgenden API-Methoden, um eine Cluster-Verbindung herzustellen:

- StartVolumePairing:

  Mit dieser API-Methode wird ein Volume-Kopplungsschlüssel erstellt und zurückgegeben, der zur Erstellung eines Volume-Paares verwendet wird. Der Schlüssel enthält Informationen, die zur Kommunikation zwischen Volumes verwendet werden.

- CompleteVolumePairing:

  Bei dieser Methode wird der mit dem erstellte Kopplschlüssel verwendet StartVolumePairing API-Methode zum Erstellen eines Volume-Paares. Stellen Sie das aus CompleteVolumePairing API-Methode mit der VolumeID und VolumePairingKey-Parameter auf das Ziel-Volume.

Es kann nur eines der gepaarten Volumes als Ziel-Volume für die Replizierung identifiziert werden. Verwenden Sie die ModifyVolumePair API-Methode zur Festlegung der Richtung der Datenreplizierung des Volume durch Identifizierung des Zieldatels Die Daten werden vom Quell-Volume auf das Ziel-Volume repliziert.

Weitere Informationen

- StartVolumePairing
- CompleteVolumePairing
- ModifyVolumePair

Unterstützte Replikationsmodi für gepaarte Cluster

Die folgenden Replikationsmodi werden auf den gepaarten Clustern unterstützt:

- Asynchrone Datenreplikation: Die an das Replikationsziel-Volume gesendeten Daten werden asynchron gesendet. Das System wartet nicht darauf, dass eine Bestätigung gesendet wird, bevor Daten geschrieben werden.
- Synchrone Datenreplizierung: Die an das Replikationsziel-Volume gesendeten Daten werden synchron gesendet. Wenn die vom Host gesendeten I/O-Vorgänge vom System bestätigt werden, wird die Systembestätigung zurück an den Host gesendet und die Daten an das Replikationsziel-Volume gesendet.
- Reine Snapshot-Replizierung von Daten: Nur Volume-Snapshots werden auf das Ziel-Cluster repliziert.

CompleteClusterPairing

Der `CompleteClusterPairing` Die Methode ist der zweite Schritt der Cluster-Paarung. Verwenden Sie diese Methode mit dem kodierten Schlüssel, der vom empfangen wurde `StartClusterPairing` Methode zum Abschließen des Cluster-Kopplungsvorgangs.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ClusterPairingKey	Eine Zeichenfolge, die von zurückgegeben wird StartClusterPairing API-Methode.	Zeichenfolge	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
ClusterPairID	Eindeutige Kennung für das Cluster-Paar.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "CompleteClusterPairing",
   "params": {
        "clusterPairingKey" :
"7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223
a2231636561313336322d346338662d343631612d626537322d373435363661393536432
6222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d633075
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a393133313432363439 2c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1,
   "result" : {
       "clusterPairID" : 1
   }
}
```

Neu seit Version

9.6

Weitere Informationen

StartClusterPairing

CompleteVolumePairing

Verwenden Sie können `CompleteVolumePairing` Um die Kopplung von zwei Volumes abzuschließen.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	Die ID des Datenträgers, der das Volume-Paar abgeschlossen.	Ganzzahl	Keine	Ja.
VolumePairingKey	Der Schlüssel wurde vom zurückgegeben StartVolumePairing API-Methode.	Zeichenfolge	Keine	Ja.

Rückgabewert

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "CompleteVolumePairing",
   "params": {
        "volumeID" : 12,
        "volumePairingKey" :
"7b22636c757374657250616972494422 3a312c22636c757374657250616972555549442 23
a2231636561313336322d346338662d343631612d626537322d373435363661393533643 26
6222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d6330755
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a3931333134323634392c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
        },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
"id": 1,
"result": {}
}
```

Neu seit Version

9.6

Weitere Informationen

StartVolumePairing

ListenClusterpaare

Sie können das verwenden `ListClusterPairs` Methode zum Auflisten aller Cluster, die mit dem aktuellen Cluster gekoppelt sind. Diese Methode gibt Informationen zu aktiven und ausstehenden Cluster-Paarungen zurück, z. B. Statistiken über die aktuelle Paarung sowie über die Konnektivität und Latenz (in Millisekunden) der Cluster-Paarung.

Parameter

Diese Methode hat keinen Eingabeparameter:

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Cluster-Paare	Informationen zu jedem gepaarten Cluster.	Cluster-Paar Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListClusterPairs",
   "params": {
      },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
 "id": 1,
 "result": {
   "clusterPairs": [
     {
      "clusterName": "cluster2",
      "clusterPairID": 3,
      "clusterPairUUID": "9866fbeb-c2f8-4df3-beb9-58a5c4e49c9b",
      "clusterUUID": 5487,
      "latency": 1,
      "mvip": "172.1.1.5",
      "status": "Connected"
      "version": "8.0.0.1361"
     },
     {
      "clusterName": "cluster3",
      "clusterPairID": 2,
      "clusterPairUUID": "8132a699-ce82-41e0-b406-fb914f976042",
      "clusterUUID": 1383,
      "latency": 1,
      "mvip": "172.1.1.6",
      "status": "Connected"
      "version": "8.0.0.1361"
     }
   ]
 }
```


Neu seit Version

9.6

ListeActivePairedVolumes

Sie können das verwenden `ListActivePairedVolumes` Methode zum Auflisten aller aktiven Volumes, die mit einem Volume gekoppelt sind. Diese Methode gibt Informationen zu Volumes mit aktiven und ausstehenden Paarungen zurück.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Volumes	Volume-Informationen für die gepaarten Volumes.	Volumepaar Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListActivePairedVolumes",
   "params": {
      },
   "id" : 1
}
```

Antwortbeispiel

Die Antworten für diese Methode ähneln dem folgenden Beispiel:

```
{
    "id": 1,
    "result": {
        "volumes": [
            {
                "access": "readWrite",
                "accountID": 1,
                "attributes": {},
                "blockSize": 4096,
                "createTime": "2016-06-24T15:21:59Z",
                "deleteTime": "",
                "enable512e": true,
                "iqn": "iqn.2010-01.com.solidfire:0oto.bk.24",
                "name": "BK",
                "purgeTime": "",
                "qos": {
                    "burstIOPS": 15000,
                    "burstTime": 60,
                    "curve": {
                        "4096": 100,
                        "8192": 160,
                        "16384": 270,
                        "32768": 500,
                        "65536": 1000,
                        "131072": 1950,
```

```
                        "262144": 3900,
                        "524288": 7600,
                        "1048576": 15000
                    },
                    "maxIOPS": 15000,
                    "minIOPS": 50
                },
                "scsiEUIDeviceID": "306f746f00000018f47acc0100000000",
                "scsiNAADeviceID": "6f47acc100000000306f746f00000018",
                "sliceCount": 1,
                "status": "active",
                "totalSize": 10737418240,
                "virtualVolumeID": null,
                "volumeAccessGroups": [],
                "volumeID": 24,
                "volumePairs": [
                    {
                        "clusterPairID": 2,
                        "remoteReplication": {
                            "mode": "Async",
                            "pauseLimit": 3145728000,
                            "remoteServiceID": 14,
                            "resumeDetails": "",
                            "snapshotReplication": {
                                "state": "Idle",
                                "stateDetails": ""
                            },
                            "state": "Active",
                            "stateDetails": ""
                        },
                        "remoteSliceID": 8,
                        "remoteVolumeID": 8,
                        "remoteVolumeName": "PairingDoc",
                        "volumePairUUID": "229fcbf3-2d35-4625-865a-
d04bb9455cef"
                    }
                ]
            }
        ]
    }
}
```


Neu seit Version

9.6

ModifyVolumePair

Sie können das verwenden `ModifyVolumePair` Methode zum Anhalten oder Neustarten der Replikation zwischen einem Volume-Paar. Diese Methode wird auf dem Quellvolume (das Volumen mit Lese-/Schreibzugriff) festgelegt.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	Identifikationsnummer des zu ändernden Volumens.	Ganzzahl	Keine	Ja.
Betriebsanleitung	Die Remote-Replikation kann auf dem Quell-Volume (Lese-/Schreib-Volume) angehalten oder neu gestartet werden. Mögliche Werte: • Wahr: Volume-Replizierung anhalten • False: Volume-Replikation neu starten. Wenn kein Wert angegeben wird, wird keine Änderung in der Replikation durchgeführt.	boolesch	Keine	Nein

Modus	Volume-Replizierungsmodus Mögliche Werte: • Async: Schreibvorgänge werden bestätigt, wenn sie lokal abgeschlossen wurden. Das Cluster wartet nicht, bis Schreibvorgänge zum Ziel-Cluster repliziert werden. • Sync: Die Quelle bestätigt den Schreibvorgang, wenn die Daten lokal und auf dem Remote-Cluster gespeichert werden. • Snapshots: Es werden nur Snapshots repliziert, die auf dem Quell-Cluster erstellt wurden. Aktive Schreibvorgänge vom Quell-Volume werden nicht repliziert.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ModifyVolumePair",
  "params": {
    "pausedManual": false,
    "volumeID": 5,
    "mode": "sync"
   },
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1,
   "result" : {}
}
```

Neu seit Version

9.6

RemoveClusterPair

Sie können das verwenden `RemoveClusterPair` Methode zum Schließen der offenen Verbindungen zwischen zwei gekoppelten Clustern.

Parameter

> Bevor Sie ein Cluster-Paar entfernen, müssen Sie zuerst alle Volume-Paarungen mit den Clustern mit der RemoveVolumePair API-Methode entfernen.

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ClusterPairID	Eindeutige Kennung, die zum Paaren von zwei Clustern verwendet wird.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "RemoveClusterPair",
   "params": {
              "clusterPairID": 1
      },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {}
}
```

Neu seit Version

9.6

RemoveVolumePair

Sie können das verwenden `RemoveVolumePair` Methode zum Entfernen der Remote-Kopplung zwischen zwei Volumes. Verwenden Sie diese Methode sowohl für die Quell- als auch für die Ziel-Volumes, die miteinander verbunden sind. Wenn Sie die Kopplungsinformationen des Volumes entfernen, werden die Daten nicht mehr auf das oder vom Volume repliziert.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	ID des Volumes, auf dem der Replikationsprozess beendet werden soll.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "RemoveVolumePair",
   "params": {
      "volumeID": 5
   "id" : 1
   }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {
   }
}
```

Neu seit Version

9.6

StartClusterPairing

Sie können das verwenden `StartClusterPairing` Methode zum Erstellen eines kodierten Schlüssels aus einem Cluster, der für das Pairing mit einem anderen Cluster verwendet wird. Der aus dieser API-Methode erstellte Schlüssel wird in verwendet `CompleteClusterPairing` Methode zum Erstellen einer Cluster-Paarung. Ein Cluster kann mit maximal vier anderen Clustern gekoppelt werden.

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
ClusterPairingKey	Eine Zeichenkette, die vom verwendet wird CompleteClusterPairing API-Methode.	Zeichenfolge
ClusterPairID	Eindeutige Kennung für das Cluster-Paar.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "StartClusterPairing",
   "params": {
      },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {
     "clusterPairID": 1,
     "clusterPairingKey":
"7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223
a2231636561313336322d346338662d343631612d626537322d373435363661393533643263
6222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f5465737432 2d6330755
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a393133313432363439 2c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
   }
}
```

Neu seit Version

9.6

Weitere Informationen

CompleteClusterPairing

StartVolumePairing

Sie können das verwenden `StartVolumePairing` Methode zum Erstellen eines kodierten Schlüssels aus einem Volume, das für das Pairing mit einem anderen Volume verwendet wird. Der Schlüssel, den diese Methode erstellt, wird in verwendet `CompleteVolumePairing` Methode zum Erstellen einer Volume-Kopplung.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Modus	Der Modus des Volumens, auf dem der Kopplungsprozess gestartet werden soll. Der Modus kann nur eingestellt werden, wenn das Volume das Quellvolume ist. Mögliche Werte: • `Async`: Die Schreibvorgänge werden anerkannt, wenn sie lokal abgeschlossen werden. Das Cluster wartet nicht, bis Schreibvorgänge zum Ziel-Cluster repliziert werden. (Standard, wenn kein Modusparameter angegeben wurde.) • `Sync`: Quelle bestätigt Schreiben, wenn die Daten lokal und auf dem entfernten Cluster gespeichert werden. • `SnapshotsOnly`: Nur Snapshots, die auf dem Quellcluster erstellt wurden, werden repliziert. Aktive Schreibvorgänge vom Quell-Volume werden nicht repliziert.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	Die ID des Volumens, auf dem der Kopplungsprozess gestartet werden soll.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumePairingKey	Eine Zeichenkette, die vom verwendet wird CompleteVolumePairing API-Methode.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "StartVolumePairing",
   "params": {
         "mode": "Async",
     "volumeID" : 14
      },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1,
   "result" : {
      "volumePairingKey" :
"7b226d766970223a223139322e3136382e3133392e313232222c22766f6c756d654944223
a312c22766f6c756d654e616d65223a2254657374222c22766f6c756d65506169725555494
4223a223639363234666622d323032652d343332352d613536392d656339633635636376
23561227d"
      }
}
```


Neu seit Version

9.6

Weitere Informationen

CompleteVolumePairing

Sicherheits-API-Methoden

AddKeyServerToProviderKmip

Sie können das verwenden `AddKeyServerToProviderKmip` Methode zum Zuweisen eines KMIP-Schlüsselservers (Key Management Interoperability Protocol) zum angegebenen Schlüsselanbieter Während der Zuweisung wird der Server kontaktiert, um die Funktionalität zu überprüfen. Wenn der angegebene Schlüsselserver bereits dem angegebenen Schlüsselanbieter zugewiesen ist, wird keine Aktion ausgeführt und es wird kein Fehler zurückgegeben. Sie können die Zuweisung mit dem entfernen `RemoveKeyServerFromProviderKmip` Methode.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ID von Schlüsselausweisungs-ID	Die ID des Schlüsselanbieters, dem der Schlüsselserver zugewiesen werden soll.	Ganzzahl	Keine	Ja.
KeyServer-ID	Die ID des zu zuweisenden Schlüsselservers.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keinen Rückgabewert. Die Zuweisung gilt als erfolgreich, solange kein Fehler zurückgegeben wurde.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "AddKeyServerToProviderKmip",
  "params": {
    "keyProviderID": 1,
    "keyServerID": 15
    },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
    }
}
```

Neu seit Version

11.7

CreateKeyProviderKmip

Sie können das verwenden `CreateKeyProviderKmip` Methode zur Erstellung eines Schlüsselanbieters für das Schlüsselmanagement mit dem angegebenen Namen (Key Management Interoperability Protocol) Ein Schlüsselanbieter definiert einen Mechanismus und einen Speicherort zum Abrufen von Authentifizierungsschlüsseln. Beim Erstellen eines neuen KMIP-Schlüsselanbieters verfügt dieser über keine KMIP-Schlüsselserver. Verwenden Sie zum Erstellen eines KMIP-Schlüsselservers das `CreateKeyServerKmip` Methode. Informationen zum Zuweisen zu einem Provider finden Sie unter `AddKeyServerToProviderKmip`.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SchlüsselProvidername	Der Name, der mit dem erstellten KMIP-Schlüsselanbieter verknüpft werden soll. Dieser Name wird nur für Anzeigezwecke verwendet und muss nicht eindeutig sein.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
KmSchlüsselanbieter	Ein Objekt, das Details zum neu erstellten Schlüsselanbieter enthält.	"KeyProviderKmip"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "CreateKeyProviderKmip",
  "params": {
    "keyProviderName": "ProviderName",
    },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {
    "kmipKeyProvider": {
        "keyProviderName": "ProviderName",
        "keyProviderIsActive": true,
        "kmipCapabilities": "SSL",
        "keyServerIDs": [
            15
        ],
        "keyProviderID": 1
    }
}
}
```

Neu seit Version

11.7

CreateKeyServerkmip

Sie können das verwenden `CreateKeyServerKmip` Methode zum Erstellen eines KMIP-Schlüsselservers (Key Management Interoperability Protocol) mit den angegebenen Attributen Während der Erstellung wird der Server nicht kontaktiert. Er muss nicht vorhanden sein, bevor Sie diese Methode verwenden. Bei Konfigurationen von geclusterten Key-Servern müssen Sie die Hostnamen oder IP-Adressen aller Serverknoten im Parameter kmipKeyServerHostnames angeben. Sie können das verwenden `TestKeyServerKmip` Methode zum Testen eines Schlüsselservers.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
KmipCaCertificate	Das öffentliche Schlüsselzertifikat der Stammzertifizierungsstelle des externen Schlüsselservers. Dies wird verwendet, um das Zertifikat, das von einem externen Schlüsselserver in der TLS-Kommunikation präsentiert wird, zu überprüfen. Stellen Sie für Schlüsselservercluster, in denen einzelne Server unterschiedliche CAS verwenden, einen verketteten String bereit, der die Stammzertifikate aller CAS enthält.	Zeichenfolge	Keine	Ja.
KmipClientZertifikat	Ein PEM-Format Base64-codiertes PKCS#10 X.509-Zertifikat, das vom SolidFire KMIP-Client verwendet wird.	Zeichenfolge	Keine	Ja.
KmipKeyServerHostnames	Array der Hostnamen oder IP-Adressen, die mit diesem KMIP-Schlüsselserver verbunden sind. Mehrere Hostnamen oder IP-Adressen dürfen nur bereitgestellt werden, wenn sich die Schlüsselserver in einer Clusterkonfiguration befinden.	String-Array	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
KmipKeyServerName	Der Name des KMIP-Schlüsselservers. Dieser Name wird nur für Anzeigezwecke verwendet und muss nicht eindeutig sein.	Zeichenfolge	Keine	Ja.
KmipKeyServerPort	Die diesem KMIP-Schlüsselserver zugeordnete Port-Nummer (in der Regel 5696).	Ganzzahl	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
KmSchlüsselserver	Ein Objekt, das Details zum neu erstellten Schlüsselserver enthält.	"KeyServerkmip"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "CreateKeyServerKmip",
  "params": {
    "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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
        }
     }
}
```


Neu seit Version

11.7

CreatePublicPrivateKeyPair

Sie können das verwenden `CreatePublicPrivateKeyPair` Methode zum Erstellen von öffentlichen und privaten SSL-Schlüsseln. Mit diesen Schlüsseln können Sie Anforderungen zum Signieren von Zertifikaten erstellen. Es kann für jedes Storage-Cluster nur ein Schlüsselpaar verwendet werden. Bevor Sie diese Methode zum Austausch vorhandener Schlüssel verwenden, stellen Sie sicher, dass die Schlüssel von keinem Provider mehr verwendet werden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
CommonName	Das X.509 Distinguished Name **Common Name** -Feld (CN).	Zeichenfolge	Keine	Nein
Land	Das X.509 Distinguished Name **Land** Feld ©.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
E-Mail-Adresse	Das X.509 Distinguished Name **E-Mail-Adresse** -Feld (MAIL).	Zeichenfolge	Keine	Nein
Ort	Das X.509 Distinguished Name **Locality Name**-Feld (L).	Zeichenfolge	Keine	Nein
Organisation	Das X.509 Distinguished Name **Organisation Name** Feld (O).	Zeichenfolge	Keine	Nein
Organisationseinheit	Das X.509-Feld Distinguished Name **Organisationseinheit Name** (OU).	Zeichenfolge	Keine	Nein
Bundesland	Das Feld X.509 Distinguished Name **State** oder **Province Name** (ST oder SP oder S).	Zeichenfolge	Keine	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte. Wenn kein Fehler auftritt, gilt die Schlüsselerstellung als erfolgreich.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "CreatePublicPrivateKeyPair",
  "params": {
    "commonName": "Name",
    "country": "US",
    "emailAddress" : "email@domain.com"
   },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
}
```

Neu seit Version

11.7

DeleteKeyProviderKmip

Sie können das verwenden `DeleteKeyProviderKmip` Methode zum Löschen des angegebenen KMIP-Schlüssels (Inactive Key Management Interoperability Protocol)

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ID von Schlüsselausweisungs-ID	Die ID des zu löschenden Schlüsselanbieters.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte. Der Löschvorgang gilt als erfolgreich, solange kein Fehler vorhanden ist.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DeleteKeyProviderKmip",
  "params": {
    "keyProviderID": "1"
    },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
}
```

Neu seit Version

11.7

DeleteKeyServerkmip

Sie können das verwenden `DeleteKeyServerKmip` Methode zum Löschen eines vorhandenen KMIP-Schlüsselservers (Key Management Interoperability Protocol) Sie können einen Schlüsselserver löschen, es sei denn, er ist der letzte seinem Provider zugewiesene, und dieser Provider stellt derzeit verwendete Schlüssel zur Verfügung.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
KeyServer-ID	Die ID des zu löschenden KMIP-Schlüsselservers.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat die Werte ohne Rückgabewert. Der Löschvorgang wird als erfolgreich betrachtet, wenn keine Fehler vorliegen.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DeleteKeyServerKmip",
  "params": {
     "keyServerID": 15
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
}
```

Neu seit Version

11.7

UnbeständigkeitVerverschlüsselungAttest

Sie können das verwenden `DisableEncryptionAtRest` Methode zum Entfernen der Verschlüsselung, die zuvor mithilfe des auf den Cluster angewendet wurde `EnableEncryptionAtRest` Methode. Diese Disable-Methode ist asynchron und gibt eine Antwort zurück, bevor die Verschlüsselung deaktiviert wird. Sie können das verwenden `GetClusterInfo` Methode zum Abfragen des Systems, um zu sehen, wann der Prozess abgeschlossen ist.

- Sie können diese Methode nicht verwenden, um die Softwareverschlüsselung im Ruhezustand zu deaktivieren. Um die Softwareverschlüsselung im Ruhezustand zu deaktivieren, müssen Sie dies durchführen "Erstellen Sie einen neuen Cluster" Bei deaktivierter Softwareverschlüsselung
- Um den aktuellen Status der Verschlüsselung ruhender Daten, der Softwareverschlüsselung ruhender Daten oder beider im Cluster anzuzeigen, verwenden Sie die "Abrufen der Cluster Info-Methode"Die Sie können die `GetSoftwareEncryptionAtRestInfo` "Methode zum Abrufen von Informationen, die das Cluster verwendet, um Daten im Ruhezustand zu verschlüsseln"Die

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "DisableEncryptionAtRest",
   "params": {},
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1,
  "result" : {}
}
```

Neu seit Version

9.6

Weitere Informationen

- "GetClusterInfo"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

EnableVerschlüsselungAtZiel

Sie können das verwenden `EnableEncryptionAtRest` Methode zur Aktivierung der 256-Bit-Verschlüsselung nach AES (Advanced Encryption Standard) im Ruhezustand im Cluster, damit der Cluster die für die Laufwerke auf jedem Node verwendete Verschlüsselung verwalten kann. Diese Funktion ist standardmäßig nicht aktiviert.

- Bei dieser Methode wird die Softwareverschlüsselung im Ruhezustand nicht aktiviert. Dies kann nur mit dem durchgeführt werden "Cluster-Methode erstellen" Mit `enableSoftwareEncryptionAtRest` Auf einstellen `true`.
- Um den aktuellen Status der Verschlüsselung ruhender Daten, der Softwareverschlüsselung ruhender Daten oder beider im Cluster anzuzeigen, verwenden Sie die "Abrufen der Cluster Info-Methode"Die Sie können die `GetSoftwareEncryptionAtRestInfo` "Methode zum Abrufen von Informationen, die das Cluster verwendet, um Daten im Ruhezustand zu verschlüsseln"Die

Wenn Sie die Verschlüsselung im Ruhezustand aktivieren, managt der Cluster automatisch die Schlüssel intern für die Laufwerke auf jedem Node im Cluster.

Wenn eine keyProviderID angegeben wird, wird das Passwort entsprechend dem Typ des Schlüsselanbieters generiert und abgerufen. Dies erfolgt in der Regel mit einem KMIP-Schlüsselserver (Key Management

Interoperability Protocol) im Fall eines KMIP-Schlüsselanbieters. Nach diesem Vorgang gilt der angegebene Anbieter als aktiv und kann erst gelöscht werden, wenn die Verschlüsselung im Ruhezustand deaktiviert ist `DisableEncryptionAtRest` Methode.

Wenn Sie über einen Node-Typ verfügen, dessen Modellnummer in „-NE“ endet, wird der angezeigt `EnableEncryptionAtRest` Der Methodenanruf schlägt mit der Antwort „Verschlüsselung nicht zulässig. Nicht verschlüsselbarer Node durch das Cluster erkannt“.

Sie sollten die Verschlüsselung nur aktivieren oder deaktivieren, wenn das Cluster ausgeführt wird und sich in einem ordnungsgemäßen Zustand befindet. Sie können die Verschlüsselung nach Ihrem Ermessen und so oft wie nötig aktivieren oder deaktivieren.

Dieser Prozess ist asynchron und gibt vor Aktivierung der Verschlüsselung eine Antwort zurück. Sie können das verwenden `GetClusterInfo` Methode zum Abfragen des Systems, um zu sehen, wann der Prozess abgeschlossen ist.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ID von Schlüsselausweisungs-ID	Die ID eines KMIP-Schlüsselanbieters zu verwenden.	Ganzzahl	Keine	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "EnableEncryptionAtRest",
   "params": {},
   "id": 1
}
```

Antwortbeispiele

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel aus der EnableVerschlüsselungAtRest-Methode ähnelt. Es gibt kein Ergebnis zu berichten.

```
{
   "id": 1,
   "result": {}
}
```

Während die Verschlüsselung im Ruhezustand auf einem Cluster aktiviert wird, gibt GetClusterInfo ein Ergebnis zurück, das den Status von Verschlüsselung im Ruhezustand („Encryption AttRestState“) als „Enabled“ beschreibt. Nachdem die Verschlüsselung im Ruhezustand vollständig aktiviert ist, ändert sich der zurückgegebene Status in „aktiviert“.

```
{
   "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"
      }
   }
}
```

Neu seit Version

9.6

Weitere Informationen

- "SecureEraseDrives"
- "GetClusterInfo"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

GetClientCertificateSignRequest

Sie können das verwenden `GetClientCertificateSignRequest` Methode zum Generieren einer Anfrage zum Signieren eines Zertifikats, die von einer Zertifizierungsstelle signiert werden kann, um ein Client-Zertifikat für das Cluster zu generieren. Signierte Zertifikate sind erforderlich, um eine Vertrauensbeziehung für die Interaktion mit externen Diensten herzustellen.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
ClientCertificateSignRequest	Eine PEM-Format Base64-codierte PKCS#10 X.509-Client-Zertifikatanforderung.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetClientCertificateSignRequest",
  "params": {
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {
        "clientCertificateSignRequest":
"MIIByjCCATMCAQAwgYkxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
   }
}
```

Neu seit Version

11.7

GetKeyProviderKmip

Sie können das verwenden `GetKeyProviderKmip` Methode zum Abrufen von Informationen über den angegebenen KMIP-Schlüsselanbieter (Key Management Interoperability Protocol)

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ID von Schlüsselausweisungs-ID	Die ID des KMIP-Schlüssels, das zurückgegeben werden soll.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
KmSchlüsselanbieter	Ein Objekt, das Details zum angeforderten Schlüsselanbieter enthält.	"KeyProviderKmip"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetKeyProviderKmip",
  "params": {
    "keyProviderID": 15
    },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
    {
    "kmipKeyProvider": {
        "keyProviderID": 15,
        "kmipCapabilities": "SSL",
        "keyProviderIsActive": true,
        "keyServerIDs": [
            1
        ],
        "keyProviderName": "ProviderName"
    }
   }
}
```

Neu seit Version

11.7

GetKeyServerkmip

Sie können das verwenden `GetKeyServerKmip` Methode zur Rückgabe von Informationen zum angegebenen KMIP-Schlüsselserver (Key Management Interoperability Protocol)

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
KeyServer-ID	Die ID des KMIP-Schlüsselservers, über den Informationen zurückgegeben werden sollen.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
KmSchlüsselserver	Ein Objekt, das Details zum angeforderten Schlüsselserver enthält.	"KeyServerkmip"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetKeyServerKmip",
  "params": {
     "keyServerID": 15
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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
        }
    }
}
```

Neu seit Version

11.7

GetSoftwareVerschlüsselungAtRestInfo

Sie können das verwenden `GetSoftwareEncryptionAtRestInfo` Methode zum Abrufen von Softwareverschlüsselungsinformationen im Ruhezustand, die das Cluster verwendet, um Daten im Ruhezustand zu verschlüsseln.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Parameter	Beschreibung	Typ	Optional
MasterKeyInfo	Informationen zum aktuellen Master-Schlüssel für Softwareverschlüsselung im Ruhezustand	VerschlüsselungKeyInfo	Richtig
RekeyMasterKeyAsyncResultID	Die Async Ergebnis-ID des aktuellen oder letzten Rekeyvorgangs (falls vorhanden), sofern sie noch nicht gelöscht wurde. `GetAsyncResult` Die Ausgabe enthält eine `newKey` Feld, das Informationen über den neuen Masterschlüssel und ein enthält `keyToDecommission` Feld, das Informationen zum alten Schlüssel enthält.	Ganzzahl	Richtig
Bundesland	Der aktuelle Status der Softwareverschlüsselung im Ruhezustand. Mögliche Werte sind `disabled` Oder `enabled`.	Zeichenfolge	Falsch
Version	Eine Versionsnummer, die bei jeder Aktivierung der Softwareverschlüsselung erhöht wird.	Ganzzahl	Falsch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
 "method": "getsoftwareencryptionatrestinfo"
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "masterKeyInfo": {
            "keyCreatedTime": "2021-09-20T23:15:56Z",
            "keyID": "4d80a629-a11b-40ab-8b30-d66dd5647cfd",
            "keyManagementType": "internal"
        },
        "state": "enabled",
        "version": 1
    }
}
```

Neu seit Version

12.3

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

ListKeyProvidersKmip

Sie können das verwenden `ListKeyProvidersKmip` Abrufen einer Liste aller vorhandenen KMIP-Schlüsselanbieter (Key Management Interoperability Protocol) Sie können die Liste filtern, indem Sie zusätzliche Parameter angeben.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SchlüsselProviderIActive	Filter haben KMIP-Schlüsselserver-Objekte zurückgegeben, basierend darauf, ob sie aktiv sind. Mögliche Werte: • Richtig: Nur KMIP-Schlüsselanbieter (die aktiv sind und Schlüssel angeben, die derzeit verwendet werden) • Falsch: Gibt nur KMIP-Schlüsselanbieter zurück, die inaktiv sind (keine Schlüssel angeben und gelöscht werden können). Wenn keine Daten angegeben, werden die zurückgegebenen KMIP-Schlüsselanbieter nicht gefiltert, weil sie aktiv sind.	boolesch	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
KmipKeyProviderHasServerAssign	Die Filter haben KMIP-Schlüsselanbieter zurückgegeben, basierend darauf, ob einem KMIP-Schlüsselserver zugewiesen ist. Mögliche Werte: • Richtig: Nur KMIP-Schlüsselanbieter, die über einen KMIP-Schlüsselserver verfügen • Falsch: Gibt nur KMIP-Schlüsselanbieter zurück, denen kein KMIP-Schlüsselserver zugewiesen ist. Wenn keine Angabe durchgeführt wird, werden die zurückgegebenen KMIP-Schlüsselanbieter nicht gefiltert, weil sie einen KMIP-Schlüsselserver zugewiesen haben.	boolesch	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
KmSchlüsselProvider	Eine Liste der erstellten KMIP-Schlüsselanbieter	"KeyProviderKmip" Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListKeyProvidersKmip",
  "params": {},
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
    {
    "kmipKeyProviders": [
        {
            "keyProviderID": 15,
            "kmipCapabilities": "SSL",
            "keyProviderIsActive": true,
            "keyServerIDs": [
                1
            ],
            "keyProviderName": "KeyProvider1"
        }
    ]
}
}
```

Neu seit Version

11.7

ListKeyServersKmip

Sie können das verwenden `ListKeyServersKmip` Methode zum Auflisten aller erstellten Key Management Interoperability Protocol (KMIP)-Schlüsselserver Sie können die Ergebnisse filtern, indem Sie zusätzliche Parameter angeben.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ID von Schlüsselausweisungs-ID	Bei Angabe der Methode werden nur KMIP-Schlüsselserver zurückgegeben, die dem angegebenen KMIP-Schlüsselanbieter zugewiesen sind. Wenn keine Angabe ausgeführt wird, werden KMIP-Schlüsselserver in zurückgegebenen Fällen nicht gefiltert, weil sie dem angegebenen KMIP-Schlüsselanbieter zugewiesen sind.	Ganzzahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
KmipAssigneedProviderIActive	Filter haben KMIP-Schlüsselserver-Objekte zurückgegeben, basierend darauf, ob sie aktiv sind. Mögliche Werte: • True: Gibt nur aktive KMIP-Schlüsselserver zurück (Angabe von Schlüsseln, die derzeit verwendet werden). • False: Gibt nur KMIP-Schlüsselserver zurück, die inaktiv sind (keine Schlüssel angeben und gelöscht werden können). Wenn keine Angabe angezeigt wird, werden die zurückgegebenen KMIP-Schlüsselserver nicht gefiltert, weil sie aktiv sind.	boolesch	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
KmipHasProviderAssign	Die Filter gaben KMIP-Schlüsselserver zurück, basierend darauf, ob ihnen ein KMIP-Schlüsselanbieter zugewiesen wurde. Mögliche Werte: • Richtig: Nur KMIP-Schlüsselserver mit einem KMIP-Schlüsselanbieter werden zurückgegeben. • Falsch: Gibt nur KMIP-Schlüsselserver zurück, denen kein KMIP-Schlüsselanbieter zugewiesen ist. Wenn keine Angabe erfolgt, werden zurückgegebene KMIP-Schlüsselserver nicht gefiltert, weil sie den KMIP-Schlüsselanbieter zugewiesen haben.	boolesch	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
KmSchlüsselserver	Vollständige Liste der erstellten KMIP-Schlüsselserver	"KeyServerkmip" Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListKeyServersKmip",
  "params": {},
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "kmipKeyServers": [
        {
            "kmipKeyServerName": "keyserverName",
            "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
            "keyServerID": 15,
            "kmipAssignedProviderIsActive": true,
            "kmipKeyServerPort": 5696,
            "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames": [
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID": 1
        }
    ]
}
```

Neu seit Version

11.7

ModifyKeyServerkmip

Sie können das verwenden `ModifyKeyServerKmip` Methode zum Ändern eines vorhandenen KMIP-Schlüsselservers (Key Management Interoperability Protocol) auf die angegebenen Attribute Obwohl der einzige erforderliche Parameter die keyServerID ist, wird eine Anforderung, die nur die keyServerID enthält, keine Aktion ausgeführt und gibt keinen Fehler zurück. Alle anderen Parameter, die Sie angeben, ersetzen die vorhandenen Werte für den Schlüsselserver durch die angegebene keyServerID. Der Schlüsselserver wird während des Betriebs kontaktiert, um sicherzustellen, dass er funktionsfähig ist. Sie können mehrere Hostnamen oder IP-Adressen mit dem Parameter kmipKeyServerHostnames bereitstellen, jedoch nur, wenn die Schlüsselserver in einer geclusterten Konfiguration sind.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
KeyServer-ID	Die ID des zu ändernden KMIP-Schlüsselservers.	Ganzzahl	Keine	Ja.
KmipCaCertificate	Das öffentliche Schlüsselzertifikat der Stammzertifizierungsstelle des externen Schlüsselservers. Dies wird verwendet, um das Zertifikat, das von einem externen Schlüsselserver in der TLS-Kommunikation präsentiert wird, zu überprüfen. Stellen Sie für Schlüsselservercluster, in denen einzelne Server unterschiedliche CAS verwenden, einen verketteten String bereit, der die Stammzertifikate aller CAS enthält.	Zeichenfolge	Keine	Nein
KmipClientZertifikat	Ein PEM-Format Base64-codiertes PKCS#10 X.509-Zertifikat, das vom SolidFire KMIP-Client verwendet wird.	Zeichenfolge	Keine	Nein

KmipKeyServerHostnames	Array der Hostnamen oder IP-Adressen, die mit diesem KMIP-Schlüsselserver verbunden sind. Mehrere Hostnamen oder IP-Adressen dürfen nur bereitgestellt werden, wenn sich die Schlüsselserver in einer Clusterkonfiguration befinden.	String-Array	Keine	Nein
KmipKeyServerName	Der Name des KMIP-Schlüsselservers. Dieser Name wird nur für Anzeigezwecke verwendet und muss nicht eindeutig sein.	Zeichenfolge	Keine	Nein
KmipKeyServerPort	Die diesem KMIP-Schlüsselserver zugeordnete Port-Nummer (in der Regel 5696).	Ganzzahl	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
KmSchlüsselserver	Ein Objekt, das Details zum neu geänderten Schlüsselserver enthält.	"KeyServerkmip"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ModifyKeyServerKmip",
  "params": {
    "keyServerID": 15
    "kmipCaCertificate": "CPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "kirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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
        }
    }
}
```

Neu seit Version

11.7

RekeySoftwareVerschlüsselungAtRestMasterKey

Sie können das verwenden `RekeySoftwareEncryptionAtRestMasterKey` Methode zum RekeyKey der Softwareverschlüsselung im Ruhezustand, die zur Verschlüsselung

von DEKs (Data Encryption Keys) verwendet wird. Während der Cluster-Erstellung wird die Softwareverschlüsselung im Ruhezustand für die Verwendung des internen Key Managements (IKM) konfiguriert. Diese Rekeymethode kann nach der Cluster-Erstellung entweder zur Verwendung von IKM oder External Key Management (EKM) verwendet werden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter. Wenn der `keyManagementType` Der Parameter wurde nicht angegeben, der Rekeyvorgang wird über die vorhandene Konfiguration für das Verschlüsselungsmanagement durchgeführt. Wenn der `keyManagementType` Ist angegeben und der Schlüsselanbieter ist extern, das `keyProviderID` Außerdem muss der Parameter verwendet werden.

Parameter	Beschreibung	Typ	Optional
SchlüsselManagementtyp	Die Art der Schlüsselverwaltung, die zum Verwalten des Hauptschlüssels verwendet wird. Mögliche Werte sind: `Internal`: Rekey mit interner Schlüsselverwaltung. `External`: Rekey mit externer Schlüsselverwaltung. Wenn dieser Parameter nicht angegeben wird, wird der Rekeyvorgang mithilfe der bestehenden Key Management-Konfiguration durchgeführt.	Zeichenfolge	Richtig
ID von Schlüsselausweisungs-ID	Die ID des zu verwendenden Schlüsselanbieters. Dies ist ein eindeutiger Wert, der als Teil eines der zurückgegeben wird `CreateKeyProvider` Methoden Die ID ist nur erforderlich, wenn `keyManagementType` Ist `External` Und ist ansonsten ungültig.	Ganzzahl	Richtig

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Parameter	Beschreibung	Typ	Optional
Asynchron	Ermitteln Sie den Status der Rekeyoperation mit diesem `asyncHandle` Wert mit `GetAsyncResult`. `GetAsyncResult` Die Ausgabe enthält eine `newKey` Feld, das Informationen über den neuen Masterschlüssel und ein enthält `keyToDecommission` Feld, das Informationen zum alten Schlüssel enthält.	Ganzzahl	Falsch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "asyncHandle": 1
}
```

Neu seit Version

12.3

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

RemoveKeyServerFromProviderKmip

Sie können das verwenden `RemoveKeyServerFromProviderKmip` Methode zum Aufheben der Zuweisung des angegebenen KMIP-Schlüsselservers (Key Management Interoperability Protocol) vom Provider, dem er zugewiesen wurde. Sie können die Zuweisung eines Schlüsselservers vom Provider aufheben, es sei denn, er ist der letzte und sein Provider aktiv (die Schlüssel, die derzeit verwendet werden). Wenn der angegebene Schlüsselserver einem Provider nicht zugewiesen ist, wird keine Aktion ausgeführt und es wird kein Fehler zurückgegeben.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
KeyServer-ID	Die ID des KMIP-Schlüsselservers, der die Zuweisung aufheben soll.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte. Die Entfernung gilt als erfolgreich, solange kein Fehler zurückgegeben wird.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "RemoveKeyServerFromProviderKmip",
  "params": {
    "keyServerID": 1
   },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
    }
}
```

Neu seit Version

11.7

Signalschlüssel

Nachdem SSH auf dem Cluster mit dem aktiviert wurde "EnableSSH-Methode", Sie können die verwenden `SignSshKeys` Methode, um Zugriff auf eine Shell auf einem Knoten zu erhalten.

Beginnend mit Element 12.5, `sfreadonly` Ist ein neues Systemkonto, das die grundlegende Fehlerbehebung für einen Node ermöglicht. Diese API ermöglicht den SSH-Zugriff über `sfreadonly` Systemkonto über alle Nodes im Cluster hinweg.

> Sofern vom NetApp Support nicht empfohlen, werden Änderungen am System nicht unterstützt, sodass Sie Ihren Support-Vertrag aufgeben und möglicherweise die Daten instabil oder unzugänglich machen können.

Nachdem Sie die Methode verwendet haben, müssen Sie die Schlüsselkette aus der Antwort kopieren, sie in das System speichern, das die SSH-Verbindung initiiert, und führen Sie dann den folgenden Befehl aus:

```
ssh -i <identity_file> sfreadonly@<node_ip>
```

```
`identity_file` Ist eine Datei, aus der die Identität (privater Schlüssel)
für die Authentifizierung öffentlicher Schlüssel gelesen wird und
`node_ip` Ist die IP-Adresse des Node. Finden Sie weitere Informationen zu
`identity_file`, Siehe SSH-man-Seite.
```

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Dauer	Ganzzahl zwischen 1 und 24, die die Anzahl der Stunden für die signierte Taste angibt, gültig zu sein. Wenn keine Dauer angegeben wird, wird der Standardwert verwendet.	Ganzzahl	1	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Publizieren	Wenn angegeben, gibt dieser Parameter nur den signierten_Public_Key zurück, anstatt eine vollständige Schlüsselkette für den Benutzer zu erstellen. Öffentliche Schlüssel, die über die URL-Leiste in einem Browser mit eingereichten + Werden als Distanzstück und Bruchsignatur interpretiert.	Zeichenfolge	Null	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Sfadmin	Ermöglicht den Zugriff auf das sfadmin-Shell-Konto, wenn Sie den API-Aufruf mit supportAdmin-Cluster-Zugriff tätigen oder wenn sich der Node nicht in einem Cluster befindet.	boolesch	Falsch	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
keygen_Status	Enthält die Identität im signierten Schlüssel, die zulässigen Prinzipale und die gültigen Start- und Enddaten für den Schlüssel.	Zeichenfolge
Privater_Schlüssel	Ein privater SSH-Schlüsselwert wird nur zurückgegeben, wenn die API eine vollständige Schlüsselkette für den Endbenutzer generiert. Der Wert ist Base64-codiert; Sie müssen den Wert decodieren, wenn er in eine Datei geschrieben wird, um sicherzustellen, dass er als gültiger privater Schlüssel gelesen wird.	Zeichenfolge

Name	Beschreibung	Typ
Öffentlicher_Schlüssel	Ein öffentlicher SSH-Schlüsselwert wird nur zurückgegeben, wenn die API eine vollständige Schlüsselkette für den Endbenutzer generiert. Wenn Sie einen Public_Key-Parameter an die API-Methode übergeben, wird nur die verwendet `signed_public_key` Der Wert wird in der Antwort zurückgegeben.	Zeichenfolge
Signiert_Public_Key	Der öffentliche SSH-Schlüssel, der sich aus dem Signieren des öffentlichen Schlüssels ergibt, unabhängig davon, ob dieser von der API bereitgestellt oder generiert wurde.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "SignSshKeys",
    "params": {
        "duration": 2,
        "publicKey":<string>
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": null,
  "result": {
    "signedKeys": {
      "keygen_status": <keygen_status>,
      "signed_public_key": <signed_public_key>
    }
  }
}
```

In diesem Beispiel wird ein öffentlicher Schlüssel signiert und zurückgegeben, der für die Dauer gültig ist (1-24 Stunden).

Neu seit Version

12.5

TestKeyProviderKmip

Sie können das verwenden `TestKeyProviderKmip` Methode zum Testen, ob der angegebene KMIP-Schlüsselanbieter (Key Management Interoperability Protocol) erreichbar ist und ordnungsgemäß funktioniert

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ID von Schlüsselausweisungs-ID	Die ID des zu testenden Schlüsselanbieters.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte. Der Test gilt als erfolgreich, solange kein Fehler zurückgegeben wird.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "TestKeyProviderKmip",
  "params": {
    "keyProviderID": 15
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
    }
}
```

Neu seit Version

11.7

TestKeyServerkmip

Sie können das verwenden `TestKeyServerKmip` Methode zum Testen, ob der angegebene KMIP-Schlüsselserver (Key Management Interoperability Protocol) erreichbar ist und ordnungsgemäß funktioniert.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
KeyServer-ID	Die ID des zu testenden KMIP-Schlüsselservers.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte. Der Test gilt als erfolgreich, wenn keine Fehler zurückgegeben werden.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "TestKeyServerKmip",
  "params": {
    "keyServerID": 15
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
    }
```

Neu seit Version

11.7

SnapMirror API-Methoden

AbortSnapMirrorBeziehung

Die Web-UI der Element Software verwendet das `AbortSnapMirrorRelationship` Methode zum Stoppen von SnapMirror Transfers, die gestartet wurden, aber noch nicht abgeschlossen sind.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Die Endpunkt-ID des Remote-ONTAP-Storage-Systems, die mit dem Element Storage-Cluster kommunizieren	Ganzzahl	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Zielvolumen	Der Zieldatenträger in der SnapMirror Beziehung.	SnapMirrorVolumeInfo	Keine	Ja.
ClearCheckpoint	Legt fest, ob der Kontrollpunkt für den Neustart gelöscht werden soll oder nicht. Mögliche Werte: • Richtig • Falsch	boolesch	Falsch	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
SnapMirror Beziehung	Ein Objekt mit Informationen über die abgebrochene SnapMirror Beziehung.	SnapMirror Beziehung

Neu seit Version

10.1

BreakSnapMirrorBeziehung

Die Element Web-UI verwendet das `BreakSnapMirrorRelationship` Methode zum Unterbrechen einer SnapMirror Beziehung. Wenn eine SnapMirror Beziehung unterbrochen wird, wird das Zielvolume schreibgeschützt und unabhängig gemacht und kann dann von der Quelle umgeleitet werden. Sie können die Beziehung zum wiederherstellen `ResyncSnapMirrorRelationship` API-Methode. Diese Methode erfordert, dass das ONTAP-Cluster verfügbar ist.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Die Endpunkt-ID des Remote-ONTAP-Storage-Systems, die mit dem Element Storage-Cluster kommunizieren	Ganzzahl	Keine	Ja.
Zielvolumen	Der Zieldatenträger in der SnapMirror Beziehung.	SnapMirrorVolumeInfo	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
SnapMirror Beziehung	Ein Objekt mit Informationen über die beschädigte SnapMirror-Beziehung.	SnapMirror Beziehung

Neu seit Version

10.1

Weitere Informationen

BreakSnapMirrorVolume

BreakSnapMirrorVolume

Die Element Web-UI verwendet das `BreakSnapMirrorVolume` Methode zum Unterbrechen der SnapMirror Beziehung zwischen einem ONTAP Quell-Container und dem Element Ziel-Volume Ein Element SnapMirror Volume zu zerbrechen ist nützlich, wenn ein ONTAP System nicht mehr verfügbar ist, während Daten in ein Element Volume repliziert werden. Mit dieser Funktion kann ein Storage-Administrator die Kontrolle über ein Element SnapMirror Volume übernehmen, die Beziehung zum Remote ONTAP System unterbrechen und das Volume zu einem früheren Snapshot zurücksetzen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	Die Lautstärke, auf der der Vorgang zum Abbrechen ausgeführt werden soll. Der Volume-Zugriffsmodus muss SnapMirrorTarget sein.	Ganzzahl	Keine	Ja.
Snapshot-ID	Führen Sie ein Rollback des Volumens auf den Snapshot durch, der durch diese ID identifiziert wurde. Standardmäßig wird ein Rollback zum neuesten Snapshot durchgeführt.	Ganzzahl	Keine	Nein
Erhalten	Bewahren Sie Snapshots auf, die neuer sind als der durch Snapshot ID identifizierte Snapshot. Mögliche Werte: • True: Snapshots erhalten, die neuer sind als Snapshot-ID. • False: Bewahren Sie keine Snapshots vor der Snapshot-ID auf. Wenn „false“, werden alle Snapshots, die neuer als SnapshotID sind, gelöscht.	boolesch	Falsch	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Datenzugriff	Resultierender Zugriffsmodus für Volumes. Mögliche Werte: • ReadWrite • ReadOnly • Gesperrt	Zeichenfolge	ReadWrite	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Neu seit Version

10.0

Weitere Informationen

BreakSnapMirrorBeziehung

CreateSnapMirrorEndpoint

Die Element Web-UI verwendet das `CreateSnapMirrorEndpoint` Methode zum Erstellen einer Beziehung zu einem Remote-SnapMirror-Endpunkt

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Management IP	Die Management-IP-Adresse des Remote-SnapMirror-Endpunkts.	Zeichenfolge	Keine	Ja.
Benutzername	Der Management-Benutzername für das ONTAP System.	Zeichenfolge	Keine	Ja.
Passwort	Das Managementpasswort für das ONTAP System.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
SnapMirror Endpoint	Der neu erstellte SnapMirror Endpunkt:	SnapMirror Endpoint

Neu seit Version

10.0

CreateSnapMirrorEndpointnicht verwaltet

Das Element Software Storage-System verwendet das `CreateSnapMirrorEndpointUnmanaged` Methode, um Remote-Endpunkte ohne Management von SnapMirror zu ermöglichen, um mit einem Element Storage-Cluster zu kommunizieren. Nicht verwaltete Endpunkte können nicht mit den Element SnapMirror APIs administriert werden. Sie müssen mit ONTAP Managementsoftware oder APIs gemanagt werden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ClusterName	Der Name des Endpunkts.	Zeichenfolge	Keine	Ja.
IpAddresses	Die Liste der IP-Adressen für einen Cluster von ONTAP Storage-Systemen, die mit diesem Element Storage-Cluster kommunizieren sollten.	String-Array	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
SnapMirror Endpoint	Der neu erstellte SnapMirror Endpunkt:	SnapMirror Endpoint

Neu seit Version

10.3

CreateSnapMirrorBeziehung

Die Element Web-UI verwendet das `CreateSnapMirrorRelationship` Methode zum Erstellen einer erweiterten SnapMirror Datensicherungsbeziehung zwischen einem Quell- und Ziel-Endpunkt

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Die Endpunkt-ID des Remote-ONTAP-Storage-Systems, die mit dem Element Storage-Cluster kommunizieren	Ganzzahl	Keine	Ja.
QuelleVolume	Das Quell-Volume in der Beziehung.	SnapMirrorVolumeInfo	Keine	Ja.
Zielvolumen	Das Zielvolumen in der Beziehung.	SnapMirrorVolumeInfo	Keine	Ja.
Beziehungstyp	Die Art der Beziehung. Auf Storage-Systemen mit Element Software beträgt dieser Wert immer „`Extended_Data_Protection`“.	Zeichenfolge	Keine	Nein
PolicyName	Gibt den Namen der ONTAP SnapMirror Richtlinie für die Beziehung an. Wenn nicht angegeben, lautet der Standardrichtliniennname MirrorLatest.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Planname	Der Name des vorbestehenden cron-Zeitplans auf dem ONTAP-System, das zum Aktualisieren der SnapMirror-Beziehung verwendet wird. Wenn kein Zeitplan festgelegt ist, werden keine SnapMirror Updates geplant und müssen manuell aktualisiert werden.	Zeichenfolge	Keine	Nein
Maximale Transferrate	Gibt die maximale Datentransferrate zwischen den Volumes in Kilobyte pro Sekunde an. Der Standardwert 0 ist unbegrenzt und erlaubt der SnapMirror Beziehung, die verfügbare Netzwerkbandbreite voll zu nutzen.	Ganzzahl	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
SnapMirror Beziehung	Informationen über die neu erstellte SnapMirror Beziehung.	SnapMirror Beziehung

Neu seit Version

10.1

CreateSnapMirrorVolume

Die Element Web-UI verwendet das `CreateSnapMirrorVolume` Methode zur Erstellung eines Volumes auf dem Remote-ONTAP-System

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Die Endpunkt-ID des Remote-ONTAP-Storage-Systems, die mit dem Element Storage-Cluster kommunizieren	Ganzzahl	Keine	Ja.
vserver	Der Name des Vserver.	Zeichenfolge	Keine	Ja.
Name	Der Name des Ziel-ONTAP-Volumes.	Zeichenfolge	Keine	Ja.
Typ	Der Volume-Typ. Mögliche Werte: • rw: Volumen für Lese- und Schreibvorgänge • ls: Volumen der Lastverteilung • datensicherung: Datensicherungs-Volume Wenn kein Typ angegeben wird, ist der Standardtyp dp.	Zeichenfolge	Keine	Nein
Aggregat	Das ONTAP Aggregat, in dem das Volume erstellt werden soll. Sie können ListSnapMirrorAggregates verwenden, um Informationen über verfügbare ONTAP Aggregate zu erhalten.	Zeichenfolge	Keine	Ja.
Größe	Die Größe des Volumes in Byte.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
SnapMirror Volume	Informationen zu einem SnapMirror Volume	SnapMirror Volume

Neu seit Version

10.1

LöteSnapMirrorEndpunkte

Die Element Web-UI verwendet `DeleteSnapMirrorEndpoints` Um einen oder mehrere SnapMirror Endpunkte aus dem System zu löschen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointIDs	Ein Array von IDs von SnapMirror Endpunkten zum Löschen.	Integer-Array	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Neu seit Version

10.0

DeleteSnapMirrorRelationships

Die Element Web-UI verwendet das `DeleteSnapMirrorRelationships` Methode zum Entfernen einer oder mehrerer SnapMirror Beziehungen zwischen einem Quell- und Ziel-Endpunkt

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Die Endpunkt-ID des Remote-ONTAP-Storage-Systems, die mit dem Element Storage-Cluster kommunizieren	Ganzzahl	Keine	Ja.
ZielVolumes	Das Ziel-Volume oder die Volumes in der SnapMirror Beziehung.	SnapMirrorVolumeInfo Array erledigen	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Ergebnis	Wenn die Löschaktion erfolgreich war, enthält dieses Objekt eine Erfolgsmeldung. Wenn die Aktion fehlgeschlagen ist, enthält sie eine Fehlermeldung.	JSON-Objekt

Neu seit Version

10.1

GetOntapVersionInfo

Die Element Web-UI verwendet `GetOntapVersionInfo` Informationen zur Unterstützung der API-Version vom ONTAP-Cluster in einer SnapMirror Beziehung

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Falls vorhanden, listet das System die Versionsinformationen vom Endpunkt mit der angegebenen SnapMirrorEndpointID auf. Falls nicht vorhanden, werden Versionsinformationen aller bekannten SnapMirror Endpunkte aufgelistet.	Ganzzahl	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
OntapVersionInfo	Die Informationen zur Softwareversion des ONTAP-Endpunkts.	OntapVersionInfo Array erledigen

Neu seit Version

10.1

GetSnapMirrorClusteridentität

Die Web-UI der Element Software verwendet `GetSnapMirrorClusterIdentity` Um Identitätsinformationen über das ONTAP Cluster anzuzeigen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Wenn vorhanden, listet das System die Cluster-Identität des Endpunkts mit der angegebenen SnapMirrorEndpointID auf. Wenn nicht angegeben, listet das System die Cluster-Identität aller bekannten SnapMirror Endpunkte auf.	Ganzzahl	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Clusteridentität	Eine Liste der Cluster-Identitäten von SnapMirror Endpunkten.	SnapMirror Clusteridentität Array erledigen

Neu seit Version

10.1

InitializeSnapMirrorRelationship

Die Web-UI der Element Software verwendet das `InitializeSnapMirrorRelationship` Methode zum Initialisieren des Ziel-Volumes in einer SnapMirror Beziehung, indem ein erster Basistransfer zwischen den Clustern durchgeführt wird.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Die ID des Remote-ONTAP-Systems.	Ganzzahl	Keine	Ja.
Zielvolumen	Der Zieldatenträger in der SnapMirror Beziehung.	SnapMirrorVolumeInfo	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Maximale Transferrate	Gibt die maximale Datentransferrate zwischen den Volumes in Kilobyte pro Sekunde an. Der Standardwert 0 ist unbegrenzt und erlaubt der SnapMirror Beziehung, die verfügbare Netzwerkbandbreite voll zu nutzen.	Ganzzahl	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Beziehung	Informationen zur initialisierten SnapMirror Beziehung.	SnapMirror Beziehung

Neu seit Version

10.1

ListSnapMirrorAggregates

Die Web-UI der Element Software verwendet das `ListSnapMirrorAggregates` Die Methode zum Auflisten aller SnapMirror Aggregate, die auf dem Remote-ONTAP-System verfügbar sind. Ein Aggregat beschreibt eine Reihe physischer Storage-Ressourcen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Gibt nur die Aggregate zurück, die mit der angegebenen Endpunkt-ID verknüpft sind. Wird keine Endpunkt-ID angegeben, listet das System Aggregate von allen bekannten SnapMirror Endpunkten auf.	Ganzzahl	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirrorAggregates	Eine Liste der Aggregate, die auf dem ONTAP Storage-System verfügbar sind.	SnapMirror Aggregat Array erledigen

Neu seit Version

10.1

ListSnapMirrorEndpunkte

Die Web-UI der Element Software verwendet das `ListSnapMirrorEndpoints` Methode zum Auflisten aller SnapMirror Endpunkte, mit denen das Element Storage-Cluster kommunizieren.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointIDs	Gibt nur die Objekte zurück, die diesen IDs zugeordnet sind. Wenn keine IDs angegeben werden oder das Array leer ist, gibt die Methode alle SnapMirror Endpunkt-IDs zurück.	Integer-Array	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Endpunkte	Eine Liste vorhandener SnapMirror Endpunkte	SnapMirror Endpoint Array erledigen

Neu seit Version

10.0

ListSnapMirrorLuns

Die Web-UI der Element Software verwendet das `ListSnapMirrorLuns` Methode zum Auflisten der LUN-Informationen für die SnapMirror Beziehung vom Remote-ONTAP-Cluster.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Listen Sie nur die LUN-Informationen auf, die mit der angegebenen Endpunkt-ID verknüpft sind.	Ganzzahl	Keine	Ja.
Zielvolumen	Der Zieldatenträger in der SnapMirror Beziehung.	SnapMirrorVolumeInfo	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
SnapMirrorLunInfos	Eine Liste von Objekten, die Informationen über SnapMirror LUNs enthalten	SnapMirrorLunInfo Array erledigen

Neu seit Version

10.1

ListSnapMirrorNetworkInterfaces

Die Web-UI der Element Software verwendet das `ListSnapMirrorNetworkInterfaces` „Method to list“ aller verfügbaren SnapMirror Schnittstellen in einem Remote ONTAP System.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Geben Sie nur die Netzwerkschnittstellen zurück, die mit der angegebenen Endpunkt-ID verknüpft sind. Wenn keine Endpunkt-ID angegeben wird, werden die Schnittstellen von allen bekannten SnapMirror Endpunkten aufgelistet.	Ganzzahl	Keine	Nein
OberflächeRole	Führen Sie nur die Netzwerkschnittstelle auf, die die angegebene Rolle bereitstellt.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirrorNetworkInterfaces	Eine Liste der SnapMirror Netzwerkschnittstellen, die auf dem Remote ONTAP Storage-System verfügbar sind.	SnapMirror Netzwerkschnittstelle Array erledigen

Neu seit Version

10.1

ListSnapMirrorNodes

Die Web-UI der Element Software verwendet das `ListSnapMirrorNodes` Methode zum Abrufen einer Liste von Knoten in einem Remote-ONTAP-Cluster.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Falls vorhanden, listet das System die Knoten des Endpunktes mit der angegebenen SnapMirrorEndpointID auf. Ist dies nicht der Fall, werden die Nodes aller bekannten SnapMirror Endpunkte aufgelistet.	Ganzzahl	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Nodes	Eine Liste der Nodes auf dem ONTAP Cluster.	SnapMirror Node Array erledigen

Neu seit Version

10.1

ListSnapMirrorPolicies

Die Web-UI der Element Software verwendet das `ListSnapMirrorPolicies` Methode zum Auflisten aller SnapMirror Richtlinien auf einem Remote ONTAP System.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Listen Sie nur die Richtlinien auf, die mit der angegebenen Endpunkt-ID verknüpft sind. Wird keine Endpunkt-ID angegeben, werden die Richtlinien von allen bekannten SnapMirror Endpunkten aufgelistet.	Ganzzahl	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Richtlinien	Eine Liste der SnapMirror Richtlinien auf dem ONTAP Storage-System.	SnapMirror Richtlinie Array erledigen

Neu seit Version

10.1

ListSnapMirrorSchedules

Die Web-UI der Element Software verwendet das `ListSnapMirrorSchedules` Methode zum Abrufen einer Liste von Zeitplänen, die in einem Remote-ONTAP-Cluster verfügbar sind.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Falls vorhanden, werden die Zeitpläne für den Endpunkt mit der angegebenen SnapMirror Endpunkt-ID aufgelistet. Falls nicht angegeben, werden die Zeitpläne für alle bekannten SnapMirror Endpunkte aufgelistet.	Ganzzahl	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirrorSchedules	Eine Liste der SnapMirror Zeitpläne auf dem Remote ONTAP Cluster.	SnapMirrorJobeCronInfo Array erledigen

Neu seit Version

10.1

ListSnapMirrorBeziehung

Die Web-UI der Element Software verwendet das `ListSnapMirrorRelationships` Methode zum Auflisten einer oder aller SnapMirror Beziehungen auf einem Element Storage-Cluster.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Listen Sie nur die Beziehungen auf, die mit der angegebenen Endpunkt-ID verknüpft sind. Wird keine Endpunkt-ID angegeben, werden die Beziehungen von allen bekannten SnapMirror Endpunkten aufgelistet.	Ganzzahl	Keine	Nein
Zielvolumen	Beziehungen auflisten, die mit dem angegebenen Zielvolume verknüpft sind.	SnapMirrorVolumeInfo	Keine	Nein
QuelleVolume	Beziehungen auflisten, die mit dem angegebenen Quell-Volume verknüpft sind	SnapMirrorVolumeInfo	Keine	Nein
vserver	Beziehungen auf dem angegebenen Vserver auflisten.	Zeichenfolge	Keine	Nein
Beziehungs-ID	Beziehungen auflisten, die mit der angegebenen Beziehungs-ID verknüpft sind.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Beziehung wird durchgeführt	Eine Liste von Objekten mit Informationen zu SnapMirror Beziehungen.	SnapMirror Beziehung Array erledigen

Neu seit Version

10.1

ListSnapMirrorVolumes

Die Web-UI der Element Software verwendet das `ListSnapMirrorVolumes` Die Methode zum Auflisten aller auf einem Remote-ONTAP-System verfügbaren SnapMirror Volumes.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Listen Sie nur die Volumes auf, die mit der angegebenen Endpunkt-ID verknüpft sind. Wird keine Endpunkt-ID angegeben, listet das System Volumes von allen bekannten SnapMirror Endpunkten auf.	Ganzzahl	Keine	Nein
vserver	Auf dem angegebenen Vserver gehostete Volumes auflisten. Der Vserver muss vom Typ „Daten“ sein.	Zeichenfolge	Keine	Nein
Name	Listen Sie nur ONTAP-Volumes mit dem angegebenen Namen auf.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Typ	Listen Sie nur ONTAP-Volumes des angegebenen Typs auf. Mögliche Werte: • rw: Volumes mit Lese- und Schreibvorgängen • ls: Volumes zur Lastverteilung • datensicherung: Volumes	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Volume	Eine Liste der SnapMirror Volumes, die auf dem ONTAP Storage-System verfügbar sind	SnapMirror Volume Array erledigen

Neu seit Version

10.1

ListSnapMirrorVserver

Die Web-UI der Element Software verwendet das `ListSnapMirrorVservers` Methode zur Auflistung aller auf einem Remote ONTAP System verfügbaren SnapMirror Vserver

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Listen Sie nur die mit der angegebenen Endpunkt-ID verknüpften Vserver auf. Wird keine Endpunkt-ID angegeben, listet das System Vserver von allen bekannten SnapMirror Endpunkten auf.	Ganzzahl	Keine	Nein
VserverType	Listen Sie nur Vserver des angegebenen Typs auf. Mögliche Werte: • Admin • Daten • Knoten • System	Zeichenfolge	Keine	Nein
VserverName	Nur Vserver mit dem angegebenen Namen auflisten.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Vserver	Eine Liste der SnapMirror Vserver, die auf dem ONTAP Storage-System verfügbar sind:	SnapMirrorVServer Array erledigen

Neu seit Version

10.1

ModifySnapMirrorEndpoint

Die Web-UI der Element Software verwendet das `ModifySnapMirrorEndpoint` Methode zum Ändern von Namen und Managementattributen für einen SnapMirror Endpunkt

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirror EndpointID	Den zu ändernden SnapMirror Endpunkt	Ganzzahl	Keine	Ja.
Management IP	Die neue Management-IP-Adresse für das ONTAP System.	Zeichenfolge	Keine	Nein
Benutzername	Der neue Management-Benutzername für das ONTAP System.	Zeichenfolge	Keine	Nein
Passwort	Das neue Managementpasswort für das ONTAP System.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Endpoint	Informationen zum geänderten SnapMirror Endpunkt.	SnapMirror Endpoint

Neu seit Version

10.0

ModifySnapMirrorEndpoint (nicht gemanagt)

Element Software verwendet diese Version des `ModifySnapMirrorEndpoint` Methode zum Ändern des Storage-Cluster-Namens oder der IP-Adressattribute für einen nicht gemanagten SnapMirror Endpunkt Nicht verwaltete Endpunkte können nicht mit den Element SnapMirror APIs administriert werden. Sie müssen mit ONTAP Managementsoftware oder APIs gemanagt werden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirror EndpointID	Den zu ändernden SnapMirror Endpunkt	Ganzzahl	Keine	Ja.
ClusterName	Der neue Name des Endpunkts.	Zeichenfolge	Keine	Nein
IpAddresses	Die neue Liste der IP-Adressen für ein Cluster von ONTAP Storage-Systemen, die mit diesem Element Storage-Cluster kommunizieren sollten.	String-Array	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Endpoint	Informationen zum geänderten SnapMirror Endpunkt.	SnapMirror Endpoint

Neu seit Version

10.3

ModifySnapMirrorRelationship

Verwenden Sie können `ModifySnapMirrorRelationship` Um die Intervalle zu ändern, in denen ein geplanter Snapshot stattfindet. Mit dieser Methode können Sie auch einen Zeitplan löschen oder anhalten.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Zielvolumen	Der Zieldatenträger in der SnapMirror Beziehung.	SnapMirror Volumeinfo	Keine	Ja.

Maximale Transferrate	Gibt die maximale Datentransferrate zwischen den Volumes in Kilobyte pro Sekunde an. Der Standardwert 0 ist unbegrenzt und erlaubt der SnapMirror Beziehung, die verfügbare Netzwerkbandbreite voll zu nutzen.	Ganzzahl	Keine	Nein
PolicyName	Gibt den Namen der ONTAP SnapMirror Richtlinie für die Beziehung an.	Zeichenfolge	Keine	Nein
Planname	Der Name des vorbestehenden cron-Zeitplans auf dem ONTAP-System, das zum Aktualisieren der SnapMirror-Beziehung verwendet wird.	Zeichenfolge	Keine	Nein
SnapMirrorEndpointID	Die Endpunkt-ID des Remote-ONTAP-Storage-Systems, die mit dem Element Storage-Cluster kommunizieren	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Beziehung	Ein Objekt, das die geänderten SnapMirror Beziehungsattribute enthält.	SnapMirror Beziehung

Neu seit Version

10.1

UpdateSnapMirrorRelationship

Die Web-UI der Element Software verwendet das `UpdateSnapMirrorRelationship` Methode, um das Ziel-Volume in einer SnapMirror Beziehung zu einer aktuellen Spiegelung des Quell-Volume zu machen.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Die Endpunkt-ID des Remote-ONTAP-Storage-Systems, die mit dem Element Storage-Cluster kommunizieren	Ganzzahl	Keine	Ja.
Zielvolumen	Der Zieldatenträger in der SnapMirror Beziehung.	SnapMirror Volumeinfo	Keine	Ja.
Maximale Transferrate	Gibt die maximale Datentransferrate zwischen den Volumes in Kilobyte pro Sekunde an. Der Standardwert 0 ist unbegrenzt und erlaubt der SnapMirror Beziehung, die verfügbare Netzwerkbandbreite voll zu nutzen.	Ganzzahl	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Beziehung	Ein Objekt mit Informationen zur aktualisierten SnapMirror Beziehung.	SnapMirror Beziehung

Neu seit Version

10.1

QuiesceSnapMirrorBeziehung

Die Web-UI der Element Software verwendet das `QuiesceSnapMirrorRelationship` Methode zum Deaktivieren zukünftiger Datentransfers für eine SnapMirror Beziehung. Wenn eine Übertragung ausgeführt wird, wird der Beziehungsstatus „stillgelegt“, bis die Übertragung abgeschlossen ist. Wenn die aktuelle Übertragung abgebrochen wird, wird sie nicht neu gestartet. Sie können Datentransfers für die Beziehung mithilfe des neu aktivieren `ResumeSnapMirrorRelationship` API-Methode.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Die Endpunkt-ID des Remote-ONTAP-Storage-Systems, die mit dem Element Storage-Cluster kommunizieren	Ganzzahl	Keine	Ja.
Zielvolumen	Der Zieldatenträger in der SnapMirror Beziehung.	SnapMirror Volumeinfo	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Beziehung	Ein Objekt mit Informationen über die stillgelegte SnapMirror Beziehung.	SnapMirror Beziehung

Neu seit Version

10.1

ResummeSnapMirrorBeziehung

Die Web-UI der Element Software verwendet das `ResumeSnapMirrorRelationship` Methode zum Aktivieren zukünftiger Transfers für eine stillgelegte SnapMirror Beziehung.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Die Endpunkt-ID des Remote-ONTAP-Storage-Systems, die mit dem Element Storage-Cluster kommunizieren	Ganzzahl	Keine	Ja.
Zielvolumen	Der Zieldatenträger in der SnapMirror Beziehung.	SnapMirror Volumeinfo	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Beziehung	Ein Objekt mit Informationen über die wieder aufgenommen SnapMirror Beziehung.	SnapMirror Beziehung

Neu seit Version

10.1

ResyncSnapMirrorRelationship

Die Web-UI der Element Software verwendet das `ResyncSnapMirrorRelationship` Methode zum Aufbau oder zur Wiederherstellung einer Spiegelbeziehung zwischen einem Quell- und Zielendpunkt Wenn Sie eine Beziehung neu synchronisieren, entfernt das System Schnappschüsse auf dem Ziel-Volume, die neuer sind als die allgemeine Snapshot-Kopie, und mountet dann das Ziel-Volume als Datensicherungs-Volume mit der gemeinsamen Snapshot-Kopie als exportierte Snapshot-Kopie.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirrorEndpointID	Die Endpunkt-ID des Remote-ONTAP-Storage-Systems, die mit dem Element Storage-Cluster kommunizieren	Ganzzahl	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Zielvolumen	Der Zieldatenträger in der SnapMirror Beziehung.	SnapMirror Volumeinfo	Keine	Ja.
Maximale Transferrate	Gibt die maximale Datentransferrate zwischen den Volumes in Kilobyte pro Sekunde an. Der Standardwert 0 ist unbegrenzt und erlaubt der SnapMirror Beziehung, die verfügbare Netzwerkbandbreite voll zu nutzen.	Ganzzahl	Keine	Nein
QuelleVolume	Das Quell-Volume in der SnapMirror Beziehung.	SnapMirror Volumeinfo	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SnapMirror Beziehung	Ein Objekt, das Informationen über die resynchronisierte SnapMirror Beziehung enthält.	SnapMirror Beziehung

Neu seit Version

10.1

Methoden für die Systemkonfiguration-API

DisableBmcColdReset

Sie können das verwenden `DisableBmcColdReset` Methode zum Deaktivieren der Hintergrundaufgabe, die den Baseboard Management Controller (BMC) regelmäßig für alle Knoten im Cluster zurücksetzt

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
CBmcResetDurationMinuten	Gibt die Zeit zwischen den Rücksetzintervallen zurück. Nach Abschluss des Befehls sollte das Intervall immer 0 sein.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DisableBmcColdReset",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "cBmcResetDurationMinutes": 0
    }
}
```

Neu seit Version

12.0

DisableClusterSsh

Sie können das verwenden `DisableClusterSsh` „Methode“ zum Deaktivieren des SSH-Service für das gesamte Storage-Cluster. Wenn Sie dem Storage-Cluster Nodes hinzufügen, übernehmen die neuen Nodes die Cluster-weite Einstellung.

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Ergebnis	Ein JSON-Objekt, das den Status des SSH-Service für das Storage-Cluster enthält, die verbleibende Zeit bis SSH deaktiviert ist, und den SSH-Servicestatus für jeden Node.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DisableClusterSsh",
  "params": {
      },
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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
    } ]
            }
    }
```

Neu seit Version

10.3

AbleSnmp

Sie können das verwenden `DisableSnmp` Methode zum Deaktivieren von SNMP auf den Clusterknoten.

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewert

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DisableSnmp",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "result" : {},
  "id" : 1
}
```

Neu seit Version

9.6

EnableBmcColdReset

Sie können das verwenden `EnableBmcColdReset` Methode zum Aktivieren einer Hintergrundaufgabe, bei der der Baseboard Management Controller (BMC) regelmäßig für alle Knoten im Cluster zurückgesetzt wird.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Zeitüberschreitung	Die Zeit zwischen BMC-Reset-Vorgängen in Minuten.	Ganzzahl	20160 Minuten	Nein

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
CBmcResetDurationMinuten	Gibt die Zeit zwischen den Rücksetzintervallen zurück. Nach Abschluss des Befehls sollte das Intervall immer 0 sein.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "EnableBmcColdReset",
    "params": {
                "timeout": 36000
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "cBmcResetDurationMinutes": 36000
    }
}
```

Neu seit Version

12.0

EntleClusterSsh

Sie können das verwenden `EnableClusterSsh` Methode zum Aktivieren des SSH-Service auf allen Nodes im Storage-Cluster.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Dauer	Die Zeitspanne, während der der SSH-Dienst aktiviert bleibt.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Ergebnis	Ein JSON-Objekt, das den Status des SSH-Service für das Storage-Cluster enthält, die verbleibende Zeit bis SSH deaktiviert ist, und den SSH-Servicestatus für jeden Node.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "EnableClusterSsh",
  "params": {
      "duration"  : "02:00:00.00"
  },
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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
    } ]
            }
    }
```

Neu seit Version

10.3

EnableSnmp

Sie können das verwenden `EnableSnmp` Methode zum Aktivieren von SNMP auf Cluster-Knoten. Wenn Sie SNMP aktivieren, gilt die Aktion für alle Knoten im Cluster und die Werte, die übergeben werden, ersetzen alle Werte, die in einem vorherigen Aufruf festgelegt wurden `EnableSnmp`.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnmpV3Enabled	Wenn auf „true“ gesetzt ist, ist SNMP v3 auf jedem Knoten im Cluster aktiviert. Wenn auf false gesetzt, ist SNMP v2 aktiviert.	boolesch	Falsch	Nein

Rückgabewert

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "EnableSnmp",
  "params": {
      "snmpV3Enabled"  : "true"
  },
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {}
}
```

Neu seit Version

9.6

GetBinAssignmentProperties

Sie können das verwenden `GetBinAssignmentProperties` Methode zum Abrufen der Eigenschaften der Fachzuordnungszuweisung in der Datenbank.

Parameter

Diese Methode verfügt über keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Eigenschaften	Zeigt die Eigenschaften für alle aktuellen bin-Zuweisungen in der Datenbank an.	BinAssignmentProperties Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "GetBinAssignmentProperties",
    "params": {
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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": []
        }
    }
}
```

Neu seit Version

12.0

GetClusterSshInfo

Sie können das verwenden `GetClusterSshInfo` Methode zum Abfragen des Status des SSH-Service für das gesamte Storage-Cluster.

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Ergebnis	Ein JSON-Objekt, das den Status des SSH-Service für das Storage-Cluster enthält, die verbleibende Zeit bis SSH deaktiviert ist, und den SSH-Servicestatus für jeden Node.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetClusterSshInfo",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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
    } ]
            }
    }
```

Neu seit Version

10.3

GetClusterStructure

Sie können das verwenden `GetClusterStructure` Methode zum Backup der aktuellen Konfigurationsinformationen des Storage Clusters. Wenn die Storage-Cluster-Konfiguration während der Ausführung dieser Methode geändert wird, ist der Inhalt des Konfigurations-Backups nicht vorhersehbar. Sie können diese Daten in einer Textdatei speichern und auf anderen Clustern oder im selben Cluster bei einem Ausfall wiederherstellen.

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Ergebnis	Ein JSON-Objekt, das die aktuellen Informationen zur Storage-Cluster-Konfiguration enthält.	ClusterStructure

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetClusterStructure",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result" : <clusterStructure object containing configuration
information>
    }
```

Neu seit Version

10.3

GetFipsReport

Sie können das verwenden `GetFipsReport` Die Methode zur Prüfung der FIPS 140-2-2-Verschlüsselungsfunktion unterstützt den Status aller Nodes im Storage-Cluster.

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Ergebnis	Ein JSON-Objekt, das den Status von FIPS 140-2-Funktionen für jeden Node unterstützt, und Fehlerinformationen für jeden Node, der nicht auf die Abfrage reagiert hat.	FipsReport

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetFipsReport",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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"
               }
        }
    ]
    }
}
```

Neu seit Version

10.3

GetLldpConfig

Sie können das verwenden `GetLldpConfig` Methode zum Abrufen der Konfiguration des Link Layer Discovery Protocol (LLDP) für jeden Knoten eines Storage-Clusters

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
LdpConfig	Informationen zur Speicher-Cluster LLDP-Konfiguration.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetLldpConfig",
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": null,
        "result": {
            "lldpConfig": {
                "enableLldp": true,
                "enableMed": false,
                "enableOtherProtocols": true
        }
    }
}
```

GetLldpInfo

Sie können das verwenden `GetLldpInfo` Methode zum Abrufen der Konfiguration des Link Layer Discovery Protocol (LLDP) für jeden Node eines Storage-Clusters oder eines einzelnen Storage Nodes.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
LldpInfo	Informationen über Chassis-, Schnittstellen- und Nachbarseinstellungen für jeden Node eines Storage-Clusters.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetLldpInfo",
   "id" : 1
}
```

Antwortbeispiel

Aufgrund der Länge dieses Antwortbeispiels wird es in einem ergänzenden Thema dokumentiert.

Neu seit Version

11.0

Weitere Informationen

GetLldpInfo

GetNodeFipsDrivesReport

Sie können das verwenden `GetNodeFipsDrivesReport` Methode zur Überprüfung des FIPS 140-2 Laufwerksverschlüsselungsstatus eines einzelnen Node im Storage Cluster. Sie müssen diese Methode für einen einzelnen Storage-Node ausführen.

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
FipsDrives	Ein JSON-Objekt, das den Status der Unterstützung von FIPS 140-2-Funktionen für diesen Node enthält. Mögliche Werte: • Keine: Node ist nicht FIPS-fähig. • Partiell: Node ist FIPS-fähig, nicht alle Laufwerke im Node sind FIPS-Laufwerke. • Bereit: Node ist FIPS-fähig und alle Laufwerke im Node sind FIPS-Laufwerke (oder es sind keine Laufwerke vorhanden).	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetNodeFipsDrivesReport",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "fipsDrives": "None"
    }
}
```

Neu seit Version

11.5

GetNtpInfo

Sie können das verwenden `GetNtpInfo` Method to get the current Network Time Protocol (NTP) Configuration information.

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Server	Liste der NTP-Server.	String-Array
BroadcastClient	Gibt an, ob die Nodes im Cluster auf NTP-Broadcast-Meldungen hören oder nicht. Mögliche Werte: • Richtig • Falsch	boolesch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetNtpInfo",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {
    "broadcastclient" : false,
    "servers" : [ "us.pool.ntp.org" ]
   }
}
```

Neu seit Version

9.6

GetNvramInfo

Sie können das verwenden `GetNvramInfo` Methode zum Abrufen von Informationen von jedem Node über die NVRAM-Karte.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Erzwingen	Der Force-Parameter muss bei dieser Methode enthalten sein, um auf allen Nodes im Cluster erfolgreich ausgeführt zu werden.	boolesch	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
NvramInformationen	Arrays von Ereignissen und Fehlern, die auf der NVRAM-Karte erkannt wurden.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetNvramInfo",
  "params": {
      "force": true
      },
  "id" : 1
}
```

Antwortbeispiel

Aufgrund der Länge dieses Antwortbeispiels wird es in einem ergänzenden Thema dokumentiert.

Neu seit Version

9.6

Weitere Informationen

GetNvramInfo

GetProtectionDomainLayout

Sie können das verwenden `GetProtectionDomainLayout` Methode zum Zurückgeben aller Schutz-Domain-Informationen für ein Cluster, einschließlich welches Chassis und in welcher benutzerdefinierten Schutz-Domäne sich die einzelnen Nodes befinden.

Parameter

Diese Methode verfügt über keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SchutzDomainLayout	Liste der Nodes mit jeweils zugehörigen Sicherungsdomänen.	JSON-Liste von "NodeProtectionDomains" Objekte:

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetProtectionDomainLayout",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
          }
        ]
```

```
        }
      ]
    }
}
```

Neu seit Version

12.0

GetRemoteLoggingHosts

Sie können das verwenden `GetRemoteLoggingHosts` Methode zum Abrufen der aktuellen Liste der Protokollserver.

Parameter

Es gibt keine Eingabeparameter für `GetRemoteLoggingHosts` Die

Rückgabewert

Der `GetRemoteLoggingHosts` Die Methode hat folgenden Rückgabewert:

Name	Beschreibung	Typ
Abnehmbare Hosts	Listet die IP-Adresse, den FQDN und die Portinformationen von Hosts auf, die für den Empfang weitergeleiteter Protokollinformationen konfiguriert sind.	LoggingServer Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "id": 3386609,
   "method": "GetRemoteLoggingHosts",
   "params": {}
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 3386609,
   "result": {
      "remoteHosts": [
         {
           "host": "172.16.1.20",
           "port": 10514
         },
         {
           "host": "172.16.1.25"
         },
         {
            "host": "syslogs.lab.company.net",
            "port": 514
         }
      ]
   }
}
```

Neu seit Version

Verfügbar ab ONTAP 9.6.

Weitere Informationen

SetRemoteLoggingHosts

GetSnmpACL

Sie können das verwenden `GetSnmpACL` Methode zum Abrufen der aktuellen SNMP-Zugriffsberechtigungen auf den Cluster-Knoten.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Netzwerke	Liste der Netzwerke und welche Art von Zugriff sie auf die SNMP-Server haben, die auf den Cluster-Knoten laufen. Dieser Wert ist vorhanden, wenn SNMP v3 deaktiviert ist.	Netzwerk Array erledigen

Name	Beschreibung	Typ
UsmUser	Liste der Benutzer und der Zugriffstyp für die SNMP-Server, die auf den Clusterknoten ausgeführt werden. Dieser Wert ist vorhanden, wenn SNMP v3 aktiviert ist.	UsmUser Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method": "GetSnmpACL",
"params": {},
"id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {
     "usmUsers"  : [
       {
          "name": "jdoe",
          "access": "rouser",
          "secLevel": "priv",
          "password": "mypassword",
          "passphrase": "mypassphrase",
       }
     ]
   }
}
```

Neu seit Version

9.6

GetSnmpInfo

Sie können das verwenden `GetSnmpInfo` Methode zum Abrufen der aktuellen Informationen über die Konfiguration des Simple Network Management Protocol (SNMP).

Parameter

GetSnmpInfo ist bei Versionen, die später als die Element-Version 8.0 sind, veraltet. Der GetSnmpState Und SetSnmpACL Methoden ersetzen die GetSnmpInfo-Methode.

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Netzwerke	Liste der für SNMP aktivierten Netzwerke und Zugriffstypen **Hinweis:** Netzwerke werden nur angezeigt, wenn SNMP v3 deaktiviert ist.	Netzwerk
Aktiviert	Gibt an, ob die Knoten im Cluster für SNMP konfiguriert sind. Mögliche Werte: • Richtig • Falsch	boolesch
SnmpV3Enabled	Wenn der Knoten im Cluster für SNMP v3 konfiguriert ist. Mögliche Werte: • Richtig • Falsch	boolesch
UsmUser	Wenn SNMP v3 aktiviert ist, wird eine Liste der Benutzerzugriffsparameter für SNMP vom Cluster zurückgegeben. Diese wird anstelle des Parameters Netzwerke zurückgegeben.	UsmUser

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetSnmpInfo",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1,
   "result" : {
      "enabled" : true,
      "networks" : [
         {
            "access" : "rosys",
            "cidr" : 0,
            "community" : "public",
            "network" : "localhost"
         }
      ]
   }
}
```

Neu seit Version

9.6

Weitere Informationen

- GetSnmpState
- SetSnmpACL

GetSnmpState

Sie können das verwenden `GetSnmpState` Methode zum Abrufen des aktuellen Status der SNMP-Funktion.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Aktiviert	Mögliche Werte: • Richtig • Falsch Der Standardwert ist false. Gibt TRUE zurück, wenn die Knoten im Cluster für SNMP konfiguriert sind.	boolesch
SnmpV3Enabled	Mögliche Werte: • Richtig • Falsch Der Standardwert ist false. Gibt TRUE zurück, wenn die Knoten im Cluster für SNMP v3 konfiguriert sind.	boolesch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetSnmpState",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {
   "enabled": true,
   "snmpV3Enabled": false
   }
}
```

Neu seit Version

9.6

Weitere Informationen

SetSnmpACL

GetSnmpTrapInfo

Sie können das verwenden `GetSnmpTrapInfo` Methode zum Abrufen der aktuellen SNMP-Trap-Konfigurationsinformationen.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Trap-Empfänger	Liste der Hosts, die die vom Cluster erzeugten Traps empfangen sollen.	SnmpTrapEmpfänger Array erledigen
ClusterFaultTrapsmentiert	Der Wert true gibt an, dass eine solidFireClusterFaultNotification so konfiguriert ist, dass sie an die Liste der Trap-Empfänger gesendet wird, wenn ein Clusterfehler protokolliert wird.	boolesch
ClusterFaultResolvedTrapsEnablier ed	Der Wert TRUE zeigt an, dass eine solidFireClusterFaultResolvedNotifi cation so konfiguriert ist, dass sie an die Liste der Trap-Empfänger gesendet wird, wenn ein Clusterfehler behoben ist.	boolesch
ClusterEventTrapsmit Funktionen	Der Wert true gibt an, dass eine solidFireClusterEventNotification so konfiguriert ist, dass sie bei einem Clusterereignis an die Liste der Trap-Empfänger gesendet wird.	boolesch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method":"GetSnmpTrapInfo"
   "params":{},
   "id":1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
     }
   ]
 }
}
```

Neu seit Version

9.6

GetSSLZertifikat

Sie können das verwenden `GetSSLCertificate` Methode zum Abrufen des SSL-Zertifikats, das derzeit auf den Storage-Nodes des Clusters aktiv ist.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Zertifikat	Der vollständige PEM-codierte Text des Zertifikats.	Zeichenfolge
Details	Die decodierten Informationen des Zertifikats.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method" : "GetSSLCertificate",
    "params" : {},
    "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:


```
{
    "id": 1,
    "result": {
        "certificate": "-----BEGIN CERTIFICATE-----
\nMIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSIb3DQEBBQUAMIGDMQswCQYD\nVQQGEw
JVUzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\nA1UEChMYV2hhdC
BIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBFh53\naGF0aGFwcGVuc0B2ZWdhc3
N0YXlzaW4udmVnYXMwHhcNMTcwMzA4MjI1MDI2WhcN\nMjcwMzA2MjI1MDI2WjCBgzELMAkGA1
UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYD\nVQQHFAxWZWdhcywgQmFieSExITAfBgNVBAoTGF
doYXQgSGFwcGVucyBpbiBWZWdh\ncy4uLjEtMCsGCSqGSIb3DQEJARYed2hhdGhhcHBlbnNAdm
VnYXNzdGF5c2luLnZl\nZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f
nLKQNWEWMR\n6akeDKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH
P4\nt6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nmrgp
GZQF3iOSIcBHtLKE5186JVT6j5dg6yjUGQO352ylc9HXHcn6lb/jyl0DmVNU\nZ0caQwAmIS3J
moyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K6lS\n7dg9cyXu4afXcgKy14Ji
NBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzxF+AC\nq+itawIDAQABo4HrMIHoMB0GA1Ud
DgQWBBRvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
```

```
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYDVQQHFAxW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbiBWZWdhcy4uLjEtMCsGCSqG
SIb3DQEJARYe\nd2hhdGhhcHBlbnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjjf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s71mQPECwVLfiE/ndtIbnpe\nMq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7JyfS37l4rRolFpX6N\niebEgAaE5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dHOlQ+WYnoO/eIMy0coT26JBl5H\nDEwvdl+DwkxnS1cx1v
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAjJDg
l0QoQDWNDoTeRBsz80nwiouA==\n-----END CERTIFICATE-----\n",
        "details": {
            "issuer":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org",
            "modulus":
"F14FB6F1F9CB290356116311E9A91E0CAB9E852A52EFDA1D2C68A0235F2A94257F0146396
4B8EAB138C1BD325546FE38CA809380DAF1DFA53B1473F8B7A3FF4A2D1A62BE28BF1979C03
A44337432CB924F07B25E94E07A003EDF9A24F078FDB41D162966F63E533ECB6041429AB82
9199405DE239221C047B4B284E75F3A2554FA8F9760EB28D41903B7E76CA573D1D71DC9FA9
5BFE3CA5D0399535467471A430026212DC99A8CB1FB38FF61AE162AAFB64AA4C05FB6D7D05
DF01C77D79D99479CCF1F113E4DFFD03E2BA952EDD83D7325EEE1A7D77202B2D78262341BE
A6C18E1809B44EFAC80CBAAD31EED313378E376471BF58F2688DCF117E002ABE8AD6B",
            "notAfter": "2027-03-06T22:50:26Z",
            "notBefore": "2017-03-08T22:50:26Z",
            "serial": "CC1B221598E37FF3",
            "sha1Fingerprint":
"1D:70:7A:6F:18:8A:CD:29:50:C7:95:B1:DD:5E:63:21:F4:FA:6E:21",
            "subject":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org"
        }
    }
}
```


Neu seit Version

10.0

ListeProtectionDomainLevels

Sie können das verwenden `ListProtectionDomainLevels` „Method to list the Tolerance and Resiliency Levels of the Storage Cluster. Toleranzstufen geben an, dass das Cluster im Fehlerfall Daten lesen und schreiben kann. Das Stabilitätsniveau gibt an, dass das Storage Cluster sich bei einem oder mehreren Ausfällen automatisch selbst heilen kann.

Parameter

Diese Methode hat keinen Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
SchutzDominLevels	Eine Liste der verschiedenen Schutz-Domain-Level, bei der jeder die Toleranz und Resiliency-Informationen des Storage-Clusters liefert.	SchutzDomainLevel

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListProtectionDomainLevels",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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
                    }
                }
            ]
        }
}
```


Neu seit Version

11.0

RemoveSSLZertifikat

Sie können das verwenden `RemoveSSLCertificate` Methode zum Entfernen des Benutzer-SSL-Zertifikats und des privaten Schlüssels für die Storage-Nodes im Cluster. Nachdem das Zertifikat und der private Schlüssel entfernt wurden, werden die Storage-Nodes so konfiguriert, dass sie das Standardzertifikat und den privaten Schlüssel verwenden.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method" : "RemoveSSLCertificate",
    "params" : {},
    "id" : 3
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id" : 3,
    "result" : {}
}
```

Neu seit Version

10.0

NetworkConfig erneut verwenden

Sie können das verwenden `ResetNetworkConfig` Methode zur Behebung von Problemen bei der Netzwerkkonfiguration für einen einzelnen Knoten. Mit dieser Methode wird die Netzwerkkonfiguration eines einzelnen Knotens auf die werkseitigen Standardeinstellungen zurückgesetzt.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ResetNetworkConfig",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt keine Antwort zurück.

Neu seit Version

11.0

RücksetzenErgänzungTlsCiphers

Sie können das verwenden `ResetSupplementalTlsCiphers` Methode zur Wiederherstellung der Liste der zusätzlichen TLS-Chiffren auf der Standardvorgabe. Sie können diese Methode für den gesamten Cluster verwenden.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ResetSupplementalTlsCiphers",
  "params": {},
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {}
}
```

Neu seit Version

11.3

SetClusterStructure

Sie können das verwenden `SetClusterStructure` Methode zum Wiederherstellen der Konfigurationsinformationen des Storage-Clusters aus einem Backup. Wenn Sie die Methode aufrufen, übergeben Sie das ClusterStructure-Objekt mit den Konfigurationsinformationen, die Sie als Parameter für Params wiederherstellen möchten.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ
Param	Ein JSON-Objekt, das die aktuellen Informationen zur Storage-Cluster-Konfiguration enthält.	ClusterStructure

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Ergebnis	Asynchroner Ergebnisgriff.	Asynchron

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "SetClusterStructure",
  "params": <insert clusterStructure object here>,
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result" : {
    "asyncHandle": 1
    }
}
```

Neu seit Version

10.3

SetLldpConfig

Sie können das verwenden `SetLldpConfig` Methode zum Konfigurieren der LLDP-Einstellungen (Link Layer Discovery Protocol) für ein Storage-Cluster.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
EnableAndereProtokolle	Ermöglichen Sie die automatische Verwendung anderer Discovery-Protokolle – CDP, FDP, EDP und SONMP.	boolesch	Richtig	Nein
EnableMed	Aktivieren Sie Media Endpoint Discovery (LLDP-MED).	boolesch	Falsch	Nein
EnableLLdp	LLDP aktivieren oder deaktivieren.	boolesch	Richtig	Nein

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
LdpConfig	Informationen zur aktuellen LLDP-Speicherkonfiguration des Clusters, einschließlich neu geänderter Einstellungen.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 3920,
  "method":"SetLldpConfig",
    "params": {
        "lldpConfig": {
            "enableMed": true
        }
    }
  }
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 3920,
  "result": {
    "lldpConfig": {
        "enableLldp": true,
        "enableMed": true,
        "enableOtherProtocols": true
     }
  }
}
```

SetNtpInfo

Sie können das verwenden `SetNtpInfo` Methode zum Konfigurieren von NTP auf Cluster-Nodes. Die mit dieser Schnittstelle festgelegten Werte gelten für alle Nodes im Cluster. Wenn ein NTP-Broadcast-Server regelmäßig Zeitinformationen über Ihr Netzwerk sendet, können Sie optional Nodes als Broadcast-Clients konfigurieren.

Parameter

Stellen Sie sicher, dass Sie NTP-Server verwenden, die intern zu Ihrem Netzwerk sind, anstatt die Installationsstandards.

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Server	Liste der NTP-Server, die zu den einzelnen Knoten NTP-Konfigurationen hinzugefügt werden sollen.	String-Array	Keine	Ja.
BroadcastClient	Aktiviert jeden Node im Cluster als Broadcast-Client	boolesch	Falsch	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "SetNtpInfo",
   "params": {
     "servers"  : [
       "ntpserver1.example.org",
       "ntpserver2.example.org",
       "ntpserver3.example.org"
     ],
     "broadcastclient" : false
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id" : 1,
    "result" : {}
}
```

Neu seit Version

9.6

SetProtectionDomainLayout

Sie können das verwenden `SetProtectionDomainLayout` Methode zum Zuweisen von Nodes zu benutzerdefinierten Schutz-Domänen

Für alle aktiven Nodes im Cluster müssen Informationen bereitgestellt werden. Für inaktive Nodes können keine Informationen bereitgestellt werden. Alle Nodes in einem bestimmten Chassis müssen derselben benutzerdefinierten Schutzdomäne zugewiesen werden. Derselbe SchutzDomainType muss für alle Knoten geliefert werden. ProtektionDomainTypes, die nicht kundenspezifisch sind, wie Knoten und Gehäuse, sollten nicht enthalten sein. Wenn eine dieser Optionen zur Verfügung gestellt wird, werden die benutzerdefinierten Schutzdomänen ignoriert und ein geeigneter Fehler zurückgegeben.

Benutzerdefinierte Schutzdomänen werden in den folgenden Konfigurationen nicht unterstützt:

- Storage-Cluster mit Shared-Chassis
- Storage-Cluster mit zwei Nodes

Die Methode gibt einen Fehler aus, wenn sie in Storage-Clustern mit diesen Konfigurationen verwendet wird.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SchutzDomainLayout	Schutz-Domain-Informationen für jeden Node.	JSON-Liste von "NodeProtectionDomains" Objekte:	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SchutzDomainLayout	Liste der Nodes mit jeweils zugehörigen Sicherungsdomänen.	JSON-Liste von "NodeProtectionDomains" Objekte:

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "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"
          }
        ]
      }
    ]
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:


```
{
  "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"
            }
          ]
        }
      ]
    }
}
```

Neu seit Version

12.0

SetRemoteLoggingHosts

Sie können das verwenden `SetRemoteLoggingHosts` Methode zur Konfiguration der Remote-Protokollierung von den Knoten im Speicher-Cluster zu einem zentralen Protokollserver oder -Server. Die Remote-Protokollierung erfolgt über TCP über den Standardport 514. Diese API wird den vorhandenen Protokollierungs-Hosts nicht hinzugefügt. Stattdessen ersetzt es, was derzeit mit neuen Werten, die durch diese API-Methode angegeben sind. Verwenden Sie können `GetRemoteLoggingHosts` Um zu bestimmen, was die aktuellen Protokollierungs-Hosts sind, und verwenden Sie sie dann `SetRemoteLoggingHosts` So legen Sie die gewünschte Liste der aktuellen und neuen Protokollierungs-Hosts fest:

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Abnehmbare Hosts	Liste der Hosts, die Empfänger von Protokollnachrichten sind.	LoggingServer Array erledigen	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "id": 1,
   "method": "SetRemoteLoggingHosts",
   "params": {
     "remoteHosts": [
        {
          "host": "172.16.1.20",
          "port": 10514
        },
        {
          "host": "172.16.1.25"
        },
        {
          "host": "syslogs.lab.company.net",
          "port": 514
        }
      ]
   }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id" : 1,
    "result" : {}
}
```

Neu seit Version

9.6

Weitere Informationen

GetRemoteLoggingHosts

SetSnmpACL

Sie können das verwenden `SetSnmpACL` Methode zum Konfigurieren von SNMP-Zugriffsberechtigungen auf den Clusterknoten. Die mit dieser Schnittstelle festgelegten Werte gelten für alle Knoten im Cluster und die Werte, die übergeben werden, ersetzen alle Werte, die in einem vorherigen Aufruf festgelegt wurden `SetSnmpACL`. Beachten Sie auch, dass die mit dieser Schnittstelle eingestellten Werte alle Netzwerk- oder usmUser-Werte ersetzen, die mit dem festgelegt wurden `SetSnmpInfo` Methode.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Netzwerke	Liste der Netzwerke und welche Art von Zugriff sie auf die SNMP-Server haben, die auf den Cluster-Knoten laufen. Weitere Informationen zu möglichen Netzwerkwerten finden Sie unter SNMP-Netzwerkobjekt. Dieser Parameter ist erforderlich, wenn SNMP v3 deaktiviert ist.	Netzwerk	Keine	Nein
UsmUser	Liste der Benutzer und der Zugriffstyp für die SNMP-Server, die auf den Clusterknoten ausgeführt werden. Dieser Parameter ist erforderlich, wenn SNMP v3 aktiviert ist.	UsmUser	Keine	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "SetSnmpACL",
  "params": {
    "usmUsers"  : [
      {
         "name": "jdoe",
         "access": "rouser",
         "secLevel": "priv",
         "password": "mypassword",
         "passphrase": "mypassphrase",
      }
    ]
  },
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {}
}
```

Neu seit Version

9.6

Weitere Informationen

SetSnmpInfo

SetSnmpInfo

Sie können das verwenden `SetSnmpInfo` Methode zur Konfiguration von SNMP Version 2 und Version 3 auf Cluster-Knoten. Die mit dieser Schnittstelle festgelegten Werte gelten für alle Knoten im Cluster und die Werte, die übergeben werden, ersetzen alle Werte, die in einem vorherigen Aufruf festgelegt wurden `SetSnmpInfo`.

Parameter

> SetSnmpInfo ist für Element Version 6.0 und höher veraltet. Verwenden Sie die EnableSnmp Und SetSnmpACL Methoden.

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Netzwerke	Liste der Netzwerke und welche Art von Zugriff sie auf die SNMP-Server haben, die auf den Cluster-Knoten laufen. Siehe SNMP Netzwerk Objekt für mögliche Werte. Dieser Parameter ist nur für SNMP v2 erforderlich.	Netzwerk Array erledigen	Keine	Nein
Aktiviert	Wenn auf true gesetzt, ist SNMP auf jedem Knoten im Cluster aktiviert.	boolesch	Falsch	Nein
SnmpV3Enabled	Wenn auf „true“ gesetzt ist, ist SNMP v3 auf jedem Knoten im Cluster aktiviert.	boolesch	Falsch	Nein
UsmUser	Wenn SNMP v3 aktiviert ist, muss dieser Wert anstelle des Netzwerkparameters übergeben werden. Dieser Parameter ist nur für SNMP v3 erforderlich.	UsmUser	Keine	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel mit aktiviertem SNMP v3

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method":"SetSnmpInfo",
"params":{
    "enabled":true,
    "snmpV3Enabled":true,
    "usmUsers":[
      {
        "name":"user1",
        "access":"rouser",
        "secLevel":"auth",
        "password":"namex1",
        "passphrase":"yourpassphrase"
      }
    ]
  },
 "id":1
}
```

Anforderungsbeispiel mit aktiviertem SNMP v2

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method":"SetSnmpInfo",
"params":{
    "enabled":true,
    "snmpV3Enabled":false,
    "networks":[
      {
        "community":"public",
        "access":"ro",
        "network":"localhost",
      }
    ]
  },
  "id":1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1
  "result" :{
  }
}
```

Neu seit Version

9.6

SetSnmpTrapInfo

Sie können das verwenden `SetSnmpTrapInfo` Methode zum Aktivieren und Deaktivieren der Generierung von Cluster-SNMP-Benachrichtigungen (Traps) und zur Angabe der Host-Set, die die Benachrichtigungen empfangen. Die Werte, die Sie mit jedem überschreiten `SetSnmpTrapInfo` Methodenanruf Ersetzen Sie alle Werte, die in einem vorherigen Anruf festgelegt wurden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ
Trap-Empfänger	Liste der Hosts, die die vom Storage-Cluster erzeugten Traps empfangen sollen. Mindestens ein Objekt ist erforderlich, wenn einer der Trap-Typen aktiviert ist. Dieser Parameter ist nur erforderlich, wenn boolesche Parameter auf true gesetzt sind. (Kein Standardwert. Nicht erforderlich.)	SnmpTrapEmpfänger Array erledigen
ClusterFaultTrapsmentiert	Wenn auf „true“ gesetzt ist, wird eine entsprechende Cluster-Fehlerbenachrichtigung an die konfigurierte Liste der Trap-Empfänger gesendet, wenn ein Cluster-Fehler protokolliert wird. (Standardwert: False. Nicht erforderlich.)	boolesch

Name	Beschreibung	Typ
ClusterFaultResolvedTrapsEnabliered	Wenn auf „true“ gesetzt ist, wird eine entsprechende Benachrichtigung über Cluster-Fehler behoben an die konfigurierte Liste der Trap-Empfänger gesendet, wenn ein Clusterfehler behoben ist. (Standardwert: False. Nicht erforderlich.)	boolesch
ClusterEventTrapsmit Funktionen	Wenn auf „true“ gesetzt ist, wird bei der Protokollierung eines Clusterereignisses eine entsprechende Cluster-Ereignisbenachrichtigung an die konfigurierte Liste der Trap-Empfänger gesendet. (Standardwert: False. Nicht erforderlich.)	boolesch

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method":"SetSnmpTrapInfo",
"params":{
    "clusterFaultTrapsEnabled":true,
    "clusterFaultResolvedTrapsEnabled":true,
    "clusterEventTrapsEnabled":true,
    "trapRecipients":[
    {
      "host":"192.30.0.10",
      "port":162,
      "community":"public"
    }
   ]
  },
  "id":1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id" : 1,
    "result" : {}
}
```

Neu seit Version

9.6

SetSSLZertifikat

Sie können das verwenden `SetSSLCertificate` Methode zum Festlegen eines Benutzer-SSL-Zertifikats und eines privaten Schlüssels für die Storage-Nodes im Cluster.

Nach Verwendung der API müssen Sie den Management-Node neu booten.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Zertifikat	Die PEM-kodierte Textversion des Zertifikats. **Hinweis:** beim Festlegen eines Node- oder Cluster-Zertifikats muss das Zertifikat die Erweiterung ExtendedKeyUsage für serverAuth enthalten. Mit dieser Erweiterung kann das Zertifikat ohne Fehler auf gängigen Betriebssystemen und Browsern verwendet werden. Wenn die Erweiterung nicht vorhanden ist, weist die API das Zertifikat als ungültig zurück.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
PrivateKey	Die PEM-codierte Textversion des privaten Schlüssels.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method" : "SetSSLCertificate",
    "params" : {
        "privateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEA8U+28fnLKQNWEWMR6akeDKuehSpS79odLGigI18qlCV/AUY5\nZLjqsT
jBvTJVRv44yoCTgNrx36U7FHP4t6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7Je\nlOB6AD7fmiTweP
20HRYpZvY+Uz7LYEFCmrgpGZQF3iOSIcBHtLKE5186JVT6j5dg\n6yjUGQO352ylc9HXHcn6lb
/jyl0DmVNUZ0caQwAmIS3Jmoyx+zj/Ya4WKq+2SqTA\nX7bX0F3wHHfXnZlHnM8fET5N/9A+K6
lS7dg9cyXu4afXcgKy14JiNBvqbBjhgJtE\n76yAy6rTHu0xM3jjdkcb9Y8miNzxF+ACq+itaw
IDAQABAoIBAH1jlIZr6/sltqVW\nO0qVC/49dyNu+KWVSq92ti9rFe7hBPueh9gklh78hP9Qli
tLkir3YK4GFsTFUMux\n7z1NRCxA/4LrmLSkAjW2kRXDfVl2bwZq0ua9NefGw92O8D2OZvbuOx
k7Put2p6se\nfgNzSjf2SI5DIX3UMe5dDN5FByu52CJ9mI4U16ngbWln2wc4nsxJg0aAEkzB7w
nq\nt+Am5/Vu1LI6rGiG6oHEW0oGSuHl1esIyXXa2hqkU+1+iF2iGRMTiXac4C8d11NU\nWGIR
CXFJAmsAQ+hQm7pmtsKdEqumj/PIoGXf0BoFVEWaIJIMEgnfuLZp8IelJQXn\nSFJbk2ECgYEA
+d5ooU4thZXylWHUZqomaxyzOruA1T53UeH69HiFTrLjvfwuaiqj\nlHzPlhms6hxexwz1dzAp
gog/NOM+2bAc0rn0dqvtV4doejtlDZKRqrNCf/cuN2QX\njaCJClCWau3sEHCckLOhWeY4HaPS
oWq0GKLmKkKDChB4nWUYg3gSWQkCgYEA9zuN\nHW8GPS+yjixeKXmkKO0x/vvxzR+J5HH5znaI
Hss48THyhzXpLr+v30Hy2h0yAlBS\nny5Ja6wsomb0mVe4NxVtVawg2E9vVvTa1UC+TNmFBBuL
RPfjcnjDerrSuQ5lYY+M\nC9MJtXGfhp//G0bzwsRzZxOBsUJb15tppaZIs9MCgYAJricpkKjM
0xlZ1jdvXsos\nPilnbho4qLngrzuUuxKXEPEnzBxUOqCpwQgdzZLYYw788TCVVIVXLEYem2s0
7dDA\nDTo+WrzQNkvC6IgqtXH1RgqegIoG1VbgQsbsYmDhdaQ+os4+AOeQXw3vgAhJ/qNJ\njQ
4Ttw3ylt7FYkRH26ACWQKBgQC74Zmf4JuRLAo5WSZFxpcmMvtnlvdutqUH4kXA\nzPssy6t+QE
La1fFbAXkZ5Pg1ITK752aiaX6KQNG6qRsA3VS1J6drD9/2AofOQU17\n+jOkGzmmoXf49Zj3iS
akwg0ZbQNGXNxEsCAUr0BYAobPp9/fB4PbtUs99fvtocFr\njS562QKBgCb+JMDP5q7jpUuspj
0obd/ZS+MsomE+gFAMBJ71KFQ7KuoNezNFO+ZE\n3rnR8AqAm4VMzqRahs2PWNe2Hl4J4hKu96
qNpNHbsW1NjXdAL9P7oqQIrhGLVdhX\nInDXvTgXMdMoet4BKnftelrXFKHgGqXJoczq4JWzGS
IHNgvkrH60\n-----END RSA PRIVATE KEY-----\n",
        "certificate": "-----BEGIN CERTIFICATE-----
\nMIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSIb3DQEBBQUAMIGDMQswCQYD\nVQQGEw
JVUzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\nA1UEChMYV2hhdC
BIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBFh53\naGF0aGFwcGVuc0B2ZWdhc3
N0YXlzaW4udmVnYXMwHhcNMTcwMzA4MjI1MDI2WhcN\nMjcwMzA2MjI1MDI2WjCBgzELMAkGA1
UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYD\nVQQHFAxWZWdhcywgQmFieSExITAfBgNVBAoTGF
```

```
doYXQgSGFwcGVucyBpbiBWZWdh\ncy4uLjEtMCsGCSqGSIb3DQEJARYed2hhdGhhcHBlbnNAdm
VnYXNzdGF5c2luLnZl\nZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f
nLKQNWEWMR\n6akeDKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH
P4\nt6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nmrgp
GZQF3iOSIcBHtLKE5186JVT6j5dg6yjUGQO352ylc9HXHcn6lb/jyl0DmVNU\nZ0caQwAmIS3J
moyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K6lS\n7dg9cyXu4afXcgKy14Ji
NBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzxF+AC\nq+itawIDAQABo4HrMIHoMB0GA1Ud
DgQWBBRvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYDVQQHFAxW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbiBWZWdhcy4uLjEtMCsGCSqG
SIb3DQEJARYe\nd2hhdGhhcHBlbnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjjf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s71mQPECwVLfiE/ndtIbnpe\nMq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7JyfS37l4rRolFpX6N\niebEgAaE5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dHOlQ+WYnoO/eIMy0coT26JBl5H\nDEwvdl+DwkxnS1cx1v
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAjJDg
l0QoQDWNDoTeRBsz80nwiouA==\n-----END CERTIFICATE-----\n"
    },
    "id" : 2
}
```


Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:


```
{
    "id" : 2,
    "result" : {}
}
```


Neu seit Version

10.0

SnmpSendTestTraps

`SnmpSendTestTraps` Ermöglicht Ihnen, SNMP-Funktionen für ein Cluster zu testen. Diese Methode weist das Cluster an, Test-SNMP-Traps an den derzeit konfigurierten SNMP-Manager zu senden.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Status	Der Status des Tests.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "SnmpSendTestTraps",
    "params": {},
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {
      "status": "complete"
   }
}
```

Neu seit Version

9.6

TestAddressAvailability

Sie können das verwenden `TestAddressAvailability` Methode, um zu überprüfen, ob eine bestimmte IP-Adresse auf einer Schnittstelle innerhalb des Storage-Clusters verwendet wird.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Schnittstelle	Die Ziel-Netzwerkschnittstelle (z. B. eth0, Bond10G usw.).	Zeichenfolge	Keine	Ja.
Adresse	Die IP-Adresse, nach der auf der Zielschnittstelle gescannt werden soll.	Zeichenfolge	Keine	Ja.
VirtualNetworkTag	Die Ziel-VLAN-ID.	Ganzzahl	Keine	Nein
Zeitüberschreitung	Die Zeitüberschreitung in Sekunden zum Testen der Zieladresse.	Ganzzahl	5	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Adresse	Die getestete IP-Adresse.	Zeichenfolge
Verfügbar	True, wenn die angeforderte IP-Adresse verwendet wird, und false, wenn nicht.	boolesch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "TestAddressAvailability",
    "params": {
        "interface": "Bond10G",
        "address": "10.0.0.1",
        "virtualNetworkTag": 1234
    }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "address":"10.0.0.1",
        "available": true
    }
}
```

Neu seit Version

11.0

Mandantenfähige Netzwerk-API-Methoden

Namenskonventionen für virtuelle Netzwerke

NetApp Element Storage-Systeme nutzen monotonen steigende Zahlen als eindeutige Identifikatoren für alle Objekte im System.

Wenn Sie ein neues Volume erstellen, erhöht sich die neue VolumeID exakt 1. Diese Konvention gilt für virtuelle Netzwerke in Storage Clustern, auf denen Element Software ausgeführt wird. Das erste virtuelle Netzwerk, das Sie in einem Element Cluster erstellen, hat eine VirtualNetworkID von 1. Diese ID entspricht nicht der VLAN-Tag-Nummer.

Sie können die VirtualNetworkID und das VirtualNetworkTag (VLAN Tag) in den API-Methoden austauschbar verwenden.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

AddVirtualNetwork

Sie können das verwenden `AddVirtualNetwork` Methode zum Hinzufügen eines neuen virtuellen Netzwerks zu einer Cluster-Konfiguration.

Wenn Sie ein virtuelles Netzwerk hinzufügen, wird für jeden Node eine Schnittstelle erstellt und jede Schnittstelle benötigt eine virtuelle Netzwerk-IP-Adresse. Die Anzahl der IP-Adressen, die Sie als Parameter für diese API-Methode angeben, muss der Anzahl der Nodes im Cluster entsprechen oder größer sein. Die Masse des Systems stellt virtuelle Netzwerkadressen bereit und weist sie den einzelnen Knoten automatisch zu. Sie müssen Knoten keine virtuellen Netzwerkadressen manuell zuweisen.

Die AddVirtualNetwork-Methode wird nur verwendet, um ein neues virtuelles Netzwerk zu erstellen. Wenn Sie Änderungen an einem vorhandenen virtuellen Netzwerk vornehmen möchten, verwenden Sie den ModifyVirtualNetwork Methode.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
AdressenSperren	Eindeutiger Bereich von IP-Adressen, die in das virtuelle Netzwerk einbezogen werden sollen. Erforderliche Mitglieder für das Objekt: • Start: Der Beginn des IP-Adressbereichs. (Zeichenfolge) • Größe: Die Anzahl der IP-Adressen, die in den Block einbezogen werden sollen. (Ganze Zahl)	JSON-Objekt-Array	Keine	Ja.
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
Gateway	Die IP-Adresse eines Gateways des virtuellen Netzwerks. Dieser Parameter ist nur gültig, wenn der Namespace-Parameter auf „true“ gesetzt ist.	Zeichenfolge	Keine	Nein
Name	Ein benutzerdefinierter Name für das neue virtuelle Netzwerk.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Namespace	Wenn diese Einstellung auf „true“ gesetzt ist, wird die Funktion für routingfähige Speicher-VLANs aktiviert, indem ein Namespace und das darin enthaltene virtuelle Netzwerk erstellt und konfiguriert werden.	boolesch	Keine	Nein
Netzmaske	Eindeutige Netzwerkmaske für das zu erstellenden virtuelle Netzwerk.	Zeichenfolge	Keine	Ja.
svip	Eindeutige Speicher-IP-Adresse für das zu erstellenden virtuelle Netzwerk.	Zeichenfolge	Keine	Ja.
VirtualNetworkTag	Ein eindeutiges VLAN-Tag (Virtual Network). Unterstützte Werte sind 1 bis 4094.	Ganzzahl	Keine	Ja.

Hinweis: Virtuelle Netzwerkparameter müssen für jedes virtuelle Netzwerk eindeutig sein, wenn Sie Namespace auf false setzen.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VirtualNetworkID	Die virtuelle Netzwerk-ID des neuen virtuellen Netzwerks.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "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
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {
        "virtualNetworkID": 5
   }
}
```

Neu seit Version

9.6

ModifyVirtualNetwork

Sie können das verwenden `ModifyVirtualNetwork` Methode zum Ändern der Attribute eines vorhandenen virtuellen Netzwerks.

Mit dieser Methode können Sie Adressblöcke hinzufügen oder entfernen, die Netmask ändern oder den Namen oder die Beschreibung des virtuellen Netzwerks ändern. Sie können damit auch Namespaces aktivieren oder deaktivieren sowie ein Gateway hinzufügen oder entfernen, wenn Namespaces auf dem virtuellen Netzwerk aktiviert sind.

Diese Methode erfordert entweder die VirtualNetworkID oder die virtualNetworkTag als Parameter, aber nicht beides.

ACHTUNG:

Durch das Aktivieren oder Deaktivieren der Routingfähige Speicher-VLANs-Funktion für ein vorhandenes virtuelles Netzwerk wird der vom virtuellen Netzwerk abgeführte Datenverkehr durch Änderung des Namespace-Parameters unterbrochen. Am besten, wenn Sie den Namespace-Parameter während eines geplanten Wartungsfensters ändern.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VirtualNetworkID	Eindeutige Kennung des zu ändernden virtuellen Netzwerks Dies ist die vom Cluster zugewiesene virtuelle Netzwerk-ID.	Ganzzahl	Keine	Nein
VirtualNetworkTag	Das Netzwerk-Tag, das das zu ändernde virtuelle Netzwerk identifiziert.	Ganzzahl	Keine	Nein

AdressenSperren	Der neue Adressblock, den für dieses virtuelle Netzwerk festgelegt werden soll. Dies kann neue Adressblöcke umfassen, die dem vorhandenen Objekt hinzugefügt werden müssen oder ungenutzte Adressblöcke weglassen, die entfernt werden müssen. Alternativ können Sie die Größe vorhandener Adressblöcke erweitern oder verkleinern. Sie können nur die Größe der StartadressenSperren für ein virtuelles Netzwerkobjekt erhöhen; Sie können es nie verkleinern. Erforderliche Mitglieder für dieses Objekt: • Start: Der Beginn des IP-Adressbereichs. (Zeichenfolge) • Größe: Die Anzahl der IP-Adressen, die in den Block einbezogen werden sollen. (Ganze Zahl)	JSON-Objekt	Keine	Nein
Gateway	Die IP-Adresse eines Gateways des virtuellen Netzwerks. Dieser Parameter ist nur gültig, wenn der Namespace-Parameter auf „true“ gesetzt ist.	Zeichenfolge	Keine	Nein

Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
Name	Der neue Name für das virtuelle Netzwerk.	Zeichenfolge	Keine	Nein
Namespace	Wenn auf „true“ gesetzt ist, wird die Funktion für routingfähige Speicher-VLANs aktiviert, indem das virtuelle Netzwerk neu erstellt und ein Namespace konfiguriert wird, der darin enthalten ist. Wenn Sie auf false setzen, deaktiviert die VRF-Funktion für das virtuelle Netzwerk. Durch die Änderung dieses Werts wird der Datenverkehr in diesem virtuellen Netzwerk unterbrochen.	boolesch	Keine	Nein
Netzmaske	Neue Netzwerkmaske für dieses virtuelle Netzwerk.	Zeichenfolge	Keine	Nein
svip	Die virtuelle Speicher-IP-Adresse für dieses virtuelle Netzwerk. Der SVIP für ein virtuelles Netzwerk kann nicht geändert werden. Sie müssen ein neues virtuelles Netzwerk erstellen, um eine andere SVIP-Adresse verwenden zu können.	Zeichenfolge	Keine	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "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
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
  }
}
```

Neu seit Version

9.6

ListVirtualNetworks

Sie können das verwenden `ListVirtualNetworks` Methode zum Auflisten aller konfigurierten virtuellen Netzwerke für das Cluster.

Mit dieser Methode können Sie die virtuellen Netzwerkeinstellungen im Cluster überprüfen. Für diese Methode sind keine erforderlichen Parameter vorhanden. Um die Ergebnisse zu filtern, können Sie einen oder mehrere VirtualNetworkID- oder VirtualNetworkTag-Werte weitergeben.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VirtualNetworkID	Netzwerk-ID zum Filtern der Liste nach einem einzelnen virtuellen Netzwerk.	Ganzzahl	Keine	Nein
VirtualNetworkTag	Netzwerk-Tag zum Filtern der Liste nach einem einzelnen virtuellen Netzwerk.	Ganzzahl	Keine	Nein
VirtualNetworkIDs	Netzwerk-IDs, die in die Liste aufgenommen werden sollen.	Integer-Array	Keine	Nein
VirtualNetworkTags	Netzwerk-Tag, das in die Liste aufgenommen werden soll.	Integer-Array	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VirtualNetworks	Objekt, das virtuelle Netzwerk-IP-Adressen enthält.	VirtualNetwork

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListVirtualNetworks",
  "params": {
     "virtualNetworkIDs": [5,6]
   },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
     },
    {
   }
  ]
}
```


Neu seit Version

9.6

RemoveVirtualNetwork

Sie können das verwenden `RemoveVirtualNetwork` Methode zum Entfernen eines zuvor hinzugefügten virtuellen Netzwerks.

> Diese Methode erfordert entweder die VirtualNetworkID oder die virtualNetworkTag als Parameter, aber nicht beides.

> Sie können ein virtuelles Netzwerk nicht entfernen, wenn ihm Initiatoren zugeordnet sind. Heben Sie die Zuordnung der Initiatoren zunächst auf, und entfernen Sie dann das virtuelle Netzwerk.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VirtualNetworkID	Netzwerk-ID, die das zu entfernende virtuelle Netzwerk identifiziert.	Ganzzahl	Keine	Ja.
VirtualNetworkTag	Netzwerk-Tag, das das zu entfernende virtuelle Netzwerk identifiziert.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "RemoveVirtualNetwork",
  "params": {
     "virtualNetworkID": 5
    }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {}
}
```

Neu seit Version

9.6

Volume-API-Methoden

CancelClone

Sie können das verwenden `CancelClone` Methode zum Anhalten eines laufenden Volume-Klons oder von Volume-Kopien Wenn Sie einen Gruppenklonvorgang abbrechen,

wird das System abgeschlossen und der damit verbundene Async Handle entfernt.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
KlonID	Die KlonID für den laufenden Klonprozess.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "CancelClone",
   "params": {
      "cloneID" : 5,
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {}
}
```

Neu seit Version

9.6

GruppenClone abbrechen

Sie können das verwenden `CancelGroupClone` Methode zum Beenden eines laufenden Klonprozesses, der in einer Gruppe von Volumes stattfindet. Wenn Sie einen Gruppenklonvorgang abbrechen, wird das System abgeschlossen und der damit verbundene Async Handle entfernt.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
GroupCloneID	Die KlonID für den laufenden Klonprozess.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "CancelGroupClone",
   "params": {
      "cloneID" : 5,
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result" : {}
}
```

Neu seit Version

9.6

CloneMultipleVolumes

Sie können das verwenden `CloneMultipleVolumes` Methode zum Erstellen eines Klons einer Gruppe von angegebenen Volumes Beim gemeinsamen Klonen können Sie einer Gruppe von mehreren Volumes einen konsistenten Satz von Merkmalen zuweisen.

Bevor Sie den Parameter groupSnapshotID zum Klonen der Volumes in einem Gruppen-Snapshot verwenden, müssen Sie zuerst den Gruppen-Snapshot mit dem erstellen CreateGroupSnapshot API-Methode oder die

Web-UI. Die Verwendung von GroupSnapshotID ist beim Klonen mehrerer Volumes optional.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Datenzugriff	Neue Standardzugriffsmethode für die neuen Volumes, wenn die Informationen, die im Array des Volumes übergeben wurden, nicht überschrieben werden.	Zeichenfolge	Keine	Nein
AbleSnapMirrorReplication	Legt fest, ob das Volume für die Replizierung mit SnapMirror Endpunkten verwendet werden kann. Mögliche Werte: • Richtig • Falsch	boolesch	Falsch	Nein
GruppenSnapshotID	Die ID des als Grundlage für den Klon zu verwendenden Gruppen-Snapshots.	Ganzzahl	Keine	Nein
NewAccountID	Neue Konto-ID für die Volumes, wenn die im Volume-Array übergebenen Informationen nicht überschrieben werden.	Ganzzahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Volumes	Sammlung von Mitgliedern, die Sie für die neuen Volumes festlegen. Mitglieder: • VolumeID: (Erforderlich) • Zugriff: (Optional) kann einer von ReadOnly, ReadWrite, Locked oder ReplikationTarget sein. • Attribute: (Optional) Liste von Name-Wert-Paaren im JSON-Objektformat. • Name: (Optional) Neuer Name für den Klon. • NewAccountID: (Optional) Account ID für die neuen Volumen. • NewSize: (Optional) Gesamtgröße des Volumens in Bytes. Die Größe wird auf den nächsten Megabyte gerundet. Wenn optionale Mitglieder nicht angegeben werden, werden die Werte von den Quell-Volumes übernommen.	JSON-Objekt-Array	Keine	Ja (VolumeID)

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Asynchron	Ein Wert, der von einem Anruf mit asynchroner Methode zurückgegeben wird.	Ganzzahl
GroupCloneID	Eindeutige ID des neuen Gruppenklon.	Ganzzahl
Mitglieder	Liste der VolumeIDs der Quell- und Ziel-Volume-Paare	JSON-Objekt-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "CloneMultipleVolumes",
   "params": {
       "volumes": [
           {
              "volumeID": 5
              "name":"foxhill",
              "access":"readOnly"
              },
           {
              "volumeID": 18
              },
           {
             "volumeID": 20
              }
     ]
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
    "asyncHandle": 12,
    "groupCloneID": 4,
    "members": [
     {
      "srcVolumeID": 5,
      "volumeID": 29
     },
     {
      "srcVolumeID": 18,
      "volumeID": 30
     },
     {
      "srcVolumeID": 20,
      "volumeID": 31
      }
    ]
  }
}
```


Neu seit Version

9.6

KlonVolume

Sie können das verwenden `CloneVolume` Methode zum Erstellen einer Kopie eines Volumes. Diese Methode ist asynchron und nimmt möglicherweise eine variable Zeit in Anspruch.

Der Klonprozess beginnt sofort, wenn Sie den erstellen `CloneVolume` Die Anforderung und steht stellvertretend für den Status des Volume, wenn die API-Methode ausgegeben wird. Sie können das verwenden GetAsyncResult Methode zur Bestimmung des Klonprozesses, und das neue Volume ist für Verbindungen verfügbar. Verwenden Sie können ListSyncJobs Um den Status des ErErstellen des Klons anzuzeigen. Die anfänglichen Attribute und die Quality of Service-Einstellungen für das Volume werden vom zu klonenden Volume übernommen. Mit können Sie diese Einstellungen ändern UmfyVolume.

> Geklonte Volumes übernehmen keine Zugriffsgruppenmitgliedschaft für Volumes vom Quell-Volume.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Datenzugriff	Zugriff für das neue Volume zulässig. Wenn kein Wert angegeben wird, ändert sich der Zugriffswert nicht. Mögliche Werte: • `readOnly`: (Optional) nur Leseoperationen sind erlaubt. • `readWrite`: (Optional) Lesen und Schreiben sind erlaubt. • `locked`: (Optional) Es sind keine Lese- oder Schreibvorgänge zulässig. Wenn nicht angegeben, wird der Zugriffswert des zu klonenden Volume verwendet. • `replicationTarget`: (Optional) Identifizieren Sie ein Volumen als Zielvolumen für eine paarweise Gruppe von Volumen. Wenn das Volume nicht gekoppelt ist, ist der Zugriffsstatus gesperrt.	Zeichenfolge	Keine	Nein
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Able512e	Gibt an, ob das neue Volume 512-Byte Sektoremulation verwenden soll. Wenn nicht angegeben, wird die Einstellung des zu klonenden Volumes verwendet.	boolesch	Einstellung der ursprünglichen Lautstärke	Nein
AbleSnapMirrorReplication	Legt fest, ob das Volume für die Replizierung mit SnapMirror Endpunkten verwendet werden kann. Mögliche Werte: • Richtig • Falsch	boolesch	Falsch	Nein
Name	Der Name des neuen geklonten Volume muss 1 bis 64 Zeichen lang sein.	Zeichenfolge	Keine	Ja.
NewAccountID	AccountID für den Besitzer des neuen Volumens. Wenn nicht angegeben, wird die AccountID des Inhabers des zu klonenden Volumes verwendet.	Ganzzahl	AccountID des Inhabers des ursprünglichen Volumens	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
NewSize	Neue Größe des Volumes, in Byte. Ist möglicherweise größer oder kleiner als die Größe des zu klonenden Volumes. Wenn diese Angabe nicht erfolgt, wird die Volume-Größe nicht geändert. Größe wird auf die nächste 1MB in Größe gerundet.	Ganzzahl	Keine	Nein
Snapshot-ID	ID des Snapshots, der als Quelle des Klons verwendet wird. Wenn keine ID angegeben wird, wird das aktuelle aktive Volume verwendet.	Ganzzahl	Keine	Nein
VolumeID	VolumeID für das zu klonendes Volume.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Asynchron	Der Handle-Wert, der zum Abrufen des Operationsergebnisses verwendet wird.	Ganzzahl
KlonID	Die KlonID für das neu geklonte Volume.	Ganzzahl
Kurve	Die QoS-Kurvenwerte, die auf den Klon angewendet werden.	JSON-Objekt
Datenmenge	Ein Objekt, das Informationen über das neu geklonte Volume enthält.	Datenmenge
VolumeID	VolumeID für das neu geklonte Volume.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "CloneVolume",
   "params": {
      "volumeID" : 5,
      "name"  : "mysqldata-snapshot1",
      "access" : "readOnly"
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
    }
}
```


Neu seit Version

9.6

Weitere Informationen

- GetAsyncResult
- ListSyncJobs
- UmfyVolume

CopyVolume

Sie können das verwenden `CopyVolume` Methode zum Überschreiben des Dateninhalts eines vorhandenen Volumes mit dem Dateninhalt eines anderen Volumes (oder Snapshots). Attribute des Ziel-Volume wie IQN, QoS-Einstellungen, Größe, Konto und Mitgliedschaft für Volume-Zugriffsgruppen werden nicht geändert. Das Ziel-Volume muss bereits vorhanden sein und dieselbe Größe aufweisen wie das Quell-Volume.

Es ist am besten, wenn Clients das Ziel-Volume unmounten, bevor der Vorgang beginnt. Wenn das Zielvolume während des Vorgangs geändert wird, gehen die Änderungen verloren. Dieser Vorgang kann eine variable Zeit in Anspruch nehmen. Sie können das verwenden GetAsyncResult Methode, um zu bestimmen, wann der Prozess abgeschlossen ist, und ListSyncJobs Um den Fortschritt der Kopie anzuzeigen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
DstVolumeID	VolumeID des zu überschreibenden Volumes.	Ganzzahl	Keine	Ja.
VolumeID	VolumeID des Volumes, aus dem gelesen werden soll.	Ganzzahl	Keine	Ja.
Snapshot-ID	ID des Snapshots, der als Quelle des Klons verwendet wird. Wenn keine ID angegeben wird, wird das aktuelle aktive Volume verwendet.	Ganzzahl	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Asynchron	Handle-Wert, der zum Abrufen des Operationsergebnisses verwendet wird.	Ganzzahl
KlonID	KlonID für das neu geklonte Volume	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "CopyVolume",
   "params": {
      "volumeID" : 3,
      "dstVolumeID" : 2
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
    "asyncHandle": 9,
    "cloneID": 5
  }
}
```

Neu seit Version

9.6

Weitere Informationen

- GetAsyncResult
- ListSyncJobs

CreateQoSPolicy

Sie können das verwenden `CreateQoSPolicy` Methode zum Erstellen eines QoSPolicy-Objekts, das Sie bei der Erstellung oder Änderung später auf ein Volume anwenden können. Eine QoS-Richtlinie besitzt eine eindeutige ID, einen Namen und QoS-Einstellungen.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Name	Der Name der QoS-Richtlinie, z. B. Gold, Platin oder Silber.	Zeichenfolge	Keine	Ja.
qos	Die QoS-Einstellungen, für die diese Richtlinie gilt.	QoS	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ

QosPolicy	Das neu erstellte QoSPolicy-Objekt.	QoSPolicy

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 68,
  "method": "CreateQoSPolicy",
  "params": {
    "name": "bronze",
    "qos": {
      "minIOPS": 50,
      "maxIOPS": 15000,
      "burstIOPS": 15000
    }
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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": []
    }
  }
}
```


Neu seit Version

10.0

CreateVolume

Sie können das verwenden `CreateVolume` Methode zum Erstellen eines neuen, leeren Volumes im Cluster Sobald das Volume erstellt wurde, ist das Volume für die Verbindung über iSCSI verfügbar.

Volumes, die ohne festgelegte QoS-Werte erstellt wurden, verwenden die Standardwerte. Sie können die Standardwerte für ein Volume mithilfe der anzeigen `GetDefaultQoS` Methode.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`access`	Zugriffsmodus für die Lautstärke. Wenn dieser Parameter enthalten ist, wird nur der unterstützte Wert unterstützt `snapMirrorTarget`.	Zeichenfolge	Keine	Nein
`accountID`	Die ID des Kontos, zu dem dieses Volume gehört.	Ganzzahl	Keine	Ja.
`associateWithQoSPolicy`	Verknüpfen Sie das Volume mit der angegebenen QoS-Richtlinie. Mögliche Werte: • `true`: Verknüpfen Sie das Volumen mit der QoS-Richtlinie, die im Parameter QoSPolicyID angegeben ist. • `false`: Verknüpfen Sie das Volume nicht mit der QoS-Richtlinie, die im Parameter QoSPolicyID angegeben ist. Wenn „false“, wird eine vorhandene Richtlinienzuordnung entfernt, unabhängig davon, ob Sie im Parameter QoSPolicy eine QoS-Richtlinie angeben.	boolesch	Richtig	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`attributes`	Liste von Name-Wert-Paaren im JSON-Objektformat. Die Gesamtgröße des Attributs muss kleiner als 1000 B oder 1 KB sein, einschließlich JSON-Formatierungszeichen.	JSON-Objekt	Keine	Nein
`dontMoveforIopsRebalance`	Verhindern Sie beim Lastausgleich mit den tatsächlichen IOPS, dass ein Volume verschoben wird. Diese Einstellung ist ab Element 12.8 verfügbar und nur wirksam, wenn "VolumeLoadBalanceOnActualIOPS"aktiviert ist. Mögliche Werte: • `true`: Volumen lädt nicht auf der Grundlage der tatsächlichen IOPS. • `false`: Volumen macht Lastenausgleich basierend auf tatsächlichen IOPS. **Hinweis**: Der Ausgleich für Hochverfügbarkeit (Node-Ausfall) hat Vorrang vor `VolumeLoadBalanceOnActualIOPS` und `dontMoveforIopsRebalance`.	boolesch	Falsch	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`enable512e`	Aktivieren Sie die 512-Byte-Sektoremulation. Mögliche Werte: • `true`: Das Volumen bietet 512-Byte-Sektor-Emulation. • `false`: 512e Emulation ist nicht aktiviert.	boolesch	Keine	Ja.
`enableSnapMirrorReplication`	Legt fest, ob das Volume für die Replizierung mit SnapMirror Endpunkten verwendet werden kann. Mögliche Werte: • `true` • `false`	boolesch	Falsch	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`fifoSize`	Gibt die maximale Anzahl von FIFO-Snapshots an, die vom Volume unterstützt werden. Beachten Sie, dass FIFO- und nicht-FIFO-Snapshots beide denselben Pool verfügbarer Snapshot-Steckplätze auf einem Volume nutzen. Verwenden Sie diese Option, um den FIFO-Snapshot-Verbrauch der verfügbaren Snapshot-Steckplätze zu begrenzen. Wenn keine Angabe erfolgt, wird der Wert standardmäßig auf 24 gesetzt.	Ganzzahl	24	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`minFifoSize`	Gibt die Mindestanzahl an FIFO-Snapshot-Steckplätzen an, die vom Volume reserviert wurden. Dies garantiert, dass, wenn Sie beide FIFO-Schnappschüsse und nicht-FIFO-Schnappschüsse auf einem Volumen verwenden, dass die nicht-FIFO-Schnappschüsse nicht unbeabsichtigt zu viele FIFO-Steckplätze verbrauchen. Es sorgt auch dafür, dass zumindest diese viele FIFO-Schnappschüsse immer verfügbar sind. Da FIFO- und nicht-FIFO-Snapshots sich den gleichen Pool teilen, wird der `minFifoSize` Reduziert die Gesamtzahl der möglichen Non-FIFO-Snapshots um die gleiche Menge. Wenn keine Angabe erfolgt, wird der Wert standardmäßig auf 0 gesetzt.	Ganzzahl	0	Nein
`name`	Name der Zugriffsgruppe des Volumes (kann vom Benutzer angegeben werden). Nicht unbedingt eindeutig, aber empfohlen. Muss 1 bis 64 Zeichen lang sein.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
`qos`	Die anfängliche Quality of Service-Einstellungen für dieses Volume Standardwerte werden verwendet, wenn keine angegeben werden. Mögliche Werte: • `minIOPS` • `maxIOPS` • `burstIOPS`	QoS-Objekt	Keine	Nein
`qosPolicyID`	Die ID für die Richtlinie, deren QoS-Einstellungen auf die angegebenen Volumes angewendet werden sollten. Dieser Parameter schließen sich gegenseitig mit dem aus `qos` Parameter.	Ganzzahl	Keine	Nein
`totalSize`	Gesamtgröße des Volumes in Byte. Die Größe wird auf den nächsten Megabyte gerundet.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Datenmenge	Objekt mit Informationen zum neu erstellten Volume	Datenmenge
VolumeID	Die Volume-ID für das neu erstellte Volume.	Ganzzahl

Name	Beschreibung	Typ
Kurve	Die Kurve ist ein Satz von Schlüsselwert-Paaren. Die Schlüssel sind die E/A-Größe in Byte. Die Werte stellen die Kosten für die Performance eines IOP bei einer bestimmten I/O-Größe dar. Die Kurve wird relativ zu einem 4096-Byte-Vorgang berechnet, der auf 100 IOPS eingestellt ist.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "CreateVolume",
   "params": {
      "name": "testit",
      "accountID": 22,
      "dontMoveForIopsRebalance": true,
      "totalSize": 100000000000,
      "enable512e": false,
      "attributes": {},
      "qos": {
         "minIOPS": 500,
         "maxIOPS": 27000,
         "burstIOPS": 27000,
         "burstTime": 60
      }
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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": "6f47acc100000000336565750000140",
```

```
            "sliceCount": 0,
            "status": "active",
            "totalSize": 1000000716800,
            "virtualVolumeID": null,
            "volumeAccessGroups": [],
            "volumeConsistencyGroupUUID": "8ed68e57-13ee-47df-8381-
29b125142718",
            "volumeID": 320,
            "volumePairs": [],
            "volumeUUID": "e0e2c938-4ecd-4de9-a1be-f6b17c93ce5d"
        },
        "volumeID": 320
    }
}
```


Neu seit Version

9.6

Weitere Informationen

GetDefaultQoS

CreateBackupTarget

Verwenden Sie können `CreateBackupTarget` So erstellen und speichern Sie Backup-Zielinformationen, damit Sie sie nicht jedes Mal, wenn ein Backup erstellt wird, erneut eingeben müssen.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Name	Name für das Backup-Ziel.	Zeichenfolge	Keine	Ja.
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Ja (kann aber leer sein)

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ

BackupTargetID	Eindeutige Kennung, die dem neuen Backupziel zugewiesen ist.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "CreateBackupTarget",
   "params": {
      "name": "mytargetbackup"
   },
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {
      "backupTargetID": 1
   }
}
```

Neu seit Version

9.6

DeleteQoSPolicy

Sie können das verwenden `DeleteQoSPolicy` Methode zum Löschen einer QoS-Richtlinie aus dem System. Die QoS-Einstellungen für alle mit dieser Richtlinie erstellten oder geänderten Volumes sind unbeeinträchtigt.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
QosPolicyID	Die ID der zu löschenden QoS-Richtlinie	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 663,
  "method": "DeleteQoSPolicy",
  "params": {
    "qosPolicyID": 4
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 663,
  "result": {}
}
```

Neu seit Version

9.6

DeleteVolume

Sie können das verwenden `DeleteVolume` Methode zum Markieren eines aktiven Volumes zum Löschen. Wenn diese Markierung markiert ist, wird das Volumen nach Ablauf des Reinigungsintervalls gelöscht (dauerhaft gelöscht).

Nachdem Sie eine Anfrage zum Löschen eines Volume gestellt haben, werden alle aktiven iSCSI-Verbindungen zum Volume sofort beendet. Während sich das Volume in diesem Zustand befindet, sind keine weiteren Verbindungen zulässig. Ein markiertes Volume wird in Zielermittlungsanfragen nicht zurückgegeben.

Snapshots eines Volumes, die zum Löschen markiert wurden, sind nicht betroffen. Snapshots werden so lange aufbewahrt, bis das Volume aus dem System entfernt wird. Wenn ein Volume zum Löschen markiert ist und gerade ein Lese- oder Schreibvorgang für das Massenvolumen ausgeführt wird, wird der Lese- oder Schreibvorgang für das Massenvolumen angehalten.

Wenn das gelöschte Volume mit einem Volume gekoppelt ist, wird die Replizierung zwischen den gepaarten Volumes ausgesetzt und es werden keine Daten an dieses Volume oder daraus übertragen, während sie sich im gelöschten Zustand befinden. Das entfernte Volume, mit dem das gelöschte Volume gekoppelt wurde, wechselt in einen Status „PausedUnkonfiguriert“ und Daten werden nicht mehr an das gelöschte Volume oder

an das gelöschte Volume gesendet. Bis das gelöschte Volume gelöscht ist, kann es wiederhergestellt werden und Datentransfers werden fortgesetzt. Wenn das gelöschte Volume aus dem System gelöscht wird, wird das Volume, mit dem es gepaart wurde, in den Status „StopedMisConfigured“ versetzt und der Status der Volume-Kopplung wurde entfernt. Das gespült Volume ist dauerhaft nicht mehr verfügbar.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	Die ID des zu löschenden Volumes.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Datenmenge	Objekt mit Informationen zum gelöschten Volume.	Datenmenge
VolumeID	Die VolumeID des gelöschten Volumes.	Ganzzahl
Kurve	Die Kurve ist ein Satz von Schlüsselwert-Paaren. Die Schlüssel sind die E/A-Größe in Byte. Die Werte stellen die Kosten für die Performance eines IOP bei einer bestimmten I/O-Größe dar. Die Kurve wird relativ zu einem 4096-Byte-Vorgang berechnet, der auf 100 IOPS eingestellt ist.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "DeleteVolume",
   "params": {
      "volumeID"  : 5
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:


```
{
  "id": 1,
  "result": {
    "volume": {
      "access": "readWrite",
      "accountID": 1,
      "attributes": {
        "name1": "value1",
        "name2": "value2",
        "name3": "value3"
      },
      "blockSize": 4096,
      "createTime": "2016-03-28T16:16:13Z",
      "deleteTime": "2016-03-31T22:59:42Z",
      "enable512e": true,
      "iqn": "iqn.2010-01.com.solidfire:jyay.1459181777648.5",
      "name": "1459181777648",
      "purgeTime": "2016-04-01T06:59:42Z",
      "qos": {
        "burstIOPS": 150,
        "burstTime": 60,
        "curve": {
          "4096": 100,
          "8192": 160,
          "16384": 270,
          "32768": 500,
          "65536": 1000,
          "131072": 1950,
          "262144": 3900,
          "524288": 7600,
          "1048576": 15000
        },
        "maxIOPS": 100,
        "minIOPS": 60
      },
      "scsiEUIDeviceID": "6a79617900000005f47acc0100000000",
      "scsiNAADeviceID": "6f47acc1000000006a79617900000005",
      "sliceCount": 1,
      "status": "deleted",
      "totalSize": 1000341504,
      "virtualVolumeID": null,
      "volumeAccessGroups": [
```

```
          1
        ],
        "volumeID": 5,
        "volumePairs": []
      }
    }
}
```

Neu seit Version

9.6

DeleteVolumes

Sie können das verwenden `DeleteVolumes` Methode zum Markieren mehrerer (bis zu 500) aktiver Volumes zum Löschen. Wenn diese Markierung markiert ist, wird das Volumen nach Ablauf des Reinigungsintervalls gelöscht (dauerhaft gelöscht).

Nachdem Sie eine Anfrage zum Löschen von Volumes gestellt haben, werden alle aktiven iSCSI-Verbindungen zu den Volumes sofort beendet und es sind keine weiteren Verbindungen zulässig, während sich die Volumes in diesem Zustand befinden. Ein markiertes Volume wird in Zielermittlungsanfragen nicht zurückgegeben.

Snapshots eines Volumes, die zum Löschen markiert wurden, sind nicht betroffen. Snapshots werden so lange aufbewahrt, bis das Volume aus dem System entfernt wird. Wenn ein Volume zum Löschen markiert ist und gerade ein Lese- oder Schreibvorgang für das Massenvolumen ausgeführt wird, wird der Lese- oder Schreibvorgang für das Massenvolumen angehalten.

Wenn die von Ihnen gelöschten Volumes mit einem Volume gekoppelt werden, wird die Replikation zwischen den gepaarten Volumes ausgesetzt und es werden keine Daten an sie oder von ihnen im gelöschten Zustand übertragen. Die Remote-Volumes, auf denen die gelöschten Volumes gekoppelt wurden, geben in einen Status „PausedMisfigured“ ein, und die Daten werden nicht mehr an sie oder aus den gelöschten Volumes gesendet. Bis die gelöschten Volumes gelöscht werden, können sie wiederhergestellt und die Datentransfers fortgesetzt werden. Wenn die gelöschten Volumes aus dem System gelöscht werden, werden die Volumes, mit denen sie gepaart wurden, in den Status StopedMisfigured eingegeben und der Status der Volume-Pairing entfernt. Die gelöschten Volumes sind dauerhaft nicht mehr verfügbar.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter.

> Mindestens einer der folgenden Parameter ist erforderlich, und Sie müssen nur einen der Parameter verwenden (sie schließen sich alle gegenseitig aus).

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeIDs	Liste der IDs der Volumes, die aus dem System gelöscht werden sollen.	Integer-Array	Keine	Siehe Hinweis.
VolumeAccessGroupIDs	Eine Liste der Zugriffsgruppen-IDs von Volumes. Alle Volumes aus allen in dieser Liste angegebenen Volume-Zugriffsgruppen werden aus dem System gelöscht.	Integer-Array	Keine	Siehe Hinweis.
AccountIDs	Eine Liste der Konto-IDs. Alle Volumes aus diesen Konten werden aus dem System gelöscht.	Integer-Array	Keine	Siehe Hinweis.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Volumes	Informationen zum neu gelöschten Volume.	Datenmenge
Kurve	Die Kurve ist ein Satz von Schlüsselwert-Paaren. Die Schlüssel sind die E/A-Größe in Byte. Die Werte stellen die Kosten für die Performance eines IOP bei einer bestimmten I/O-Größe dar. Die Kurve wird relativ zu einem 4096-Byte-Vorgang berechnet, der auf 100 IOPS eingestellt ist.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "DeleteVolumes",
   "params": {
      "accountIDs" : [1, 2, 3]
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result": {
    "volumes" : [ {
      "access": "readWrite",
      "accountID": 1,
      "attributes": {},
      "blockSize": 4096,
      "createTime": "2015-03-06T18:50:56Z",
      "deleteTime": "",
      "enable512e": False,
      "iqn": "iqn.2010-01.com.solidfire:pzsr.vclient-030-v00001.1",
      "name": "vclient-030-v00001",
      "qos": {
        "burstIOPS": 15000,
        "burstTime": 60,
        "curve": {},
        "maxIOPS": 15000,
        "minIOPS": 100
      },
      "purgeTime": "",
      "sliceCount": 1,
      "scsiEUIDeviceID": "707a737200000001f47acc0100000000",
      "scsiNAADeviceID": "6f47acc100000000707a737200000001",
      "status": "active",
      "totalSize": 10000003072,
      "virtualVolumeID": 5,
      "volumeAccessGroups": [],
      "volumePairs": [],
      "volumeID": 1
    } ]
  }
}
```


Neu seit Version

9.6

GetBackupTarget

Sie können das verwenden `GetBackupTarget` Methode zur Rückgabe von Informationen zu einem bestimmten Backup-Ziel, das Sie erstellt haben.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
BackupTargetID	Eindeutige Kennung, die dem Backup-Ziel zugewiesen ist.	Ganzzahl	Keine	Ja.
Name	Name des Backup-Ziels.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
BackupTarget	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 1,
  "method": "GetBackupTarget",
  "params": {
      "backupTargetID": 1
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {
     "backupTarget": {
     "attributes" : {
        "size" : 100
     },
     "backupTargetID" : 1,
     "name" : "mytargetbackup"
    }
  }
}
```

Neu seit Version

9.6

GetVolumeStats

Sie können das verwenden `GetVolumeStats` Methode, um allgemeine Aktivitätsmessungen für ein einzelnes Volume zu erhalten. Bei der Erstellung des Volumes werden die Werte kumuliert.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	Gibt das Volume an, für das Statistiken gesammelt werden sollen.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeStatistik	Informationen zur Volume-Aktivität	VolumeStatistik

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetVolumeStats",
   "params": {
      "volumeID": 32
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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": 0.0002666666666666667,
        "writeBytes": 1385173585408,
        "writeBytesLastSample": 12288,
        "writeLatencyUSec": 474,
        "writeLatencyUSecTotal": 11233350905,
        "writeOps": 157060458,
        "writeOpsLastSample": 2,
        "zeroBlocks": 489356778
    }
  }
}
```


Neu seit Version

9.6

GetDefaultQoS

Sie können das verwenden `GetDefaultQoS` Methode zum Abrufen der

standardmäßigen QoS-Werte (Quality of Service) für ein neu erstelltes Volume

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
QoS	Die Standard-QoS-Werte.	QoS

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetDefaultQoS",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "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
   }
}
```

Neu seit Version

9.6

GetQoSPolicy

Sie können das verwenden `GetQoSPolicy` Methode zum Abrufen von Details zu einer bestimmten QoS-Richtlinie aus dem System

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
QosPolicyID	Die ID der abzurufenden Richtlinie.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
QosPolicy	Details der angeforderten QoS-Richtlinie	QoSPolicy

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "GetQoSPolicy",
    "params": {
        "qosPolicyID": 2
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
      ]
    }
  }
}
```

Neu seit Version

10.0

GetVolumeCount

Sie können das verwenden `GetVolumeCount` „Method to get the Anzahl der Volumes, die sich derzeit im System befinden.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Zählen	Die Anzahl der Volumes, die sich derzeit im System befinden.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetVolumeCount",
    "params": {
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
    "count": 7
  }
}
```

Neu seit Version

9.6

GetVolumeEffizienz

Sie können das verwenden `GetVolumeEfficiency` Methode zum Abrufen von Informationen zu einem Volume. Nur das Volumen, das Sie als Parameter in dieser API-Methode angeben, wird zur Berechnung der Kapazität verwendet.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	Gibt das Volumen an, für das die Kapazität berechnet wird.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Komprimierung	Die Menge an Speicherplatz, der durch die Komprimierung von Daten auf einem einzelnen Volume eingespart wird Als Verhältnis angegeben, wobei 1 bedeutet, dass Daten ohne komprimiert gespeichert wurden.	Schweben
Deduplizierung	Die Menge an Speicherplatz, die in einem einzelnen Volume gespeichert wird, indem Daten nicht dupliziert werden. Als Verhältnis angegeben.	Schweben
MisingVolumes	Die Volumes, die nicht nach Effizienzdaten abgefragt werden konnten. Fehlende Volumes können dadurch verursacht werden, dass die Garbage Collection (GC) seit dem GC-Zyklus weniger als eine Stunde alt ist, ein temporärer Netzwerkverlust verursacht oder Dienste neu gestartet werden.	Integer-Array
Thin Provisioning	Das Verhältnis des belegten Speicherplatzes zum zugewiesenen Speicherplatz zum Speichern von Daten. Als Verhältnis angegeben.	Schweben
Zeitstempel	Die letzten Effizienzdaten wurden nach GC erfasst.	ISO 8601-Datenzeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetVolumeEfficiency",
   "params": {
      "volumeID": 606
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {
       "compression": 2.001591240821456,
       "deduplication": 1,
       "missingVolumes": [],
       "thinProvisioning": 1.009861932938856,
       "timestamp": "2014-03-10T16:06:33Z"
   }
}
```

Neu seit Version

9.6

ListeActiveVolumes

Sie können das verwenden `ListActiveVolumes` Methode zum Abrufen der Liste der aktiven Volumes, die sich derzeit im System befinden. Die Liste der VolumeID ist in VolumeID-Reihenfolge sortiert und kann in mehreren Teilen (Seiten) zurückgegeben werden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
InbegriffenVirtualVolumes	Virtuelle Volumes sind standardmäßig in der Antwort enthalten. Um virtuelle Volumes auszuschließen, setzen Sie auf false.	boolesch	Richtig	Nein
StartVolumeID	Starten der VolumeID für die Rückgabe. Wenn kein Volume mit dieser VolumeID vorhanden ist, wird das nächste Volume nach VolumeID-Reihenfolge als Beginn der Liste verwendet. Um durch die Liste zu blättern, übergeben Sie die VolumeID des letzten Volumes in der vorherigen Antwort + 1.	Ganzzahl	0	Nein
Grenze	Maximale Anzahl der zurückkehrbaren Volume-Infoobjekte. 0 (null) liefert alle Volumes (unbegrenzt) zurück.	Ganzzahl	(Unbegrenzt)	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Volumes	Liste der aktiven Volumes.	Datenmenge Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListActiveVolumes",
   "params": {
      "startVolumeID"  : 0,
      "limit" : 1000
   },
   "id" : 1
}
```

Antwortbeispiel

Aufgrund der Länge dieses Antwortbeispiels wird es in einem ergänzenden Thema dokumentiert.

Neu seit Version

9.6

ListBackupTargets

Sie können das verwenden `ListBackupTargets` Methode zum Abrufen von Informationen über alle erstellten Backup-Ziele.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
BackupTargets	Für jedes Backup-Ziel zurückgegebene Objekte. Enthaltene Objekte: • Attribute: Liste von Name-Wert-Paaren im JSON-Objektformat. (JSON-Objekt) • BackupTargetID: Eindeutige Kennung, die dem Backup-Ziel zugewiesen ist. (Ganze Zahl) • Name: Name des Backupziels. (Zeichenfolge)	JSON-Objekt

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListBackupTargets",
   "params": {},
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {
     "backupTargets": [
       {
        "attributes" : {},
        "backupTargetID" : 1,
        "name" : "mytargetbackup"
       }
    ]
  }
}
```

Neu seit Version

9.6

ListBulkVolumeJobs

Sie können das verwenden `ListBulkVolumeJobs` Methode, um Informationen zu jedem Lese- oder Schreibvorgang des Massenvolumens im System zu erhalten.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SperVolumes	Ein Array von Informationen für jeden Massenvolumenjob.	BulkVolumeJob Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListBulkVolumeJobs",
   "params": {
      },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
    "bulkVolumeJobs": [
        {
          "attributes": {
            "blocksPerTransfer": 1024,
            "firstPendingLba": 216064,
            "nLbas": 2441472,
            "nextLba": 226304,
            "pendingLbas": "[220160, 223232, 221184, 224256, 217088,
225280, 222208, 218112, 219136, 216064]",
            "percentComplete": 8,
            "startLba": 0
          },
          "bulkVolumeID": 2,
          "createTime": "2015-05-07T14:52:17Z",
          "elapsedTime": 44,
          "format": "native",
          "key": "eaffb0526d4fb47107061f09bfc9a806",
          "percentComplete": 8,
          "remainingTime": 506,
          "script": "bv_internal.py",
          "snapshotID": 509,
          "srcVolumeID": 3,
          "status": "running",
          "type": "read"
        }
      ]
   }
}
```


Neu seit Version

9.6

ListDeletedVolumes

Sie können das verwenden `ListDeletedVolumes` Methode zum Abrufen der Liste der Volumes, die zum Löschen markiert und aus dem System gelöscht wurden.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
InbegriffenVirtualVolumes	Virtuelle Volumes sind standardmäßig in der Antwort enthalten. Um virtuelle Volumes auszuschließen, setzen Sie auf false.	boolesch	Richtig	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Volumes	Liste der gelöschten Volumes.	Datenmenge Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListDeletedVolumes",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Die Antworten für diese Methode ähneln dem folgenden Beispiel:

```
{
    "id": 1,
    "result": {
        "volumes": [
            {
                "access": "readWrite",
                "accountID": 2,
                "attributes": {},
                "blockSize": 4096,
                "createTime": "2018-06-24T03:13:13Z",
                "deleteTime": "2018-07-22T16:12:39Z",
                "enable512e": true,
                "iqn": "iqn.2010-01.com.solidfire:0oto.deletethis.23",
                "name": "deleteThis",
                "purgeTime": "2016-07-23T00:12:39Z",
                "qos": {
                    "burstIOPS": 15000,
                    "burstTime": 60,
                    "curve": {
                        "4096": 100,
                        "8192": 160,
                        "16384": 270,
                        "32768": 500,
                        "65536": 1000,
                        "131072": 1950,
                        "262144": 3900,
                        "524288": 7600,
                        "1048576": 15000
                    },
                    "maxIOPS": 15000,
                    "minIOPS": 50
                },
                "scsiEUIDeviceID": "306f746f00000017f47acc0100000000",
                "scsiNAADeviceID": "6f47acc100000000306f746f00000017",
                "sliceCount": 1,
                "status": "deleted",
                "totalSize": 1396703232,
                "virtualVolumeID": null,
                "volumeAccessGroups": [],
                "volumeID": 23,
                "volumePairs": []
            }
        ]
    }
}
```

Neu seit Version

9.6

ListQoSPolicies

Sie können das verwenden `ListQoSPolicies` Methode zum Auflisten der Einstellungen aller QoS-Richtlinien im System.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
QosPolicies	Eine Liste mit Details zu den einzelnen QoS-Richtlinien.	QoSPolicy Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 231,
  "method": "ListQoSPolicies",
  "params": {}
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
        ]
      }
    ]
  }
}
```

Neu seit Version

10.0

ListSyncJobs

Sie können das verwenden `ListSyncJobs` Methode zum Abrufen von Informationen über Synchronisierungsjobs, die auf einem Element Storage Cluster ausgeführt werden. Diese Methode gibt Informationen zu Slice-, Clone-, Block- und Remote-Synchronisierungsjobs zurück.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
SyncJobs	Liste der Objekte, die Synchronisierungsprozesse beschreiben, die derzeit im System ausgeführt werden.	SyncJob Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListSyncJobs",
   "params": { },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "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"
        }
      ]
    }
}
```


Neu seit Version

9.6

ListVolumeQoSHistogramme

Sie können das verwenden `ListVolumeQoSHistograms` Methode zum Generieren eines Histogramm der QoS-Nutzung von Volumes für ein oder mehrere Volumes Dadurch können Sie besser verstehen, wie Volumes QoS verwenden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeIDs	Eine optionale Liste von Volume-IDs, in der festgelegt wird, welche Volumes QoS-Histogramme generiert werden sollen.	Integer-Array	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
QosHistogramme	Liste von Objekten, die die Volume-Nutzung für ein oder mehrere Volumes beschreiben	JSON-Objekt-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
    "method": "ListVolumeQoSHistograms",
        "params": {
            "volumeIDs": [1]
        },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
```

```
    "result": {
        "qosHistograms": [
        {
            "histograms": {
            "belowMinIopsPercentages": {
                "Bucket1To19": 2406,
                "Bucket20To39": 3,
                "Bucket40To59": 0,
                "Bucket60To79": 4,
                "Bucket80To100": 0
            },
                "minToMaxIopsPercentages": {
                "Bucket101Plus": 0,
                "Bucket1To19": 0,
                "Bucket20To39": 0,
                "Bucket40To59": 2,
                "Bucket60To79": 0,
                "Bucket80To100": 0
            },
                "readBlockSizes": {
                "Bucket131072Plus": 0,
                "Bucket16384To32767": 0,
                "Bucket32768To65535": 0,
                "Bucket4096To8191": 0,
                "Bucket65536To131071": 0,
                "Bucket8192To16383": 0
            },
                "targetUtilizationPercentages": {
                "Bucket0": 134943,
                "Bucket101Plus": 0,
                "Bucket1To19": 2409,
                "Bucket20To39": 4,
                "Bucket40To59": 0,
                "Bucket60To79": 2,
                "Bucket80To100": 0
            },
                "throttlePercentages": {
                "Bucket0": 137358,
                "Bucket1To19": 0,
                "Bucket20To39": 0,
                "Bucket40To59": 0,
                "Bucket60To79": 0,
                "Bucket80To100": 0
            },
                "writeBlockSizes": {
                "Bucket131072Plus": 0,
```

```
                "Bucket16384To32767": 0,
                "Bucket32768To65535": 0,
                "Bucket4096To8191": 0,
                "Bucket65536To131071": 0,
                "Bucket8192To16383": 0
            }
        },
            "timestamp": "2018-06-21T18:45:52.010844Z",
            "volumeID": 1
        }
    ]
}
}
```

ListVolumes

Sie können das verwenden `ListVolumes` Methode zum Abrufen einer Liste der Volumes in einem Cluster. Sie können die Volumes angeben, die in der Liste zurückgegeben werden sollen, indem Sie die verfügbaren Parameter verwenden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Konten	Es werden nur Volumes zurückgegeben, die im Besitz der hier angegebenen Konten sind. Schließen sich gegenseitig aus dem Parameter VolumeIDs.	Integer-Array	Keine	Nein
InbegriffenVirtualVolumes	Virtuelle Volumes sind standardmäßig in der Antwort enthalten. Um virtuelle Volumes auszuschließen, setzen Sie auf false.	boolesch	Richtig	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Iserlüftet	Gibt Volumes zurück, die gekoppelt oder nicht gekoppelt sind. Mögliche Werte: • True: Gibt alle gepaarten Volumes zurück. • False: Gibt alle Volumes zurück, die nicht gekoppelt sind.	boolesch	Keine	Nein
Grenze	Hiermit können Sie die maximale Anzahl an zurückgegebenen Volume-Ergebnissen festlegen. Schließen sich gegenseitig aus dem Parameter VolumeIDs.	Ganzzahl	10.000	Nein
StartVolumeID	Es werden nur Volumes mit einer ID zurückgegeben, die größer oder gleich diesem Wert ist. Schließen sich gegenseitig aus dem Parameter VolumeIDs.	Ganzzahl	Keine	Nein
VolumeIDs	Eine Liste der Volume-IDs. Wenn Sie diesen Parameter angeben, werden andere Parameter nur für diesen Volume-Satz verwendet. Beide Seiten schließen sich gegenseitig aus den Konten, startVolumeID und den Grenzparametern.	Integer-Array	Nein	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeName	Es werden nur Volume-Objektinformationen zurückgegeben, die mit dem Volume-Namen übereinstimmen.	Zeichenfolge	Nein	Nein
VolumeStatus	Es werden nur Volumes mit einem Status zurückgegeben, der dem Statuswert entspricht. Mögliche Werte: • Wird erstellt • Snapshots • Aktiv • Gelöscht	Zeichenfolge	Nein	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Volumes	Liste der Volumes	Datenmenge Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListVolumes",
    "params": {
        "volumeIDs": [1],
        "volumeStatus": "active",
        "isPaired": "false"
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "volumes": [
            {
                "access": "readWrite",
                "accountID": 1,
                "attributes": {},
                "blockSize": 4096,
                "createTime": "2016-03-28T14:39:05Z",
                "deleteTime": "",
                "enable512e": true,
                "iqn": "iqn.2010-01.com.solidfire:testvolume1.1",
                "name": "testVolume1",
                "purgeTime": "",
                "qos": {
                    "burstIOPS": 15000,
                    "burstTime": 60,
                    "curve": {
                        "4096": 100,
                        "8192": 160,
                        "16384": 270,
                        "32768": 500,
                        "65536": 1000,
                        "131072": 1950,
                        "262144": 3900,
                        "524288": 7600,
                        "1048576": 15000
                    },
                    "maxIOPS": 15000,
                    "minIOPS": 50
                },
                "scsiEUIDeviceID": "6a79617900000001f47acc0100000000",
                "scsiNAADeviceID": "6f47acc1000000006a79617900000001",
                "sliceCount": 1,
                "status": "active",
                "totalSize": 5000658944,
                "virtualVolumeID": null,
                "volumeAccessGroups": [],
                "volumeID": 1,
                "volumePairs": []
            }
        ]
    }
}
```

Neu seit Version

9.6

ListVolumeStats

Sie können das verwenden `ListVolumeStats` Methode zum Abrufen von allgemeinen Aktivitätsmessungen für ein einzelnes Volume, eine Liste von Volumes oder alle Volumes (wenn Sie den Parameter VolumeIDs weglassen) Die Messwerte werden durch die Erstellung des Volumens kumulativ erfasst.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
InbegriffenVirtualVolumes	Virtuelle Volumes sind standardmäßig in der Antwort enthalten. Um virtuelle Volumes auszuschließen, setzen Sie auf false.	boolesch	Richtig	Nein
VolumeIDs	Eine Liste von Volumes, aus denen Aktivitätsinformationen abgerufen werden können.	Integer-Array	Nein	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeStatistik	Liste der Volume-Aktivitätsinformationen	VolumeStatistik Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListVolumeStats",
    "params": {
        "volumeIDs": [1]
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
      }
    ]
  }
}
```


Neu seit Version

9.6

ListVolumesForAccount

Sie können das verwenden `ListVolumesForAccount` Methode zum Auflisten aktiver und (ausstehend) gelöschter Volumes für ein Konto.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
InbegriffenVirtualVolumes	Virtuelle Volumes sind standardmäßig in der Antwort enthalten. Um virtuelle Volumes auszuschließen, setzen Sie auf false.	boolesch	Richtig	Nein
AccountID	Alle Volumes, die dieser Buchhaltungs-ID gehören, werden zurückgegeben.	Ganzzahl	Nein	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Volumes	Liste der Volume-Informationen	Datenmenge Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListVolumesForAccount",
   "params": {
      "accountID"  : 1
   },
   "id" : 1
}
```

Antwortbeispiel

Die Antworten für diese Methode ähneln dem folgenden Beispiel:

```
{
    "id": 1,
    "result": {
        "volumes": [
            {
                "access": "readWrite",
                "accountID": 1,
                "attributes": {},
                "blockSize": 4096,
                "createTime": "2018-07-22T16:15:25Z",
                "deleteTime": "",
                "enable512e": false,
                "iqn": "iqn.2010-01.com.solidfire:0oto.test1.25",
                "name": "test1",
                "purgeTime": "",
                "qos": {
                    "burstIOPS": 15000,
                    "burstTime": 60,
                    "curve": {
                        "4096": 100,
                        "8192": 160,
                        "16384": 270,
                        "32768": 500,
                        "65536": 1000,
                        "131072": 1950,
                        "262144": 3900,
                        "524288": 7600,
                        "1048576": 15000
                    },
                    "maxIOPS": 15000,
                    "minIOPS": 50
                },
                "scsiEUIDeviceID": "306f746f00000019f47acc0100000000",
                "scsiNAADeviceID": "6f47acc100000000306f746f00000019",
                "sliceCount": 1,
                "status": "active",
                "totalSize": 1000341504,
                "virtualVolumeID": null,
                "volumeAccessGroups": [],
                "volumeID": 25,
                "volumePairs": []
            }
        ]
    }
}
```

Neu seit Version

9.6

ListVolumeStatsByKonto

Sie können das verwenden `ListVolumeStatsByAccount` Methode zum Auflisten von Messungen der Volumenaktivität auf hoher Ebene für jedes Konto. Werte werden aus allen Volumes des Kontos zusammengefasst.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
InbegriffenVirtualVolumes	Virtuelle Volumes sind standardmäßig in der Antwort enthalten. Um virtuelle Volumes auszuschließen, setzen Sie auf false.	boolesch	Richtig	Nein
Konten	Eine Liste der Account-IDs, für die Volume-Statistiken zurückgegeben werden sollen. Wenn keine Daten angegeben werden, werden Statistiken für alle Konten zurückgegeben.	Integer-Array	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeStatistik	Liste der Volume-Aktivitätsinformationen für jedes Konto.**Hinweis:** das volumeID-Mitglied ist für jeden Eintrag 0, da die Werte die Zusammenfassung aller Volumes darstellen, die dem Konto gehören.	VolumeStatistik Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method": "ListVolumeStatsByAccount",
  "params": {"accounts": [3]},
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
      }
    ]
  }
}
```

Neu seit Version

9.6

ListVolumeStatsByVirtualVolume

Sie können das verwenden `ListVolumeStatsByVirtualVolume` Methode zum Auflisten von Volume-Statistiken für alle Volumes im System, die mit dem virtuellen Volume verknüpft sind. Die Erstellung des Volumes ermöglicht die kumulative Statistik.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VirtualVolumeIDs	Eine Liste mit einer oder mehreren virtuellen Volume-IDs, für die Informationen abgerufen werden sollen. Wenn Sie diesen Parameter angeben, gibt die Methode Informationen nur zu diesen virtuellen Volumes zurück.	UUID-String-Array	Nein	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeStatistik	Eine Liste von Objekten, die Aktivitätsinformationen für jedes virtuelle Volume im System enthalten	VolumeStatistik Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListVolumeStatsByVirtualVolume",
  "params": {},
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:


```
{
  "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
```

```
        }
      ]
    }
}
```

Neu seit Version

9.6

ListVolumeStatsByVolume

Sie können das verwenden `ListVolumeStatsByVolume` Methode zum Auflisten von allgemeinen Aktivitätsmessungen für jedes Volumen, nach Volumen. Bei der Erstellung des Volumes werden die Werte kumuliert.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
InbegriffenVirtualVolumes	Virtuelle Volumes sind standardmäßig in der Antwort enthalten. Um virtuelle Volumes auszuschließen, setzen Sie auf false.	boolesch	Richtig	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeStatistik	Liste der Volume-Aktivitätsinformationen	VolumeStatistik Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListVolumeStatsByVolume",
   "params": {},
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:


```
{
  "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": 0.0002666666666666667,
            "writeBytes": 1385173585408,
            "writeBytesLastSample": 12288,
            "writeLatencyUSec": 474,
            "writeLatencyUSecTotal": 11233350905,
            "writeOps": 157060458,
            "writeOpsLastSample": 2,
            "zeroBlocks": 489356778
        }
    ]
  }
}
```


Neu seit Version

9.6

ListVolumeStatsByVolumeAccessGroup

Sie können das verwenden `ListVolumeStatsByVolumeAccessGroup` Methode zum Auflisten der Gesamtaktivitätsmessungen für alle Volumes, die zu den angegebenen Volume-Zugriffsgruppen gehören.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
InbegriffenVirtualVolumes	Virtuelle Volumes sind standardmäßig in der Antwort enthalten. Um virtuelle Volumes auszuschließen, setzen Sie auf false.	boolesch	Richtig	Nein
VolumeAccessGroups	Ein Array von VolumeAccessGroupIDs, für die Volume-Aktivität zurückgegeben wird. Wenn keine Angaben gemacht werden, werden Statistiken für alle Volume-Zugriffsgruppen zurückgegeben.	Integer-Array	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeStatistik	Liste der Volume-Aktivitätsinformationen für alle Volumes in der angegebenen Volume Access Group.**Hinweis:** das volumeID-Mitglied ist für jeden Eintrag 0, da die Werte die Summe aller Volumes darstellen, die dem Konto gehören.	VolumeStatistik

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListVolumeStatsByVolumeAccessGroup",
    "params": {"volumeAccessGroups": [1]},
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
      }
    ]
  }
}
```

Neu seit Version

9.6

ModifyBackupTarget

Sie können das verwenden `ModifyBackupTarget` Methode zum Ändern von Attributen eines Backup-Ziels.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
BackupTargetID	Eindeutige Ziel-ID für das zu ändernde Ziel	Ganzzahl	Keine	Ja.
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
Name	Neuer Name für das Backup-Ziel.	Zeichenfolge	Keine	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ModifyBackupTarget",
   "params": {
      "backupTargetID" : 1,
      "name": "yourtargetS3"
      "attributes" : {
          "size" : 500,
      }
   },
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {}
}
```

Neu seit Version

9.6

ModifyQoSPolicy

Sie können das verwenden `ModifyQoSPolicy` Methode zum Ändern einer vorhandenen QoS-Richtlinie im System

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
QosPolicyID	Die ID der Richtlinie, die geändert werden soll.	Ganzzahl	Keine	Ja.
Name	Sofern angegeben, wird der Name der QoS-Richtlinie (z. B. Gold, Platin, Silber) in diesen Wert geändert.	Zeichenfolge	Keine	Nein
qos	Falls angegeben, werden die QoS-Einstellungen für diese Richtlinie auf diese Einstellungen geändert. Sie können teilweise QoS-Werte liefern und nur einige der QoS-Einstellungen ändern.	QoS-Objekt	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
QosPolicy	Details der neu geänderten QoS-Richtlinie	QoSPolicy

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 1950,
  "method": "ModifyQoSPolicy",
  "params": {
    "qosPolicyID": 2,
    "qos": {
      "minIOPS": 51,
      "maxIOPS": 15002,
      "burstIOPS": 15002
    }
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
      ]
    }
  }
}
```


Neu seit Version

10.0

UmfyVolume

Sie können das verwenden `ModifyVolume` Methode zum Ändern der Einstellungen für ein vorhandenes Volume Sie können Änderungen an einem Volume gleichzeitig vornehmen, und sofortige Änderungen finden statt.

Wenn Sie beim Ändern eines Volume keine QoS-Werte angeben, bleiben diese unverändert vor der Änderung. Sie können Standard-QoS-Werte für ein neu erstelltes Volume abrufen, indem Sie das ausführen `GetDefaultQoS` Methode.

Wenn Sie die Größe eines Volumes erhöhen müssen, das repliziert wird, gehen Sie folgendermaßen vor, um Replizierungsfehler zu vermeiden:

1. Erhöhen Sie die Größe des Volumes mit replizierungTarget-Zugriff.
2. Erhöhen Sie die Größe des Quell- oder Volume mit ReadWrite-Zugriff.

Stellen Sie sicher, dass sowohl die Ziel- als auch die Quell-Volumes dieselbe Größe haben.

Wenn Sie den Zugriffsstatus in gesperrt oder ReplikationTarget ändern, werden alle vorhandenen iSCSI-Verbindungen beendet.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	Die VolumeID des zu ändernden Volumes	Ganzzahl	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Datenzugriff	Zugriff für das Volume zulässig. Mögliche Werte: • `readOnly`: Nur Leseoperationen sind erlaubt. • `readWrite`: Lesen und Schreiben sind erlaubt. • `locked`: Es sind keine Lese- oder Schreibvorgänge zulässig. Wenn nicht angegeben, ändert sich der Zugriffswert nicht. • `replicationTarget`: Identifizieren Sie ein Volumen als Zielvolumen für eine gepaarte Menge von Volumen. Wenn das Volume nicht gekoppelt ist, ist der Zugriffsstatus gesperrt. Wenn kein Wert angegeben wird, ändert sich der Zugriffswert nicht. • `snapMirrorTarget`: Identifizieren Sie ein Volume als Ziel-Volume für die SnapMirror Replikation.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
AccountID	Die AccountID, der das Volumen neu zugeordnet wird. Wenn keine angegeben wird, wird der vorherige Kontoname verwendet.	Ganzzahl	Keine	Nein
AssoziateWithQoSPolicy	Verknüpfen Sie das Volume mit der angegebenen QoS-Richtlinie. Mögliche Werte: • `true`: Verknüpfen Sie das Volumen mit der QoS-Richtlinie, die im Parameter QoSPolicyID angegeben ist. • `false`: Verknüpfen Sie das Volume nicht mit der QoS-Richtlinie, die im Parameter QoSPolicyID angegeben ist. Wenn „false“, wird eine vorhandene Richtlinienzuordnung entfernt, unabhängig davon, ob Sie im Parameter QoSPolicy eine QoS-Richtlinie angeben.	boolesch	Keine	Nein
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
CreateTime	Eine ISO 8601-Datumszeichenfolge, die als Erstellungsdatum des neuen Volumes festgelegt werden soll. Erforderlich, wenn setCreateTime auf true gesetzt ist.	ISO 8601-Zeichenfolge	Keine	Nein
DontMoveforIopsRebalance	Verhindern Sie beim Lastausgleich mit den tatsächlichen IOPS, dass ein Volume verschoben wird. Diese Einstellung ist ab Element 12.8 verfügbar und nur wirksam, wenn "VolumeLoadBalanceOnActualIOPS"aktiviert ist. Mögliche Werte: • `true`: Volumen lädt nicht auf der Grundlage der tatsächlichen IOPS. • `false`: Volumen macht Lastenausgleich basierend auf tatsächlichen IOPS. **Hinweis**: Der Ausgleich für Hochverfügbarkeit (Node-Ausfall) hat Vorrang vor `VolumeLoadBalanceOnActualIOPS` und `dontMoveforIopsRebalance`.	boolesch	Falsch	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
AbleSnapMirrorReplication	Legt fest, ob das Volume für die Replizierung mit SnapMirror Endpunkten verwendet werden kann. Mögliche Werte: • `true` • `false`	boolesch	Falsch	Nein
FifoGröße	Gibt die maximale Anzahl von FIFO-Snapshots an, die vom Volume unterstützt werden. Beachten Sie, dass FIFO- und nicht-FIFO-Snapshots beide denselben Pool verfügbarer Snapshot-Steckplätze auf einem Volume nutzen. Verwenden Sie diese Option, um den FIFO-Snapshot-Verbrauch der verfügbaren Snapshot-Steckplätze zu begrenzen. Beachten Sie, dass Sie diesen Wert nicht so ändern können, dass er kleiner als die aktuelle FIFO-Snapshot-Anzahl ist.	Ganzzahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Min50 Größe	Gibt die Anzahl der Snapshot-Steckplätze an, die nur für FIFO-Snapshots (First in First out) reserviert sind. Da FIFO- und nicht-FIFO-Snapshots sich den gleichen Pool teilen, reduziert der minFifoSize-Parameter die Gesamtzahl der möglichen Non-FIFO-Schnappschüsse um die gleiche Menge. Beachten Sie, dass Sie diesen Wert nicht ändern können, damit er mit der aktuellen Anzahl nicht-FIFO-Snapshots in Konflikt steht.	Ganzzahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Modus	Volume-Replizierungsmodus Mögliche Werte: • `asynch`: Wartet darauf, dass das System bestätigt, dass die Daten auf der Quelle gespeichert werden, bevor sie auf das Ziel geschrieben werden. • `sync`: Wartet nicht auf die Bestätigung der Datenübermittlung von der Quelle, um mit dem Schreiben von Daten auf das Ziel zu beginnen.	Zeichenfolge	Keine	Nein
qos	Die neue Quality of Service-Einstellungen für dieses Volume. Wenn nicht angegeben, werden die QoS-Einstellungen nicht geändert. Mögliche Werte: • `minIOPS` • `maxIOPS` • `burstIOPS`	QoS	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
QosPolicyID	Die ID für die Richtlinie, deren QoS-Einstellungen auf die angegebenen Volumes angewendet werden sollten. Dieser Parameter schließen sich gegenseitig mit dem qos-Parameter aus.	Ganzzahl	Keine	Nein
SetCreateTime	Setzen Sie auf true, um das aufgezeichnete Datum der Volume-Erstellung zu ändern.	boolesch	Keine	Nein
Summengröße	Die neue Größe des Volumes in Byte. 1000000000 entspricht 1 GB. Die Größe wird auf den nächsten Megabyte aufgerundet. Mit diesem Parameter kann nur die Größe eines Volumes erhöht werden.	Ganzzahl	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Datenmenge	Objekt mit Informationen zum neu geänderten Volume.	Datenmenge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ModifyVolume",
  "params": {
     "volumeID": 319,
     "access": "readWrite",
     "dontMoveForIopsRebalance": false
     },
     "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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": "6f47acc1000000003365657500000013f",
        "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"
      }
  }
}
```


Neu seit Version

9.6

Weitere Informationen

GetDefaultQoS

ModifyVolumes

Sie können das verwenden `ModifyVolumes` Methode zur Konfiguration von bis zu 500 vorhandenen Volumes gleichzeitig Änderungen finden sofort statt. Wenn `ModifyVolumes` Ändert nichts von den angegebenen Volumes, keines der angegebenen Volumes wird geändert.

Falls Sie bei dem Ändern von Volumes keine QoS-Werte angeben, bleiben die QoS-Werte für jedes Volume unverändert. Sie können Standard-QoS-Werte für ein neu erstelltes Volume abrufen, indem Sie das ausführen `GetDefaultQoS` Methode.

Wenn Sie die Größe der Volumes erhöhen müssen, die repliziert werden, gehen Sie folgendermaßen vor, um Replizierungsfehler zu vermeiden:

1. Erhöhen Sie die Größe des Volumes mit replizierungTarget-Zugriff.
2. Erhöhen Sie die Größe des Quell- oder Volume mit ReadWrite-Zugriff.

Stellen Sie sicher, dass sowohl die Ziel- als auch die Quell-Volumes dieselbe Größe haben.

Wenn Sie den Zugriffsstatus in gesperrt oder ReplikationTarget ändern, werden alle vorhandenen iSCSI-Verbindungen beendet.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Datenzugriff	Zugriff für die Volumes zulässig. Mögliche Werte: • `readOnly`: Nur Leseoperationen sind erlaubt. • `readWrite`: Lesen und Schreiben sind erlaubt. • `locked`: Es sind keine Lese- oder Schreibvorgänge zulässig. Wenn nicht angegeben, ändert sich der Zugriffswert nicht. • `replicationTarget`: Identifizieren Sie ein Volumen als Zielvolumen für eine gepaarte Menge von Volumen. Wenn das Volume nicht gekoppelt ist, ist der Zugriffsstatus gesperrt. Wenn kein Wert angegeben wird, ändert sich der Zugriffswert nicht.	Zeichenfolge	Keine	Nein
AccountID	Die AccountID, der die Volumes neu zugeordnet werden. Wenn keine angegeben wird, wird der vorherige Kontoname verwendet.	Ganzzahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
AssoziateWithQoSPolicy	Verknüpfen Sie das Volume mit der angegebenen QoS-Richtlinie. Mögliche Werte: • `true`: Verknüpfen Sie das Volumen mit der QoS-Richtlinie, die im Parameter QoSPolicyID angegeben ist. • `false`: Verknüpfen Sie das Volume nicht mit der QoS-Richtlinie, die im Parameter QoSPolicyID angegeben ist. Wenn „false“, wird eine vorhandene Richtlinienzuordnung entfernt, unabhängig davon, ob Sie im Parameter QoSPolicy eine QoS-Richtlinie angeben.	boolesch	Keine	Nein
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
CreateTime	Eine ISO 8601-Datumszeichenfolge, die als Erstellungsdatum des neuen Volumes festgelegt werden soll. Erforderlich, wenn setCreateTime auf true gesetzt ist.	ISO 8601-Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
DontMoveforIopsRebalance	Verhindern Sie beim Lastausgleich mit den tatsächlichen IOPS, dass ein Volume verschoben wird. Diese Einstellung ist ab Element 12.8 verfügbar und nur wirksam, wenn "VolumeLoadBalanceOnActualIOPS"aktiviert ist. Mögliche Werte: • `true`: Volumen lädt nicht auf der Grundlage der tatsächlichen IOPS. • `false`: Volumen macht Lastenausgleich basierend auf tatsächlichen IOPS. **Hinweis**: Der Ausgleich für Hochverfügbarkeit (Node-Ausfall) hat Vorrang vor `VolumeLoadBalanceOnActualIOPS` und `dontMoveforIopsRebalance`.	boolesch	Falsch	Nein
AbleSnapMirrorReplication	Legt fest, ob das Volume für die Replizierung mit SnapMirror Endpunkten verwendet werden kann. Mögliche Werte: • `true` • `false`	boolesch	Falsch	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
FifoGröße	Gibt die maximale Anzahl von FIFO-Snapshots an, die vom Volume unterstützt werden. Beachten Sie, dass FIFO- und nicht-FIFO-Snapshots beide denselben Pool verfügbarer Snapshot-Steckplätze auf einem Volume nutzen. Verwenden Sie diese Option, um den FIFO-Snapshot-Verbrauch der verfügbaren Snapshot-Steckplätze zu begrenzen. Beachten Sie, dass Sie diesen Wert nicht so ändern können, dass er kleiner als die aktuelle FIFO-Snapshot-Anzahl ist.	Ganzzahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Min50 Größe	Gibt die Anzahl der Snapshot-Steckplätze an, die nur für FIFO-Snapshots (First in First out) reserviert sind. Da FIFO- und nicht-FIFO-Snapshots sich den gleichen Pool teilen, reduziert der minFifoSize-Parameter die Gesamtzahl der möglichen Non-FIFO-Schnappschüsse um die gleiche Menge. Beachten Sie, dass Sie diesen Wert nicht ändern können, damit er mit der aktuellen Anzahl nicht-FIFO-Snapshots in Konflikt steht.	Ganzzahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Modus	Volume-Replizierungsmodus Mögliche Werte: • `asynch`: Wartet darauf, dass das System bestätigt, dass die Daten auf der Quelle gespeichert werden, bevor sie auf das Ziel geschrieben werden. • `sync`: Wartet nicht auf die Bestätigung der Datenübermittlung von der Quelle, um mit dem Schreiben von Daten auf das Ziel zu beginnen.	Zeichenfolge	Keine	Nein
qos	Die neue Quality-of-Service-Einstellungen für die Volumes. Wenn nicht angegeben, werden die QoS-Einstellungen nicht geändert. Mögliche Werte: • `minIOPS` • `maxIOPS` • `burstIOPS`	QoS	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
QosPolicyID	Die ID für die Richtlinie, deren QoS-Einstellungen auf die angegebenen Volumes angewendet werden sollten. Dieser Parameter schließen sich gegenseitig mit dem qos-Parameter aus.	Ganzzahl	Keine	Nein
SetCreateTime	Setzen Sie auf true, um das aufgezeichnete Datum der Volume-Erstellung zu ändern.	boolesch	Keine	Nein
Summengröße	Die neue Größe der Volumen in Byte. 1000000000 entspricht 1 GB. Die Größe wird auf den nächsten Megabyte aufgerundet. Mit diesem Parameter kann nur die Größe eines Volumes erhöht werden.	Ganzzahl	Keine	Nein
VolumeIDs	Eine Liste der VolumeIDs der zu ändernden Volumes	Integer-Array	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Datenmenge	Ein Array von Objekten, die Informationen zu jedem neu geänderten Volume enthalten.	Datenmenge Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ModifyVolumes",
  "params": {
    "volumeIDs": [319,22],
    "access": "readWrite",
    "dontMoveForIopsRebalance": false
  },
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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": "6f47acc1000000003365657500000013f",
        "sliceCount": 1,
        "status": "active",
        "totalSize": 1000000716800,
        "virtualVolumeID": null,
        "volumeAccessGroups": [
        22
        ],
        "volumeConsistencyGroupUUID": "3003109e-6e75-444c-8cee-
470d641a09c3",
        "volumeID": 319,
        "volumePairs": [],
        "
      }
  }
}
```


Neu seit Version

9.6

Weitere Informationen

GetDefaultQoS

PurgeDeletedVolume

Sie können das verwenden `PurgeDeletedVolume` Methode zum sofortigen und dauerhaften Löschen eines gelöschten Volumes. Sie müssen ein Volume mit löschen `DeleteVolume` Bevor er gereinigt werden kann.

Volumes werden nach einem gewissen Zeitraum automatisch gelöscht, daher ist die Nutzung dieser Methode in der Regel nicht erforderlich.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	Die VolumeID des zu reinenden Volumes.	Ganzzahl	Nein	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "PurgeDeletedVolume",
   "params": {
      "volumeID"  : 5
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result": {}
}
```

Neu seit Version

9.6

Weitere Informationen

DeleteVolume

PurgeDeletedVolumes

Sie können das verwenden `PurgeDeletedVolumes` Methode zum sofortigen und dauerhaften Löschen von gelöschten Volumes; mit dieser Methode können Sie bis zu 500 Volumes gleichzeitig löschen.

Sie müssen Volumes mit löschen `DeleteVolumes` Bevor sie gereinigt werden können. Volumes werden nach einem gewissen Zeitraum automatisch gelöscht, daher ist die Nutzung dieser Methode in der Regel nicht erforderlich.

> Wenn Sie eine große Anzahl von Volumes gleichzeitig löschen oder wenn die Volumes, die Sie löschen, jeden mit vielen damit verbundenen Snapshots haben, könnte die Methode fehlschlagen und den Fehler „xDBConnectionLoss“ zurückgeben. In diesem Fall wiederholen Sie den Methodenaufruf mit weniger Volumen.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeIDs	Liste der Volume-IDs, die aus dem System entfernt werden sollen	Integer-Array	Nein	Nein
AccountIDs	Eine Liste der Rechnungs-IDs. Alle Volumes aus allen angegebenen Konten werden aus dem System gelöscht.	Integer-Array	Nein	Nein
VolumeAccessGroupIDs	Eine Liste der VolumeAccessGroupIDs. Alle Volumes aus allen angegebenen Volume-Zugriffsgruppen werden aus dem System gelöscht.	Integer-Array	Nein	Nein

Hinweis: Sie können pro Methodenaufruf nur einen der oben genannten Parameter angeben. Wenn mehr als ein oder keine angegeben wird, führt dies zu einem Fehler.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "PurgeDeletedVolumes",
   "params": {
      "accountIDs" : [1, 2, 3]
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result": {}
}
```

Neu seit Version

9.6

Weitere Informationen

DeleteVolumes

RemoveBackupTarget

Sie können das verwenden `RemoveBackupTarget` Methode zum Entfernen von Backup-Zielen.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
BackupTargetID	Eindeutige Ziel-ID des zu entfernenden Ziels.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "RemoveBackupTarget",
   "params": {
        "backupTargetID" : 1
   },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {}
}
```

Neu seit Version

9.6

RestoreDeletedVolumen

Sie können das verwenden `RestoreDeletedVolume` Methode, um ein gelöschtes Volume erneut als aktiv zu markieren. Durch diese Aktion wird das Volume sofort für die iSCSI-Verbindung verfügbar.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	Die Volume-ID des wiederherzustellenden gelöschten Volumes.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "RestoreDeletedVolume",
   "params": {
      "volumeID"  : 5
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id" : 1,
  "result": {}
}
```

Neu seit Version

9.6

SetdefaultQoS

Sie können das verwenden `SetDefaultQoS` Methode zur Konfiguration der standardmäßigen QoS-Werte (Quality of Service) für ein Volume (gemessen in ein- und Ausgaben pro Sekunde oder IOPS)

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
IOPS-Minimum	Die Mindestanzahl kontinuierlich IOPS, die vom Cluster zu einem Volume bereitgestellt wird.	Ganzzahl	Keine	Nein
Maximale IOPS-Werte	Die maximale Anzahl kontinuierlicher IOPS, die vom Cluster zu einem Volume bereitgestellt wird.	Ganzzahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
IOPS	Die maximale Anzahl an IOPS, die in einem kurzen Burst-Szenario zulässig sind.	Ganzzahl	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
IOPS-Minimum	Die Mindestanzahl kontinuierlich IOPS, die vom Cluster zu einem Volume bereitgestellt wird.	Ganzzahl
Maximale IOPS-Werte	Die maximale Anzahl kontinuierlicher IOPS, die vom Cluster zu einem Volume bereitgestellt wird.	Ganzzahl
IOPS	Die maximale Anzahl an IOPS, die in einem kurzen Burst-Szenario zulässig sind.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "SetDefaultQoS",
    "params": {
        "burstIOPS":8000,
        "maxIOPS":1000,
        "minIOPS":200
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
    "id":1,
    "result": {
        "burstIOPS":8000,
        "maxIOPS":1000,
        "minIOPS":200
    }
}
```

Neu seit Version

9.6

StartBulkVolumeRead

Sie können das verwenden `StartBulkVolumeRead` Methode zum Starten einer Lesesitzung für Massenvolumes auf einem angegebenen Volume

Auf einem Volume können nur zwei Massenvorgänge gleichzeitig ausgeführt werden. Wenn Sie die Sitzung initialisieren, werden Daten von einem SolidFire-Speicher-Volume gelesen, das in einer externen Backup-Quelle gespeichert werden soll. Auf die externen Daten wird von einem Webserver zugegriffen, der auf einem Element Storage Node ausgeführt wird. Server-Interaktionsinformationen für externen Datenzugriff werden von einem auf dem Speichersystem ausgeführten Skript übergeben.

Zu Beginn eines Massenvolumes-Lesevorgangs wird ein Snapshot des Volumes erstellt und der Snapshot wird gelöscht, sobald der Lesevorgang abgeschlossen ist. Sie können auch einen Snapshot des Volumes lesen, indem Sie die ID des Snapshot als Parameter eingeben. Wenn Sie einen vorherigen Snapshot lesen, erstellt das System keinen neuen Snapshot des Volumes und löscht auch nicht den vorherigen Snapshot, wenn der Lesevorgang abgeschlossen ist.

> Durch diesen Prozess wird ein neuer Snapshot erstellt, wenn die ID eines vorhandenen Snapshots nicht angegeben wird. Snapshots können erstellt werden, wenn die Cluster-Fülle in Phase 2 oder 3 liegt. Snapshots werden nicht erstellt, wenn die Cluster-Fülle in Phase 4 oder 5 liegt.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Formatieren	Das Format der Volume-Daten. Kann entweder sein: • `uncompressed`: Jedes Byte des Volumens wird ohne Kompression zurückgegeben. • `native`: Opaque Daten werden zurückgegeben, die kleiner und effizienter gespeichert und auf einem nachfolgenden Massenvolumen geschrieben sind.	Zeichenfolge	Keine	Ja.
VolumeID	Die ID des zu lesenden Volumes.	Ganzzahl	Keine	Ja.
Snapshot-ID	Die ID eines zuvor erstellten Snapshots, der für das Lesen des Massen-Volumes verwendet wird. Wenn keine ID eingegeben wird, wird ein Snapshot des aktuellen aktiven Volume-Images erstellt.	Ganzzahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Skript	Der Name eines ausführbaren Skripts. Wenn kein Skriptname angegeben wird, sind der Schlüssel und die URL erforderlich, um auf Element Storage-Nodes zuzugreifen. Das Skript wird auf dem primären Knoten ausgeführt, und der Schlüssel und die URL werden an das Skript zurückgegeben, so dass der lokale Webserver kontaktiert werden kann.	Zeichenfolge	Keine	Nein
ScriptParameter	JSON-Parameter, die an das Skript übergeben werden sollen.	JSON-Objekt	Keine	Nein
Merkmale	Liste der Name-Wert-Paare im JSON-Objektformat. "Weitere Informationen .".	JSON-Objekt	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Asynchron	Die ID des asynchronen Prozesses, der auf den Abschluss überprüft werden soll.	Ganzzahl
Taste	Undurchsichtige Taste, die die Sitzung eindeutig identifiziert.	Zeichenfolge
url	URL zum Zugriff auf den Webserver des Knotens.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "StartBulkVolumeRead",
   "params": {
      "volumeID" : 5,
      "format"  : "native",
      "snapshotID" : 2
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
      "id" : 1,
   "result" : {
      "asyncHandle" : 1,
      "key" : "11eed8f086539205beeaadd981aad130",
      "url" : "https://127.0.0.1:44000/"
   }
}
```

Neu seit Version

9.6

StartBulkVolumeWrite

Sie können das verwenden `StartBulkVolumeWrite` Methode zum Starten einer Schreibsitzung für das Massenvolumen auf einem angegebenen Volume

Auf einem Volume können nur zwei Massenvorgänge gleichzeitig ausgeführt werden. Beim Initialisieren der Sitzung werden Daten von einer externen Backup-Quelle in ein Element Storage Volume geschrieben. Auf die externen Daten wird von einem Webserver zugegriffen, der auf einem Element Storage Node ausgeführt wird. Server-Interaktionsinformationen für externen Datenzugriff werden von einem auf dem Speichersystem ausgeführten Skript übergeben.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Formatieren	Das Format der Volume-Daten. Kann entweder sein: • `uncompressed`: Jedes Byte des Volumens wird ohne Kompression zurückgegeben. • `native`: Opaque Daten werden zurückgegeben, die kleiner und effizienter gespeichert und auf einem nachfolgenden Massenvolumen geschrieben sind.	Zeichenfolge	Keine	Ja.
VolumeID	Die ID des Volumes, auf das geschrieben werden soll.	Ganzzahl	Keine	Ja.
Skript	Der Name eines ausführbaren Skripts. Wenn kein Skriptname angegeben wird, sind der Schlüssel und die URL erforderlich, um auf Element Storage-Nodes zuzugreifen. Das Skript wird auf dem primären Knoten ausgeführt, und der Schlüssel und die URL werden an das Skript zurückgegeben, so dass der lokale Webserver kontaktiert werden kann.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
ScriptParameter	JSON-Parameter, die an das Skript übergeben werden sollen.	JSON-Objekt	Keine	Nein
Merkmale	Liste der Name-Wert-Paare im JSON-Objektformat. "Weitere Informationen .".	JSON-Objekt	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Asynchron	Die ID des asynchronen Prozesses, der auf den Abschluss überprüft werden soll.	Ganzzahl
Taste	Undurchsichtige Taste, die die Sitzung eindeutig identifiziert.	Zeichenfolge
url	URL zum Zugriff auf den Webserver des Knotens.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "StartBulkVolumeWrite",
   "params": {
      "volumeID" : 5,
      "format"  : "native",
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1,
   "result" : {
      "asyncHandle" : 1,
      "key" : "11eed8f086539205beeaadd981aad130",
      "url" : "https://127.0.0.1:44000/"
   }
}
```

Neu seit Version

9.6

UpdateBulkVolumeStatus

Sie können das verwenden `UpdateBulkVolumeStatus` Methode zum Aktualisieren des Status eines Jobs mit Massenvolumen, den Sie mit dem gestartet haben `StartBulkVolumeRead` Oder `StartBulkVolumeWrite` Methoden

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Taste	Der bei der Initialisierung von A zugewiesene Schlüssel StartBulkVolumeRead Oder StartBulkVolumeWrite Session:	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Status	Das System legt den Status des angegebenen Massenvolume-Jobs fest. Mögliche Werte: • Läuft: Jobs, die noch aktiv sind. • Abgeschlossen: Aufträge, die ausgeführt werden. • Fehlgeschlagen: Jobs, die ausgefallen sind.	Zeichenfolge	Keine	Ja.
%Kompletete	Der abgeschlossene Fortschritt des Jobs für das Massenvolumen als Prozentsatz.	Zeichenfolge	Keine	Nein
Nachricht	Gibt den Status des Jobs für das Massenvolumen zurück, wenn der Job abgeschlossen ist.	Zeichenfolge	Keine	Nein
Merkmale	JSON-Attribute; aktualisiert, was auf dem Massenvolumenjob steht.	JSON-Objekt	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ

Status	Status der angeforderten Sitzung. Zurückgegebener Status: • Vorbereitung • Aktiv • Fertig • Fehlgeschlagen	Zeichenfolge
Merkmale	Gibt Attribute zurück, die im Methodenaufruf angegeben wurden. Werte werden zurückgegeben, ob sie sich geändert haben oder nicht.	Zeichenfolge
url	Die URL für den Zugriff auf den Webserver des Knotens; wird nur angegeben, wenn die Sitzung noch aktiv ist.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "UpdateBulkVolumeStatus",
   "params": {
          "key": "0b2f532123225febda2625f55dcb0448",
          "status": "running"
      },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1,
   "result": {
      "status" : "running",
      "url" : "https://10.10.23.47:8443/"
    }
}
```

Neu seit Version

9.6

Weitere Informationen

- StartBulkVolumeRead
- StartBulkVolumeWrite

API-Methoden für Volume-Zugriffsgruppen

AddInitiatorsToVolumeAccessGroup

Sie können das verwenden `AddInitiatorsToVolumeAccessGroup` Methode zum Hinzufügen von Initiatoren zu einer bestimmten Volume-Zugriffsgruppe.

Das akzeptierte Format eines Initiator IQN ist iqn.yyy-mm, wobei y und m Ziffern sind, gefolgt von Text, der nur Ziffern, Kleinbuchstaben alphabetische Zeichen, einen Punkt (.), Doppelpunkt (:) oder Strich (-) enthalten darf. Das folgende Beispiel zeigt:

```
iqn.2010-01.com.solidfire:17oi.solidfire-0.1
```

Das akzeptierte Format eines Fibre Channel Initiator-WWPN lautet AA:BB:CC:dd:11:22:33:44 oder AabBCCdd11223344. Das folgende Beispiel zeigt:

```
21:00:00:0e:1e:11:f1:81
```

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Initiatoren	Liste der Initiator-IDs oder Namen (IQNs und WWPNs), die in die Volume-Zugriffsgruppe aufgenommen werden sollen Wenn Sie eine Liste der Initiatornamen übergeben, werden die Initiatoren erstellt, wenn sie noch nicht vorhanden sind. Wenn Sie eine Liste der Initiator-IDs übergeben, gibt die Methode einen Fehler aus, wenn einer der Initiatoren nicht bereits vorhanden ist. Die Weitergabe von Initiatorgruppen ist veraltet. Sie sollten Initiator-IDs verwenden, sobald möglich.	Integer-Array oder String-Array (veraltet)		Ja.
VolumeAccessGroupID	Die ID der Volume-Zugriffsgruppe zum Hinzufügen des Initiators.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeAccessGroup	Ein Objekt mit Informationen über die neu geänderte Volume-Zugriffsgruppe.	VolumeAccessGroup

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 13171,
  "method": "AddInitiatorsToVolumeAccessGroup",
  "params": {
    "initiators": [116,117],
    "volumeAccessGroupID": 96
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
      ]
    }
  }
}
```

Neu seit Version

9.6

AddVolumesToVolumeAccessGroup

Sie können das verwenden `AddVolumesToVolumeAccessGroup` Methode zum

Hinzufügen von Volumes zu einer bestimmten Volume-Zugriffsgruppe.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Volumes	Liste der Volume-IDs, die zur Volume-Zugriffsgruppe hinzugefügt werden sollen	Integer-Array	Keine	Ja.
VolumeAccessGroupID	VolumeAccessGroupID der Volume Access Group, zu der Volumes hinzugefügt werden.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeAccessGroup	Ein Objekt mit Informationen über die neu geänderte Volume-Zugriffsgruppe.	VolumeAccessGroup

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "AddVolumesToVolumeAccessGroup",
   "params": {
      "volumeAccessGroupID": 96,
      "volumes": [1,2]
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
      ]
    }
  }
}
```


Neu seit Version

9.6

CreateVolumeAccessGroup

Verwenden Sie können `CreateVolumeAccessGroup` So erstellen Sie eine neue Zugriffsgruppe für Volumes: Wenn Sie die Volume-Zugriffsgruppe erstellen, müssen Sie ihr einen Namen geben und optional Initiatoren und Volumes eingeben.

Jeder Initiator-IQN, den Sie der Volume Access Group hinzufügen, kann ohne CHAP-Authentifizierung auf beliebige Volumes in der Gruppe zugreifen.

> Geklonte Volumes übernehmen keine Zugriffsgruppenmitgliedschaft für Volumes vom Quell-Volume.

Bei der Erstellung von Volume-Zugriffsgruppen ist Folgendes zu beachten:

- Eine Volume-Zugriffsgruppe kann bis zu 64 Initiator-IQNs enthalten.
- Ein Initiator kann nur zu einer Volume-Zugriffsgruppe gehören.

- Eine Volume-Zugriffsgruppe kann bis zu 2000 Volumes enthalten.
- Jede Volume-Zugriffsgruppe kann zu maximal vier Volume-Zugriffsgruppen gehören.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Initiatoren	Liste der Initiator-IDs oder Namen (IQNs und WWPNs), die in die Volume-Zugriffsgruppe aufgenommen werden sollen Wenn Sie eine Liste der Initiatornamen übergeben, werden die Initiatoren erstellt, wenn sie noch nicht vorhanden sind. Wenn Sie eine Liste der Initiator-IDs übergeben, gibt die Methode einen Fehler aus, wenn einer der Initiatoren nicht bereits vorhanden ist. Die Weitergabe von Initiatorgruppen ist veraltet. Sie sollten Initiator-IDs verwenden, sobald möglich.	Integer-Array oder String-Array (veraltet)		Nein
Name	Name der Zugriffsgruppe für Volumes. Nicht unbedingt eindeutig, aber empfohlen. Muss 1 bis 64 Zeichen lang sein.	Zeichenfolge	Keine	Ja.
Volumes	Liste der Volume-IDs, die in die Volume-Zugriffsgruppe einbezogen werden sollen	Integer-Array		Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	{}	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
VolumeAccessGroup	Ein Objekt, das Informationen über die neu erstellte Volume-Zugriffsgruppe enthält.	VolumeAccessGroup
VolumeAccessGroupID	Die ID der neu erstellten Volume Zugriffsgruppe.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "CreateVolumeAccessGroup",
   "params": {
      "name": "myaccessgroup",
      "initiators": ["iqn.1993-08.org.debian: 01: a31b1d799d5c"],
      "volumes": [327],
      "attributes": {}
   }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": null,
  "result": {
    "volumeAccessGroup": {
      "attributes": {},
      "deletedVolumes": [],
      "initiatorIDs": [
        95
      ],
      "initiators": [
        "iqn.1993-08.org.debian: 01: a31b1d799d5c"
      ],
      "name": "myaccessgroup",
      "volumeAccessGroupID": 96,
      "volumes": [
        327
      ]
    },
    "volumeAccessGroupID": 96
  }
}
```


Neu seit Version

9.6

Weitere Informationen

- GetAsyncResult
- ListSyncJobs
- UmfyVolume

DeleteVolumeAccessGroup

Verwenden Sie können `DeleteVolumeAccessGroup` Zum Löschen einer Zugriffsgruppe für Volumes.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeAccessGroupID	Die ID der zu löschenden Volume-Zugriffsgruppe.	Ganzzahl	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
DeleteOrphanInitiatoren	Gibt an, ob Initiatorgruppen gelöscht werden sollen oder nicht. Mögliche Werte: • True: Löschen von Initiatorobjekten, nachdem sie aus einer Volume-Zugriffsgruppe entfernt wurden. • False: Löschen Sie keine Initiator-Objekte, nachdem sie aus einer Volume-Zugriffsgruppe entfernt wurden. Dies ist die Standardeinstellung.	boolesch	Falsch	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Erzwingen	Durch das Hinzufügen dieses Flags wird die Zugriffsgruppe des Volumes auch dann gelöscht, wenn sie über eine virtuelle Netzwerk-ID oder ein virtuelles Tag verfügt. Mögliche Werte: • True: Volume Access Group wird gelöscht. • False: Standard. Löschen Sie die Zugriffsgruppe für Volumes nicht, wenn sie über eine virtuelle Netzwerk-ID oder ein virtuelles Tag verfügt.	boolesch	Falsch	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "DeleteVolumeAccessGroup",
   "params": {
          "force": true,
      "volumeAccessGroupID"  : 3
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1,
   "result": {}
}
```

Neu seit Version

9.6

ListVolumeAccessGroups

Sie können das verwenden `ListVolumeAccessGroups` Methode zum Abrufen von Informationen zu den Volume-Zugriffsgruppen, die sich derzeit im System befinden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Grenze	Maximale Anzahl der zurückzukehrbaren VolumeAccessGroup-Objekte. Sich gegenseitig ausschließen mit dem Parameter VolumeAccessGroups.	Ganzzahl	Unbegrenzt	Nein
StartVolumeAccessGroupID	Die Zugriffsgruppen-ID des Volumes, mit der die Liste gestartet werden soll. Sich gegenseitig ausschließen mit dem Parameter VolumeAccessGroups.	Ganzzahl	0	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeAccessGroups	Liste der abzurufenden VolumeAccessGroupID-Werte. Die startVolumeAccessGroupID und die Parameter Limit schließen sich gegenseitig aus.	Integer-Array		Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
VolumeAccessGroups	Eine Liste von Objekten, die die einzelnen Volume-Zugriffsgruppen beschreiben	VolumeAccessGroup Array erledigen
VolumeAccessGroupsNotFound	Eine Liste der Volume-Zugriffsgruppen, die vom System nicht gefunden wurden. Diese Option wird angezeigt, wenn Sie den Parameter „VolumeAccessGroups“ verwendet haben und das System eine oder mehrere von Ihnen angegebene Volume-Zugriffsgruppen nicht finden konnte.	Integer-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListVolumeAccessGroups",
   "params": {
      "startVolumeAccessGroupID": 3,
      "limit"   : 1
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
    "volumeAccessGroups": [
      {
        "attributes": {},
        "deletedVolumes": [],
        "initiatorIDs": [],
        "initiators": [],
        "name": "example1",
        "volumeAccessGroupID": 3,
        "volumes": []
      }
    ]
  }
}
```

Neu seit Version

9.6

EntfernenVolumeFromVolumeAccessGroup

Sie können das verwenden `RemoveVolumesFromVolumeAccessGroup` Methode zum Entfernen von Volumes aus einer bestimmten Zugriffsgruppe für Volumes.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeAccessGroupID	VolumeAccessGroupID zum Entfernen von Volumes aus.	Ganzzahl	Keine	Ja.
Volumes	VolumeIDs von Volumes, die aus der Volume-Zugriffsgruppe entfernt werden sollen.	Integer-Array	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeAccessGroup	Ein Objekt mit Informationen über die neu geänderte Volume-Zugriffsgruppe.	VolumeAccessGroup

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "RemoveVolumesFromVolumeAccessGroup",
   "params": {
      "volumeAccessGroupID": 96,
      "volumes": [1,2]
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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": []
    }
  }
}
```


Neu seit Version

9.6

RemoveInitiatorsFromVolumeAccessGroup

Sie können das verwenden `RemoveInitiatorsFromVolumeAccessGroup` Methode zum Entfernen von Initiatoren aus einer bestimmten Volume-Zugriffsgruppe.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeAccessGroupID	Die ID der Volume-Zugriffsgruppe, aus der Initiatoren entfernt werden.	Ganzzahl	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Initiatoren	Liste der Initiator-IDs oder Namen (IQNs und WWPNs), die in die Volume-Zugriffsgruppe aufgenommen werden sollen Wenn Sie eine Liste der Initiatornamen übergeben, werden die Initiatoren erstellt, wenn sie noch nicht vorhanden sind. Wenn Sie eine Liste der Initiator-IDs übergeben, gibt die Methode einen Fehler aus, wenn einer der Initiatoren nicht bereits vorhanden ist. Die Weitergabe von Initiatorgruppen ist veraltet. Sie sollten Initiator-IDs verwenden, sobald möglich.	Integer-Array (empfohlen) oder String-Array (veraltet)	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
DeleteOrphanInitiatoren	Gibt an, ob Objekte gelöscht werden, nachdem sie aus einer Volume-Zugriffsgruppe entfernt wurden oder nicht. Mögliche Werte: • True: Löschen von Initiatorobjekten, nachdem sie aus einer Volume-Zugriffsgruppe entfernt wurden. • False: Löschen Sie keine Initiator-Objekte, nachdem sie aus einer Volume-Zugriffsgruppe entfernt wurden. Dies ist die Standardeinstellung.	boolesch	Falsch	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeAccessGroup	Ein Objekt mit Informationen über die neu geänderte Volume-Zugriffsgruppe.	VolumeAccessGroup

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 13171,
  "method": "RemoveInitiatorsFromVolumeAccessGroup",
  "params": {
    "initiators": [114,115],
    "volumeAccessGroupID": 96
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 13171,
  "result": {
    "volumeAccessGroup": {
      "attributes": {},
      "deletedVolumes": [
        327
      ],
      "initiatorIDs": [],
      "initiators": [],
      "name": "test",
      "volumeAccessGroupID": 96,
      "volumes": [
        346
      ]
    }
  }
}
```

Neu seit Version

9.6

ModifyVolumeAccessGroup

Sie können das verwenden `ModifyVolumeAccessGroup` Methode zum Aktualisieren von Initiatoren und Hinzufügen oder Entfernen von Volumes aus einer Volume-Zugriffsgruppe.

Wenn ein angegebener Initiator oder Volume eine Duplizierung der derzeitigen vorhanden ist, bleibt die Volume-Zugriffsgruppe ohne den ist-Wert. Wenn Sie keinen Wert für Volumes oder Initiatoren angeben, wird die aktuelle Liste der Initiatoren und Volumes nicht geändert.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeAccessGroupID	Die ID der zu ändernden Volume-Zugriffsgruppe.	Ganzzahl	Keine	Ja.
Name	Der neue Name für diese Zugriffsgruppe.	Zeichenfolge	Keine	Nein
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
Initiatoren	Liste der Initiator-IDs oder Namen (IQNs und WWPNs), die in die Volume-Zugriffsgruppe aufgenommen werden sollen Wenn Sie eine Liste der Initiatornamen übergeben, werden die Initiatoren erstellt, wenn sie noch nicht vorhanden sind. Wenn Sie eine Liste der Initiator-IDs übergeben, gibt die Methode einen Fehler aus, wenn einer der Initiatoren nicht bereits vorhanden ist. Die Weitergabe von Initiatorgruppen ist veraltet. Sie sollten Initiator-IDs verwenden, sobald möglich.	Integer-Array (empfohlen) oder String-Array (veraltet)	Keine	Nein

DeleteOrphanInitiatoren	Gibt an, ob Objekte gelöscht werden, nachdem sie aus einer Volume-Zugriffsgruppe entfernt wurden oder nicht. Mögliche Werte: • True: Löschen von Initiatorobjekten, nachdem sie aus einer Volume-Zugriffsgruppe entfernt wurden. • False: Löschen Sie keine Initiator-Objekte, nachdem sie aus einer Volume-Zugriffsgruppe entfernt wurden. Dies ist die Standardeinstellung.	boolesch	Falsch	Nein
Volumes	Liste der zu ändernden Volume-IDs	Integer-Array	Keine	VolumeAccessGroup

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
VolumeAccessGroup	Ein Objekt mit Informationen über die neu geänderte Volume-Zugriffsgruppe.	VolumeAccessGroup

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ModifyVolumeAccessGroup",
   "params": {
      "volumeAccessGroupID": 96,
      "name": "accessgrouptest",
      "initiators": [115,114],
      "volumes": [
         346
    ],
      "attributes": {}
   }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
      ]
    }
  }
}
```

Neu seit Version

9.6

Weitere Informationen

- AddInitiatorsToVolumeAccessGroup
- AddVolumesToVolumeAccessGroup
- RemoveInitiatorsFromVolumeAccessGroup
- EntfernenVolumeFromVolumeAccessGroup

GetVolumeAccessGroupEffizienz

Sie können das verwenden `GetVolumeAccessGroupEfficiency` Methode zum Abrufen von Effizienzinformationen über eine Volume-Zugriffsgruppe. Nur die Volume-Zugriffsgruppe, die Sie in dieser API-Methode als Parameter angeben, wird zur Berechnung der Kapazität verwendet.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeAccessGroupID	Gibt die Zugriffsgruppe des Volumes an, für die die Kapazität berechnet wird.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Komprimierung	Die Menge an Speicherplatz, der durch die Datenkomprimierung für alle Volumes in der Volume-Zugriffsgruppe eingespart wurde Angegeben als Verhältnis, in dem ein Wert von 1 bedeutet, dass Daten ohne Komprimierung gespeichert wurden.	Schweben

Deduplizierung	Die Menge an Speicherplatz, die gespeichert wird, indem keine Daten für alle Volumes in der Zugriffsgruppe für Volumes dupliziert werden. Als Verhältnis angegeben.	Schweben
Thin Provisioning	Das Verhältnis des belegten Speicherplatzes zum zugewiesenen Speicherplatz zum Speichern von Daten. Als Verhältnis angegeben.	Schweben
Zeitstempel	Das letzte Mal wurden Effizienzdaten nach der Speicherbereinigung erfasst.	ISO 8601-Datenzeichenfolge
MisingVolumes	Die Volumes, die nicht nach Effizienzdaten abgefragt werden konnten. Fehlende Volumes können durch eine kürzlich erfolgte Speicherbereinigung, einen vorübergehenden Netzwerkverlust oder durch einen Neustart von Diensten seit dem Speicherbereinigung verursacht werden.	Integer-Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "GetVolumeAccessGroupEfficiency",
   "params": {
      "volumeAccessGroupID": 1
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result": {
       "compression": 2.006012925331075,
       "deduplication": 1,
       "missingVolumes": [],
       "thinProvisioning": 1.009861932938856,
       "timestamp": "2014-03-10T17:05:27Z"
   }
}
```


Neu seit Version

9.6

Volume Snapshot-API-Methoden

Snapshots – Überblick

Ein Volume Snapshot ist eine zeitpunktgenaue Kopie eines Volumes. Sie können Snapshots verwenden, um ein Volume wieder in den Zustand zu versetzen, in dem es zum Zeitpunkt der Snapshot-Erstellung war.

Sie können Volume Snapshots gruppieren, sodass zugehörige Volumes konsistent gesichert oder gesichert werden können. Ein GruppenSnapshot erfasst ein Point-in-Time-Image aller Volume-Slice-Dateien. Anschließend können Sie mit dem Image ein Rollback einer Gruppe von Volumes in einen Zustand mit einem bestimmten Zeitpunkt durchführen und sicherstellen, dass alle Daten über alle Volumes in der Gruppe hinweg konsistent sind.

Sie können Volumen-Snapshots so planen, dass sie in definierten Intervallen autonom auftreten. Sie können Intervalle nach Zeit, Wochentagen oder Monatstagen festlegen. Sie können auch geplante Snapshots verwenden, um sicherzustellen, dass Snapshots zur Archivierung auf einem Remote-Speicher gesichert werden.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

CreateGroupSnapshot

Verwenden Sie können `CreateGroupSnapshot` Erstellen einer zeitpunktgenauen Kopie einer Volume-Gruppe

Sie können diesen Snapshot später als Backup oder Rollback verwenden, um sicherzustellen, dass die Daten in der Gruppe von Volumes für den Zeitpunkt, zu dem Sie den Snapshot erstellt haben, konsistent sind.

CLUSTER_FÜLLE

Sie können Snapshots erstellen, wenn die Cluster-Fülle sich an Phase 1, 2 oder 3 befindet. Sie können keine Snapshots erstellen, wenn die Cluster-Fülle die Phase 4 oder 5 erreicht.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`attributes`	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
`enableRemoteReplication`	Gibt an, ob der Snapshot zum Remote-Speicher repliziert werden soll oder nicht. Mögliche Werte: • `true`: Der Snapshot wird auf den Remote-Speicher repliziert. • `false`: Der Snapshot wird nicht auf den Remote-Speicher repliziert werden.	boolesch	Falsch	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`ensureSerialCreation`	Gibt an, dass der Snapshot nicht erstellt werden soll, wenn eine vorherige Snapshot-Replikation ausgeführt wird. Mögliche Werte sind: • `true`: So wird sichergestellt, dass jeweils nur ein Snapshot repliziert wird. Die Erstellung eines neuen Snapshots schlägt fehl, wenn noch eine vorherige Snapshot-Replikation ausgeführt wird. • `false`: Standard. Diese Snapshot-Erstellung ist zulässig, wenn noch eine andere Snapshot-Replikation ausgeführt wird.	boolesch	`false`	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`expirationTime`	Geben Sie die Zeit an, nach der der Snapshot entfernt werden kann. Kann nicht mit verwendet werden `retention`. Wenn keine `expirationTime`, Oder `retention` Sind angegeben, dass der Snapshot nicht abläuft. Das Zeitformat ist eine Datumstringfolge nach ISO 8601 für die zeitbasierte Ablaufzeit, da sie sonst nicht abläuft. Der Wert von `null` Bewirkt, dass der Snapshot dauerhaft aufbewahrt wird. Der Wert von `fifo` Bewirkt, dass der Snapshot im Verhältnis zu anderen FIFO-Snapshots auf dem Volumen auf First in First out (FIFO)-Basis beibehalten wird. Die API schlägt fehl, wenn kein FIFO-Speicherplatz verfügbar ist.	ISO 8601-Datumszeichenfolge	Keine	Nein
`name`	Der Name des Gruppen-Snapshots. Wenn kein Name eingegeben wird, wird das Datum und die Uhrzeit der Erstellung des Gruppenschnappschusses verwendet. Die maximal zulässige Namenslänge beträgt 255 Zeichen.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`retention`	Dieser Parameter ist mit dem identisch `expirationTime` Parameter, außer das Zeitformat ist HH:mm:ss Wenn keine `expirationTime` Und `retention` Sind angegeben, dass der Snapshot nicht abläuft.	Zeichenfolge	Keine	Nein
`snapMirrorLabel`	Das von der SnapMirror Software verwendete Etikett, um die Richtlinie zur Snapshot-Aufbewahrung auf einem SnapMirror Endpunkt anzugeben.	Zeichenfolge	Keine	Nein
`volumes`	Eindeutige ID des Volume-Images, aus dem kopiert werden soll	VolumeID-Array	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ

Mitglieder	Liste der Prüfsummen, Volume-IDs und Snapshot-IDs für jedes Mitglied der Gruppe. Gültige Werte: • Prüfsumme: Eine kleine Zeichenfolgendarstellung der Daten im gespeicherten Snapshot. Diese Prüfsumme kann später verwendet werden, um andere Snapshots zu vergleichen, um Fehler in den Daten zu erkennen. (Zeichenfolge) • Snapshot ID: Eindeutige ID eines Snapshots, aus dem der neue Snapshot erstellt wird. Die Snapshot-ID muss von einem Snapshot auf dem angegebenen Volume stammen. (Ganze Zahl) • VolumeID: Die Quell-Volume-ID für den Snapshot. (Ganze Zahl)	JSON-Objekt-Array
GruppenSnapshotID	Eindeutige ID des neuen Gruppen-Snapshots.	Gruppen-Snapshot-ID
GroupSnapshot	Objekt mit Informationen zum neu erstellten Gruppen-Snapshot.	GroupSnapshot

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "CreateGroupSnapshot",
   "params": {
      "volumes": [1,2]
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
      }
    ]
  }
}
```

Neu seit Version

9.6

Erstellen Sie einen Zeitplan

Verwenden Sie können `CreateSchedule` So planen Sie einen automatischen Snapshot eines Volumes in einem definierten Intervall.

Sie können den erstellten Snapshot später als Backup oder Rollback verwenden, um sicherzustellen, dass die Daten auf einem Volume oder einer Gruppe von Volumes für den Zeitpunkt, zu dem der Snapshot erstellt wurde, konsistent sind. Wenn Sie einen Snapshot für einen Zeitraum planen, der nicht durch 5 Minuten teilbar ist, wird der Snapshot zum nächsten Zeitraum ausgeführt, der durch 5 Minuten teilbar ist. Wenn Sie beispielsweise einen Snapshot für die Ausführung um 12:42:00 UTC planen, wird dieser um 12:45:00 UTC ausgeführt. Ein Snapshot kann nicht in Intervallen von weniger als 5 Minuten ausgeführt werden.

Sie können Snapshots erstellen, wenn die Cluster-Fülle sich an Phase 1, 2 oder 3 befindet. Sie können keine Snapshots erstellen, wenn die Cluster-Fülle die Phase 4 oder 5 erreicht.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`attributes`	Geben Sie mit der Zeichenfolge „`Frequency`“ die Häufigkeit des Snapshots an. Mögliche Werte: • `Days of Week` • `Days of Month` • `Time Interval`	JSON-Objekt	Keine	Nein
`hasError`	**Hilfe mit Beschreibung erforderlich**	boolesch	`false`	Nein
`hours`	Anzahl der Stunden zwischen wiederkehrenden Snapshots oder Stunden in GMT-Zeit, die der Snapshot in Tagen der Woche oder Tage des Monats-Modus stattfinden wird. Gültige Werte sind 0 bis 23.	Ganzzahl	Keine	Nein
`lastRunStatus`	Das Ergebnis oder der Status der letzten geplanten Snapshot-Erstellung.	Zeichenfolge	Keine	Nein
`name`	Der Name des Snapshots. Wenn kein Name eingegeben wird, wird das Datum und die Uhrzeit der Erstellung des Gruppenschnappschusses verwendet. Die maximal zulässige Namenslänge beträgt 244 Zeichen.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`minutes`	Anzahl der Minuten zwischen wiederkehrenden Snapshots oder der Minute in GMT-Zeit, die der Snapshot im Wochentag oder Tage im Monat-Modus stattfindet. Gültige Werte sind 5 bis 59.	Ganzzahl	Keine	Nein
`paused`	Gibt an, ob der Zeitplan angehalten werden soll oder nicht. Gültige Werte: • `true` • `false`	boolesch	Keine	Nein
`recurring`	Gibt an, ob der Zeitplan wiederholt wird oder nicht. Gültige Werte sind: • `true` • `false`	boolesch	Keine	Nein
`runNextInterval`	Gibt an, ob der Snapshot beim nächsten Mal ausgeführt werden soll, wenn der Scheduler aktiv ist. Wenn der geplante Snapshot auf „true“ gesetzt ist, wird der geplante Snapshot beim nächsten Mal ausgeführt, wenn der Scheduler aktiviert ist, und er wird auf FALSE zurückgesetzt. Gültige Werte sind: • `true` • `false`	boolesch	`false`	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`scheduleName`	Eindeutiger Name für den Zeitplan. Die maximal zulässige Länge des Plannamens beträgt 244 Zeichen.	Zeichenfolge	Keine	Ja.
`scheduleType`	Gibt den Typ des zu erstellenden Zeitplans an. Gültiger Wert ist Snapshot.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
`scheduleInfo`	Der eindeutige Name, der dem Zeitplan, den Aufbewahrungszeitraum für den erstellten Snapshot und die Volume-ID des Volumes, aus dem der Snapshot erstellt wurde, gegeben wurde. Gültige Werte: • `volumeID`: Die ID des Volumens, das in den Schnappschuss aufgenommen werden soll. (Ganze Zahl) • `volumes`: Eine Liste der Volume-IDs, die in den Gruppen-Snapshot aufgenommen werden sollen. (Ganzzahliges Array) • `name`: Der zu verwendenden Snapshot-Name. (Zeichenfolge) • `enableRemoteReplication`: Gibt an, ob der Snapshot in die Remote-Replikation aufgenommen werden soll. (boolesch) • `retention`: Die Zeit, die der Schnappschuss in HH:mm:ss beibehalten wird Wenn leer, wird der Snapshot für immer aufbewahrt. (Zeichenfolge)	JSON-Objekt	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
`snapMirrorLabel`	Das von der SnapMirror Software verwendete Etikett, um die Richtlinie zur Snapshot-Aufbewahrung auf einem SnapMirror Endpunkt anzugeben.	Zeichenfolge	Keine	Nein
`startingDate`	Zeit, nach der der Zeitplan ausgeführt wird. Wenn nicht festgelegt, beginnt der Zeitplan sofort. In UTC-Zeit formatiert.	ISO 8601-Datumszeichenfolge	Keine	Nein
`toBeDeleted`	Gibt an, dass dieser Snapshot-Zeitplan nach Abschluss der Snapshot-Erstellung gelöscht werden soll.	boolesch	`false`	Nein
`monthdays`	Die Tage des Monats, an denen ein Schnappschuss gemacht wird. Gültige Werte sind 1 bis 31.	Integer-Array	Keine	Ja (bei Terminplanung an Wochentagen des Monats)

Name	Beschreibung	Typ	Standardwert	Erforderlich
`weekdays`	Tag der Woche wird der Snapshot erstellt. Erforderliche Werte (sofern verwendet): • `Day`: 0 bis 6 (Sonntag bis Samstag) • `Offset`: Für jede mögliche Woche in einem Monat, 1 bis 6 (Wenn größer als 1, nur am Nth-1 Tag der Woche abgestimmt. Zum Beispiel Offset:3 für Sonntag bedeutet der dritte Sonntag des Monats, während Offset:4 für Mittwoch bedeutet der vierte Mittwoch des Monats. Offset:0 bedeutet, dass keine Aktion ausgeführt wird. Offset:1 (Standard) bedeutet, dass der Snapshot für diesen Tag der Woche erstellt wird, unabhängig davon, wo er in den Monat fällt)	JSON-Objekt-Array	Keine	Ja (bei Terminplanung für Wochentage)

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ

ScheduleID	ID des erstellten Zeitplans.	Ganzzahl
Zeitplan	Ein Objekt mit Informationen zum neu erstellten Zeitplan.	Zeitplan

Anforderungsbeispiel 1

Die folgende Beispiel-Planung verfügt über die folgenden Parameter:

- Es werden keine Startzunden oder Minuten angegeben, sodass der Zeitplan so genau wie möglich bis Mitternacht (00:00:00Z) beginnt.
- Sie ist nicht immer wiederkehrend (wird nur einmal ausgeführt).
- Es läuft einmal am ersten Sonntag oder Mittwoch nach dem 1. Juni 2015, UTC 19:17:15Z (welcher Tag zuerst kommt).
- Es umfasst nur ein 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
}
}
}
```

Antwortbeispiel 1

Die obige Anforderung gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
  }
}
```


Anforderungsbeispiel 2

Die folgende Beispiel-Planung verfügt über die folgenden Parameter:

- Sie wird wiederholt (wird zu jedem geplanten Intervall des Monats zur angegebenen Zeit ausgeführt).

- Er läuft am 1., 10., 15. Und 30. Jedes Monats nach dem Startdatum.
- Sie läuft um 12:15 Uhr an jedem Tag, an dem sie stattfinden soll.
- Es umfasst nur ein 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
}
```

Antwortbeispiel 2

Die obige Anforderung gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
  }
}
```


Anforderungsbeispiel 3

Die folgende Beispiel-Planung verfügt über die folgenden Parameter:

- Sie beginnt innerhalb von 5 Minuten nach dem geplanten Intervall am 2. April 2015.
- Sie wird wiederholt (wird zu jedem geplanten Intervall des Monats zur angegebenen Zeit ausgeführt).
- Er läuft am zweiten, dritten und vierten des Monats nach dem Startdatum.
- Sie läuft um 14:45 Uhr an jedem Tag, an dem sie stattfinden soll.
- Sie umfasst eine Gruppe von Volumes (Volumes = 1 und 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
}
```

Antwortbeispiel 3

Die obige Anforderung gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
  }
}
```


Neu seit Version

9.6

Erstellen von Snapshot

Verwenden Sie können `CreateSnapshot` Erstellen einer zeitpunktgenauen Kopie eines Volumes Sie können einen Snapshot von einem beliebigen Volume oder von einem

vorhandenen Snapshot erstellen.

Wenn Sie mit dieser API-Methode keine SnapshotID bereitstellen, wird ein Snapshot aus dem aktiven Zweig des Volumes erstellt. Wenn das Volume, von dem der Snapshot erstellt wird, in einem Remote-Cluster repliziert wird, kann der Snapshot auch auf dasselbe Ziel repliziert werden. Verwenden Sie den Parameter enableRemoteReplication, um die Snapshot-Replikation zu aktivieren.

Sie können Snapshots erstellen, wenn die Cluster-Fülle sich an Phase 1, 2 oder 3 befindet. Sie können keine Snapshots erstellen, wenn die Cluster-Fülle die Phase 4 oder 5 erreicht.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`attributes`	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
`enableRemoteReplication`	Gibt an, ob der Snapshot zum Remote-Speicher repliziert werden soll oder nicht. Mögliche Werte: • `true`: Der Snapshot wird auf den Remote-Speicher repliziert. • `false`: Der Snapshot wird nicht auf den Remote-Speicher repliziert werden.	boolesch	Falsch	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`ensureSerialCreation`	Gibt an, dass der Snapshot nicht erstellt werden soll, wenn eine vorherige Snapshot-Replikation ausgeführt wird. Mögliche Werte sind: • `true`: So wird sichergestellt, dass jeweils nur ein Snapshot repliziert wird. Die Erstellung eines neuen Snapshots schlägt fehl, wenn noch eine vorherige Snapshot-Replikation ausgeführt wird. • `false`: Standard. Diese Snapshot-Erstellung ist zulässig, wenn noch eine andere Snapshot-Replikation ausgeführt wird.	boolesch	`false`	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Zeit für AufwandsZeit	Geben Sie die Zeit an, nach der der Snapshot entfernt werden kann. Kann nicht mit verwendet werden `retention`. Wenn weder ExpirationTime noch Retention angegeben werden, läuft der Snapshot nicht ab. Das Zeitformat ist eine Datumstringfolge nach ISO 8601 für die zeitbasierte Ablaufzeit, da sie sonst nicht abläuft. Der Wert von `null` Bewirkt, dass der Snapshot dauerhaft aufbewahrt wird. Der Wert von `fifo` Bewirkt, dass der Snapshot im ersten Schritt beibehalten wird, relativ zu anderen FIFO-Snapshots auf dem Volumen. Die API schlägt fehl, wenn kein FIFO-Speicherplatz verfügbar ist.	Zeichenfolge	Keine	Nein
`name`	Der Name des Snapshots. Wenn kein Name eingegeben wird, wird das Datum und die Uhrzeit der Snapshot-Erstellung verwendet. Die maximal zulässige Namenslänge beträgt 255 Zeichen.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`retention`	Dieser Parameter ist mit dem identisch `expirationTime` Parameter, außer das Zeitformat ist HH:mm:ss Wenn keine `expirationTime` Und `retention` Sind angegeben, dass der Snapshot nicht abläuft.	Zeichenfolge	Keine	Nein
`snapMirrorLabel`	Das von der SnapMirror Software verwendete Etikett, um die Richtlinie zur Snapshot-Aufbewahrung auf einem SnapMirror Endpunkt anzugeben.	Zeichenfolge	Keine	Nein
`snapshotID`	Eindeutige ID eines Snapshots, aus dem der neue Snapshot erstellt wird. Die übergebene Snapshot-ID muss ein Snapshot auf dem angegebenen Volume sein.	Ganzzahl	Keine	Nein
`volumeID`	Eindeutige ID des Volume-Images, aus dem kopiert werden soll	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ

Prüfsumme	Eine Zeichenfolge, die die richtigen Ziffern im gespeicherten Snapshot darstellt. Diese Prüfsumme kann später verwendet werden, um andere Snapshots zu vergleichen, um Fehler in den Daten zu erkennen.	Zeichenfolge
Snapshot-ID	Eindeutige ID des neuen Snapshots.	Snapshot-ID
snapshot	Ein Objekt, das Informationen über den neu erstellten Snapshot enthält.	snapshot

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "CreateSnapshot",
   "params": {
      "volumeID": 1
   },
   "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
  }
}
```


Ausnahme

Wenn der angezeigt wird, wird eine xNotPrimärausnahme angezeigt `CreateSnapshot` Die API wird aufgerufen und der Snapshot wird nicht erstellt. Dieses Verhalten ist zu erwarten. Wiederholen Sie den `CreateSnapshot` API-Aufruf.

Neu seit Version

9.6

DeleteGroupSnapshot

Verwenden Sie können `DeleteGroupSnapshot` Zum Löschen eines Gruppen-Snapshots.

Sie können den Parameter saveMembers verwenden, um alle Snapshots zu erhalten, die für die Volumes in der Gruppe erstellt wurden, aber die Gruppenzuordnung wird entfernt.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
GruppenSnapshotID	Eindeutige ID des Gruppen-Snapshot.	Ganzzahl	Keine	Ja.
SaveMitglieder	Gibt an, was beim Löschen eines Gruppen-Snapshots gelöscht werden soll. Gültige Werte: • True: Snapshots werden beibehalten, aber die Gruppenzuordnung wird entfernt. • False: Die Gruppe und die Snapshots werden gelöscht.	boolesch	Falsch	Nein

Rückgabewert

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "DeleteGroupSnapshot",
     "params": {
       "groupSnapshotID": 10,
       "saveMembers" : true
        },
     "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {}
}
```

Neu seit Version

9.6

LöschSnapshot

Sie können das verwenden `DeleteSnapshot` Methode zum Löschen eines Snapshots.

Ein Snapshot, der derzeit der aktive Snapshot ist, kann nicht gelöscht werden. Sie müssen einen Rollback durchführen und einen weiteren Snapshot aktivieren, bevor der aktuelle Snapshot gelöscht werden kann.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Snapshot-ID	Die ID des zu löschenden Snapshots.	Ganzzahl	Keine	Ja.
OverrideSnapMirror Hold	Überschreiben Sie die Sperre, die während der Replikation auf Snapshots platziert wurde. Sie können diesen Parameter verwenden, um veraltete SnapMirror Snapshots zu löschen, nachdem die zugehörige SnapMirror-Beziehung gelöscht wurde.	boolesch	Falsch	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "DeleteSnapshot",
"params": {
"snapshotID": 8,
"overrideSnapMirrorHold": true
},
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {}
}
```

Neu seit Version

9.6

Weitere Informationen

RollbackToSnapshot

GetSchedule

Verwenden Sie können `GetSchedule` Um Informationen über einen geplanten Snapshot zu erhalten.

Sie können Informationen zu einem bestimmten Zeitplan anzeigen, wenn im System viele Snapshot-Zeitpläne vorhanden sind. Mit dieser Methode können Sie auch Informationen über mehr als einen Zeitplan abrufen, indem Sie zusätzliche IDs im Parameter ScheduleID angeben.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ScheduleID	Eindeutige ID des Zeitplans oder mehrere anzuzeigende Zeitpläne.	Ganzzahl	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Zeitplan	Ein Array von Zeitplanattributen.	Zeitplan Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
"method": "GetSchedule",
  "params": {
              "scheduleID" : 2
      },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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": []
      }
   }
}
```


Neu seit Version

9.6

ListenSnapshots

Verwenden Sie können `ListGroupSnapshots` Methode zum Zurückgeben von Informationen über alle erstellten Gruppenschnappschüsse.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
GruppenSnapshotID	Abrufen von Informationen für die Snapshot-ID einer einzelnen Gruppe.	Ganzzahl	Keine	Nein
Volumes	Ein Array eindeutiger Volume-IDs, die abgefragt werden sollen. Wenn Sie diesen Parameter nicht angeben, enthalten alle Gruppen-Snapshots im Cluster.	VolumeID-Array	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
GruppenSnapshot	Eine Liste von Objekten mit Informationen zu den einzelnen Gruppen-Snapshots.	GroupSnapshot Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListGroupSnapshots",
  "params": {
  "volumes": [
     31,
     49
    ]
  },
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
```

```
  "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"
      }
```

```
    ]
}
```

Neu seit Version

9.6

ListSchedules

Verwenden Sie können `ListSchedules` Informationen zu allen geplanten Snapshots, die erstellt wurden, erhalten.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Zeitpläne	Eine Liste der derzeit auf dem Cluster befindlichen Zeitpläne.	Zeitplan Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListSchedules",
    "params": {},
"id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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": []
        }
      ]
   }
}
```

Neu seit Version

9.6

ListenSnapshots

Verwenden Sie können `ListSnapshots` Um die Attribute der einzelnen Snapshots, die auf dem Volume gemacht wurden, zurückzugeben.

Informationen über Snapshots, die sich auf dem Zielcluster befinden, werden auf dem Quellcluster angezeigt, wenn diese Methode vom Quellcluster aufgerufen wird.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	Ruft Snapshots für ein Volume ab. Falls keine VolumeID angegeben wird, werden alle Snapshots für alle Volumes zurückgegeben.	Ganzzahl	Keine	Nein
Snapshot-ID	Ruft Informationen für eine einzelne Snapshot-ID ab.	Ganzzahl	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Snapshots	Informationen zu jedem Snapshot für jedes Volume. Falls keine VolumeID angegeben wird, werden alle Snapshots für alle Volumes zurückgegeben. Snapshots, die sich in einer Gruppe befinden, werden mit einer Gruppen-ID zurückgegeben.	snapshot Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListSnapshots",
   "params": {
             "volumeID": "1"
       },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
        }
      ]
    }
  }
```


Neu seit Version

9.6

ModifyGroupSnapshot

Verwenden Sie können `ModifyGroupSnapshot` So ändern Sie die Attribute einer Snapshot-Gruppe. Sie können diese Methode auch verwenden, um die auf dem Quell-Volume (Quell-)erstellten Snapshots einer Remote-Replizierung auf ein Ziel-Storage-System zu aktivieren.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich

EnableRemoteReplication	Aktivieren Sie, damit der erstellte Snapshot zu einem Remote-Cluster repliziert werden kann. Mögliche Werte: • `true`: Der Snapshot wird auf den Remote-Speicher repliziert. • `false`: Der Snapshot wird nicht auf den Remote-Speicher repliziert werden.	boolesch	Falsch	Nein

Zeit für AufwandsZeit	Geben Sie die Zeit an, nach der der Snapshot entfernt werden kann. Kann nicht mit Aufbewahrung verwendet werden. Wenn weder ExpirationTime noch Retention auf dem ursprünglichen Snapshot angegeben werden, läuft der Snapshot nicht ab. Das Zeitformat ist eine Datumstringfolge nach ISO 8601 für die zeitbasierte Ablaufzeit, da sie sonst nicht abläuft. Der Wert von `null` Bewirkt, dass der Snapshot dauerhaft aufbewahrt wird. Ein Wert von fifo bewirkt, dass der Snapshot auf einer First-in-First-Out (FIFO)-Basis, relativ zu anderen FIFO-Snapshots auf dem Volumen erhalten bleibt. Die API schlägt fehl, wenn kein FIFO-Speicherplatz verfügbar ist.	ISO 8601-Datumszeichenfolge	Keine	Nein
Name	Der Name des Gruppen-Snapshots. Wenn kein Name eingegeben wird, wird das Datum und die Uhrzeit der Erstellung des Gruppenschnappschusses verwendet. Die maximal zulässige Namenslänge beträgt 255 Zeichen.	Zeichenfolge	Keine	Nein

GruppenSnapshotID	Die ID der Snapshot-Gruppe.	Zeichenfolge	Keine	Ja.
SnapMirror Label	Das von der SnapMirror Software verwendete Etikett, um die Richtlinie zur Snapshot-Aufbewahrung auf einem SnapMirror Endpunkt anzugeben.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
GroupSnapshot	Objekt mit Informationen zum neu geänderten Gruppen-Snapshot.	GroupSnapshot

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 695,
  "method": "ModifyGroupSnapshot",
  "params": {
    "groupSnapshotID": 3,
    "enableRemoteReplication": true,
    "expirationTime": "2016-04-08T22:46:25Z"
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
    }
  }
}
```


Neu seit Version

9.6

ModifySchedule

Verwenden Sie können `ModifySchedule` Um die Intervalle zu ändern, in denen ein geplanter Snapshot stattfindet. Mit dieser Methode können Sie auch einen Zeitplan löschen oder anhalten.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Merkmale	Mit dieser können Sie die Häufigkeit des Snapshot-Auftretens ändern. Mögliche Werte: • `Days of Week` • `Days of Month` • `Time Interval`	JSON-Objekt	Keine	Nein
Stunden	Anzahl Stunden zwischen Snapshots oder Stunden, bei denen der Snapshot im Wochentag- oder Monatsmodus stattfinden wird. Gültige Werte sind 0 bis 24.	Zeichenfolge	Keine	Nein
Name	Der Name des Snapshots. Wenn kein Name eingegeben wird, wird das Datum und die Uhrzeit der Erstellung des Gruppenschnappschusses verwendet. Die maximal zulässige Namenslänge beträgt 244 Zeichen.	Zeichenfolge	Keine	Nein
Minuten	Anzahl der Minuten zwischen Snapshots oder Minuten, bei denen Snapshots im Wochentag- oder Monatsmodus stattfinden. Gültige Werte sind 0 bis 59.	Ganzzahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
LastRunStatus	Das Ergebnis oder der Status der letzten geplanten Snapshot-Erstellung.	Zeichenfolge	Keine	Nein
Angehalten	Gibt an, ob der Zeitplan angehalten werden soll oder nicht. Gültige Werte: • `true` • `false`	boolesch	Keine	Nein
Wiederkehrend	Gibt an, ob der Zeitplan wiederholt wird oder nicht. Gültige Werte sind: • `true` • `false`	boolesch	Keine	Nein
RunNextInterval	Verwenden Sie diese Option, um auszuwählen, ob der Snapshot beim nächsten Mal ausgeführt werden soll, wenn der Scheduler aktiv ist. Gültige Werte: • `true` • `false` Wenn der geplante Snapshot auf „true“ gesetzt ist, wird der geplante Snapshot bei der nächsten Aktivierung des Planers ausgeführt und dann auf „false“ zurückgesetzt.	boolesch	Falsch	Nein
ScheduleID	Eindeutige ID des Zeitplans.	Ganzzahl	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Planname	Eindeutiger Name für den Zeitplan. Die maximal zulässige Länge des Plannamens beträgt 244 Zeichen.	Zeichenfolge	Keine	Nein
Planungstyp	Gibt den Typ des zu erstellenden Zeitplans an. Der einzige unterstützte Wert ist `snapshot`.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
`scheduleInfo`	Der eindeutige Name, der dem Zeitplan, den Aufbewahrungszeitraum für den erstellten Snapshot und die Volume-ID des Volumes, aus dem der Snapshot erstellt wurde, gegeben wurde. Gültige Werte: • `enableRemoteReplication`: Gibt an, ob der Snapshot in die Remote-Replikation aufgenommen werden soll. (boolesch) • `ensureSerialCreation`: Legt fest, ob eine neue Snapshot-Erstellung zulässig sein soll, wenn eine vorherige Snapshot-Replikation ausgeführt wird. (boolesch) • `name`: Der zu verwendenden Snapshot-Name. (Zeichenfolge) • `retention`: Die Zeit, die der Snapshot aufbewahrt wird. Je nach Uhrzeit wird es in einem der folgenden Formate angezeigt: ◦ `fifo`: Der Snapshot wird auf First-in-First-Out-Basis (FIFO) beibehalten.	"Zeitplan"	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
SnapMirror Label	Das von der SnapMirror Software verwendete Etikett, um die Richtlinie zur Snapshot-Aufbewahrung auf einem SnapMirror Endpunkt anzugeben.	Zeichenfolge	Keine	Nein
ToBeDeleted	Gibt an, ob der Zeitplan zum Löschen markiert ist. Gültige Werte: • `true` • `false`	boolesch	Keine	Nein
Startdatum	Gibt das Datum an, an dem der Zeitplan zum ersten Mal gestartet wurde oder beginnt.	ISO 8601-Datumszeichenfolge	Keine	Nein
Monthdays	Die Tage des Monats, an denen ein Schnappschuss gemacht wird. Gültige Werte sind 1 bis 31.	Integer-Array	Keine	Ja.
Wochentage	Tag der Woche wird der Snapshot erstellt. Der Wochentag beginnt am Sonntag mit dem Wert 0 und einem Offset von 1.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Zeitplan	Ein Objekt, das die geänderten Terminplanattribute enthält.	Zeitplan

Anforderungsbeispiel

```
{
  "method": "ModifySchedule",
  "params": {
    "scheduleName" : "Chicago",
    "scheduleID" : 3
    },
  "id": 1
}
```

Antwortbeispiel

```
{
  "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
      }
      ]
    }
  }
}
```


Neu seit Version

9.6

UmfySnapshot

Verwenden Sie können `ModifySnapshot` So ändern Sie die Attribute, die derzeit einem Snapshot zugewiesen sind. Sie können diese Methode auch verwenden, um die auf dem Quell-Volume (Lese-/Schreibzugriff) erstellten Snapshots einer Remote-Replizierung auf einem Ziel-Storage-Cluster mit der Element Software zu aktivieren.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
EnableRemoteReplication	Aktivieren Sie, damit der erstellte Snapshot in ein Remote-Storage-Cluster repliziert werden kann. Mögliche Werte: • `true`: Der Snapshot wird auf den Remote-Speicher repliziert. • `false`:Der Snapshot wird nicht auf Remote-Speicher repliziert werden.	boolesch	Falsch	Nein

Zeit für AufwandsZeit	Geben Sie die Zeit an, nach der der Snapshot entfernt werden kann. Kann nicht mit Aufbewahrung verwendet werden. Wenn weder ExpirationTime noch Retention auf dem ursprünglichen Snapshot angegeben werden, läuft der Snapshot nicht ab. Das Zeitformat ist eine Datumstringfolge nach ISO 8601 für die zeitbasierte Ablaufzeit, da sie sonst nicht abläuft. Ein Wert von null bewirkt, dass der Snapshot dauerhaft erhalten bleibt. Ein Wert von fifo bewirkt, dass der Snapshot auf einer First-in-First-Out (FIFO)-Basis, relativ zu anderen FIFO-Snapshots auf dem Volumen erhalten bleibt. Die API schlägt fehl, wenn kein FIFO-Speicherplatz verfügbar ist.	ISO 8601-Datumszeichenfolge	Keine	Nein
Name	Der Name des Snapshots. Wenn kein Name eingegeben wird, wird das Datum und die Uhrzeit der Snapshot-Erstellung verwendet. Die maximal zulässige Namenslänge beträgt 255 Zeichen.	Zeichenfolge	Keine	Nein

SnapMirror Label	Das von der SnapMirror Software verwendete Etikett, um die Richtlinie zur Snapshot-Aufbewahrung auf einem SnapMirror Endpunkt anzugeben.	Zeichenfolge	Keine	Nein
Snapshot-ID	Kennung des Snapshots.	Zeichenfolge	Keine	Ja.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
snapshot	Ein Objekt, das Informationen über den neu geänderten Snapshot enthält.	snapshot

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ModifySnapshot",
  "params": {
    "snapshotID": 3114,
    "enableRemoteReplication": "true",
    "name" : "Chicago"
  },
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
    }
  }
}
```


Neu seit Version

9.6

RollbackToGroupSnapshot

Verwenden Sie können `RollbackToGroupSnapshot` Um alle einzelnen Volumen in einer Snapshot-Gruppe auf den individuellen Snapshot jedes Volumes zurück zu verschieben.

Bei einem Rollback zu einem Gruppen-Snapshot wird ein temporärer Snapshot jedes Volumes innerhalb des Gruppen-Snapshots erstellt.

- Das Erstellen eines Snapshots ist zulässig, wenn die Cluster-Fülle an Phase 1, 2 oder 3 liegt. Snapshots werden nicht erstellt, wenn die Cluster-Fülle in Phase 4 oder 5 liegt.
- Das Rollback von Volumes auf einen Gruppen-Snapshot kann fehlschlagen, wenn die Slice-Synchronisierung ausgeführt wird. Wiederholen `RollbackToGroupSnapshot` Nach Abschluss der Synchronisierung.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`groupSnapshotID`	Eindeutige ID des Gruppen-Snapshot.	Ganzzahl	Keine	Ja.
`attributes`	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
`name`	Name für den Gruppen-Snapshot des aktuellen Status des Volumes, der erstellt wird, wenn `saveCurrentState` Ist auf „true“ gesetzt. Wenn Sie keinen Namen angeben, wird der Name der Snapshots (Gruppe und einzelnes Volume) auf einen Zeitstempel der Zeit gesetzt, zu der das Rollback durchgeführt wurde.	Zeichenfolge	Keine	Nein
`saveCurrentState`	Gibt an, ob das vorherige aktive Volume-Image gespeichert werden soll oder nicht. Gültige Werte: • `true`: Das vorherige aktive Volumenbild wird beibehalten. • `false`: Das vorherige aktive Volume-Bild wird gelöscht.	boolesch	Falsch	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ

Mitglieder	Ein Array mit VolumeIDs und Snapshot-IDs der Mitglieder des Gruppen-Snapshots. Werte: • Prüfsumme: Eine kleine Zeichenfolgendarstellung der Daten im gespeicherten Snapshot. Diese Prüfsumme kann später verwendet werden, um andere Snapshots zu vergleichen, um Fehler in den Daten zu erkennen. (Zeichenfolge) • Snapshot ID: Eindeutige ID eines Snapshots, aus dem der neue Snapshot erstellt wird. Die Snapshot-ID muss ein Snapshot auf dem angegebenen Volume sein. (Ganze Zahl) • VolumeID: Die Quell-Volume-ID für den Snapshot. (Ganze Zahl)	JSON-Objekt-Array
GruppenSnapshotID	Wenn `saveCurrentState` Wurde auf false gesetzt, dieser Wert ist Null. Wenn `saveCurrentState` Wurde auf true gesetzt, die eindeutige ID des neu erstellten Gruppen-Snapshots.	Ganzzahl
GroupSnapshot	Wenn `saveCurrentState` Wurde auf false gesetzt, dieser Wert ist Null. Wenn `saveCurrentState` Wurde auf „true“ gesetzt, ein Objekt mit Informationen über den Gruppen-Snapshot, der enthält `RollbackToGroupSnapshot` Ich habe gerade wieder zurück zu.	GroupSnapshot

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 438,
  "method": "RollbackToGroupSnapshot",
  "params": {
    "groupSnapshotID": 1,
    "name": "grpsnap1",
    "saveCurrentState": true
  }
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
      }
    ]
  }
}
```


Neu seit Version

9.6

RollbackToSnapshot

Sie können das verwenden `RollbackToSnapshot` Methode zum Erstellen eines vorhandenen Snapshots des aktiven Volume-Images. Mit dieser Methode wird ein neuer Snapshot aus einem vorhandenen Snapshot erstellt.

Der neue Snapshot wird aktiv und der vorhandene Snapshot bleibt erhalten, bis er manuell gelöscht wird. Der zuvor aktive Snapshot wird gelöscht, es sei denn, Sie setzen den Parameter saveCurrentState auf true.

CLUSTER_FÜLLE

- Sie können Snapshots erstellen, wenn die Cluster-Fülle sich an Phase 1, 2 oder 3 befindet. Sie können keine Snapshots erstellen, wenn die Cluster-Fülle die Phase 4 oder 5 erreicht.
- Das Rollback eines Volumes auf einen Snapshot kann fehlschlagen, wenn die Slice-Synchronisierung ausgeführt wird. Wiederholen `RollbackToSnapshot` Nach Abschluss der Synchronisierung.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VolumeID	VolumeID für das Volume.	Ganzzahl	Keine	Ja.
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Attribute	Keine	Nein
Name	Name für den Snapshot. Wenn kein Name angegeben wird, wird der Name des zurückgerollten Snapshots mit „-copy“ am Ende des Namens angehängt.	Zeichenfolge	Keine	Nein
Snapshot-ID	ID eines zuvor erstellten Snapshots auf dem angegebenen Volume.	Ganzzahl	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
SaveCurrentState	Gibt an, ob das vorherige aktive Volume-Image gespeichert werden soll oder nicht. Gültige Werte: • True: Das vorherige aktive Volume-Image wird beibehalten. • False: Das vorherige aktive Volume-Image wird gelöscht.	boolesch	Falsch	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Prüfsumme	Eine kleine Zeichenfolgendarstellung der Daten im gespeicherten Snapshot.	Zeichenfolge
Snapshot-ID	Wenn saveCurrentState auf false gesetzt wurde, ist dieser Wert Null. Wenn saveCurrentState auf true gesetzt wurde, lautet die eindeutige ID des neu erstellten Snapshots.	Ganzzahl
snapshot	Wenn saveCurrentState auf false gesetzt wurde, ist dieser Wert Null. Wenn saveCurrentState auf true gesetzt wurde, enthält ein Objekt Informationen über den neu erstellten Snapshot.	snapshot

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
 "method": "RollbackToSnapshot",
 "params": {
    "volumeID": 1,
    "snapshotID": 3114,
    "saveCurrentState": true
  },
  "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
  }
}
```

Neu seit Version

9.6

API-Methoden für virtuelle Volumes

CreateStorageContainer

Sie können das verwenden `CreateStorageContainer` Methode zur Erstellung eines Virtual Volume (VVol)-Storage-Containers. Sie können Storage-Container für Berichterstellung und Ressourcenzuweisung verwenden. Sie müssen mindestens einen Storage-Container erstellen, um die Virtual Volumes-Funktion verwenden zu können.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Name	Name des Speichercontainers. Befolgen Sie die Beschränkungen für die Benennung von Konten der Element Software.	Zeichenfolge	Keine	Ja.
AccountID	Ein Konto, das nicht im Speicher gespeichert wird, wird zu einem Speichercontainer.	Ganzzahl	Keine	Nein
InitiatorSecret	Der Schlüssel für die CHAP-Authentifizierung für den Initiator.	Zeichenfolge	Keine	Nein
TargetSecret	Der Schlüssel zur CHAP-Authentifizierung für das Ziel.	Zeichenfolge	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Storage Container	Objekt mit Informationen über den neu erstellten Storage-Container.	Storage Container

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "CreateStorageContainer",
    "params": {
        "name" : "example"
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
    }
  }
}
```

Neu seit Version

9.6

DeleteStorageContainers

Sie können das verwenden `DeleteStorageContainers` Methode, um bis zu 2000 Virtual Volume (VVol) Storage-Container gleichzeitig aus dem System zu entfernen. Die aus Ihnen entfernt enthaltenen Storage-Container dürfen keine VVols enthalten.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SpeicherkontainerIDs	Eine Liste der IDs der zu löschenden Speichercontainer. Sie können bis zu 2000 IDs in der Liste angeben.	UUID-Array	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "DeleteStorageContainers",
    "params": {
        "storageContainerIDs" : ["a9ec1138-e386-4a44-90d7-b9acbbc05176"]
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {}
}
```

Neu seit Version

9.6

GetStorageContainerEffizienz

Sie können das verwenden `GetStorageContainerEfficiency` Methode zum Abrufen von Effizienzinformationen über einen virtuellen Volume-Storage-Container

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SpeicherkontainerID	Die ID des Storage Containers, für den Effizienzinformation en abgerufen werden sollen.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Komprimierung	Die Menge an Speicherplatz, der durch die Datenkomprimierung für alle virtuellen Volumes im Storage-Container eingespart wird Angegeben als Verhältnis, in dem ein Wert von 1 bedeutet, dass Daten ohne Komprimierung gespeichert wurden.	Schweben
Deduplizierung	Die Menge an Speicherplatz, die eingespart wird, indem Daten für alle virtuellen Volumes im Storage-Container nicht dupliziert werden. Als Verhältnis angegeben.	Schweben
MisingVolumes	Die virtuellen Volumes, die nicht nach Effizienzdaten abgefragt werden konnten. Fehlende Volumes können durch den GC-Zyklus (Garbage Collection) verursacht werden, der weniger als eine Stunde alt ist, vorübergehend keine Netzwerkverbindung mehr besteht oder Services seit dem GC-Zyklus neu gestartet werden.	Integer-Array
Thin Provisioning	Das Verhältnis des belegten Speicherplatzes zum zugewiesenen Speicherplatz zum Speichern von Daten. Als Verhältnis angegeben.	Schweben
Zeitstempel	Die letzten Effizienzdaten wurden nach GC erfasst.	ISO 8601-Datenzeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetStorageContainerEfficiency",
  "params": {
    "storageContainerID" : "6c95e24f-9f0b-4793-affb-5a4bc6c3d7e1"
  },
  "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
    "compression": 1,
    "deduplication": 1,
    "missingVolumes": [],
    "thinProvisioning": 1,
    "timestamp": "2016-04-12T15:39:49Z"
  }
}
```

Neu seit Version

9.6

GetVirtualVolumeCount

Sie können das verwenden `GetVirtualVolumeCount` Methode zum Abrufen der Anzahl der virtuellen Volumes, die sich derzeit im System befinden.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Zählen	Die Anzahl der virtuellen Volumes, die sich derzeit im System befinden.	Ganzzahl

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "GetVirtualVolumeCount",
    "params": {
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
    "count": 5
  }
}
```

Neu seit Version

9.6

ListProtocolEndpunkte

Sie können das verwenden `ListProtocolEndpoints` Methode zum Abrufen von Informationen über alle Protokollendpunkte im Cluster Protokollendpunkte regeln den Zugriff auf die zugehörigen virtuellen Volume-Storage-Container.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Protokoll-EndpointIDs	Eine Liste der Protokollendpunkt-IDs, für die Informationen abgerufen werden sollen. Wenn Sie diesen Parameter nicht angeben, gibt die Methode Informationen zu allen Protokollendpunkten zurück.	ProtocolEndpointID UUID-Array	Keine	Nein

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Protokoll-Endpunkte	Liste der Objekte, die Informationen zu den einzelnen Protokollendpunkstellen im System enthalten.	ProtocolEndpoint Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "id": 1,
  "method": "ListProtocolEndpoints",
  "params": {}
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
      }
    ]
  }
}
```


Neu seit Version

9.6

ListStorageContainer

Sie können das verwenden `ListStorageContainers` Methode zum Abrufen von Informationen über alle dem System bekannten virtuellen Volume Storage-Container

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SpeicherkontainerIDs	Eine Liste der Speicher-Container-IDs, für die Informationen abgerufen werden können. Wenn Sie diesen Parameter nicht angeben, gibt die Methode Informationen zu allen Storage-Containern im System zurück.	UUID-Array	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Speicherkontainer	Liste der Objekte, die Informationen zu allen Speichercontainern im System enthalten	Storage Container Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
   "method": "ListStorageContainers",
   "params": {
      "storageContainerIDs": ["efda8307-b916-4424-979e-658a3f16894d"]
   },
   "id" : 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:


```
{
  "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": []
      }
    ]
  }
}
```


Neu seit Version

9.6

ListVirtualVolumeBindungen

Sie können das verwenden `ListVirtualVolumeBindings` Erhalten Sie eine Liste aller virtuellen Volumes im Cluster, die an Protokollendpunkte gebunden sind.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VirtualVolumeBindingIDs	Eine Liste der Bindungskennungen für virtuelle Volumes, für die Informationen abgerufen werden können. Wenn Sie diesen Parameter nicht angeben, gibt die Methode Informationen zu allen Bindungen des virtuellen Volumes zurück.	Integer-Array	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Bindungen	Eine Liste von Objekten, die alle virtuellen Volumes im Cluster beschreiben, die an Protokollendpunkte gebunden sind	Verbindlich

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListVirtualVolumeBindings",
    "params": {
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
      }
    ]
  }
}
```


Neu seit Version

9.6

ListVirtualVolumeHosts

Sie können das verwenden `ListVirtualVolumeHosts` Methode zum Abrufen einer Liste aller dem Cluster bekannten virtuellen Volume-Hosts Ein virtueller Volume-Host ist ein VMware ESX-Host, der eine Sitzung mit dem VASA API-Provider initiiert hat.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VirtualVolumeHost-IDs	Eine Liste der Host-IDs des virtuellen Volumes, für die Informationen abgerufen werden sollen. Wenn Sie diesen Parameter nicht angeben, gibt die Methode Informationen zu allen virtuellen Volume-Hosts zurück.	VirtualVolumeHost ID UUID-Array	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Hosts	Eine Liste von Objekten, die die Hosts der virtuellen Volumes im Cluster beschreiben	Host Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListVirtualVolumeHosts",
    "params": {
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "id": 1,
  "result": {
    "hosts": [
      {
        "bindings": [],
        "clusterID": "5ebdb4ad-9617-4647-adfd-c1013578483b",
        "hostAddress": "172.30.89.117",
        "initiatorNames": [
          "iqn.1998-01.com.vmware:zdc-dhcp-0-c-29-d6-4b-f1-1a0cd614",
          "iqn.1998-01.com.vmware:zdc-dhcp-0-c-29-d6-4b-f1-5bcf9254"
        ],
        "virtualVolumeHostID": "564de1a4-9a99-da0f-8b7c-3a41dfd64bf1",
        "visibleProtocolEndpointIDs": [
          "5dd53da0-b9b7-43f9-9b7e-b41c2558e92b"
        ]
      }
    ]
  }
}
```

Neu seit Version

9.6

ListVirtualVolumes

Sie können das verwenden `ListVirtualVolumes` Methode zum Auflisten der virtuellen Volumes, die sich derzeit im System befinden. Mit dieser Methode können Sie alle virtuellen Volumes auflisten oder nur eine Teilmenge auflisten.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Details	Das Niveau der Details in der Antwort. Mögliche Werte: • Richtig: Fügen Sie weitere Details zu jedem VVol in der Antwort ein. • Falsch: Fügen Sie die Standarddetaile bene über jedes VVol in der Antwort ein.	boolesch	Falsch	Nein
Grenze	Die maximale Anzahl der virtuellen Volumes, die aufgelistet werden sollen.	Ganzzahl	10.000	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Rekursiv	Gibt an, ob Informationen zu den Kindern jedes VVol in der Antwort enthalten sind oder nicht. Mögliche Werte: • Wahr: Include Informationen über die Kinder jedes VVol in der Antwort. • Falsch: Nehmen Sie keine Informationen über die Kinder jedes VVol in die Antwort auf.	boolesch	Falsch	Nein
StartVirtualVolumeID	Die ID des virtuellen Volumes, bei dem die Liste in der Antwort gestartet werden soll.	UUIDType	Keine	Nein
VirtualVolumeIDs	Eine Liste der virtuellen Volume-IDs, für die Informationen abgerufen werden sollen. Wenn Sie diesen Parameter nicht angeben, gibt die Methode nur Informationen zu diesen virtuellen Volumes zurück.	VirtualVolumeID UUID-Array	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
NextVirtualVolumeID	Die ID des nächsten virtuellen Volumes in der Liste.	UUID

VirtuellesVolumes	Eine Liste von Objekten, die die virtuellen Volumes beschreiben, die sich derzeit im System befinden.	VirtualVolume Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListVirtualVolumes",
    "params": {
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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
      }
    ]
  }
}
```


Neu seit Version

9.6

ListVirtualVolumeTasks

Sie können das verwenden `ListVirtualVolumeTasks` Methode zum Abrufen einer Liste der Aufgaben für virtuelle Volumes im System.

Parameter

Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
VirtualVolumeTaskIDs	Eine Liste der Task-IDs für virtuelle Volumes, für die Informationen abgerufen werden sollen. Wenn Sie diesen Parameter nicht angeben, gibt die Methode Informationen zu allen Aufgaben des virtuellen Volumes zurück.	UUID-Array	Keine	Nein

Rückgabewert

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Aufgaben	Eine Liste von Objekten, die die Aufgaben von virtuellen Volumes im Cluster beschreiben	Aufgabe Array erledigen

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ListVirtualVolumeTasks",
    "params": {
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
      }
    ]
  }
}
```


Neu seit Version

9.6

ModifyStorageContainer

Sie können das verwenden `ModifyStorageContainer` Methode zum Ändern eines vorhandenen virtuellen Volume-Storage-Containers.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich

SpeicherkontainerID	Die eindeutige ID des zu ändernden virtuellen Volume-Speichercontainers.	UUID	Keine	Ja.
InitiatorSecret	Der neue Schlüssel für die CHAP-Authentifizierung für den Initiator.	Zeichenfolge	Keine	Nein
TargetSecret	Der neue Schlüssel zur CHAP-Authentifizierung für das Ziel.	Zeichenfolge	Keine	Nein

Rückgabewerte

Diese Methode hat den folgenden Rückgabewert:

Name	Beschreibung	Typ
Storage Container	Informationen über den neu erstellten Speicher-Container.	Storage Container

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "ModifyStorageContainer",
    "params": {
      "storageContainerID": "6c95e24f-9f0b-4793-affb-5a4bc6c3d7e1",
      "targetSecret": "O,IM;tOQdn9$JJ*8"
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
  "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"
    }
  }
}
```


Neu seit Version

9.6

Zugriffssteuerung

Die verfügbaren Element-API-Methoden variieren je nach Zugriffstyp.

Über die API sind Zugriffstypen verfügbar, die in der Element UI nicht verfügbar sind.

Konten

Für den Zugriffstyp „Accounts“ stehen folgende Methoden zur Verfügung:

AddAccount
GetAccountByID
ModifyAccount
GetAccountByName
Listenkonten
GetAccountEffizienz
RemoveAccount

Verwalter

Alle Methoden stehen dem Zugriffstyp des Administrators zur Verfügung.

ClusterAdmin

Die folgenden Methoden sind für den Zugriffstyp „Cluster-Admin“ verfügbar:

AddClusterAdmin
ListBackupTargets
AddInitiatorsToVolumeAccessGroup
ListBulkVolumeJobs
AddLdapClusterAdmin
ListenClusteradministratoren
AddVirtualNetwork
ListenClusterpaare
AddVirtualNetwork
ListNodeFiberChannelPortInfo
AddVolumeVolumeAccessGroup
ListBackupTargets
CloneMultipleVolumes
ListDriveHardware
CompleteClusterPairing
ListFiberChannelSessions
CompleteVolumePairing
ListFiberChannelPortInfo
CreateBackupTarget

ListenSnapshots
Erstellen Sie einen Zeitplan
ListeActivePairedVolumes
Erstellen von Snapshot
ModifyBackupTarget
CreateSupportBundle
ModifyClusterAdmin
CreateClusterSupportBundle
ModifyGroupSnapshot
CreateGroupSnapshot
ModifyClusterFullThreshold
CreateVolumeAccessGroup
ModifyVolumeAccessGroup
DeleteAllSupportBundles
ModifyVolumeAccessGroupLunAssignments
LöschSnapshot
ModifyVolumePair
DeleteGroupSnapshot
ModifyVirtualNetwork
DeleteVolumeAccessGroup
RemoveClusterAdmin
UnbeständigkeitVerverschlüsselungAttest

RemoveVolumePair
DisableLdapAuthentifizierung
RemoveVirtualNetwork
AbleSnmp
EntfernenVolumeFromVolumeAccessGroup
EnableVerschlüsselungAtZiel
RemoveInitiatorsFromVolumeAccessGroup
EnableLdapAuthentifizierung
RollbackToSnapshot
EnableSnmp
RollbackToGroupSnapshot
GetBackupTarget
SetLoginSessionInfo
GetClusterFullThreshold
SetNtpInfo
GetClusterMasterNodeID
SetSnmpACL
VMware HardwareConfig
SetSnmpInfo
GetLdapConfiguration
SetSnmpTrapInfo
GetLoginSessionInfo

SetRemoteLoggingHosts
GetNtpInfo
Herunterfahren
GetNvramInfo
StartBulkVolumeRead
GetRawStats
StartBulkVolumeWrite
GetSnmpACL
StartClusterPairing
GetVolumeAccessGroupEffizienz
StartVolumePairing
GetVolumeAccessLunAssignments
TestLdapAuthentifizierung
GetVirtualNetwork

Laufwerke

Für den Laufwerkszugriffstyp stehen folgende Methoden zur Verfügung:

ListenLaufwerke
RemoveDrives
AddDrives
SecureEraseDrives

Knoten

Die folgenden Methoden sind für den Node-Zugriffstyp verfügbar:

AddNodes
ListenPendingKnoten
ListenActiveNodes
RemoveNodes

Lesen

Die folgenden Methoden sind für den Lesetyp verfügbar:

GetAccountByID
ListenKloneJobs
GetAccountByName
ListDeletedVolumes
GetAsyncResult
ListDriveHardware
GetClusterCapacity
ListenLaufwerke
GetDefaultQoS
ListEvents
GetDriveStats
ListISSessions
GetSoftwareUpgrade
ListenPendingKnoten
GetVolumeStats
ListSyncJobs

Listenkonten
ListVolumeAccessGroups
ListenActiveNodes
ListVolumeStatsByKonto
ListenActiveNodes
ListVolumeStatsByVolume
ListeActiveVolumes
ListVolumeStatsByVolumeAccessGroup
ListenAllNodes
ListVolumesForAccount
ListBackupTargets

Berichterstellung

Für den Zugriffstyp Berichterstellung sind folgende Methoden verfügbar:

ClearClusterStandards
GetVolumeEffizienz
GetAccountEffizienz
GetVolumeStats
GetClusterCapacity
ListenKloneJobs
GetClusterHardware-Informationen
ListenClusterstandards
GetClusterInfo

ListenClusterpaare
GetClusterMasterNodeID
ListDriveHardware
GetClusterStats
ListEvents
GetDriveHardwareInfo
ListISSessions
GetDriveStats
ListSchedules
GetNetworkConfig
ListServices
GetNodeHardwareInfo
ListSyncJobs
GetNodeStats
ListVirtualNetworks
GetSnmpInfo
ListVolumeStatsByKonto
GetSnmpTrapInfo
ListVolumeStatsByVolume
GetVolumeAccessGroupEffizienz
ListVolumeStatsByVolumeAccessGroup

Repositorys

Die Methode ListAllNodes steht dem Zugriffstyp Repositories zur Verfügung.

Volumes

Die folgenden Methoden stehen für den Zugriffstyp Volumes zur Verfügung:

CreateVolume
DeleteVolume
ModifyBackupTarget
KlonVolume
DeleteVolumePairing
ModifyVolumes
CloneMultipleVolumes
GetBackupTarget
ModifyVolumePair
CreateBackupTarget
GetDefaultQoS
PurgeDeletedVolume
Erstellen von Snapshot
ListeActiveVolumes
RemoveBackupTarget
CreateGroupSnapshot
ListBackupTarget
RemoveVolumePair
CompleteVolumePairing

ListenSnapshots
RestoreDeletedVolumen
CloneMultipleVolumes
ListVolumesForAccount
RollbackToGroupSnapshot
DeleteGroupSnapshot
ListDeletedVolumes
RollbackToSnapshot
LöschSnapshot
ListenSnapshots
StartBulkVolumeRead
StartBulkVolumeWrite
StartVolumePairing
UpdateBulkVolumeStatus

Schreiben

Für den Schreibzugriffstyp stehen folgende Methoden zur Verfügung:

AddDrives
RemoveNodes
AddNodes
RemoveAccount
AddAccount
EntfernenVolumeFromVolumeAccessGroup

AddVolumeToVolumeAccessGroup
RemoveInitiatorsFromVolumeAccessGroup
AddInitiatorsToVolumeAccessGroup
DeleteVolumeAccessGroup
CreateVolumeAccessGroup
DeleteVolume
ModifyVolumeAccessGroup
RestoreDeletedVolumen
ModifyAccount
PurgeDeletedVolume
CreateVolume
UmfyVolume
KlonVolume
GetAsyncResult
RemoveDrives

Verwandte Informationen

"Informieren Sie sich über die in der Element UI verfügbaren Zugriffstypen"

Antwortbeispiele

Getconfig

Der `GetConfig` Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt. Aufgrund der Länge enthält die Antwort nur Informationen für einen Node des Clusters.

```
{
    "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
            }
        }
        }
    }
}
```

GetClusterHardware-Informationen

Der `GetClusterHardwareInfo` Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt.

```
{
 "id": null,
  "result": {
   "clusterHardwareInfo": {
     "drives": {
      "1": {
        "description": "ATA      Drive",
        "dev": "8:0",
        "devpath": "/dev/disk/by-id/scsi-SATA_VRFSD3400GNCVMT205121562-
part4",
        "driveSecurityAtMaximum": false,
        "driveSecurityFrozen": true,
        "driveSecurityLocked": false,
        "logicalname": "/dev/sda",
        "product": "VRFSD3400GNCVMTJS1",
        "securityFeatureEnabled": false,
        "securityFeatureSupported": true,
        "serial": "205121562",
        "size": 299988156416,
        "uuid": "febe39ae-4984-edc0-e3a7-3c47608cface",
        "version": "515ABBF0"
      },
      "2": {...
      },
      "3": {...
      },
      "4": {...
      },
      "5": {...
```

```
      },
      "6": {...
      },
         .
         .
         .
    "44": {...
      }
      },
"nodes":{
  "1":{                        Storage Node
    "core_DMI:0200": {
    "description": "Motherboard",
    "physid": "0",
    "vendor": "SolidFire"
  },
    "fiber:0_PCI:0000:04:00.0": {
      "businfo": "pci@0000:04:00.0",
      "clock": "33000000",
      "description": "Fibre Channel",
      "physid": "0",
      "product": "ISP8324-based 16Gb Fibre Channel to PCI Express
Adapter",
      "vendor": "QLogic Corp.",
      "version": "02",
      "width": "64"
  },
    "Repeat fiber information": {...}
    "Repeat fiber": {...},
    "Repeat fiber": {...},
   }
 },
   "fans": {
     "Fan1A RPM": {
     "baseUnit": "RPM",
     "threshold": 840,
     "value": 4800
 },
     "Fan1B RPM": {...},
         .
         .
         .
     "Fan7B RPM": {...
     },
     "fibreChannelPorts": [
       {
```

```
        "firmware": "7.04.00 (d0d5)",
        "hbaPort": 1,
        "model": "QLE2672",
        "nPortID": "0x110c36",
        "pciSlot": 3,
        "serial": "BFE1341E09329",
        "speed": "8 Gbit",
        "state": "Online",
        "switchWwn": "20:01:00:2a:6a:a0:25:01",
        "wwnn": "5f:47:ac:c8:82:23:e0:00",
        "wwpn": "5f:47:ac:c0:82:23:e0:02"
      },
      {
        "firmware": "7.04.00 (d0d5)", {...}
        "firmware": "7.04.00 (d0d5)", {...}
        "firmware": "7.04.00 (d0d5)", {...}
      }
    ],
    "hardwareConfig": {
      "BIOS_REVISION": {
        "Passed": true,
        "actual": "1.1",
        "comparator": ">=",
        "expected": "1.0"
      },
      "BIOS_VENDOR": {
        "Passed": true,
        "actual": "SolidFire",
        "comparator": "==",
        "expected": "SolidFire"
      },
      "BIOS_VERSION": {
        "Passed": true,
        "actual": "1.1.2",
        "comparator": ">=",
        "expected": "1.1.2"
      },
      "BMC_FIRMWARE_REVISION": {
        "Passed": true,
        "actual": "1.6",
        "comparator": ">=",
        "expected": "1.6"
      },
      "BMC_IPMI_VERSION": {
        "Passed": true,
        "actual": "2.0",
```

```
 "comparator": ">=",
 "expected": "2.0"
},
"CHASSIS_TYPE": {
 "Passed": true,
 "actual": "R620",
 "comparator": "==",
 "expected": "R620"
},
"CPU_CORES_00": {
 "Passed": true,
 "actual": "6",
 "comparator": "==",
 "expected": "6"
},
"CPU_CORES_01": {
 "Passed": true,
 "actual": "6",
 "comparator": "==",
 "expected": "6"
},
"CPU_CORES_ENABLED_00": {
 "Passed": true,
 "actual": "6",
 "comparator": "==",
 "expected": "6"
},
"CPU_CORES_ENABLED_01": {
 "Passed": true,
 "actual": "6",
 "comparator": "==",
 "expected": "6"
},
"CPU_MODEL_00": {
 "Passed": true,
 "actual": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
 "comparator": "==",
 "expected": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz"
},
"CPU_MODEL_01": {
 "Passed": true,
 "actual": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
 "comparator": "==",
 "expected": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz"
},
"CPU_THREADS_00": {
```

```
        "Passed": true,
        "actual": "12",
        "comparator": "==",
        "expected": "12"
      },
      "CPU_THREADS_01": {
        "Passed": true,
        "actual": "12",
        "comparator": "==",
        "expected": "12"
      },
      "DRIVE_SIZE_BYTES_SDIMM0": {
        "Passed": true,
        "actual": "100030242816",
        "comparator": ">=",
        "expected": "100030242816"
      },
      "FIBRE_CHANNEL_FIRMWARE_REVISION": {
        "Passed": true,
        "actual": "FW:v7.04.00",
        "comparator": "==",
        "expected": "FW:v7.04.00"
      },
      "FIBRE_CHANNEL_MODEL": {
        "Passed": true,
        "actual": "QLE2672",
        "comparator": "==",
        "expected": "QLE2672"
      },
      "IDRAC_VERSION": {
        "Passed": true,
        "actual": "1.06.06",
        "comparator": ">=",
        "expected": "1.06.06"
      },
      "LIFECYCLE_VERSION": {
        "Passed": true,
        "actual": "1.0.0.5747",
        "comparator": ">=",
        "expected": "1.0.0.5747"
      },
      "MEMORY_GB": {
        "Passed": true,
        "actual": "32",
        "comparator": ">=",
        "expected": "32"
```

```
        },
        "MEMORY_MHZ_00": {
         "Passed": true,
         "actual": "1333",
         "comparator": ">=",
         "expected": "1333"
        },
        "MEMORY_MHZ_01": {
         "Passed": true,
         "actual": "1333",
         "comparator": ">=",
         "expected": "1333"
        },
        "MEMORY_MHZ_02": {
        "Passed": true,
        "actual": "1333",
        "comparator": ">=",
        "expected": "1333"
       },
       "MEMORY_MHZ_03": {
        "Passed": true,
        "actual": "1333",
        "comparator": ">=",
        "expected": "1333"
       },
       "NETWORK_DRIVER_ETH0": {
        "Passed": true,
        "actual": "bnx2x",
        "comparator": "=~",
        "expected": "^bnx2x$"
       },
       {
        "NETWORK_DRIVER_ETH1":, {...
       },
        "NETWORK_DRIVER_ETH2":, {...
       },
        "NETWORK_DRIVER_ETH3":, {...
       },
        "NETWORK_DRIVER_ETH4":, {...
       },
        "NETWORK_DRIVER_ETH5":, {...
       },
        "NODE_TYPE": {
        "Passed": true,
        "actual": "FC0025",
        "comparator": "==",
```

```
 "expected": "FC0025"
},
"NUM_CPU": {
 "Passed": true,
 "actual": "2",
 "comparator": "==",
 "expected": "2"
},
"NUM_DRIVES": {
 "Passed": true,
 "actual": "0",
 "comparator": "==",
 "expected": "0"
},
"NUM_DRIVES_INTERNAL": {
 "Passed": true,
 "actual": "1",
 "comparator": "==",
 "expected": "1"
},
"NUM_FIBRE_CHANNEL_PORTS": {
 "Passed": true,
 "actual": "4",
 "comparator": "==",
 "expected": "4"
},
"NVRAM_VENDOR": {
 "Passed": true,
 "actual": "",
 "comparator": "==",
 "expected": ""
},
"ROOT_DRIVE_REMOVABLE": {
 "Passed": true,
 "actual": "false",
 "comparator": "==",
 "expected": "false"
}
},
"memory": {
  "firmware_": {
   "capacity": "8323072",
   "date": "03/08/2012",
   "description": "BIOS",
   "physid": "0",
   "size": "65536",
```

```
        "vendor": "SolidFire",
        "version": "1.1.2"
      },
      "memory_DMI:1000": {
        "description": "System Memory",
        "physid": "1000",
        "size": "34359738368",
        "slot": "System board or motherboard"
      }
      },
      "network": {
       "network:0_PCI:0000:01:00.0": {
        "businfo": "pci@0000:01:00.0",
        "capacity": "1000000000",
        "clock": "33000000",
        "description": "Ethernet interface",
        "logicalname": "eth0",
        "physid": "0",
        "product": "NetXtreme II BCM57800 1/10 Gigabit Ethernet",
        "serial": "c8:1f:66:e0:97:2a",
        "vendor": "Broadcom Corporation",
        "version": "10",
        "width": "64"
      },
       "network:0_PCI:0000:41:00.0": {...
      },
       "network:1_PCI:0000:01:00.1": {...
      },
       "network:1_PCI:0000:41:00.1": {...
      },
       "network:2_PCI:0000:01:00.2": {...
      },
       "network:3_PCI:0000:01:00.3": {...
      }
      },
      "networkInterfaces": {
       "Bond10G": {
        "isConfigured": true,
        "isUp": true
      },
      "Bond1G": {
       "isConfigured": true,
       "isUp": true
      },
      "eth0": {
       "isConfigured": true,
```

```
      "isUp": true
     },
     "eth1": {...
     },
     "eth2": {...
     },
     "eth3": {...
     },
     "eth4": {...
     },
     "eth5": {...
     }
    },
    "nvram": {
     "errors": {
      "numOfErrorLogEntries": "0"
     },
     "extended": {
      "dialogVersion": "4",
      "event": [
      {
       "name": "flushToFlash",
       "time": "2015-08-06 01:19:39",
       "value": "0"
      },
      {
       "name": "flushToFlash",
       "time": "2015-08-06 01:26:44",
       "value": "0"
      },
      {... next "flushToFlash"
      },
      {... next "flushToFlash"
      },
      {... next "flushToFlash"
      },
      {... next "flushToFlash"
      },
      {... next "flushToFlash"
      },
      {... next "flushToFlash"
      },
      {... next "flushToFlash"
      }
     ],
     "eventOccurrences": [
```

```
        {
          "count": "740",
          "name": "flushToFlash"
        },
        {
          "count": "1",
          "name": "excessiveCurrent"
        }
      ],
      "initialCapacitance": "6.630 F",
      "initialEsr": "0.101 Ohm",
      "measurement": [
       {
         "level_0": " 0",
         "level_1": " 3969",
         "level_2": " 4631",
         "level_3": " 12875097",
         "level_4": " 1789948",
         "level_5": " 0",
         "level_6": " 0",
         "level_7": " 0",
         "level_8": " 0",
         "level_9": " 0",
         "name": "enterpriseFlashControllerTemperature",
         "recent": "66 C"
      },
      {
         "level_0": " 0",
         "level_1": " 58",
         "level_2": " 1479058",
         "level_3": " 12885356",
         "level_4": " 308293",
         "level_5": " 851",
         "level_6": " 29",
         "level_7": " 0",
         "level_8": " 0",
         "level_9": " 0",
         "name": "capacitor1And2Temperature",
         "recent": "30.69 C"
      },
      {...next temp measurement
      },
      {...next temp measurement
      },
      {...next temp measurement
      },
```

```
      }
       "name": "voltageOfCapacitor1",
       "recent": "2.198 V"
      },
      {
       "name": "voltageOfCapacitor2",
       "recent": "2.181 V"
      },
      {
       "name": "voltageOfCapacitor3",
       "recent": "2.189 V"
      },
      {
       "name": "voltageOfCapacitor4",
       "recent": "2.195 V"
      },
      {
       "level_0": " 4442034",
       "level_1": " 6800018",
       "level_2": " 2846869",
       "level_3": " 119140",
       "level_4": " 29506",
       "level_5": " 428935",
       "level_6": " 7143",
       "level_7": " 0",
       "level_8": " 0",
       "level_9": " 0",
       "name": "capacitorPackVoltage",
       "recent": "8.763 V"
      },
      {
       "level_0": " 0",
       "level_1": " 0",
       "level_2": " 0",
       "level_3": " 0",
       "level_4": " 189",
       "level_5": " 17",
       "level_6": " 36",
       "level_7": " 0",
       "level_8": " 2",
       "level_9": " 490",
       "name": "capacitorPackVoltageAtEndOfFlushToFlash",
       "recent": "4.636 V"
      },
      {
       "name": "currentDerivedFromV3V4",
```

```
        "recent": "-0.004 A"
       },
       {
        "level_0": " 230",
        "level_1": " 482",
        "level_2": " 22",
        "level_3": " 0",
        "level_4": " 0",
        "level_5": " 0",
        "level_6": " 0",
        "level_7": " 0",
        "level_8": " 0",
        "level_9": " 0",
        "name": "derivedEnergy",
        "recent": "172 Joules"
       },
       {...next voltage measurement
       },
       {...next voltage measurement
       },
       {...next voltage measurement
       },
     ],
     "smartCounters": [
       {
        "name": "numberOf512ByteBlocksReadFromDdr",
        "value": "10530088847"
       },
       {
        "name": "numberOf512ByteBlocksWrittenToDdr",
        "value": "1752499453837"
       },
       {
        "name": "numberOfHostReadCommands",
        "value": "235317769"
       },
       {...next smartCounters measurement
       },
       {...next smartCounters measurement
       },
       {...next smartCounters measurement
       },
     ],
     "snapshotTime": "2015-08-20 16:30:01"
    },
    "firmware": {
```

```
    "activeSlotNumber": "2",
    "slot1Version": "1e5817bc",
    "slot2Version": "5fb7565c",
    "slot3Version": "1e5817bc",
    "slot4Version": "1e5817bc"
  },
  "identify": {
    "firmwareVersion": "5fb7565c on slot 2",
    "hardwareRevision": "B04",
    "modelNumber": "RMS-200",
    "serialNumber": "0000862"
  },
  "smart": {
    "availableSpace": "0%",
    "availableSpaceThreshold": "0%",
    "controllerBusyTimeMinutes": "6793",
    "criticalErrorVector": "0x0",
    "mediaErrors": "0",
    "numberOf512ByteBlocksRead": "10530088847",
    "numberOf512ByteBlocksWritten": "1752499439063",
    "numberOfErrorInfoLogs": "1",
    "numberOfHostReadCommands": "235317769",
    "numberOfHostWriteCommands": "126030374065",
    "numberOfPowerCycles": "709",
    "powerOnHours": "11223",
    "temperature": "324 Kelvin",
    "unsafeShutdowns": "357"
     }
     },
     "origin": null,
     "platform": {
      "chassisType": "R620",
      "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
      "nodeMemoryGB": 32,
      "nodeType": "FC0025"
     },
     "powerSupplies": {
      "PS1 status": {
       "powerSupplyFailureDetected": false,
       "powerSupplyHasAC": true,
       "powerSupplyPredictiveFailureDetected": false,
       "powerSupplyPresent": true,
       "powerSupplyPresentLastCheck": true
     },
      "PS2 status": {
       "powerSupplyFailureDetected": false,
```

```
        "powerSupplyHasAC": true,
        "powerSupplyPredictiveFailureDetected": false,
        "powerSupplyPresent": true,
        "powerSupplyPresentLastCheck": true
      }
      },
      "storage": {
       "storage_PCI:0000:00:1f.2": {
        "businfo": "pci@0000:00:1f.2",
        "clock": "66000000",
        "description": "SATA controller",
        "physid": "1f.2",
        "product": "C600/X79 series chipset 6-Port SATA AHCI Controller",
        "vendor": "Intel Corporation",
        "version": "05",
        "width": "32"
      }
      },
      "system": {
       "ubuntu_DMI:0100": {
        "description": "Rack Mount Chassis",
        "product": "SFx010 ()",
        "serial": "HTW1DZ1",
        "vendor": "SolidFire",
        "width": "64"
      }
      },
      "temperatures": {
       "Exhaust Temp": {
        "baseUnit": "C",
        "threshold": 70,
        "value": 41
      },
      "Inlet Temp": {
       "baseUnit": "C",
       "threshold": 42,
       "value": 18
      }
      },
      "uuid": "4C4C4544-0054-5710-8031-C8C04F445A31"
    },
  "2": {...},                    Storage Node "2"
  "3": {...},                    Storage Node "3"
  "4": {...},                    Storage Node "4"
  "5": {                       Fibre Channel Node
       }
```

```
      }
    }
  }
```

GetLldpInfo

Der `GetLldpInfo` Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt.

```
{
  "id": null,
  "result": {
    "lldpInfo": {
        "lldpChassis": {
        "local-chassis": [
        {
          "chassis": [
            {
              "capability": [
                {
                  "enabled": false,
                  "type": "Bridge"
                },
                {
                  "enabled": false,
                  "type": "Router"
                },
                {
                  "enabled": false,
                  "type": "Wlan"
                },
                {
                  "enabled": true,
                  "type": "Station"
                }
              ],
              "descr": [
                {
                  "value": "Element OS 11.0"
                }
              ],
              "id": [
                {
                  "type": "mac",
                  "value": "08:00:27:3c:0a:f4"
                }
```

```
            ],
            "mgmt-ip": [
              {
                "value": "10.0.2.15"
              },
              {
                "value": "fe80::a00:27ff:fe3c:af4"
              }
            ],
            "name": [
              {
                "value": "SF-93FF"
              }
            ]
          }
        ],
        "lldp-med": [
          {
            "capability": [
              {
                "available": true,
                "type": "Capabilities"
              },
              {
                "available": true,
                "type": "Policy"
              },
              {
                "available": true,
                "type": "Location"
              },
              {
                "available": true,
                "type": "MDI/PSE"
              },
              {
                "available": true,
                "type": "MDI/PD"
              },
              {
                "available": true,
                "type": "Inventory"
              }
            ],
            "device-type": [
              {
```

```
                "value": "Generic Endpoint (Class I)"
              }
            ],
            "inventory": [
              {
                "firmware": [
                  {
                    "value": "VirtualBox"
                  }
                ],
                "hardware": [
                  {
                    "value": "1.2"
                  }
                ],
                "manufacturer": [
                  {
                    "value": "innotek GmbH"
                  }
                ],
                "model": [
                  {
                    "value": "VirtualBox"
                  }
                ],
                "serial": [
                  {
                    "value": "0"
                  }
                ],
                "software": [
                  {
                    "value": "4.14.27-solidfire2"
                  }
                ]
              }
            ]
          }
        ]
      }
    ]
  },
  "lldpInterfaces": {
    "lldp": [
      {
        "interface": [
```

```
            {
              "age": "0 day, 00:01:04",
              "chassis": [
                {
                  "capability": [
                    {
                      "enabled": false,
                      "type": "Bridge"
                    },
                    {
                      "enabled": false,
                      "type": "Router"
                    },
                    {
                      "enabled": false,
                      "type": "Wlan"
                    },
                    {
                      "enabled": true,
                      "type": "Station"
                    }
                  ],
                  "descr": [
                    {
                      "value": "Element OS 11.0"
                    }
                  ],
                  "id": [
                    {
                      "type": "mac",
                      "value": "08:00:27:3c:0a:f4"
                    }
                  ],
                  "mgmt-ip": [
                    {
                      "value": "10.0.2.15"
                    },
                    {
                      "value": "fe80::a00:27ff:fe3c:af4"
                    }
                  ],
                  "name": [
                    {
                      "value": "SF-93FF"
                    }
                  ]
```

```
        }
      ],
      "lldp-med": [
        {
          "capability": [
            {
              "available": true,
              "type": "Capabilities"
            },
            {
              "available": true,
              "type": "Policy"
            },
            {
              "available": true,
              "type": "Location"
            },
            {
              "available": true,
              "type": "MDI/PSE"
            },
            {
              "available": true,
              "type": "MDI/PD"
            },
            {
              "available": true,
              "type": "Inventory"
            }
          ],
          "device-type": [
            {
              "value": "Generic Endpoint (Class I)"
            }
          ],
          "inventory": [
            {
              "firmware": [
                {
                  "value": "VirtualBox"
                }
              ],
              "hardware": [
                {
                  "value": "1.2"
                }
```

```
                    ],
                    "manufacturer": [
                      {
                        "value": "innotek GmbH"
                      }
                    ],
                    "model": [
                      {
                        "value": "VirtualBox"
                      }
                    ],
                    "serial": [
                      {
                        "value": "0"
                      }
                    ],
                    "software": [
                      {
                        "value": "4.14.27-solidfire2"
                      }
                    ]
                  }
                ]
              }
            ],
            "name": "eth0",
            "port": [
              {
                "aggregation": [
                  {
                    "value": "7"
                  }
                ],
                "auto-negotiation": [
                  {
                    "advertised": [
                      {
                        "fd": true,
                        "hd": true,
                        "type": "10Base-T"
                      },
                      {
                        "fd": true,
                        "hd": true,
                        "type": "100Base-TX"
                      },
```

```
                    {
                      "fd": true,
                      "hd": false,
                      "type": "1000Base-T"
                    }
                  ],
                  "current": [
                    {
                      "value": "full duplex mode"
                    }
                  ],
                  "enabled": true,
                  "supported": true
                }
              ],
              "descr": [
                {
                  "value": "eth0"
                }
              ],
              "id": [
                {
                  "type": "mac",
                  "value": "08:00:27:3c:0a:f4"
                }
              ]
            }
          ],
          "ttl": [
            {
              "ttl": "120"
            }
          ],
          "via": "unknown"
        },
        {
          "age": "17722 days, 17:14:28",
          "chassis": [
            {
              "capability": [
                {
                  "enabled": false,
                  "type": "Bridge"
                },
                {
                  "enabled": false,
```

```
                "type": "Router"
              },
              {
                "enabled": false,
                "type": "Wlan"
              },
              {
                "enabled": true,
                "type": "Station"
              }
            ],
            "descr": [
              {
                "value": "Element OS 11.0"
              }
            ],
            "id": [
              {
                "type": "mac",
                "value": "08:00:27:3c:0a:f4"
              }
            ],
            "mgmt-ip": [
              {
                "value": "10.0.2.15"
              },
              {
                "value": "fe80::a00:27ff:fe3c:af4"
              }
            ],
            "name": [
              {
                "value": "SF-93FF"
              }
            ]
          }
        ],
        "lldp-med": [
          {
            "capability": [
              {
                "available": true,
                "type": "Capabilities"
              },
              {
                "available": true,
```

```
        "type": "Policy"
      },
      {
        "available": true,
        "type": "Location"
      },
      {
        "available": true,
        "type": "MDI/PSE"
      },
      {
        "available": true,
        "type": "MDI/PD"
      },
      {
        "available": true,
        "type": "Inventory"
      }
    ],
    "device-type": [
      {
        "value": "Generic Endpoint (Class I)"
      }
    ],
    "inventory": [
      {
        "firmware": [
          {
            "value": "VirtualBox"
          }
        ],
        "hardware": [
          {
            "value": "1.2"
          }
        ],
        "manufacturer": [
          {
            "value": "innotek GmbH"
          }
        ],
        "model": [
          {
            "value": "VirtualBox"
          }
        ],
```

```
                    "serial": [
                      {
                        "value": "0"
                      }
                    ],
                    "software": [
                      {
                        "value": "4.14.27-solidfire2"
                      }
                    ]
                  }
                ]
              }
            ],
            "name": "eth1",
            "port": [
              {
                "aggregation": [
                  {
                    "value": "7"
                  }
                ],
                "auto-negotiation": [
                  {
                    "advertised": [
                      {
                        "fd": true,
                        "hd": true,
                        "type": "10Base-T"
                      },
                      {
                        "fd": true,
                        "hd": true,
                        "type": "100Base-TX"
                      },
                      {
                        "fd": true,
                        "hd": false,
                        "type": "1000Base-T"
                      }
                    ],
                    "current": [
                      {
                        "value": "unknown"
                      }
                    ],
```

```
                "enabled": true,
                "supported": true
              }
            ],
            "descr": [
              {
                "value": "eth1"
              }
            ],
            "id": [
              {
                "type": "mac",
                "value": "08:00:27:36:79:78"
              }
            ]
          }
        ],
        "ttl": [
          {
            "ttl": "120"
          }
        ],
        "via": "unknown"
      },
      {
        "age": "0 day, 00:01:01",
        "chassis": [
          {
            "capability": [
              {
                "enabled": false,
                "type": "Bridge"
              },
              {
                "enabled": false,
                "type": "Router"
              },
              {
                "enabled": false,
                "type": "Wlan"
              },
              {
                "enabled": true,
                "type": "Station"
              }
            ],
```

```
            "descr": [
              {
                "value": "Element OS 11.0"
              }
            ],
            "id": [
              {
                "type": "mac",
                "value": "08:00:27:3c:0a:f4"
              }
            ],
            "mgmt-ip": [
              {
                "value": "10.0.2.15"
              },
              {
                "value": "fe80::a00:27ff:fe3c:af4"
              }
            ],
            "name": [
              {
                "value": "SF-93FF"
              }
            ]
          }
        ],
        "lldp-med": [
          {
            "capability": [
              {
                "available": true,
                "type": "Capabilities"
              },
              {
                "available": true,
                "type": "Policy"
              },
              {
                "available": true,
                "type": "Location"
              },
              {
                "available": true,
                "type": "MDI/PSE"
              },
              {
```

```
                    "available": true,
                    "type": "MDI/PD"
                  },
                  {
                    "available": true,
                    "type": "Inventory"
                  }
                ],
                "device-type": [
                  {
                    "value": "Generic Endpoint (Class I)"
                  }
                ],
                "inventory": [
                  {
                    "firmware": [
                      {
                        "value": "VirtualBox"
                      }
                    ],
                    "hardware": [
                      {
                        "value": "1.2"
                      }
                    ],
                    "manufacturer": [
                      {
                        "value": "innotek GmbH"
                      }
                    ],
                    "model": [
                      {
                        "value": "VirtualBox"
                      }
                    ],
                    "serial": [
                      {
                        "value": "0"
                      }
                    ],
                    "software": [
                      {
                        "value": "4.14.27-solidfire2"
                      }
                    ]
                  }
```

```
            ]
          }
        ],
        "name": "eth2",
        "port": [
          {
            "aggregation": [
              {
                "value": "6"
              }
            ],
            "auto-negotiation": [
              {
                "advertised": [
                  {
                    "fd": true,
                    "hd": true,
                    "type": "10Base-T"
                  },
                  {
                    "fd": true,
                    "hd": true,
                    "type": "100Base-TX"
                  },
                  {
                    "fd": true,
                    "hd": false,
                    "type": "1000Base-T"
                  }
                ],
                "current": [
                  {
                    "value": "full duplex mode"
                  }
                ],
                "enabled": true,
                "supported": true
              }
            ],
            "descr": [
              {
                "value": "eth2"
              }
            ],
            "id": [
              {
```

```
                "type": "mac",
                "value": "08:00:27:fc:f0:a9"
              }
            ]
          }
        ],
        "ttl": [
          {
            "ttl": "120"
          }
        ],
        "via": "LLDP"
      },
      {
        "age": "0 day, 00:01:01",
        "chassis": [
          {
            "capability": [
              {
                "enabled": false,
                "type": "Bridge"
              },
              {
                "enabled": false,
                "type": "Router"
              },
              {
                "enabled": false,
                "type": "Wlan"
              },
              {
                "enabled": true,
                "type": "Station"
              }
            ],
            "descr": [
              {
                "value": "Element OS 11.0"
              }
            ],
            "id": [
              {
                "type": "mac",
                "value": "08:00:27:3c:0a:f4"
              }
            ],
```

```
            "mgmt-ip": [
              {
                "value": "10.0.2.15"
              },
              {
                "value": "fe80::a00:27ff:fe3c:af4"
              }
            ],
            "name": [
              {
                "value": "SF-93FF"
              }
            ]
          }
        ],
        "lldp-med": [
          {
            "capability": [
              {
                "available": true,
                "type": "Capabilities"
              },
              {
                "available": true,
                "type": "Policy"
              },
              {
                "available": true,
                "type": "Location"
              },
              {
                "available": true,
                "type": "MDI/PSE"
              },
              {
                "available": true,
                "type": "MDI/PD"
              },
              {
                "available": true,
                "type": "Inventory"
              }
            ],
            "device-type": [
              {
                "value": "Generic Endpoint (Class I)"
```

```
          }
        ],
        "inventory": [
          {
            "firmware": [
              {
                "value": "VirtualBox"
              }
            ],
            "hardware": [
              {
                "value": "1.2"
              }
            ],
            "manufacturer": [
              {
                "value": "innotek GmbH"
              }
            ],
            "model": [
              {
                "value": "VirtualBox"
              }
            ],
            "serial": [
              {
                "value": "0"
              }
            ],
            "software": [
              {
                "value": "4.14.27-solidfire2"
              }
            ]
          }
        ]
      }
    ],
    "name": "eth3",
    "port": [
      {
        "aggregation": [
          {
            "value": "6"
          }
        ],
```

```
            "auto-negotiation": [
              {
                "advertised": [
                  {
                    "fd": true,
                    "hd": true,
                    "type": "10Base-T"
                  },
                  {
                    "fd": true,
                    "hd": true,
                    "type": "100Base-TX"
                  },
                  {
                    "fd": true,
                    "hd": false,
                    "type": "1000Base-T"
                  }
                ],
                "current": [
                  {
                    "value": "full duplex mode"
                  }
                ],
                "enabled": true,
                "supported": true
              }
            ],
            "descr": [
              {
                "value": "eth3"
              }
            ],
            "id": [
              {
                "type": "mac",
                "value": "08:00:27:2c:e4:f8"
              }
            ]
          }
        ],
        "ttl": [
          {
            "ttl": "120"
          }
        ],
```

```
            "via": "LLDP"
          }
        ]
      }
    ]
  },
  "lldpNeighbors": {
    "lldp": [
      {
        "interface": [
          {
            "age": "0 day, 00:04:34",
            "chassis": [
              {
                "capability": [
                  {
                    "enabled": true,
                    "type": "Bridge"
                  },
                  {
                    "enabled": true,
                    "type": "Router"
                  },
                  {
                    "enabled": true,
                    "type": "Wlan"
                  },
                  {
                    "enabled": false,
                    "type": "Station"
                  }
                ],
                "descr": [
                  {
                    "value": "x86_64"
                  }
                ],
                "id": [
                  {
                    "type": "mac",
                    "value": "50:7b:9d:2b:36:84"
                  }
                ],
                "mgmt-ip": [
                  {
                    "value": "192.168.100.1"
```

```
            },
            {
              "value": "fe80::a58e:843:952e:d8eb"
            }
          ],
          "name": [
            {
              "value": "ConventionalWisdom.wlan.netapp.com"
            }
          ]
        }
      ],
      "name": "eth2",
      "port": [
        {
          "auto-negotiation": [
            {
              "current": [
                {
                  "value": "full duplex mode"
                }
              ],
              "enabled": false,
              "supported": false
            }
          ],
          "descr": [
            {
              "value": "vboxnet1"
            }
          ],
          "id": [
            {
              "type": "mac",
              "value": "0a:00:27:00:00:01"
            }
          ],
          "ttl": [
            {
              "value": "120"
            }
          ]
        }
      ],
      "rid": "2",
      "via": "LLDP"
```

```
        },
        {
          "age": "0 day, 00:01:01",
          "chassis": [
            {
              "capability": [
                {
                  "enabled": false,
                  "type": "Bridge"
                },
                {
                  "enabled": false,
                  "type": "Router"
                },
                {
                  "enabled": false,
                  "type": "Wlan"
                },
                {
                  "enabled": true,
                  "type": "Station"
                }
              ],
              "descr": [
                {
                  "value": "Element OS 11.0"
                }
              ],
              "id": [
                {
                  "type": "mac",
                  "value": "08:00:27:3c:0a:f4"
                }
              ],
              "mgmt-ip": [
                {
                  "value": "10.0.2.15"
                },
                {
                  "value": "fe80::a00:27ff:fe3c:af4"
                }
              ],
              "name": [
                {
                  "value": "SF-93FF"
                }
```

```
            ]
          }
        ],
        "lldp-med": [
          {
            "capability": [
              {
                "available": true,
                "type": "Capabilities"
              },
              {
                "available": true,
                "type": "Policy"
              },
              {
                "available": true,
                "type": "Location"
              },
              {
                "available": true,
                "type": "MDI/PSE"
              },
              {
                "available": true,
                "type": "MDI/PD"
              },
              {
                "available": true,
                "type": "Inventory"
              }
            ],
            "device-type": [
              {
                "value": "Generic Endpoint (Class I)"
              }
            ],
            "inventory": [
              {
                "firmware": [
                  {
                    "value": "VirtualBox"
                  }
                ],
                "hardware": [
                  {
                    "value": "1.2"
```

```
                    }
                  ],
                  "manufacturer": [
                    {
                      "value": "innotek GmbH"
                    }
                  ],
                  "model": [
                    {
                      "value": "VirtualBox"
                    }
                  ],
                  "serial": [
                    {
                      "value": "0"
                    }
                  ],
                  "software": [
                    {
                      "value": "4.14.27-solidfire2"
                    }
                  ]
                }
              ]
            }
          ],
          "name": "eth2",
          "port": [
            {
              "aggregation": [
                {
                  "value": "6"
                }
              ],
              "auto-negotiation": [
                {
                  "advertised": [
                    {
                      "fd": true,
                      "hd": true,
                      "type": "10Base-T"
                    },
                    {
                      "fd": true,
                      "hd": true,
                      "type": "100Base-TX"
```

```
                    },
                    {
                      "fd": true,
                      "hd": false,
                      "type": "1000Base-T"
                    }
                  ],
                  "current": [
                    {
                      "value": "full duplex mode"
                    }
                  ],
                  "enabled": true,
                  "supported": true
                }
              ],
              "descr": [
                {
                  "value": "eth3"
                }
              ],
              "id": [
                {
                  "type": "mac",
                  "value": "08:00:27:2c:e4:f8"
                }
              ],
              "ttl": [
                {
                  "value": "120"
                }
              ]
            }
          ],
          "rid": "1",
          "via": "LLDP"
        },
        {
          "age": "0 day, 00:04:34",
          "chassis": [
            {
              "capability": [
                {
                  "enabled": true,
                  "type": "Bridge"
                },
```

```
            {
              "enabled": true,
              "type": "Router"
            },
            {
              "enabled": true,
              "type": "Wlan"
            },
            {
              "enabled": false,
              "type": "Station"
            }
          ],
          "descr": [
            {
              "value": "x86_64"
            }
          ],
          "id": [
            {
              "type": "mac",
              "value": "50:7b:9d:2b:36:84"
            }
          ],
          "mgmt-ip": [
            {
              "value": "192.168.100.1"
            },
            {
              "value": "fe80::a58e:843:952e:d8eb"
            }
          ],
          "name": [
            {
              "value": ""
            }
          ]
        }
      ],
      "name": "eth3",
      "port": [
        {
          "auto-negotiation": [
            {
              "current": [
                {
```

```
                    "value": "full duplex mode"
                  }
                ],
                "enabled": false,
                "supported": false
              }
            ],
            "descr": [
              {
                "value": "vboxnet1"
              }
            ],
            "id": [
              {
                "type": "mac",
                "value": "0a:00:27:00:00:01"
              }
            ],
            "ttl": [
              {
                "value": "120"
              }
            ]
          }
        ],
        "rid": "2",
        "via": "LLDP"
      },
      {
        "age": "0 day, 00:01:01",
        "chassis": [
          {
            "capability": [
              {
                "enabled": false,
                "type": "Bridge"
              },
              {
                "enabled": false,
                "type": "Router"
              },
              {
                "enabled": false,
                "type": "Wlan"
              },
              {
```

```
                    "enabled": true,
                    "type": "Station"
                  }
                ],
                "descr": [
                  {
                    "value": "Element OS 11.0"
                  }
                ],
                "id": [
                  {
                    "type": "mac",
                    "value": "08:00:27:3c:0a:f4"
                  }
                ],
                "mgmt-ip": [
                  {
                    "value": "10.0.2.15"
                  },
                  {
                    "value": "fe80::a00:27ff:fe3c:af4"
                  }
                ],
                "name": [
                  {
                    "value": "SF-93FF"
                  }
                ]
              }
            ],
            "lldp-med": [
              {
                "capability": [
                  {
                    "available": true,
                    "type": "Capabilities"
                  },
                  {
                    "available": true,
                    "type": "Policy"
                  },
                  {
                    "available": true,
                    "type": "Location"
                  },
                  {
```

```
          "available": true,
          "type": "MDI/PSE"
        },
        {
          "available": true,
          "type": "MDI/PD"
        },
        {
          "available": true,
          "type": "Inventory"
        }
      ],
      "device-type": [
        {
          "value": "Generic Endpoint (Class I)"
        }
      ],
      "inventory": [
        {
          "firmware": [
            {
              "value": "VirtualBox"
            }
          ],
          "hardware": [
            {
              "value": "1.2"
            }
          ],
          "manufacturer": [
            {
              "value": "innotek GmbH"
            }
          ],
          "model": [
            {
              "value": "VirtualBox"
            }
          ],
          "serial": [
            {
              "value": "0"
            }
          ],
          "software": [
            {
```

```
                    "value": "4.14.27-solidfire2"
                  }
                ]
              }
            ]
          }
        ],
        "name": "eth3",
        "port": [
          {
            "aggregation": [
              {
                "value": "6"
              }
            ],
            "auto-negotiation": [
              {
                "advertised": [
                  {
                    "fd": true,
                    "hd": true,
                    "type": "10Base-T"
                  },
                  {
                    "fd": true,
                    "hd": true,
                    "type": "100Base-TX"
                  },
                  {
                    "fd": true,
                    "hd": false,
                    "type": "1000Base-T"
                  }
                ],
                "current": [
                  {
                    "value": "1000BaseTFD"
                  }
                ],
                "enabled": true,
                "supported": true
              }
            ],
            "descr": [
              {
                "value": "eth2"
```

```
                    }
                  ],
                  "id": [
                    {
                      "type": "mac",
                      "value": "08:00:27:fc:f0:a9"
                    }
                  ],
                  "ttl": [
                    {
                      "value": "120"
                    }
                  ]
                }
              ],
              "rid": "1",
              "via": "LLDP"
            }
          ]
        }
      ]
    }
    }
 }
}
```

GetNetworkConfig

Der `GetNetworkConfig` Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt.

```
{
    "id": 1,
    "result": {
        "network": {
            "Bond10G": {
                "#default": false,
                "address": "10.1.1.0",
                "auto": true,
                "bond-downdelay": "0",
                "bond-fail_over_mac": "None",
                "bond-miimon": "100",
                "bond-mode": "ActivePassive",
                "bond-primary_reselect": "Failure",
                "bond-slaves": "eth0 eth1",
```

```
                "bond-updelay": "200",
                "dns-nameservers": "10.1.1.0, 10.1.1.0",
                "dns-search": "ten.test.company.net., company.net.",
                "family": "inet",
                "gateway": "10.1.1.0",
                "linkSpeed": 10000,
                "macAddress": "c8:1f:66:ee:59:b9",
                "macAddressPermanent": "00:00:00:00:00:00",
                "method": "static",
                "mtu": "9000",
                "netmask": "255.255.240.0",
                "network": "10.1.1.0",
                "physical": {
                    "address": "10.1.1.0",
                    "macAddress": "c8:1f:66:ee:59:b9",
                    "macAddressPermanent": "00:00:00:00:00:00",
                    "mtu": "9000",
                    "netmask": "255.255.240.0",
                    "network": "10.1.1.0",
                    "upAndRunning": true
                },
                "routes": [],
                "status": "UpAndRunning",
                "symmetricRouteRules": [
                    "ip route add 10.1.1.1/20 dev Bond1G src 10.1.2.2
table Bond1G",
                    "ip rule add from 10.1.1.1 table Bond1G",
                    "ip route add default via 10.1.1.254"
                ],
                "upAndRunning": true,
                "virtualNetworkTag": "0"
            },
            "Bond1G": {
                "#default": true,
                "address": "10.1.1.0",
                "addressV6": "",
                "auto": true,
                "bond-downdelay": "0",
                "bond-fail_over_mac": "None",
                "bond-miimon": "100",
                "bond-mode": "ActivePassive",
                "bond-primary_reselect": "Failure",
                "bond-slaves": "eth2 eth3",
                "bond-updelay": "200",
                "dns-nameservers": "10.1.1.0, 10.1.1.0",
                "dns-search": "ten.test.company.net., company.net.",
```

```
                "family": "inet",
                "gateway": "10.1.1.254",
                "gatewayV6": "",
                "linkSpeed": 1000,
                "macAddress": "c8:1f:66:ee:59:bd",
                "macAddressPermanent": "00:00:00:00:00:00",
                "method": "static",
                "mtu": "1500",
                "netmask": "255.255.240.0",
                "network": "10.1.1.0",
                "physical": {
                    "address": "10.1.1.0",
                    "macAddress": "c8:1f:66:ee:59:bd",
                    "macAddressPermanent": "00:00:00:00:00:00",
                    "mtu": "1500",
                    "netmask": "255.255.240.0",
                    "network": "10.1.1.0",
                    "upAndRunning": true
                },
                "routes": [],
                "status": "UpAndRunning",
                "symmetricRouteRules": [
                    "ip route add 10.1.1.1/20 dev Bond1G src 10.1.2.2
table Bond1G",
                    "ip rule add from 10.1.1.1 table Bond1G",
                    "ip route add default via 10.1.1.254"
                ],
                "upAndRunning": true,
                "virtualNetworkTag": "0"
            },
            "eth0": {
                "auto": true,
                "bond-master": "Bond10G",
                "family": "inet",
                "linkSpeed": 10000,
                "macAddress": "c8:1f:66:ee:59:b9",
                "macAddressPermanent": "c8:1f:66:ee:59:b9",
                "method": "bond",
                "physical": {
                    "address": "0.0.0.0",
                    "macAddress": "c8:1f:66:ee:59:b9",
                    "macAddressPermanent": "c8:1f:66:ee:59:b9",
                    "netmask": "N/A",
                    "network": "N/A",
                    "upAndRunning": true
                },
```

```
            "status": "UpAndRunning",
            "upAndRunning": true
        },
        "eth1": {
            "auto": true,
            "bond-master": "Bond10G",
            "family": "inet",
            "linkSpeed": 10000,
            "macAddress": "c8:1f:66:ee:59:b9",
            "macAddressPermanent": "c8:1f:66:ee:59:bb",
            "method": "bond",
            "physical": {
                "address": "0.0.0.0",
                "macAddress": "c8:1f:66:ee:59:b9",
                "macAddressPermanent": "c8:1f:66:ee:59:bb",
                "netmask": "N/A",
                "network": "N/A",
                "upAndRunning": true
            },
            "status": "UpAndRunning",
            "upAndRunning": true
        },
        "eth2": {
            "auto": true,
            "bond-master": "Bond1G",
            "family": "inet",
            "linkSpeed": 1000,
            "macAddress": "c8:1f:66:ee:59:bd",
            "macAddressPermanent": "c8:1f:66:ee:59:bd",
            "method": "bond",
            "physical": {
                "address": "0.0.0.0",
                "macAddress": "c8:1f:66:ee:59:bd",
                "macAddressPermanent": "c8:1f:66:ee:59:bd",
                "netmask": "N/A",
                "network": "N/A",
                "upAndRunning": true
            },
            "status": "UpAndRunning",
            "upAndRunning": true
        },
        "eth3": {
            "auto": true,
            "bond-master": "Bond1G",
            "family": "inet",
            "linkSpeed": 1000,
```

```
                "macAddress": "c8:1f:66:ee:59:bd",
                "macAddressPermanent": "c8:1f:66:ee:59:bf",
                "method": "bond",
                "physical": {
                    "address": "0.0.0.0",
                    "macAddress": "c8:1f:66:ee:59:bd",
                    "macAddressPermanent": "c8:1f:66:ee:59:bf",
                    "netmask": "N/A",
                    "network": "N/A",
                    "upAndRunning": true
                },
                "status": "UpAndRunning",
                "upAndRunning": true
            },
            "lo": {
                "auto": true,
                "family": "inet",
                "linkSpeed": 0,
                "macAddress": "00:00:00:00:00:00",
                "macAddressPermanent": "00:00:00:00:00:00",
                "method": "loopback",
                "physical": {
                    "address": "0.0.0.0",
                    "macAddress": "00:00:00:00:00:00",
                    "macAddressPermanent": "00:00:00:00:00:00",
                    "netmask": "N/A",
                    "network": "N/A",
                    "upAndRunning": true
                },
                "status": "UpAndRunning",
                "upAndRunning": true
            }
        }
    }
}
```


GetNodeHardwareInfo (Ausgabe für iSCSI)

Der `GetNodeHardwareInfo` Bei der Methode für iSCSI wird eine ähnliche Antwort wie im folgenden Beispiel zurückgegeben.


```
{
    "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 (Ausgabe für Fibre Channel Nodes)

Der `GetNodeHardwareInfo` Bei der Methode für Fibre Channel Nodes wird eine Antwort zurückgegeben, die dem folgenden Beispiel ähnelt.


```
{
"id": null,
"result": {
"nodeHardwareInfo": {
"bus": {
"core_DMI:0200": {
"description": "Motherboard",
"physid": "0",
"product": "0H47HH",
```

```
"serial": "..CN747513AA0541.",
"version": "A07"
},
"fiber:0_PCI:0000:04:00.0": {
"businfo": "pci@0000:04:00.0",
"clock": "33000000",
"description": "Fibre Channel",
"physid": "0",
"product": "ISP8324-based 16Gb Fibre Channel to PCI Express Adapter",
"vendor": "QLogic Corp.",
"version": "02",
"width": "64"
},
"fiber:0_PCI:0000:42:00.0": {
"businfo": "pci@0000:42:00.0",
"clock": "33000000",
"description": "Fibre Channel",
"physid": "0",
"product": "ISP8324-based 16Gb Fibre Channel to PCI Express Adapter",
"vendor": "QLogic Corp.",
"version": "02",
"width": "64"
},
"fiber:1_PCI:0000:04:00.1": {
"businfo": "pci@0000:04:00.1",
"clock": "33000000",
"description": "Fibre Channel",
"physid": "0.1",
"product": "ISP8324-based 16Gb Fibre Channel to PCI Express Adapter",
"vendor": "QLogic Corp.",
"version": "02",
"width": "64"
},
"fiber:1_PCI:0000:42:00.1": {
"businfo": "pci@0000:42:00.1",
"clock": "33000000",
"description": "Fibre Channel",
"physid": "0.1",
"product": "ISP8324-based 16Gb Fibre Channel to PCI Express Adapter",
"vendor": "QLogic Corp.",
"version": "02",
"width": "64"
}
},
"fans": {
"Fan1A RPM": {
```

```
"baseUnit": "RPM",
"threshold": 840,
"value": 3360
},
"Fan1B RPM": {
"baseUnit": "RPM",
"threshold": 840,
"value": 3120
}
},
"fibreChannelPorts": [
{
"firmware": "7.04.00 (d0d5)",
"hbaPort": 1,
"internalPortID": 2,
"model": "QLE2672",
"nPortID": "0x060019",
"nodeID": 6,
"pciSlot": 3,
"serial": "BFE1335E04217",
"speed": "8 Gbit",
"state": "Online",
"switchWwn": "20:01:00:2a:6a:9c:71:01",
"wwnn": "5f:47:ac:c8:30:26:c9:00",
"wwpn": "5f:47:ac:c0:30:26:c9:0a"
},
{
"firmware": "7.04.00 (d0d5)",
"hbaPort": 2,
"internalPortID": 3,
"model": "QLE2672",
"nPortID": "0xc70019",
"nodeID": 6,
"pciSlot": 3,
"serial": "BFE1335E04217",
"speed": "8 Gbit",
"state": "Online",
"switchWwn": "20:01:00:2a:6a:98:a3:41",
"wwnn": "5f:47:ac:c8:30:26:c9:00",
"wwpn": "5f:47:ac:c0:30:26:c9:0b"
},
{
"firmware": "7.04.00 (d0d5)",
"hbaPort": 1,
"internalPortID": 0,
"model": "QLE2672",
```

```
"nPortID": "0xc70017",
"nodeID": 6,
"pciSlot": 2,
"serial": "BFE1341E09515",
"speed": "8 Gbit",
"state": "Online",
"switchWwn": "20:01:00:2a:6a:98:a3:41",
"wwnn": "5f:47:ac:c8:30:26:c9:00",
"wwpn": "5f:47:ac:c0:30:26:c9:08"
},
{
"firmware": "7.04.00 (d0d5)",
"hbaPort": 2,
"internalPortID": 1,
"model": "QLE2672",
"nPortID": "0x060017",
"nodeID": 6,
"pciSlot": 2,
"serial": "BFE1341E09515",
"speed": "8 Gbit",
"state": "Online",
"switchWwn": "20:01:00:2a:6a:9c:71:01",
"wwnn": "5f:47:ac:c8:30:26:c9:00",
"wwpn": "5f:47:ac:c0:30:26:c9:09"
}
],
"memory": {
"firmware_": {
"capacity": "8323072",
"date": "08/29/2013",
"description": "BIOS",
"physid": "0",
"size": "65536",
"version": "2.0.19"
},
"memory_DMI:1000": {
"description": "System Memory",
"physid": "1000",
"size": "34359738368",
"slot": "System board or motherboard"
}
},
"network": {
"network:0_": {
"description": "Ethernet interface",
"logicalname": "Bond1G",
```

```
"physid": "1",
"serial": "c8:1f:66:df:04:da"
},
"network:0_PCI:0000:01:00.0": {
"businfo": "pci@0000:01:00.0",
"capacity": "1000000000",
"clock": "33000000",
"description": "Ethernet interface",
"logicalname": "eth0",
"physid": "0",
"product": "NetXtreme II BCM57800 1/10 Gigabit Ethernet",
"serial": "c8:1f:66:df:04:d6",
"vendor": "Broadcom Corporation",
"version": "10",
"width": "64"
},
"network:0_PCI:0000:41:00.0": {
"businfo": "pci@0000:41:00.0",
"capacity": "1000000000",
"clock": "33000000",
"description": "Ethernet interface",
"logicalname": "eth4",
"physid": "0",
"product": "NetXtreme II BCM57810 10 Gigabit Ethernet",
"serial": "00:0a:f7:41:7a:30",
"vendor": "Broadcom Corporation",
"version": "10",
"width": "64"
},
"network:1_": {
"description": "Ethernet interface",
"logicalname": "Bond10G",
"physid": "2",
"serial": "c8:1f:66:df:04:d6"
},
"network:1_PCI:0000:01:00.1": {
"businfo": "pci@0000:01:00.1",
"capacity": "1000000000",
"clock": "33000000",
"description": "Ethernet interface",
"logicalname": "eth1",
"physid": "0.1",
"product": "NetXtreme II BCM57800 1/10 Gigabit Ethernet",
"serial": "c8:1f:66:df:04:d8",
"vendor": "Broadcom Corporation",
"version": "10",
```

```
"width": "64"
},
"network:1_PCI:0000:41:00.1": {
"businfo": "pci@0000:41:00.1",
"capacity": "1000000000",
"clock": "33000000",
"description": "Ethernet interface",
"logicalname": "eth5",
"physid": "0.1",
"product": "NetXtreme II BCM57810 10 Gigabit Ethernet",
"serial": "00:0a:f7:41:7a:32",
"vendor": "Broadcom Corporation",
"version": "10",
"width": "64"
},
"network:2_PCI:0000:01:00.2": {
"businfo": "pci@0000:01:00.2",
"capacity": "1000000000",
"clock": "33000000",
"description": "Ethernet interface",
"logicalname": "eth2",
"physid": "0.2",
"product": "NetXtreme II BCM57800 1/10 Gigabit Ethernet",
"serial": "c8:1f:66:df:04:da",
"size": "1000000000",
"vendor": "Broadcom Corporation",
"version": "10",
"width": "64"
},
"network:3_PCI:0000:01:00.3": {
"businfo": "pci@0000:01:00.3",
"capacity": "1000000000",
"clock": "33000000",
"description": "Ethernet interface",
"logicalname": "eth3",
"physid": "0.3",
"product": "NetXtreme II BCM57800 1/10 Gigabit Ethernet",
"serial": "c8:1f:66:df:04:dc",
"size": "1000000000",
"vendor": "Broadcom Corporation",
"version": "10",
"width": "64"
}
},
"networkInterfaces": {
"Bond10G": {
```

```
"isConfigured": true,
"isUp": true
},
"Bond1G": {
"isConfigured": true,
"isUp": true
},
"eth0": {
"isConfigured": true,
"isUp": true
},
"eth1": {
"isConfigured": true,
"isUp": true
},
"eth2": {
"isConfigured": true,
"isUp": true
},
"eth3": {
"isConfigured": true,
"isUp": true
},
"eth4": {
"isConfigured": true,
"isUp": true
},
"eth5": {
"isConfigured": true,
"isUp": true
}
},
"platform": {
"chassisType": "R620",
"cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
"nodeMemoryGB": 32,
"nodeType": "SFFC"
},
"powerSupplies": {
"PS1 status": {
"powerSupplyFailureDetected": false,
"powerSupplyHasAC": true,
"powerSupplyPredictiveFailureDetected": false,
"powerSupplyPresent": true
},
"PS2 status": {
```

```
"powerSupplyFailureDetected": false,
"powerSupplyHasAC": true,
"powerSupplyPredictiveFailureDetected": false,
"powerSupplyPresent": true
}
},
"storage": {
"storage_PCI:0000:00:1f.2": {
"businfo": "pci@0000:00:1f.2",
"clock": "66000000",
"description": "SATA controller",
"physid": "1f.2",
"product": "C600/X79 series chipset 6-Port SATA AHCI Controller",
"vendor": "Intel Corporation",
"version": "05",
"width": "32"
}
},
"system": {
"fcn-2_DMI:0100": {
"description": "Rack Mount Chassis",
"product": "(SKU=NotProvided;ModelName=)",
"serial": "HTX1DZ1",
"width": "64"
}
},
"temperatures": {
"Exhaust Temp": {
"baseUnit": "C",
"threshold": 70,
"value": 38
},
"Inlet Temp": {
"baseUnit": "C",
"threshold": 42,
"value": 13
  },
"uuid": "4C4C4544-004D-5310-8052-C4C04F335431"
    }
   }
  }
 }
}
```

GetNvramInfo

Der `GetNvramInfo` Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt.

```
{
  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"
     }
   }
}
```

ListenActiveNodes

Der `ListActiveNodes` Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt.

```
  {
```

```
    "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
                    }
                ]
            }
        ]
    }
 }
```

ListeActiveVolumes

Der `ListActiveVolumes` Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt.


```
{
    "id": 1,
    "result": {
        "volumes": [
            {
                "access": "readWrite",
                "accountID": 1,
                "attributes": {},
                "blockSize": 4096,
                "createTime": "2016-06-23T14:19:12Z",
                "deleteTime": "",
                "enable512e": false,
                "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo1.1",
                "name": "HulkDemo1",
                "purgeTime": "",
                "qos": {
                    "burstIOPS": 1500,
                    "burstTime": 60,
                    "curve": {
                        "4096": 100,
                        "8192": 160,
                        "16384": 270,
                        "32768": 500,
                        "65536": 1000,
                        "131072": 1950,
                        "262144": 3900,
                        "524288": 7600,
                        "1048576": 15000
                    },
                    "maxIOPS": 1000,
                    "minIOPS": 100
                },
                "scsiEUIDeviceID": "306f746f00000001f47acc0100000000",
                "scsiNAADeviceID": "6f47acc100000000306f746f00000001",
                "sliceCount": 1,
                "status": "active",
                "totalSize": 53687091200,
                "virtualVolumeID": null,
                "volumeAccessGroups": [
                    1
                ],
```

```
            "volumeID": 1,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:14Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo6.6",
            "name": "HulkDemo6",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f00000006f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000006",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 6,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
```

```
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:14Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo7.7",
            "name": "HulkDemo7",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f00000007f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000007",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 7,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:15Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo8.8",
```

```
            "name": "HulkDemo8",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f00000008f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000008",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 8,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:15Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo9.9",
            "name": "HulkDemo9",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
```

```
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f00000009f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000009",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 9,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:16Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo12.12",
            "name": "HulkDemo12",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
```

```
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f0000000cf47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f0000000c",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 12,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:18Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo16.16",
            "name": "HulkDemo16",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
```

```
            },
            "scsiEUIDeviceID": "306f746f00000010f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000010",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 16,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:18Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo17.17",
            "name": "HulkDemo17",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f00000011f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000011",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
```

```
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 17,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:18Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo18.18",
            "name": "HulkDemo18",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f00000012f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000012",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 18,
            "volumePairs": []
```

```
            },
            {
                "access": "readWrite",
                "accountID": 1,
                "attributes": {},
                "blockSize": 4096,
                "createTime": "2016-06-24T15:21:59Z",
                "deleteTime": "",
                "enable512e": true,
                "iqn": "iqn.2010-01.com.solidfire:0oto.bk.24",
                "name": "BK",
                "purgeTime": "",
                "qos": {
                    "burstIOPS": 15000,
                    "burstTime": 60,
                    "curve": {
                        "4096": 100,
                        "8192": 160,
                        "16384": 270,
                        "32768": 500,
                        "65536": 1000,
                        "131072": 1950,
                        "262144": 3900,
                        "524288": 7600,
                        "1048576": 15000
                    },
                    "maxIOPS": 15000,
                    "minIOPS": 50
                },
                "scsiEUIDeviceID": "306f746f00000018f47acc0100000000",
                "scsiNAADeviceID": "6f47acc100000000306f746f00000018",
                "sliceCount": 1,
                "status": "active",
                "totalSize": 10737418240,
                "virtualVolumeID": null,
                "volumeAccessGroups": [],
                "volumeID": 24,
                "volumePairs": [
                    {
                        "clusterPairID": 2,
                        "remoteReplication": {
                            "mode": "Async",
                            "pauseLimit": 3145728000,
                            "remoteServiceID": 14,
                            "resumeDetails": "",
                            "snapshotReplication": {
```

```
                                "state": "Idle",
                                "stateDetails": ""
                            },
                            "state": "Active",
                            "stateDetails": ""
                        },
                        "remoteSliceID": 8,
                        "remoteVolumeID": 8,
                        "remoteVolumeName": "PairingDoc",
                        "volumePairUUID": "229fcbf3-2d35-4625-865a-
d04bb9455cef"
                    }
                ]
            }
        ]
    }
}
```

TestHardwareConfig

Der `TestHardwareConfig` Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt.

```
{
"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"
            }
        }
    ]
}
}
```

NetApp Element Plug-in für vCenter Server

Das NetApp Element Plug-in für vCenter Server stellt ein Plug-in für die Schnittstelle von VMware vSphere bereit, sodass Sie Storage-Cluster, auf denen die NetApp Element Software ausgeführt wird, managen und überwachen können.

Informationen zum Element Plug-in für vCenter Server finden Sie im "Dokumentation zum NetApp Element-Plug-in für vCenter Server".

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"

Monitoring von Storage mit SolidFire Active IQ

"SolidFire Active IQ" Ist ein webbasiertes Tool, das kontinuierlich aktualisierte historische Ansichten von clusterweiten Daten bietet. Sie können Benachrichtigungen für bestimmte Ereignisse, Schwellenwerte oder Metriken einrichten. Mit SolidFire Active IQ können Sie die Performance und Kapazität des Systems überwachen und über den Cluster-Zustand auf dem Laufenden bleiben.

Folgende Informationen zu Ihrem System finden Sie im SolidFire Active IQ:

- Anzahl der Nodes und Status der Nodes: Ordnungsgemäß, offline oder Fehler
- Grafische Darstellung der CPU-, Speichernutzung und Knotendrosselung
- Details zum Node, z. B. Seriennummer, Steckplatz im Chassis, Modell und Version der NetApp Element Software, die auf dem Storage-Node ausgeführt wird
- CPU- und Storage-bezogene Informationen zu Virtual Machines

Weitere Informationen zu SolidFire Active IQ finden Sie im "SolidFire Active IQ-Dokumentation".

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"
- "NetApp Support-Website gt; Tools für Active IQ"

Arbeiten Sie mit dem Management-Node

Übersicht über Management-Nodes

Sie können den Management-Node (mNode) verwenden, um Systemdienste zu verwenden, Cluster-Assets und -Einstellungen zu managen, Systemtests und Dienstprogramme auszuführen, Active IQ für das System-Monitoring zu konfigurieren und den NetApp Support-Zugriff zur Fehlerbehebung zu aktivieren.

> Als Best Practice wird nur ein Management Node mit einer VMware vCenter Instanz verknüpft, sodass nicht dieselben Storage- und Computing-Ressourcen oder vCenter Instanzen in mehreren Management Nodes definiert werden müssen.

Für Cluster mit Element Softwareversion 11.3 oder höher können Sie mit dem Management-Node über eine von zwei Schnittstellen arbeiten:

- Mit der Management-Node-UI (`https://[mNode IP]:442`) Können Sie Änderungen an Netzwerk- und Clustereinstellungen vornehmen, Systemtests ausführen oder Systemdienstprogramme verwenden.
- Mit der integrierten REST API UI (`https://[mNode IP]/mnode`) Können Sie APIs ausführen oder verstehen, die mit den Management-Knoten-Services verbunden sind, einschließlich Proxy-Server-Konfiguration, Service-Level-Updates oder Asset-Management.

Installation oder Wiederherstellung eines Management-Node:

- "Installieren Sie einen Management-Node"
- "Konfigurieren eines Speicher-Netzwerkschnittstellentoncontrollers (NIC)"
- "Wiederherstellung eines Management-Node"

Zugriff auf den Management-Node:

- "Zugriff auf den Management-Node (UI oder REST-API)"

Ändern Sie das Standard-SSL-Zertifikat:

- "Ändern Sie das Standard-SSL-Zertifikat für den Management-Node"

Führen Sie Aufgaben mit der Management-Node-UI durch:

- "Übersicht über die Management-Node-UI"

Aufgaben mit den MANAGEMENT-Node-REST-APIs:

- "Übersicht über DIE REST-API-UI für den Management-Node"

Deaktivieren oder aktivieren Sie Remote-SSH-Funktionen oder starten Sie mit NetApp Support eine Remote-Support-Tunnelsitzung, um Unterstützung bei der Fehlerbehebung zu bieten:

- "Zugriff auf Storage-Nodes mithilfe von SSH für die grundlegende Fehlerbehebung"
  - "Aktivieren von Remote-Verbindungen mit NetApp Support"
  - "Verwalten der SSH-Funktionalität auf dem Management-Node"

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Installation oder Wiederherstellung eines Management-Node

Installieren Sie einen Management-Node

Sie können den Management-Node für Ihr Cluster, auf dem die NetApp Element Software ausgeführt wird, manuell installieren. Verwenden Sie dabei das entsprechende Image für Ihre Konfiguration.

Dieses Handbuch richtet sich an SolidFire All-Flash-Storage-Administratoren, die die NetApp Deployment Engine nicht zur Installation von Management-Nodes verwenden.

Bevor Sie beginnen

- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Ihre Installation verwendet IPv4. Der Management-Node 11.3 unterstützt IPv6 nicht.

  Wenn IPv6 unterstützt werden soll, können Sie den Management-Node 11.1 verwenden.

- Sie sind berechtigt, Software von der NetApp Support Site herunterzuladen.
- Sie haben den für Ihre Plattform korrekten Managementknoten-Image-Typ identifiziert:

Plattform	Bildtyp der Installation
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

- (Management-Node 12.0 und höher mit Proxy-Server) Sie haben die Version 2.16 von NetApp Hybrid Cloud Control auf Managementservices aktualisiert, bevor Sie einen Proxy-Server konfigurieren.

Über diese Aufgabe

Der Element 12.2 Management-Node ist ein optionales Upgrade. Bei bestehenden Implementierungen wird dieser Bedarf nicht benötigt.

Bevor Sie dieses Verfahren befolgen, sollten Sie verstehen, "Persistente Volumes"ob Sie sie verwenden möchten oder nicht. Persistente Volumes sind optional, jedoch im Falle eines Datenverlusts bei der Management-Node-Konfiguration empfohlen.

Schritt 1: ISO oder OVA herunterladen und VM bereitstellen

Laden Sie das entsprechende ISO oder OVA von der NetApp-Support-Website herunter, und installieren Sie die VM.

Schritte

1. Laden Sie die OVA oder ISO für Ihre Installation von der Seite auf der NetApp Support-Website herunter"Element Software".
   a. Wählen Sie **Letzte Version herunterladen** und akzeptieren Sie die EULA.
   b. Wählen Sie das Management-Node-Image aus, das Sie herunterladen möchten.
2. Wenn Sie die OVA heruntergeladen haben, gehen Sie wie folgt vor:
   a. OVA bereitstellen.
   b. Wenn sich Ihr Storage-Cluster in einem separaten Subnetz vom Management-Node (eth0) befindet und Sie persistente Volumes verwenden möchten, fügen Sie der VM im Storage-Subnetz einen zweiten NIC (Network Interface Controller) hinzu (z. B. eth1) oder stellen Sie sicher, dass das Managementnetzwerk zum Storage-Netzwerk weiterleiten kann.
3. Wenn Sie die ISO heruntergeladen haben, führen Sie die folgenden Schritte aus:
   a. Erstellen Sie mit der folgenden Konfiguration eine neue 64-Bit-VM aus Ihrem Hypervisor:
      - Sechs virtuelle CPUs
      - 24 GB RAM
      - Speicheradaptertyp auf LSI Logic Parallel eingestellt

        Der Standard für Ihren Management-Node ist möglicherweise LSI Logic SAS. Überprüfen Sie im Fenster **New Virtual Machine** die Konfiguration des Speicheradapters, indem Sie **Hardware anpassen** > **Virtual Hardware** wählen. Ändern Sie bei Bedarf LSI Logic SAS in **LSI Logic Parallel**.

      - 400 GB virtuelle Festplatte, Thin Provisioning
      - Eine virtuelle Netzwerkschnittstelle mit Internetzugang und Zugriff auf den Speicher MVIP.
      - (Optional) eine virtuelle Netzwerkschnittstelle mit Managementnetzwerkzugriff auf das Storage-Cluster. Wenn sich Ihr Storage-Cluster in einem separaten Subnetz vom Management-Node (eth0) befindet und Sie persistente Volumes verwenden möchten, fügen Sie der VM im Storage-Subnetz (eth1) einen zweiten NIC (Network Interface Controller) hinzu oder stellen Sie sicher, dass das Managementnetzwerk zum Speichernetzwerk umgeleitet werden kann.

        Schalten Sie die VM nicht ein, bevor Sie den Schritt angeben, der später in diesem Verfahren ausgeführt werden soll.

   b. Verbinden Sie die ISO mit der VM und starten Sie sie am .iso-Installations-Image.

      Wenn Sie einen Management-Node mithilfe des Images installieren, kann dies zu einer Verzögerung von 30 Sekunden führen, bevor der Startbildschirm angezeigt wird.

4. Schalten Sie die VM nach Abschluss der Installation für den Management-Node ein.

Schritt 2: Erstellen Sie den Verwaltungsknoten admin und konfigurieren Sie das Netzwerk

Erstellen Sie nach Abschluss der VM-Installation den Admin-Benutzer des Management-Nodes, und konfigurieren Sie das Management-Node-Netzwerk.

Schritte

1. Erstellen Sie über die Terminal User Interface (TUI) einen Management Node Admin User.

   Um durch die Menüoptionen zu navigieren, drücken Sie die nach-oben- oder nach-unten-Taste. Um durch die Tasten zu navigieren, drücken Sie Tab. Um von den Schaltflächen zu den Feldern zu wechseln, drücken Sie Tab. Um zwischen Feldern zu navigieren, drücken Sie die nach-oben- oder nach-unten-Taste.

2. Wenn im Netzwerk ein DHCP-Server (Dynamic Host Configuration Protocol) vorhanden ist, der IPs mit einer MTU (Maximum Transmission Unit) von weniger als 1500 Byte zuweist, müssen Sie die folgenden Schritte durchführen:

   a. Versetzen Sie den Management-Node vorübergehend in ein vSphere-Netzwerk ohne DHCP, z. B. iSCSI,.

   b. Starten Sie die VM neu, oder starten Sie das VM-Netzwerk neu.

   c. Konfigurieren Sie über TUI die korrekte IP-Adresse im Managementnetzwerk mit einer MTU größer oder gleich 1500 Bytes.

   d. Weisen Sie der VM das richtige VM-Netzwerk erneut zu.

   Ein DHCP, der IPs mit einer MTU unter 1500 Byte zuweist, kann Sie verhindern, dass Sie das Management-Node-Netzwerk konfigurieren oder die Management-Node-UI verwenden.

3. Konfigurieren Sie das Management-Node-Netzwerk (eth0).

   Wenn Sie eine zusätzliche NIC benötigen, um den Speicherdatenverkehr zu isolieren, lesen Sie die Anweisungen zum Konfigurieren einer anderen NIC: "Konfigurieren eines Speicher-Netzwerkschnittstellentoncontrollers (NIC)".

Schritt 3: Konfigurieren der Zeitsynchronisierung

Synchronisieren Sie vor dem Einrichten des Management-Node die Zeit zwischen dem Management-Node und dem Storage-Cluster.

Schritte

1. Überprüfen Sie mithilfe von NTP, ob die Zeit zwischen dem Management-Node und dem Storage-Cluster synchronisiert ist:

   Ab Element 12.3 werden die Teilschritte a bis (e) automatisch ausgeführt. Fahren Sie für Management-Knoten 12.3 mit fortUnterschritt (f), um die Konfiguration der Zeitsynchronisierung abzuschließen.

1. Melden Sie sich über SSH oder die vom Hypervisor bereitgestellte Konsole beim Management-Node an.
2. NTPD stoppen:

```
sudo service ntpd stop
```

3. Bearbeiten Sie die NTP-Konfigurationsdatei `/etc/ntp.conf`:
   a. Kommentieren Sie die Standardserver (`server 0.gentoo.pool.ntp.org`) Durch Hinzufügen von a `#` Vor jedem.
   b. Fügen Sie für jeden hinzuzufügenden Standardzeitserver eine neue Zeile hinzu. Die Standardzeitserver müssen dieselben NTP-Server sein, die auf dem Speichercluster verwendet werden, den Sie auch verwenden werden. Später SchrittDie

```
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. Speichern Sie die Konfigurationsdatei nach Abschluss.
4. Erzwingen einer NTP-Synchronisierung mit dem neu hinzugefügten Server.

```
sudo ntpd -gq
```

5. NTPD neu starten.

```
sudo service ntpd start
```

6. Zeitsynchronisierung mit Host über den Hypervisor deaktivieren (im Folgenden ein VMware-Beispiel):

> Wenn Sie den mNode in einer anderen Hypervisor-Umgebung als VMware bereitstellen, zum Beispiel vom .iso-Image in einer OpenStack-Umgebung, finden Sie in der Hypervisor-Dokumentation die entsprechenden Befehle.

   a. Periodische Zeitsynchronisierung deaktivieren:

```
vmware-toolbox-cmd timesync disable
```

   b. Den aktuellen Status des Dienstes anzeigen und bestätigen:

```
vmware-toolbox-cmd timesync status
```

c. Überprüfen Sie in vSphere das `Synchronize guest time with host` Das Kontrollkästchen ist in den VM-Optionen nicht aktiviert.

> Aktivieren Sie diese Option nicht, wenn Sie zukünftige Änderungen an der VM vornehmen.

> Bearbeiten Sie den NTP-Server nicht mehr, nachdem Sie die Zeitsynchronisierung abgeschlossen haben, da dies Auswirkungen auf den NTP-Server hat, wenn Sie den Befehl ausführen. Setup-Befehl auf dem Management-Knoten.

Schritt 4: Einrichten des Management-Knotens

Konfigurieren Sie den Management-Node mit dem `setup-mnode` Befehl.

Schritte

1. Konfigurieren und Ausführen des Management-Node-Setup-Befehls:

> Sie werden aufgefordert, Passwörter in einer sicheren Eingabeaufforderung einzugeben. Wenn sich Ihr Cluster hinter einem Proxy-Server befindet, müssen Sie die Proxy-Einstellungen konfigurieren, damit Sie ein öffentliches Netzwerk erreichen können.

```
sudo /sf/packages/mnode/setup-mnode --mnode_admin_user [username]
--storage_mvip [mvip] --storage_username [username] --telemetry_active
[true]
```

a. Ersetzen Sie den Wert in [ ] Klammern (einschließlich der Klammern) für jeden der folgenden erforderlichen Parameter:

> Die gekürzte Form des Befehlsnamens ist in Klammern ( ) und kann durch den vollständigen Namen ersetzt werden.

- **--mnode_admin_user (-mu) [username]**: Der Benutzername für das Administrator-Konto des Management-Node. Dies ist wahrscheinlich der Benutzername für das Benutzerkonto, mit dem Sie sich beim Management-Node anmelden.
- **--storage_mvip (-sm) [MVIP-Adresse]**: Die Management Virtual IP-Adresse (MVIP) des Speicherclusters, auf dem die Element-Software ausgeführt wird. Konfigurieren Sie den Verwaltungsknoten mit demselben Speichercluster, den Sie während Konfiguration von NTP-ServernDie
- **--Storage_username (-su) [username]**: Der Benutzername des Speicherclusters für den vom angegebenen Cluster `--storage_mvip` Parameter.
- **--Telemetrie_Active (-t) [true]**: Den Wert TRUE beibehalten, der die Datenerfassung zur Analyse durch Active IQ ermöglicht.

b. (Optional): Fügen Sie dem Befehl Active IQ-Endpunkt-Parameter hinzu:

- **--Remote_Host (-rh) [AIQ_Endpunkt]**: Der Endpunkt, an dem Active IQ Telemetriedaten zur Verarbeitung gesendet werden. Wenn der Parameter nicht enthalten ist, wird der Standardendpunkt verwendet.

c. (Empfohlen): Fügen Sie die folgenden persistenten Volume-Parameter hinzu. Ändern oder löschen Sie das Konto und die Volumes, die für die Funktion „persistente Volumes“ erstellt wurden, nicht, oder die Managementfunktion kann verloren gehen.

   - **--use_persistent_Volumes (-pv) [true/false, default: False]**: Aktivieren oder deaktivieren Sie persistente Volumes. Geben Sie den Wert TRUE ein, um die Funktion persistenter Volumes zu aktivieren.
   - **--persistent_Volumes_Account (-pva) [Account_Name]**: Wenn `--use_persistent_volumes` Ist auf „true“ gesetzt. Verwenden Sie diesen Parameter, und geben Sie den Namen des Speicherkontos ein, der für persistente Volumes verwendet wird.

     Verwenden Sie einen eindeutigen Kontonamen für persistente Volumes, der sich von jedem vorhandenen Kontonamen im Cluster unterscheidet. Es ist von zentraler Bedeutung, dass das Konto für persistente Volumes getrennt von der übrigen Umgebung bleibt.

   - **--persistent_Volumes_mvip (-pvm) [mvip]**: Geben Sie die virtuelle Management-IP-Adresse (MVIP) des Storage-Clusters ein, auf dem Element Software ausgeführt wird, die mit persistenten Volumes verwendet wird. Dies ist nur erforderlich, wenn vom Management-Node mehrere Storage-Cluster gemanagt werden. Wenn nicht mehrere Cluster verwaltet werden, wird der Standard-Cluster MVIP verwendet.

d. Proxy-Server konfigurieren:

   - **--use_Proxy (-up) [true/false, default: False]**: Aktivieren oder deaktivieren Sie die Verwendung des Proxy. Dieser Parameter ist erforderlich, um einen Proxyserver zu konfigurieren.
   - **--Proxy_Hostname_or_ip (-pi) [Host]**: Der Proxy-Hostname oder die IP. Dies ist erforderlich, wenn Sie einen Proxy verwenden möchten. Wenn Sie dies angeben, werden Sie zur Eingabe aufgefordert `--proxy_port`.
   - **--Proxy_username (-pu) [username]**: Der Proxy-Benutzername. Dieser Parameter ist optional.
   - **--Proxy_password (-pp) [password]**: Das Proxy-Passwort. Dieser Parameter ist optional.
   - **--Proxy_Port (-pq) [Port, Standard: 0]**: Der Proxy-Port. Wenn Sie dies angeben, werden Sie aufgefordert, den Proxy-Hostnamen oder die IP einzugeben (`--proxy_hostname_or_ip`).
   - **--Proxy_SSH_Port (-ps) [Port, Standard: 443]**: Der SSH-Proxy-Port. Standardmäßig ist der Port 443.

e. (Optional) Verwenden Sie die Parameterhilfe, wenn Sie zusätzliche Informationen über die einzelnen Parameter benötigen:

   - **--help (-h)**: Gibt Informationen über jeden Parameter zurück. Parameter werden basierend auf der ursprünglichen Implementierung als erforderlich oder optional definiert. Die Parameteranforderungen für Upgrades und Neuimplementierungen können variieren.

f. Führen Sie die aus `setup-mnode` Befehl.

Schritt 5: Konfiguration der Controller-Assets

Suchen Sie die Installations-ID, und fügen Sie eine vCenter-Controller-Ressource hinzu.

Schritte

1. Suchen Sie die Installations-ID:

   a. Melden Sie sich in einem Browser bei DER REST API-UI für den Management-Node an:

b. Wechseln Sie zum Speicher-MVIP und melden Sie sich an. Durch diese Aktion wird das Zertifikat für den nächsten Schritt akzeptiert.

c. Öffnen Sie die REST API-UI für den Bestandsdienst auf dem Managementknoten:

```
https://<ManagementNodeIP>/inventory/1/
```

d. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:

   i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.

   ii. Geben Sie die Client-ID als ein `mnode-client`.

   iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

e. Wählen Sie in DER REST API UI **GET /Installations** aus.

f. Wählen Sie **Probieren Sie es aus**.

g. Wählen Sie **Ausführen**.

h. Kopieren Sie aus dem Code 200 Response Body den und speichern Sie den `id` Für die Installation in einem späteren Schritt.

   Die Installation verfügt über eine Basiskonfiguration, die während der Installation oder eines Upgrades erstellt wurde.

2. Fügen Sie dem Management-Node bekannte Ressourcen eine vCenter Controller-Ressource für NetApp Hybrid Cloud Control hinzu:

a. Rufen Sie die mNode-Service-API-UI auf dem Management-Node auf, indem Sie die Management-Node-IP-Adresse, gefolgt von eingeben `/mnode`:

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

b. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:

   i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.

   ii. Geben Sie die Client-ID als ein `mnode-client`.

   iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

   iv. Schließen Sie das Fenster.

c. Wählen Sie **POST /Assets/{Asset_id}/Controllers** aus, um eine Unterressource des Controllers hinzuzufügen.

> Sie sollten eine neue NetApp HCC-Rolle in vCenter erstellen, um eine Controller-Unterressource hinzuzufügen. Diese neue NetApp HCC-Rolle beschränkt die Management Node Services-Ansicht auf reine NetApp Ressourcen. Siehe "Erstellen einer NetApp HCC-Rolle in vCenter".

d. Wählen Sie **Probieren Sie es aus**.

e. Geben Sie im Feld **Asset_id** die ID der übergeordneten Basis ein, die Sie in die Zwischenablage kopiert haben.

f. Geben Sie die erforderlichen Nutzlastwerte mit dem Typ ein `vCenter` Und vCenter Zugangsdaten.

g. Wählen Sie **Ausführen**.

Weitere Informationen

- "Persistente Volumes"
- "Fügen Sie dem Management-Node eine Controller-Ressource hinzu"
- "Konfigurieren Sie eine Speicher-NIC"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Erstellen einer NetApp HCC-Rolle in vCenter

Sie sollten eine NetApp HCC-Rolle in vCenter erstellen, um nach der Installation des Management-Node manuell vCenter Assets (Controller) hinzuzufügen oder vorhandene Controller zu ändern.

Diese NetApp HCC-Rolle beschränkt Ihre Management-Node-Services-Ansicht auf reine NetApp Ressourcen.

Über diese Aufgabe

- Dieses Verfahren beschreibt die in Version 6.7 von vSphere verfügbaren Schritte. Ihre vSphere Benutzeroberfläche kann sich je nach installierter Version von der Beschreibung leicht unterscheiden. Weitere Hilfe finden Sie in der Dokumentation zu VMware vCenter.
- Bis "Erstellen einer neuen NetApp HCC-Rolle", Sie richten zunächst ein neues Benutzerkonto in vCenter ein, erstellen eine NetApp HCC-Rolle und weisen dann die Benutzerberechtigungen zu.
- Bei NetApp ESXi Host-Konfigurationen sollten Sie das von nde erstellte Benutzerkonto auf die neue NetApp HCC-Rolle aktualisieren:
  - Nutzung "Diese Option" Wenn Ihr NetApp ESXi-Host nicht in einem vCenter-Host-Cluster vorhanden ist
  - Nutzung "Diese Option" Wenn der NetApp ESXi Host innerhalb eines vCenter Host-Clusters vorhanden ist
- Das können Sie "Konfigurieren Sie ein Controller-Asset" Die ist bereits auf dem Management-Node vorhanden.
- Verwenden Sie die neue NetApp HCC-Rolle für "Fügen Sie eine Anlage hinzu" Zum Management-Node.

Erstellen einer neuen NetApp HCC-Rolle

Richten Sie in vCenter ein neues Benutzerkonto ein, erstellen Sie eine NetApp HCC-Rolle und weisen Sie dann die Benutzerberechtigungen zu.

Richten Sie ein neues Benutzerkonto in vCenter ein

Führen Sie folgende Schritte aus, um ein neues Benutzerkonto in vCenter einzurichten:

Schritte

1. Melden Sie sich beim vSphere Web Client unter an `administrator@vsphere.local` Oder gleichwertig.

2. Wählen Sie im Menü die Option **Verwaltung**.
3. Wählen Sie im Abschnitt **Single Sign On** die Option **Benutzer** und **Gruppen** aus.
4. Wählen Sie in der Liste **Domäne** die Option aus `vsphere.local` Oder Ihre LDAP-Domäne.
5. Wählen Sie **Benutzer Hinzufügen**.
6. Füllen Sie das Formular **Benutzer hinzufügen** aus.

Neue NetApp HCC-Rolle in vCenter erstellen

Führen Sie folgende Schritte aus, um eine neue NetApp HCC-Rolle in vCenter zu erstellen:

Schritte

1. Wählen Sie **Rolle bearbeiten** aus, und weisen Sie die erforderlichen Berechtigungen zu.
2. Wählen Sie im linken Navigationsbereich **Global**.
3. Wählen Sie **Diagnose** und **Lizenzen**.
4. Wählen Sie im linken Navigationsbereich **Hosts** aus.
5. Wählen Sie **Wartung**, **Leistung**, **Konfiguration der Speicherpartition** und **Firmware**.
6. Speichern unter `NetApp Role`.

Weisen Sie vCenter Benutzerberechtigungen zu

Führen Sie die folgenden Schritte aus, um die Benutzerberechtigungen der neuen NetApp HCC-Rolle in vCenter zuzuweisen.

Schritte

1. Wählen Sie im Menü die Option **Hosts** und **Cluster** aus.
2. Wählen Sie im linken Navigationsbereich eine der folgenden Optionen aus:
   - VCenter auf oberster Ebene
   - Ihr gewünschtes vCenter, wenn Sie sich im verknüpften Modus befinden.

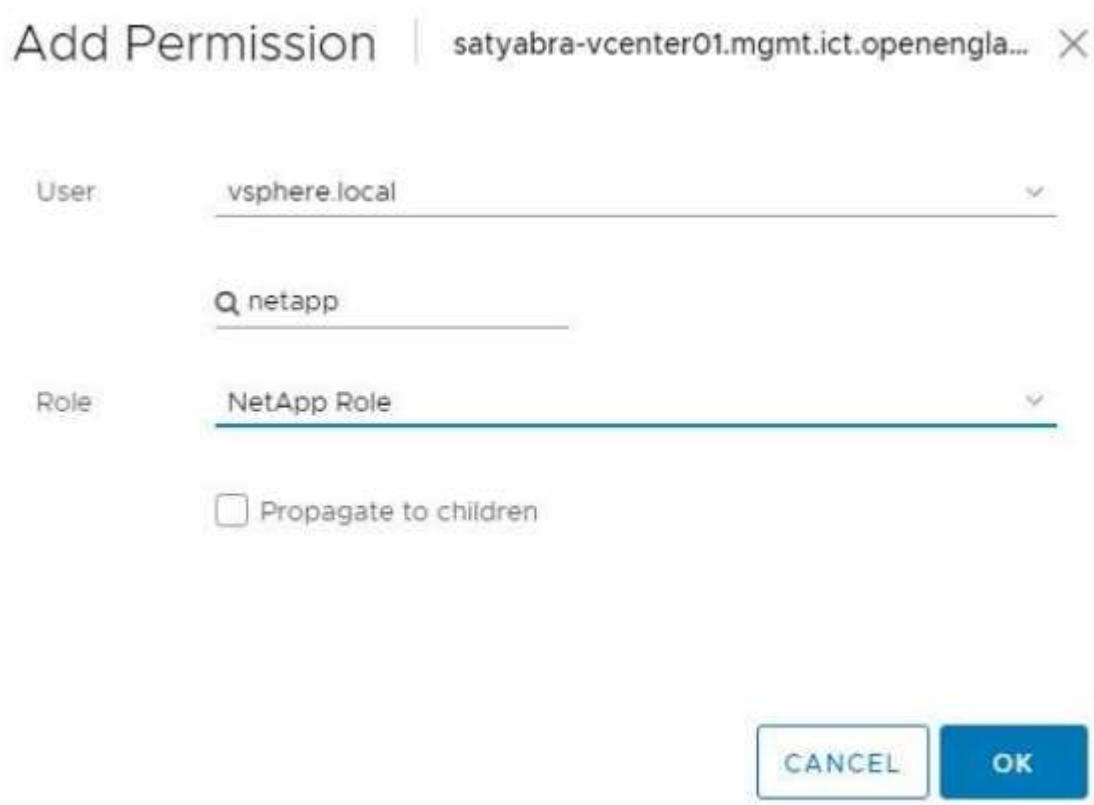
> - Ab dem NetApp Element Plug-in für vCenter Server 5.0 ist die Verwendung einfacher "VCenter Linked Mode", Sie registrieren das Element Plug-in für jeden vCenter Server, der NetApp SolidFire Storage Cluster managt (empfohlen) über einen separaten Management-Node.
> - Mit dem NetApp Element Plug-in für vCenter Server 4.10 und früher verwalten Sie Clusterressourcen von anderen vCenter Servern mithilfe "VCenter Linked Mode" Ist auf lokale Storage-Cluster beschränkt

3. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
4. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie `vsphere.local` Oder Ihre LDAP-Domäne
   b. Verwenden Sie die Suche, um den neuen Benutzer zu finden, den Sie in erstellt haben Richten Sie ein neues Benutzerkonto in vCenter ein.
   c. Wählen Sie `NetApp Role`.

Do * NOT* select **propagieren auf Kinder**.



Weisen Sie dem Rechenzentrum Benutzerberechtigungen zu

Führen Sie die folgenden Schritte aus, um dem Rechenzentrum in vCenter die Benutzerberechtigungen zuzuweisen.

Schritte

1. Wählen Sie im linken Fensterbereich **Datacenter** aus.
2. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
3. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie `vsphere.local` Oder Ihre LDAP-Domäne.

   b. Verwenden Sie die Suche, um den neuen HCC-Benutzer zu finden, den Sie in erstellt haben Richten Sie ein neues Benutzerkonto in vCenter ein.

   c. Wählen Sie `ReadOnly role`.

   Do * NOT* select **propagieren auf Kinder**.

Weisen Sie NetApp HCI-Datastores Benutzerberechtigungen zu

Führen Sie die folgenden Schritte aus, um den NetApp HCI-Datastores in vCenter die Benutzerberechtigungen zuzuweisen.

Schritte

1. Wählen Sie im linken Fensterbereich **Datacenter** aus.
2. Erstellen Sie einen neuen Speicherordner. Klicken Sie mit der rechten Maustaste auf **Datacenter** und wählen Sie **Speicherordner erstellen**.
3. Übertragen Sie alle NetApp HCI-Datastores vom Storage-Cluster und lokal auf den Computing-Node in den neuen Speicherordner.
4. Wählen Sie den neuen Speicherordner aus.
5. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
6. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie `vsphere.local` Oder Ihre LDAP-Domäne.
   b. Verwenden Sie die Suche, um den neuen HCC-Benutzer zu finden, den Sie in erstellt haben Richten Sie ein neues Benutzerkonto in vCenter ein.
   c. Wählen Sie `Administrator role`
   d. Wählen Sie **auf Kinder übertragen**.

Weisen Sie einem NetApp Host-Cluster Benutzerberechtigungen zu

Führen Sie die folgenden Schritte durch, um die Benutzerberechtigungen einem NetApp Host-Cluster in vCenter zuzuweisen.

Schritte

1. Wählen Sie im linken Navigationsbereich das NetApp Host-Cluster aus.
2. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
3. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie `vsphere.local` Oder Ihre LDAP-Domäne.
   b. Verwenden Sie die Suche, um den neuen HCC-Benutzer zu finden, den Sie in erstellt haben Richten Sie ein neues Benutzerkonto in vCenter ein.
   c. Wählen Sie `NetApp Role` Oder `Administrator`.
   d. Wählen Sie **auf Kinder übertragen**.

NetApp ESXi Hostkonfigurationen

Bei NetApp ESXi Hostkonfigurationen sollten Sie das von der nde erstellte Benutzerkonto auf die neue NetApp HCC-Rolle aktualisieren.

Der NetApp ESXi-Host ist nicht in einem vCenter-Host-Cluster vorhanden

Wenn der NetApp ESXi-Host nicht in einem vCenter-Host-Cluster vorhanden ist, können Sie das folgende Verfahren verwenden, um die NetApp HCC-Rolle und Benutzerberechtigungen in vCenter zuzuweisen.

Schritte

1. Wählen Sie im Menü die Option **Hosts** und **Cluster** aus.
2. Wählen Sie im linken Navigationsbereich den NetApp ESXi Host aus.
3. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
4. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie `vsphere.local` Oder Ihre LDAP-Domäne.
   b. Verwenden Sie die Suche, um den neuen Benutzer zu finden, den Sie in erstellt haben Richten Sie ein neues Benutzerkonto in vCenter ein.
   c. Wählen Sie `NetApp Role` Oder `Administrator`.
5. Wählen Sie **auf Kinder übertragen**.

Der NetApp ESXi-Host ist in einem vCenter-Host-Cluster vorhanden

Wenn ein NetApp ESXi Host innerhalb eines vCenter Host Clusters mit ESXi Hosts anderer Anbieter vorhanden ist, können Sie im folgenden Verfahren die NetApp HCC-Rolle und die Benutzerberechtigungen in vCenter zuweisen.

1. Wählen Sie im Menü die Option **Hosts** und **Cluster** aus.
2. Erweitern Sie im linken Navigationsbereich den gewünschten Host-Cluster.
3. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
4. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie `vsphere.local` Oder Ihre LDAP-Domäne.
   b. Verwenden Sie die Suche, um den neuen Benutzer zu finden, den Sie in erstellt haben Richten Sie ein neues Benutzerkonto in vCenter ein.
   c. Wählen Sie `NetApp Role`.

   > Do * NOT* select **propagieren auf Kinder**.
5. Wählen Sie im linken Navigationsbereich einen NetApp ESXi Host aus.
6. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
7. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie `vsphere.local` Oder Ihre LDAP-Domäne.
   b. Verwenden Sie die Suche, um den neuen Benutzer zu finden, den Sie in erstellt haben Richten Sie ein neues Benutzerkonto in vCenter ein.
   c. Wählen Sie `NetApp Role` Oder `Administrator`.
   d. Wählen Sie **auf Kinder übertragen**.
8. Wiederholen Sie diesen Vorgang für verbleibende NetApp ESXi Hosts im Host-Cluster.

Die Controller-Ressource ist bereits auf dem Management-Node vorhanden

Wenn bereits ein Controller-Asset auf dem Management-Node vorhanden ist, führen Sie die folgenden Schritte aus, um den Controller mithilfe von zu konfigurieren `PUT /assets /{asset_id} /controllers /{controller_id}`.

Schritte

1. Zugriff auf die mNode-Service-API-UI auf dem Management-Node:

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

2. Wählen Sie **autorisieren** aus, und geben Sie die Anmeldeinformationen ein, um auf die API-Aufrufe zuzugreifen.
3. Wählen Sie `GET /assets` Um die übergeordnete ID zu erhalten.
4. Wählen Sie `PUT /assets /{asset_id} /controllers /{controller_id}`.
   a. Geben Sie die im Account-Setup erstellten Anmeldeinformationen in den Text der Anforderung ein.

Fügen Sie dem Management-Node eine Ressource hinzu

Wenn Sie eine neue Anlage nach der Installation manuell hinzufügen müssen, verwenden Sie das neue HCC-Benutzerkonto, das Sie in erstellt haben Richten Sie ein neues Benutzerkonto in vCenter ein. Weitere Informationen finden Sie unter "Fügen Sie dem Management-Node eine Controller-Ressource hinzu".

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Konfigurieren eines Speicher-Netzwerkschnittstellentoncontrollers (NIC)

Wenn Sie eine zusätzliche NIC für den Speicher verwenden, können Sie SSH in den Management-Knoten einlegen oder die vCenter-Konsole verwenden und einen Curl-Befehl ausführen, um eine getaggte oder nicht getaggte Netzwerkschnittstelle einzurichten.

Bevor Sie beginnen

- Sie kennen Ihre eth0-IP-Adresse.
- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node 11.3 oder höher implementiert.

Konfigurationsoptionen

Wählen Sie die für Ihre Umgebung relevante Option:

- Konfigurieren Sie einen Speicher Network Interface Controller (NIC) für eine nicht getaggte Netzwerkschnittstelle
- Konfigurieren Sie einen Speicher Network Interface Controller (NIC) für eine getaggte Netzwerkschnittstelle

Konfigurieren Sie einen Speicher Network Interface Controller (NIC) für eine nicht getaggte Netzwerkschnittstelle

Schritte

1. Öffnen Sie eine SSH oder vCenter Konsole.
2. Ersetzen Sie die Werte in der folgenden Befehlsvorlage und führen Sie den Befehl aus:

> Werte werden durch dargestellt `$` Für jeden der erforderlichen Parameter für die neue Storage-Netzwerk-Schnittstelle. Der `cluster` Das Objekt in der folgenden Vorlage ist erforderlich und kann für die Umbenennung des Management-Node-Host-Namens verwendet werden. `--insecure` Oder `-k` Optionen sollten nicht in Produktionsumgebungen verwendet werden.

```
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"
}
'
```

Konfigurieren Sie einen Speicher Network Interface Controller (NIC) für eine getaggte Netzwerkschnittstelle

Schritte

1. Öffnen Sie eine SSH oder vCenter Konsole.
2. Ersetzen Sie die Werte in der folgenden Befehlsvorlage und führen Sie den Befehl aus:

Werte werden durch dargestellt `$` Für jeden der erforderlichen Parameter für die neue Storage-Netzwerk-Schnittstelle. Der `cluster` Das Objekt in der folgenden Vorlage ist erforderlich und kann für die Umbenennung des Management-Node-Host-Namens verwendet werden. `--insecure` Oder `-k` Optionen sollten nicht in Produktionsumgebungen verwendet werden.

```
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"
}
'
```

Weitere Informationen

- "Fügen Sie dem Management-Node eine Controller-Ressource hinzu"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Wiederherstellung eines Management-Node

Sie können den Management-Node für Ihren Cluster, auf dem die NetApp Element Software ausgeführt wird, manuell wiederherstellen und neu bereitstellen, wenn der

vorherige Management-Node persistente Volumes verwendete.

Sie können eine neue OVA implementieren und ein Neuimplementierung-Skript ausführen, um Konfigurationsdaten aus einem zuvor installierten Management Node, auf dem Version 11.3 und höher ausgeführt wird, zu übertragen.

Was Sie benötigen

- Auf dem vorherigen Management-Node wurde die NetApp Element Softwareversion 11.3 oder höher mit ausgeführt "Persistente Volumes" Funktionalität eingebunden.
- Sie kennen die MVIP und SVIP des Clusters, der die persistenten Volumes enthält.
- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Ihre Installation verwendet IPv4. Der Management-Node 11.3 unterstützt IPv6 nicht.
- Sie sind berechtigt, Software von der NetApp Support Site herunterzuladen.
- Sie haben den für Ihre Plattform korrekten Managementknoten-Image-Typ identifiziert:

Plattform	Bildtyp der Installation
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

Schritte

1. und implementieren Sie die VM
2. Konfigurieren des Netzwerks
3. Konfigurieren Sie die Zeitsynchronisierung
4. Konfigurieren Sie den Management-Node

Laden Sie ISO oder OVA herunter, und implementieren Sie die VM

1. Laden Sie die OVA oder ISO für Ihre Installation im herunter "Element Software" Auf der NetApp Support Site finden.
   a. Wählen Sie **Letzte Version herunterladen** und akzeptieren Sie die EULA.
   b. Wählen Sie das Management-Node-Image aus, das Sie herunterladen möchten.
2. Wenn Sie die OVA heruntergeladen haben, gehen Sie wie folgt vor:
   a. OVA bereitstellen.
   b. Wenn sich Ihr Storage-Cluster in einem separaten Subnetz vom Management-Node (eth0) befindet und Sie persistente Volumes verwenden möchten, fügen Sie der VM im Storage-Subnetz einen zweiten NIC (Network Interface Controller) hinzu (z. B. eth1) oder stellen Sie sicher, dass das Managementnetzwerk zum Storage-Netzwerk weiterleiten kann.
3. Wenn Sie die ISO heruntergeladen haben, führen Sie die folgenden Schritte aus:
   a. Erstellen Sie aus Ihrem Hypervisor eine neue 64-Bit-Virtual Machine mit der folgenden Konfiguration:

- Sechs virtuelle CPUs
- 24 GB RAM
- 400 GB virtuelle Festplatte, Thin Provisioning
- Eine virtuelle Netzwerkschnittstelle mit Internetzugang und Zugriff auf den Speicher MVIP.
- (Optional für SolidFire All-Flash Storage) eine virtuelle Netzwerkschnittstelle mit Managementnetzwerkzugriff auf den Storage-Cluster. Wenn sich Ihr Storage-Cluster in einem separaten Subnetz vom Management-Node (eth0) befindet und Sie persistente Volumes verwenden möchten, fügen Sie der VM im Storage-Subnetz (eth1) einen zweiten NIC (Network Interface Controller) hinzu oder stellen Sie sicher, dass das Managementnetzwerk zum Speichernetzwerk umgeleitet werden kann.

> Schalten Sie die virtuelle Maschine nicht vor dem Schritt ein, der später in diesem Verfahren angezeigt wird.

b. Verbinden Sie die ISO mit der virtuellen Maschine, und starten Sie sie am .iso-Installations-Image.

> Wenn Sie einen Management-Node mithilfe des Images installieren, kann dies zu einer Verzögerung von 30 Sekunden führen, bevor der Startbildschirm angezeigt wird.

4. Schalten Sie die virtuelle Maschine für den Managementknoten ein, nachdem die Installation abgeschlossen ist.

Konfigurieren des Netzwerks

1. Erstellen Sie über die Terminal User Interface (TUI) einen Management Node Admin User.

> Um durch die Menüoptionen zu navigieren, drücken Sie die nach-oben- oder nach-unten-Taste. Um durch die Tasten zu navigieren, drücken Sie Tab. Um von den Schaltflächen zu den Feldern zu wechseln, drücken Sie Tab. Um zwischen Feldern zu navigieren, drücken Sie die nach-oben- oder nach-unten-Taste.

2. Konfigurieren Sie das Management-Node-Netzwerk (eth0).

> Wenn Sie eine zusätzliche NIC benötigen, um den Speicherdatenverkehr zu isolieren, lesen Sie die Anweisungen zum Konfigurieren einer anderen NIC: "Konfigurieren eines Speicher-Netzwerkschnittstellentoncontrollers (NIC)".

Konfigurieren Sie die Zeitsynchronisierung

1. Überprüfen Sie mithilfe von NTP, ob die Zeit zwischen dem Management-Node und dem Storage-Cluster synchronisiert ist:

> Ab Element 12.3 werden die Teilschritte a bis (e) automatisch ausgeführt. Für Management-Node 12.3.1 oder höher fahren Sie mit fort Unterschritt (f) Um die Konfiguration der Zeitsynchronisation abzuschließen.

1. Melden Sie sich über SSH oder die vom Hypervisor bereitgestellte Konsole beim Management-Node an.
2. NTPD stoppen:

```
sudo service ntpd stop
```

3. Bearbeiten Sie die NTP-Konfigurationsdatei `/etc/ntp.conf`:
   a. Kommentieren Sie die Standardserver (`server 0.gentoo.pool.ntp.org`) Durch Hinzufügen von a `#` Vor jedem.
   b. Fügen Sie für jeden Standardserver, den Sie hinzufügen möchten, eine neue Zeile hinzu. Die Standardzeitserver müssen die gleichen NTP-Server sein, die auf dem Speicher-Cluster verwendet werden, die Sie in A verwenden "Später Schritt".

```
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. Speichern Sie die Konfigurationsdatei nach Abschluss.
4. Erzwingen einer NTP-Synchronisierung mit dem neu hinzugefügten Server.

```
sudo ntpd -gq
```

5. NTPD neu starten.

```
sudo service ntpd start
```

6. Zeitsynchronisierung mit Host über den Hypervisor deaktivieren (im Folgenden ein VMware-Beispiel):

> Wenn Sie den mNode in einer anderen Hypervisor-Umgebung als VMware bereitstellen, zum Beispiel vom .iso-Image in einer OpenStack-Umgebung, finden Sie in der Hypervisor-Dokumentation die entsprechenden Befehle.

   a. Periodische Zeitsynchronisierung deaktivieren:

```
vmware-toolbox-cmd timesync disable
```

   b. Den aktuellen Status des Dienstes anzeigen und bestätigen:

```
vmware-toolbox-cmd timesync status
```

c. Überprüfen Sie in vSphere das `Synchronize guest time with host` Das Kontrollkästchen ist in den VM-Optionen nicht aktiviert.

> Aktivieren Sie diese Option nicht, wenn Sie zukünftige Änderungen an der VM vornehmen.

> Bearbeiten Sie NTP nicht, nachdem Sie die Konfiguration zur Zeitsynchronisation abgeschlossen haben, da es sich auf das NTP beim Ausführen des auswirkt Befehl „Neuimplementierung“ Auf dem Management-Node.

Konfigurieren Sie den Management-Node

1. Erstellen eines temporären Zielverzeichnisses für den Inhalt des Management Services-Pakets:

```
mkdir -p /sf/etc/mnode/mnode-archive
```

2. Laden Sie das Management-Services-Bundle (Version 2.15.28 oder höher) herunter, das zuvor auf dem vorhandenen Management-Node installiert wurde, und speichern Sie es im `/sf/etc/mnode/` Verzeichnis.
3. Extrahieren Sie das heruntergeladene Bundle mit dem folgenden Befehl und ersetzen Sie den Wert in [ ] Klammern (einschließlich der Klammern) durch den Namen der Bundle-Datei:

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle
file]
```

4. Extrahieren Sie die resultierende Datei in das `/sf/etc/mnode-archive` Verzeichnis:

```
tar -C /sf/etc/mnode/mnode-archive -xvf
/sf/etc/mnode/services_deploy_bundle.tar.gz
```

5. Eine Konfigurationsdatei für Konten und Volumes erstellen:

```
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. Ersetzen Sie den Wert in [ ] Klammern (einschließlich der Klammern) für jeden der folgenden erforderlichen Parameter:

- **[mvip IP-Adresse]**: Die Management-virtuelle IP-Adresse des Storage-Clusters. Konfigurieren Sie den Management-Node mit demselben Storage-Cluster, das Sie während verwendet haben "Konfiguration von NTP-Servern".
- **[Kontoname des persistenten Volumes]**: Der Name des Kontos, der mit allen persistenten Volumes in diesem Speicher-Cluster verknüpft ist.

1. Konfigurieren und Ausführen des Befehls „Management Node Neuimplementierung“, um eine Verbindung zu persistenten Volumes zu herstellen, die im Cluster gehostet werden, und um Services mit früheren Management-Node-Konfigurationsdaten zu starten:

   Sie werden aufgefordert, Passwörter in einer sicheren Eingabeaufforderung einzugeben. Wenn sich Ihr Cluster hinter einem Proxy-Server befindet, müssen Sie die Proxy-Einstellungen konfigurieren, damit Sie ein öffentliches Netzwerk erreichen können.

   ```
   sudo /sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
   ```

   a. Ersetzen Sie den Wert in [ ]-Klammern (einschließlich der Klammern) durch den Benutzernamen für das Administratorkonto für den Managementknoten. Dies ist wahrscheinlich der Benutzername für das Benutzerkonto, mit dem Sie sich beim Management-Node anmelden.

      Sie können den Benutzernamen hinzufügen oder dem Skript erlauben, Sie zur Eingabe der Informationen zu auffordern.

   b. Führen Sie die aus `redeploy-mnode` Befehl. Das Skript zeigt eine Erfolgsmeldung an, wenn die erneute Implementierung abgeschlossen ist.

   c. Wenn Sie auf Element-Webschnittstellen (z. B. den Management-Node oder NetApp Hybrid Cloud Control) mit dem vollständig qualifizierten Domain-Namen (FQDN) des Systems zugreifen, "Konfigurieren Sie die Authentifizierung für den Management-Node neu".

   SSH-Funktion, die bietet "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist auf Management-Nodes mit Management-Services 2.18 und höher standardmäßig deaktiviert. Wenn Sie zuvor die SSH-Funktion auf dem Management-Node aktiviert hatten, müssen Sie möglicherweise auch "Deaktivieren Sie SSH erneut" Auf dem wiederhergestellten Management-Node.

Weitere Informationen

- "Persistente Volumes"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Greifen Sie auf den Management-Node zu

Ab der NetApp Element Softwareversion 11.3 enthält der Managementknoten zwei UIs: Eine Benutzeroberfläche für die Verwaltung VON REST-basierten Diensten und eine UI pro Node zum Verwalten von Netzwerk- und Clustereinstellungen sowie Betriebssystemtests und -Dienstprogrammen.

Für Cluster mit Element Softwareversion 11.3 oder höher können Sie eine von zwei Schnittstellen verwenden:

- Mithilfe der Management-Node-UI (`https:// [mNode IP}:442`) Können Sie Änderungen an Netzwerk- und Clustereinstellungen vornehmen, Systemtests ausführen oder Systemdienstprogramme verwenden.
- Über die integrierte REST-API-UI (`https://[mNode IP}/mnode`) Können Sie APIs ausführen oder

verstehen, die mit den Management-Knoten-Services verbunden sind, einschließlich Proxy-Server-Konfiguration, Service-Level-Updates oder Asset-Management.

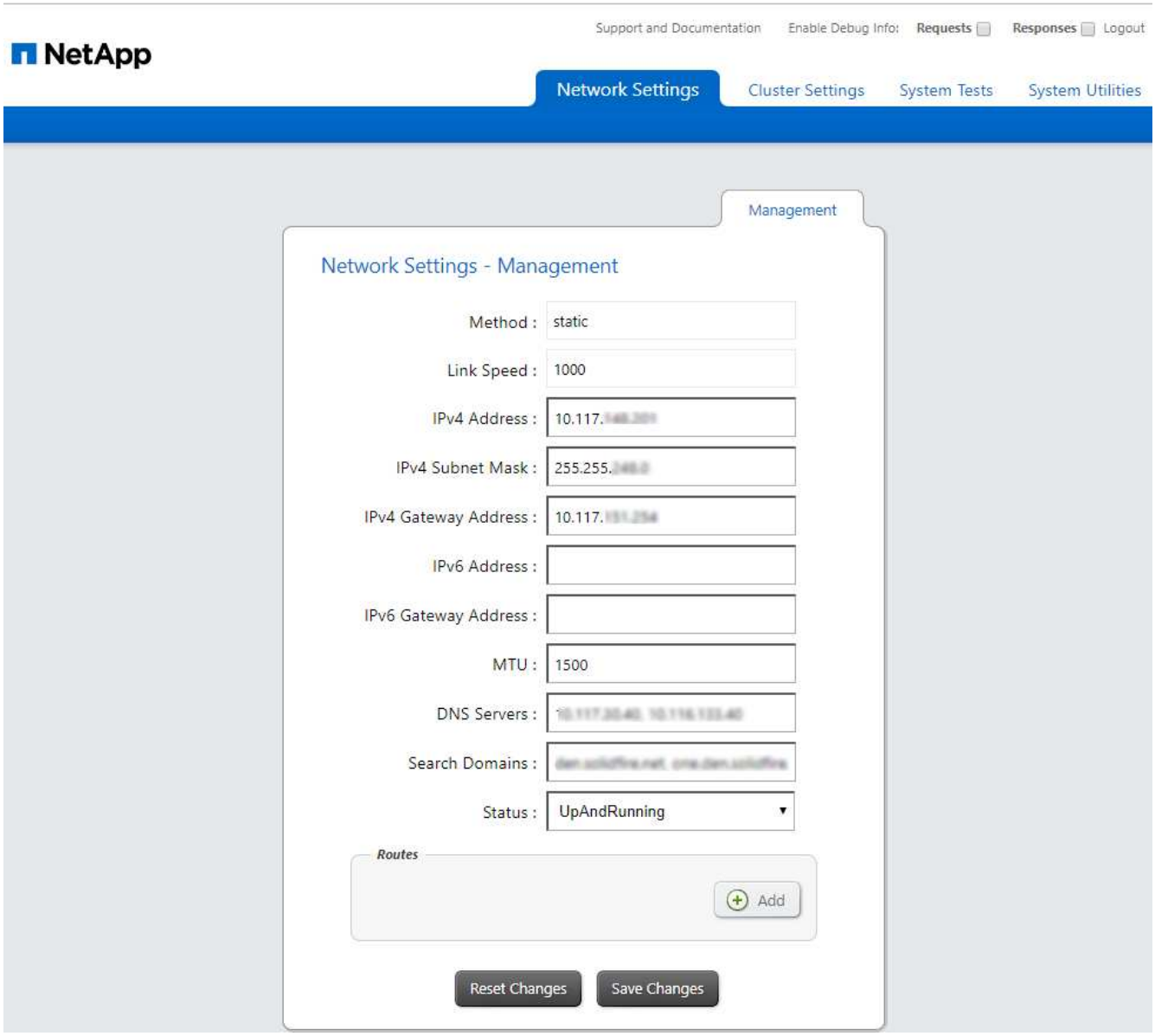
Greifen Sie über die UI auf den Management-Node zu

Über die UI pro Node können Sie auf Netzwerk- und Cluster-Einstellungen zugreifen und Systemtests und Dienstprogramme verwenden.

Schritte

1. Greifen Sie auf die UI pro Node für den Management-Node zu, indem Sie die IP-Adresse des Management-Knotens eingeben, gefolgt von :442

```
https://[IP address]:442
```



2. Geben Sie bei der entsprechenden Eingabeaufforderung den Benutzernamen und das Passwort für den Management-Node ein.

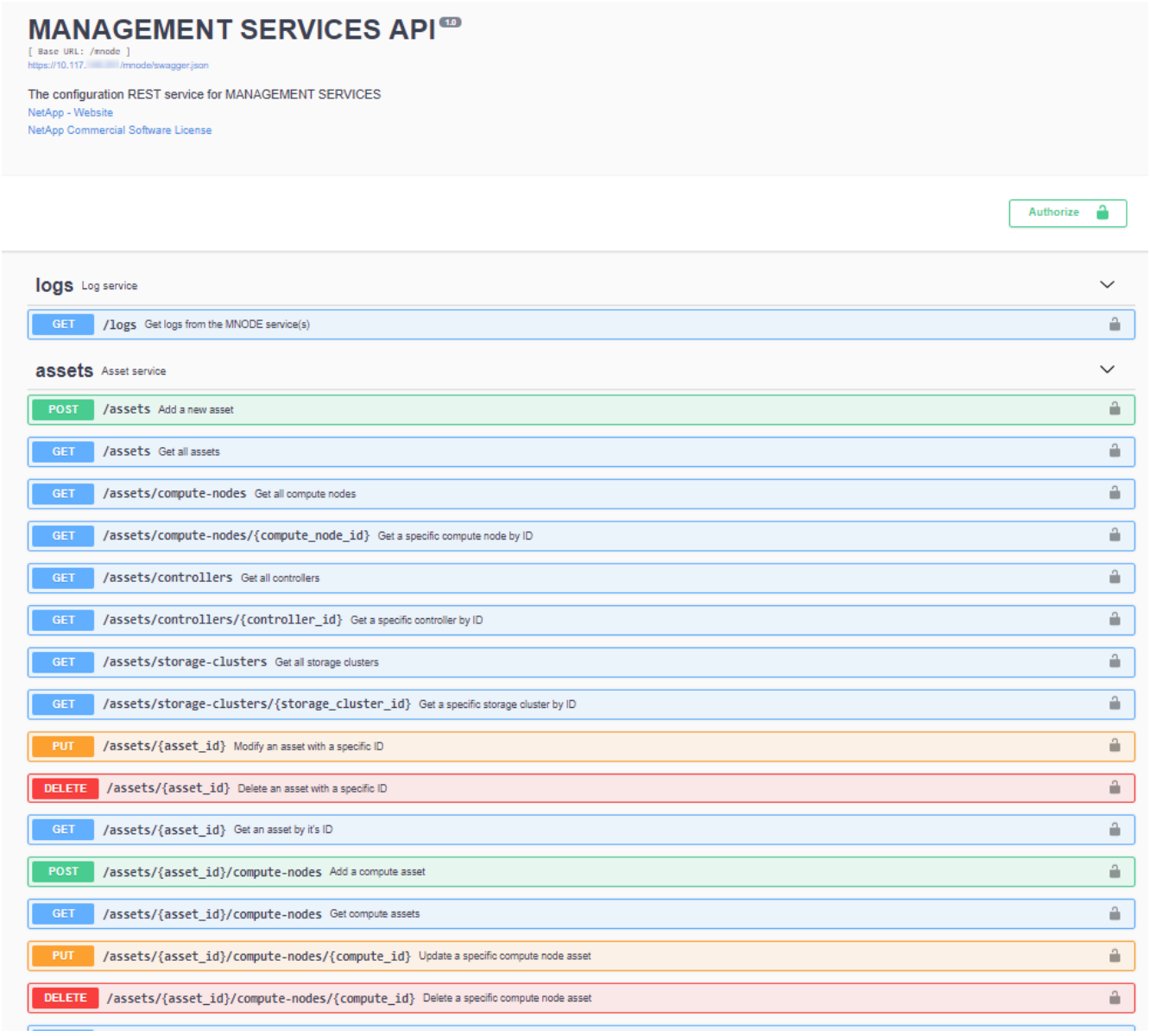
Greifen Sie auf DIE REST-API-UI für den Management-Node zu

Über DIE REST-API-UI erhalten Sie den Zugriff auf ein Menü mit Service-bezogenen APIs, die Managementservices auf dem Management-Node steuern.

Schritte

1. Um auf die REST-API-UI für Managementservices zuzugreifen, geben Sie die Management-Node-IP-Adresse gefolgt von ein `/mnode`:

```
https://[IP address]/mnode
```



2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus und geben Sie Cluster-Administrator-Anmeldeinformationen ein, um APIs zu verwenden.

Weitere Informationen

- "Monitoring von Active IQ und NetApp"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Ändern Sie das Standard-SSL-Zertifikat für den Management-Node

Sie können das Standard-SSL-Zertifikat und den privaten Schlüssel des Management-Node mithilfe der NetApp Element-API ändern.

Wenn Sie einen Verwaltungsknoten konfigurieren, erstellt er ein eindeutiges, selbstsigniertes SSL-Zertifikat (Secure Sockets Layer) und einen privaten Schlüssel, der für die gesamte HTTPS-Kommunikation über die Element-Benutzeroberfläche, die Benutzeroberfläche pro Knoten oder APIs verwendet wird. Die Element Software unterstützt selbstsignierte Zertifikate sowie Zertifikate, die von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt und verifiziert werden.

Sie können die folgenden API-Methoden verwenden, um mehr Informationen über das Standard-SSL-Zertifikat zu erhalten und Änderungen vorzunehmen.

- **GetNodeSSLZertifikat**

  Sie können das verwenden "GetNodeSSLCertificate-Methode" So rufen Sie Informationen zum derzeit installierten SSL-Zertifikat ab, einschließlich aller Zertifikatdetails.

- **SetNodeSSLZertifikat**

  Sie können das verwenden "SetNodeSSLCertificate-Methode" Zum Festlegen der Cluster- und Node-SSL-Zertifikate auf das von Ihnen zur Verfügung gestellt Zertifikat und den privaten Schlüssel. Das System überprüft das Zertifikat und den privaten Schlüssel, um zu verhindern, dass ein ungültiges Zertifikat angewendet wird.

- **RemoveNodeSSLZertifikat**

  Das "RemoveNodeSSLCertificate-Methode" Entfernt das derzeit installierte SSL-Zertifikat und den privaten Schlüssel. Das Cluster generiert dann ein neues selbstsigniertes Zertifikat und einen privaten Schlüssel.

Weitere Informationen

- "Ändern Sie das Standard-SSL-Zertifikat der Element Software"
- "Welche Anforderungen gelten für das Festlegen benutzerdefinierter SSL-Zertifikate in der Element Software?"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Arbeiten Sie mit der Management-Node-UI

Übersicht über die Management-Node-UI

Mit der Management-Node-UI (`https://<ManagementNodeIP>:442`) Können Sie

Änderungen an Netzwerk- und Clustereinstellungen vornehmen, Systemtests ausführen oder Systemdienstprogramme verwenden.

Aufgaben, die Sie mit der Management-Node-UI durchführen können:

- "Konfigurieren der Meldungsüberwachung"
- "Ändern und Testen der Netzwerk-, Cluster- und Systemeinstellungen des Management-Node"
- "Führen Sie Systemdienstprogramme vom Management-Node aus"

Weitere Informationen

- "Greifen Sie auf den Management-Node zu"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Konfigurieren der Meldungsüberwachung

Die Tools zur Überwachung von Warnmeldungen sind für das NetApp HCI-Warnungsüberwachung konfiguriert. Diese Tools werden nicht für SolidFire All-Flash-Storage konfiguriert oder verwendet. Die Ausführung der Tools für diese Cluster führt zu dem folgenden Fehler 405, der bei der Konfiguration erwartet wird: `webUIParseError : Invalid response from server. 405`

Weitere Informationen zum Konfigurieren von Alarmüberwachung für NetApp HCI finden Sie unter "Konfigurieren der Meldungsüberwachung"

Ändern und Testen der Netzwerk-, Cluster- und Systemeinstellungen des Management-Node

Sie können die Einstellungen für das Management-Node-Netzwerk, das Cluster und das System ändern und testen.

- Aktualisieren der Netzwerkeinstellungen für den Management-Node
- Aktualisiert die Cluster-Einstellungen des Management-Node
- Testen Sie die Einstellungen für den Management-Node

Aktualisieren der Netzwerkeinstellungen für den Management-Node

Auf der Registerkarte „Netzwerkeinstellungen“ der Benutzeroberfläche für Management-Node pro Node können Sie die Felder für die Netzwerkschnittstelle des Managementknoten ändern.

1. Öffnen Sie die Management-Node-UI pro Node.
2. Wählen Sie die Registerkarte **Netzwerkeinstellungen** aus.
3. Die folgenden Informationen anzeigen oder eingeben:
   a. **Methode**: Wählen Sie eine der folgenden Methoden, um die Schnittstelle zu konfigurieren:
      - `loopback`: Verwenden Sie, um die IPv4-Loopback-Schnittstelle zu definieren.

- `manual`: Verwenden Sie, um Schnittstellen zu definieren, für die keine Konfiguration erfolgt standardmäßig.
- `dhop`: Nutzung, um eine IP-Adresse über DHCP zu erhalten.
- `static`: Zur Definition von Ethernet-Schnittstellen mit statisch zugewiesenen IPv4-Adressen.

b. **Verbindungsgeschwindigkeit**: Die Geschwindigkeit, die von der virtuellen NIC ausgehandelt wird.
c. **IPv4-Adresse**: Die IPv4-Adresse für das eth0-Netzwerk.
d. **IPv4-Subnetzmaske**: Adressenunterteilungen des IPv4-Netzwerks.
e. **IPv4 Gateway-Adresse**: Router-Netzwerkadresse zum Senden von Paketen aus dem lokalen Netzwerk.
f. **IPv6-Adresse**: Die IPv6-Adresse für das eth0-Netzwerk.
g. **IPv6 Gateway-Adresse**: Router-Netzwerkadresse zum Senden von Paketen aus dem lokalen Netzwerk.

> Die IPv6-Optionen werden für Version 11.3 oder höher des Management-Node nicht unterstützt.

h. **MTU**: Größte Paketgröße, die ein Netzwerkprotokoll übertragen kann. Muss größer als oder gleich 1500 sein. Wenn Sie eine zweite Speicher-NIC hinzufügen, sollte der Wert 9000 sein.
i. **DNS Server**: Netzwerkschnittstelle für die Clusterkommunikation.
j. **Domänen suchen**: Suche nach zusätzlichen MAC-Adressen, die dem System zur Verfügung stehen.
k. **Status**: Mögliche Werte:
   - `UpAndRunning`
   - `Down`
   - `Up`
l. **Routen**: Statische Routen zu bestimmten Hosts oder Netzwerken über die zugehörige Schnittstelle werden die Routen konfiguriert.

Aktualisiert die Cluster-Einstellungen des Management-Node

Auf der Registerkarte Cluster-Einstellungen der Benutzeroberfläche pro Node für den Managementknoten können Sie die Felder für die Cluster-Schnittstelle ändern, wenn sich der Status eines Node im Status „verfügbar“, „Ausstehend“, „Pendingaktiv“ und „aktiv“ befindet.

1. Öffnen Sie die Management-Node-UI pro Node.
2. Wählen Sie die Registerkarte **Cluster-Einstellungen** aus.
3. Die folgenden Informationen anzeigen oder eingeben:
   - **Rolle**: Rolle, die der Management-Knoten im Cluster hat. Möglicher Wert: `Management`.
   - **Version**: Element Software Version läuft auf dem Cluster.
   - **Standardschnittstelle**: Standard-Netzwerkschnittstelle für die Kommunikation mit dem Cluster, auf dem die Element-Software ausgeführt wird.

Testen Sie die Einstellungen für den Management-Node

Nachdem Sie die Einstellungen für das Änderungsmanagement und das Netzwerk für den Management-Node geändert und die Änderungen übernommen haben, können Sie Tests durchführen, um die durchgeführten Änderungen zu validieren.

1. Öffnen Sie die Management-Node-UI pro Node.
2. Wählen Sie in der Management-Knoten-UI **System-Tests** aus.
3. Führen Sie eine der folgenden Aktionen durch:
   a. Um zu überprüfen, ob die von Ihnen konfigurierten Netzwerkeinstellungen für das System gültig sind, wählen Sie **Netzwerk-Konfiguration testen**.
   b. Um die Netzwerkverbindung zu allen Knoten im Cluster sowohl auf 1G- als auch 10G-Schnittstellen mit ICMP-Paketen zu testen, wählen Sie **Test Ping** aus.
4. Folgendes anzeigen oder eingeben:
   - **Hosts**: Geben Sie eine kommagetrennte Liste von Adressen oder Host-Namen von Geräten an, die ping werden sollen.
   - **Versuche**: Geben Sie an, wie oft das System den Ping-Test wiederholen soll. Standard: 5.
   - **Paketgröße**: Geben Sie die Anzahl der Bytes an, die in das ICMP-Paket gesendet werden sollen, das an jede IP gesendet wird. Die Anzahl der Bytes muss kleiner sein als die in der Netzwerkkonfiguration angegebene maximale MTU.
   - **Timeout ms**: Geben Sie die Anzahl der Millisekunden an, die auf jede einzelne Ping-Antwort warten soll. Standard: 500 ms.
   - **Total Timeout sec**: Geben Sie die Zeit in Sekunden an, die der Ping auf eine Systemantwort warten soll, bevor Sie den nächsten Ping-Versuch starten oder den Prozess beenden. Standard: 5.
   - **Fragmentierung verbieten**: Aktivieren Sie das DF-Flag (nicht fragmentieren) für die ICMP-Pakete.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Führen Sie Systemdienstprogramme vom Management-Node aus

Sie können die UI pro Node für den Management-Node verwenden, um Cluster-Supportpakete zu erstellen oder zu löschen, die Node-Konfigurationseinstellungen zurückzusetzen oder das Netzwerk neu zu starten.

Schritte

1. Öffnen Sie die Management-Node-UI pro Node mithilfe der Anmeldedaten für den Management-Node-Administrator.
2. Wählen Sie **System Utilities**.
3. Wählen Sie die Schaltfläche für das Dienstprogramm aus, das Sie ausführen möchten:
   a. **Control Power**: Startet neu, schaltet den Knoten aus oder schaltet den Knoten ab. Geben Sie eine der folgenden Optionen an.

      Dieser Vorgang führt zu einem vorübergehenden Verlust der Netzwerkverbindung.

- **Aktion**: Optionen beinhalten `Restart` Und `Halt` (Ausschalten).
- **Wartezeit**: Jede zusätzliche Zeit, bevor der Knoten wieder online kommt.

b. **Cluster Support Bundle erstellen**: Erstellt das Cluster Support Bundle zur Unterstützung der NetApp Support diagnostischen Evaluierungen von einem oder mehreren Knoten in einem Cluster. Legen Sie die folgenden Optionen fest:
   - **Paketname**: Eindeutiger Name für jedes erstellte Supportpaket. Wenn kein Name angegeben wird, werden „Supportbundle“ und der Node-Name als Dateiname verwendet.
   - **MVIP**: Das MVIP des Clusters. Bundles werden von allen Nodes im Cluster gesammelt. Dieser Parameter ist erforderlich, wenn der Parameter Nodes nicht angegeben wird.
   - **Knoten**: Die IP-Adressen der Knoten, aus denen Pakete gesammelt werden. Geben Sie die Knoten, aus denen Pakete gesammelt werden sollen, entweder Knoten oder MVIP, jedoch nicht beides an. Dieser Parameter ist erforderlich, wenn MVIP nicht angegeben wird.
   - **Benutzername**: Der Cluster Admin Benutzername.
   - **Passwort**: Das Cluster-Admin-Passwort.
   - **Unvollständigkeit zulassen**: Lässt das Skript weiter laufen, wenn Bündel nicht von einem oder mehreren Knoten gesammelt werden können.
   - **Extra Args**: Dieser Parameter wird dem zugeführt `sf_make_support_bundle` Skript: Dieser Parameter sollte nur auf Anfrage des NetApp Support verwendet werden.

c. **Alle Support-Pakete löschen**: Löscht alle aktuellen Support-Bundles auf dem Management-Knoten.

d. **Reset Node**: Setzt den Management Node auf ein neues Installations-Image zurück. Dadurch werden alle Einstellungen außer der Netzwerkkonfiguration in den Standardzustand geändert. Legen Sie die folgenden Optionen fest:
   - **Build**: Die URL zu einem Remote Element Software-Image, auf das der Knoten zurückgesetzt wird.
   - **Optionen**: Spezifikationen für die Ausführung der Reset-Vorgänge. Details werden vom NetApp Support zur Verfügung gestellt, falls erforderlich.

   Dieser Vorgang führt zu einem vorübergehenden Verlust der Netzwerkverbindung.

e. **Netzwerk neu starten**: Startet alle Netzwerkdienste auf dem Management-Knoten neu.

   Dieser Vorgang führt zu einem vorübergehenden Verlust der Netzwerkverbindung.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Arbeiten mit DER REST-API des Management-Node

Übersicht über DIE REST-API-UI für den Management-Node

Über die integrierte REST-API-UI (`https://<ManagementNodeIP>/mnode`) Können Sie APIs ausführen oder verstehen, die mit den Management-Knoten-Services

verbunden sind, einschließlich Proxy-Server-Konfiguration, Service-Level-Updates oder Asset-Management.

Aufgaben, die Sie mit REST-APIs durchführen können:

Autorisierung

- "Autorisierung zur Verwendung VON REST-APIs"

Konfiguration der Ressourcen

- "Monitoring von Active IQ und NetApp"
- "Konfigurieren Sie einen Proxy-Server für den Management-Node"
- "Konfiguration von NetApp Hybrid Cloud Control für mehrere vCenter"
- "Fügen Sie dem Management-Node eine Controller-Ressource hinzu"
- "Erstellen und Managen von Storage-Cluster-Assets"

Asset Management

- "Vorhandene Controller-Assets können angezeigt oder bearbeitet werden"
- "Erstellen und Managen von Storage-Cluster-Assets"
- "Verwenden Sie die REST API, um die Protokolle des Element-Systems zu erfassen"
- "Überprüfen Sie die Betriebssystem- und Servicestversionen der Management-Nodes"
- "Abrufen von Protokollen von Managementservices"

Weitere Informationen

- "Greifen Sie auf den Management-Node zu"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Autorisierung zur Verwendung VON REST-APIs

Sie müssen autorisieren, bevor Sie APIs für Managementservices in der REST API-UI verwenden können. Dazu erhalten Sie ein Zugriffstoken.

Um ein Token zu erhalten, geben Sie Cluster-Admin-Anmeldedaten und eine Client-ID an. Jedes Token dauert etwa zehn Minuten. Nachdem ein Token abgelaufen ist, können Sie erneut eine Genehmigung für ein neues Access Token erteilen.

Während der Installation und Implementierung des Management-Node werden Autorisierungsfunktionen für Sie eingerichtet. Der Token-Service basiert auf dem Storage-Cluster, das Sie während des Setups definiert haben.

Bevor Sie beginnen

- Auf Ihrer Cluster-Version sollte die NetApp Element Software 11.3 oder höher ausgeführt werden.
- Sie sollten einen Management-Node mit Version 11.3 oder höher implementiert haben.

API-Befehl

```
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`
```

SCHRITTE DER REST API-UI

1. Greifen Sie auf die REST-API-UI für den Service zu, indem Sie beispielsweise die Management-Node-IP-Adresse gefolgt vom Dienstnamen eingeben `/mnode/`:

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

2. Wählen Sie **Autorisieren** Aus.

   Alternativ können Sie auf einem Sperrsymbol neben einer beliebigen Service-API wählen.

3. Gehen Sie wie folgt vor:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Geben Sie keinen Wert für das Clientgeheimnis ein.
   d. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
4. Schließen Sie das Dialogfeld * Verfügbare Berechtigungen*.

   Wenn Sie versuchen, einen Befehl auszuführen, nachdem das Token abgelaufen ist, wird ein angezeigt `401 Error: UNAUTHORIZED` Meldung wird angezeigt. Wenn Sie dies sehen, autorisieren Sie erneut.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Monitoring von Active IQ und NetApp

Sie können die Active IQ Storage-Überwachung aktivieren, wenn Sie dies bei der Installation oder einem Upgrade nicht bereits getan haben. Möglicherweise müssen Sie dieses Verfahren anwenden, wenn Sie SolidFire Active IQ nicht während der Installation für ein SolidFire All-Flash-Storage-System eingerichtet haben.

Der Active IQ Collector Service leitet Konfigurationsdaten und softwarebasierte Element Cluster-Performance-Metriken an SolidFire Active IQ weiter, um historische Berichte zu erstellen und Performance-Monitoring nahezu in Echtzeit zu überwachen. Der NetApp Monitoring Service ermöglicht die Weiterleitung von Storage-Cluster-Fehlern an vCenter zur Alarmbenachrichtigung.

Bevor Sie beginnen

- Einige Funktionen in Active IQ, beispielsweise Quality of Service (QoS), erfordern Element 11.3 oder höher die ordnungsgemäße Funktion. Um sicherzustellen, dass Sie alle Active IQ-Funktionen nutzen können, empfiehlt NetApp Folgendes:
  - Im Storage Cluster wird die NetApp Element Software 11.3 oder höher ausgeführt.
  - Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.
- Sie haben Internetzugang. Der Active IQ Collector Service kann nicht von dunklen Standorten verwendet werden, die keine externe Verbindung haben.

Schritte

1. Holen Sie sich die Basis-Asset-ID für die Installation:
   a. Öffnen Sie die REST API-UI für den Bestandsdienst auf dem Managementknoten:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
      ii. Geben Sie die Client-ID als ein `mnode-client`.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Fenster.
   c. Wählen Sie in DER REST API UI **GET /Installations** aus.
   d. Wählen Sie **Probieren Sie es aus**.
   e. Wählen Sie **Ausführen**.
   f. Kopieren Sie aus dem Text Code 200 Antwort den `id` Für die Installation.

      ```
      {
        "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",
      ```

      Die Installation verfügt über eine Basiskonfiguration, die während der Installation oder eines Upgrades erstellt wurde.

2. Telemetrie aktivieren:
   a. Rufen Sie die mNode-Service-API-UI auf dem Management-Node auf, indem Sie die Management-

Node-IP-Adresse, gefolgt von eingeben `/mnode`:

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

b. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:
   i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   ii. Geben Sie die Client-ID als ein `mnode-client`.
   iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   iv. Schließen Sie das Fenster.
c. Konfigurieren der BasisinAssets:
   i. Wählen Sie **PUT /Assets/{Asset_id}** aus.
   ii. Wählen Sie **Probieren Sie es aus**.
   iii. Geben Sie die folgende in die JSON-Nutzlast ein:

```
{
"telemetry_active": true
"config": {}
}
```

   iv. Geben Sie die Basis-ID des vorherigen Schritts in **Asset_ID** ein.
   v. Wählen Sie **Ausführen**.

   Der Active IQ Service wird automatisch neu gestartet, sobald die Assets geändert werden. Das Ändern von Anlagen führt zu einer kurzen Verzögerung, bevor Einstellungen angewendet werden.

3. Falls noch nicht geschehen, fügen Sie dem Management-Node bekannte Ressourcen eine vCenter Controller Ressource für NetApp Hybrid Cloud Control hinzu:

   Für NetApp Monitoring Services ist ein Controller-Asset erforderlich.

   a. Wählen Sie **POST /Assets/{Asset_id}/Controllers** aus, um eine Unterressource des Controllers hinzuzufügen.
   b. Wählen Sie **Probieren Sie es aus**.
   c. Geben Sie im Feld **Asset_id** die ID der übergeordneten Basis ein, die Sie in die Zwischenablage kopiert haben.
   d. Geben Sie die erforderlichen Nutzlastwerte mit ein `type` Als `vCenter` Und vCenter Zugangsdaten.

```
{
"username": "string",
"password": "string",
"ip": "string",
"type": "vCenter",
"host_name": "string",
"config": {}
}
```

`ip` Ist die vCenter IP-Adresse.

e. Wählen Sie **Ausführen**.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Konfiguration von NetApp Hybrid Cloud Control für mehrere vCenter

Sie können NetApp Hybrid Cloud Control so konfigurieren, dass Assets von zwei oder mehr vCenters gemanagt werden, die nicht den verknüpften Modus verwenden.

Sie sollten diesen Prozess nach der Erstinstallation verwenden, wenn Sie Assets für eine kürzlich skalierte Installation hinzufügen müssen oder wenn Ihre Konfiguration nicht automatisch neue Assets hinzugefügt wurde. Mithilfe dieser APIs können Sie Ressourcen hinzufügen, die zu Ihrer Installation hinzugefügt wurden.

Was Sie benötigen

- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.

Schritte

1. "Fügen Sie neue vCenters als Controller Assets hinzu" Für die Konfiguration des Management-Node.
2. Aktualisieren Sie die BestandsdienstAPI auf dem Managementknoten:

```
https://<ManagementNodeIP>/inventory/1/
```

Alternativ können Sie 2 Minuten warten, bis der Bestand in der Benutzeroberfläche von NetApp Hybrid Cloud Control aktualisiert wird.

a. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
   i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   ii. Geben Sie die Client-ID als ein `mnode-client`.
   iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

iv. Schließen Sie das Fenster.

b. Wählen Sie in DER REST API UI **GET /Installations** aus.

c. Wählen Sie **Probieren Sie es aus**.

d. Wählen Sie **Ausführen**.

e. Kopieren Sie als Antwort die Installations-Asset-ID (`"id"`).

f. Wählen Sie in DER REST-API-UI **GET /installations/{id}** aus.

g. Wählen Sie **Probieren Sie es aus**.

h. Stellen Sie „Aktualisieren“ auf fest `True`.

i. Fügen Sie die Installations-Asset-ID in das Feld **id** ein.

j. Wählen Sie **Ausführen**.

3. Aktualisieren Sie den Browser NetApp Hybrid Cloud Control, um die Änderungen anzuzeigen.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Fügen Sie dem Management-Node eine Controller-Ressource hinzu

Mithilfe der REST API UI können Sie der Management-Node-Konfiguration eine Controller-Ressource hinzufügen.

Möglicherweise müssen Sie ein Asset hinzufügen, wenn Sie vor Kurzem Ihre Installation skaliert haben und neue Ressourcen nicht automatisch zu Ihrer Konfiguration hinzugefügt wurden. Mithilfe dieser APIs können Sie Ressourcen hinzufügen, die zu Ihrer Installation hinzugefügt wurden.

Was Sie benötigen

- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.
- Sie haben eine neue NetApp HCC-Rolle in vCenter erstellt, um die Management-Node-Services-Ansicht auf reine NetApp Ressourcen zu begrenzen. Siehe "Erstellen einer NetApp HCC-Rolle in vCenter"

Schritte

1. Holen Sie sich die Basis-Asset-ID für die Installation:

   a. Öffnen Sie die REST API-UI für den Bestandsdienst auf dem Managementknoten:

   ```
   https://<ManagementNodeIP>/inventory/1/
   ```

   b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:

      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.

      ii. Geben Sie die Client-ID als ein `mnode-client`.

      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

iv. Schließen Sie das Fenster.

c. Wählen Sie in DER REST API UI **GET /Installations** aus.

d. Wählen Sie **Probieren Sie es aus**.

e. Wählen Sie **Ausführen**.

f. Kopieren Sie aus dem Text Code 200 Antwort den `id` Für die Installation.

```
{
  "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",
```

Die Installation verfügt über eine Basiskonfiguration, die während der Installation oder eines Upgrades erstellt wurde.

g. Wählen Sie in DER REST-API-UI **GET /installations/{id}** aus.

h. Wählen Sie **Probieren Sie es aus**.

i. Fügen Sie die Installations-Asset-ID in das Feld **id** ein.

j. Wählen Sie **Ausführen**.

k. Kopieren Sie aus der Antwort die Cluster-Controller-ID und speichern Sie sie (`"controllerId"`) Für den Einsatz in einem späteren Schritt.

2. Um einer vorhandenen Basisinressource eine Controller-Unterressource hinzuzufügen, wählen Sie:

```
POST /assets/{asset_id}/controllers
```

a. Öffnen Sie die MNODE-Service-REST-API-UI auf dem Management-Node:

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

b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:

i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.

ii. Geben Sie die Client-ID als ein `mnode-client`.

iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

iv. Schließen Sie das Fenster.

c. Wählen Sie **POST /Assets/{Asset_id}/Controllers** aus.

d. Wählen Sie **Probieren Sie es aus**.

e. Geben Sie die übergeordnete Basis-Asset-ID in das Feld **Asset_id** ein.

f. Fügen Sie die erforderlichen Werte der Nutzlast hinzu.

g. Wählen Sie **Ausführen**.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Erstellen und Managen von Storage-Cluster-Assets

Sie können dem Managementknoten neue Storage-Cluster-Assets hinzufügen, die gespeicherten Zugangsdaten für bekannte Storage-Cluster-Assets bearbeiten und Storage-Cluster-Assets über DIE REST-API vom Managementknoten löschen.

Was Sie benötigen

- Stellen Sie sicher, dass auf Ihrer Speichercluster-Version die NetApp Element-Software 11.3 oder höher ausgeführt wird.
- Stellen Sie sicher, dass Sie einen Management-Node mit Version 11.3 oder höher bereitgestellt haben.

Optionen für das Storage Cluster Asset Management

Wählen Sie eine der folgenden Optionen:

- Rufen Sie die Installations-ID und die Cluster-ID einer Storage-Cluster-Ressource ab
- Fügen Sie eine neue Storage-Cluster-Ressource hinzu
- Bearbeiten Sie die gespeicherten Anmeldedaten für eine Storage-Cluster-Ressource
- Löschen einer Speichercluster-Ressource

Rufen Sie die Installations-ID und die Cluster-ID einer Storage-Cluster-Ressource ab

Sie können die REST API verwenden, um die Installations-ID und die ID des Storage-Clusters zu erhalten. Sie benötigen die Installations-ID, um eine neue Storage Cluster-Ressource hinzuzufügen, und die Cluster-ID, um eine bestimmte Storage-Cluster-Ressource zu ändern oder zu löschen.

Schritte

1. Greifen Sie auf die REST-API-UI für den Bestandsdienst zu, indem Sie die IP-Adresse des Management-Node gefolgt von eingeben `/inventory/1/`:

   ```
   https://<ManagementNodeIP>/inventory/1/
   ```

2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:

   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.

   b. Geben Sie die Client-ID als ein `mnode-client`.

c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

d. Schließen Sie das Fenster.

3. Wählen Sie **GET /Installations**.
4. Wählen Sie **Probieren Sie es aus**.
5. Wählen Sie **Ausführen**.

   Die API gibt eine Liste aller bekannten Installationen zurück.

6. Speichern Sie aus dem Code 200 Response Body den Wert im `id` Feld, das Sie in der Liste der Installationen finden können. Dies ist die Installations-ID. Beispiel:

```
"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. Rufen Sie die REST-API-UI für den Storage-Service auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

8. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
9. Wählen Sie **GET /Clusters** aus.
10. Wählen Sie **Probieren Sie es aus**.
11. Geben Sie die Installations-ID ein, die Sie zuvor in gespeichert haben `installationId` Parameter.
12. Wählen Sie **Ausführen**.

    Die API gibt eine Liste aller bekannten Storage-Cluster in dieser Installation zurück.

13. Suchen Sie aus dem Code 200 Response Body den richtigen Storage Cluster und speichern Sie den Wert im Cluster `storageId` Feld. Dies ist die Storage-Cluster-ID.

Fügen Sie eine neue Storage-Cluster-Ressource hinzu

Mithilfe der REST API können Sie dem Management-Node-Bestand eine oder mehrere neue Storage-Cluster-Ressourcen hinzufügen. Wenn Sie eine neue Storage-Cluster-Ressource hinzufügen, wird diese automatisch beim Management-Node registriert.

Was Sie benötigen

- Sie haben die kopiert Storage Cluster-ID und Installations-ID Für jeden Storage-Cluster, den Sie hinzufügen möchten.
- Wenn Sie mehr als einen Storage-Node hinzufügen, haben Sie die Einschränkungen von gelesen und verstanden "Autorisierende Cluster" Unterstützung für mehrere Storage-Cluster.

> Alle Benutzer, die auf dem autorisierenden Cluster definiert werden, werden als Benutzer auf allen anderen Clustern definiert, die an die NetApp Hybrid Cloud Control Instanz gebunden sind.

Schritte

1. Rufen Sie die REST-API-UI für den Storage-Service auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/storage/1/`:

   ```
   https://<ManagementNodeIP>/storage/1/
   ```

2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie **POST /Cluster**.
4. Wählen Sie **Probieren Sie es aus**.
5. Geben Sie im Feld **Text anfordern** die Informationen des neuen Speicherclusters in die folgenden Parameter ein:

   ```
   {
     "installationId": "a1b2c34d-e56f-1a2b-c123-1ab2cd345d6e",
     "mvip": "10.0.0.1",
     "password": "admin",
     "userId": "admin"
   }
   ```

Parameter	Typ	Beschreibung
`installationId`	Zeichenfolge	Die Installation, in der der neue Speicher-Cluster hinzugefügt werden soll. Geben Sie die Installations-ID ein, die Sie zuvor in diesen Parameter gespeichert haben.
`mvip`	Zeichenfolge	Die virtuelle IPv4-Management-IP-Adresse (MVIP) des Speicherclusters.
`password`	Zeichenfolge	Das Passwort, das für die Kommunikation mit dem Storage-Cluster verwendet wird.
`userId`	Zeichenfolge	Die Benutzer-ID für die Kommunikation mit dem Speicher-Cluster (der Benutzer muss über Administratorrechte verfügen).

6. Wählen Sie **Ausführen**.

   Die API gibt ein Objekt mit Informationen über die neu hinzugefügte Storage-Cluster-Ressource zurück, z. B. Informationen über Name, Version und IP-Adresse.

Bearbeiten Sie die gespeicherten Anmeldedaten für eine Storage-Cluster-Ressource

Sie können die gespeicherten Anmeldeinformationen bearbeiten, die der Management-Node zur Anmeldung bei einem Storage-Cluster verwendet. Der von Ihnen gewählte Benutzer muss über einen Cluster-Admin-Zugriff verfügen.

Vergewissern Sie sich, dass Sie die Schritte in befolgt haben Rufen Sie die Installations-ID und die Cluster-ID einer Storage-Cluster-Ressource ab Bevor Sie fortfahren.

Schritte

1. Rufen Sie die REST-API-UI für den Storage-Service auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/storage/1/`:

   ```
   https://<ManagementNodeIP>/storage/1/
   ```

2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie **PUT /Clusters/{storageId}** aus.
4. Wählen Sie **Probieren Sie es aus**.

5. Fügen Sie die Storage-Cluster-ID ein, die Sie zuvor in kopiert haben `storageId` Parameter.
6. Ändern Sie im Feld **Text anfordern** einen oder beide der folgenden Parameter:

```
{
  "password": "adminadmin",
  "userId": "admin"
}
```

Parameter	Typ	Beschreibung
`password`	Zeichenfolge	Das Passwort, das für die Kommunikation mit dem Storage-Cluster verwendet wird.
`userId`	Zeichenfolge	Die Benutzer-ID für die Kommunikation mit dem Speicher-Cluster (der Benutzer muss über Administratorrechte verfügen).

7. Wählen Sie **Ausführen**.

Löschen einer Speichercluster-Ressource

Sie können eine Storage-Cluster-Ressource löschen, wenn das Storage-Cluster nicht mehr in Betrieb ist. Wenn Sie eine Storage-Cluster-Ressource entfernen, wird diese automatisch vom Management-Node registriert.

Vergewissern Sie sich, dass Sie die Schritte in befolgt haben Rufen Sie die Installations-ID und die Cluster-ID einer Storage-Cluster-Ressource ab Bevor Sie fortfahren.

Schritte

1. Rufen Sie die REST-API-UI für den Storage-Service auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie **DELETE /Clusters/{storageId}** aus.
4. Wählen Sie **Probieren Sie es aus**.
5. Geben Sie die Storage-Cluster-ID ein, die Sie zuvor in kopiert haben `storageId` Parameter.
6. Wählen Sie **Ausführen**.

Bei Erfolg gibt die API eine leere Antwort zurück.

Weitere Informationen

- "Autorisierende Cluster"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Vorhandene Controller-Assets können angezeigt oder bearbeitet werden

Sie können Informationen zu vorhandenen VMware vCenter Controllern in der Management-Node-Konfiguration über DIE REST-API anzeigen und bearbeiten. Controller sind VMware vCenter Instanzen, die bei Ihrer NetApp SolidFire Installation auf dem Management-Node registriert sind.

Bevor Sie beginnen

- Stellen Sie sicher, dass auf Ihrer Cluster-Version NetApp Element 11.3 oder höher ausgeführt wird.
- Stellen Sie sicher, dass Sie einen Management-Node mit Version 11.3 oder höher bereitgestellt haben.

Zugriff auf DIE REST-API für Managementservices

Schritte

1. Rufen Sie die REST-API-UI für Managementservices auf, indem Sie die IP-Adresse des Management-Node gefolgt von eingeben `/vcenter/1/`:

   ```
   https://<ManagementNodeIP>/vcenter/1/
   ```

2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.

Anzeigen gespeicherter Informationen zu vorhandenen Controllern

Sie können vorhandene vCenter Controller, die beim Management-Node registriert sind, auflisten und gespeicherte Informationen über sie mithilfe der REST-API anzeigen.

Schritte

1. Wählen Sie **GET /Compute/Controller** aus.
2. Wählen Sie **Probieren Sie es aus**.
3. Wählen Sie **Ausführen**.

   Die API gibt eine Liste aller bekannten vCenter-Controller sowie die IP-Adresse, Controller-ID, Hostname und Benutzer-ID zurück, die für die Kommunikation mit jedem Controller verwendet wurden.

4. Wenn Sie den Verbindungsstatus eines bestimmten Controllers möchten, kopieren Sie die Controller-ID von `id` Feld dieses Controllers in der Zwischenablage und siehe Den Status eines vorhandenen Controllers anzeigen.

Den Status eines vorhandenen Controllers anzeigen

Sie können den Status aller vorhandenen vCenter Controller anzeigen, die beim Management-Node registriert sind. Die API gibt einen Status zurück, der angibt, ob NetApp Hybrid Cloud Control sich sowohl mit dem vCenter Controller verbinden kann als auch mit dem Grund für diesen Status.

Schritte

1. Wählen Sie **GET /Compute/Controllers/{Controller_id}/Status** aus.
2. Wählen Sie **Probieren Sie es aus**.
3. Geben Sie die Controller-ID ein, die Sie zuvor in kopiert haben `controller_id` Parameter.
4. Wählen Sie **Ausführen**.

   Die API gibt einen Status dieses bestimmten vCenter-Controllers zurück, zusammen mit einem Grund für diesen Status.

Bearbeiten Sie die gespeicherten Eigenschaften eines Controllers

Sie können den gespeicherten Benutzernamen oder das gespeicherte Passwort für einen der vorhandenen vCenter Controller bearbeiten, die beim Management-Node registriert sind. Sie können die gespeicherte IP-Adresse eines vorhandenen vCenter-Controllers nicht bearbeiten.

Schritte

1. Wählen Sie **PUT /Compute/Controllers/{Controller_id}** aus.
2. Geben Sie die Controller-ID eines vCenter Controllers in ein `controller_id` Parameter.
3. Wählen Sie **Probieren Sie es aus**.
4. Ändern Sie einen der folgenden Parameter im Feld **Text anfordern**:

Parameter	Typ	Beschreibung
`userId`	Zeichenfolge	Ändern Sie die Benutzer-ID, die für die Kommunikation mit dem vCenter Controller verwendet wird (der Benutzer muss über Administratorrechte verfügen).
`password`	Zeichenfolge	Ändern Sie das Passwort, das für die Kommunikation mit dem vCenter Controller verwendet wird.

5. Wählen Sie **Ausführen**.

   Die API gibt aktualisierte Controller-Informationen zurück.

Weitere Informationen

- "Fügen Sie dem Management-Node eine Controller-Ressource hinzu"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Konfigurieren Sie einen Proxyserver

Wenn Ihr Cluster hinter einem Proxy-Server liegt, müssen Sie die Proxy-Einstellungen so konfigurieren, dass Sie ein öffentliches Netzwerk erreichen können.

Für Telemetrie-Kollektoren und Reverse-Tunnel-Verbindungen wird ein Proxy-Server verwendet. Sie können einen Proxy-Server mithilfe der REST API-UI aktivieren und konfigurieren, falls Sie während der Installation oder dem Upgrade noch keinen Proxy-Server konfiguriert haben. Sie können auch vorhandene Proxy-Server-Einstellungen ändern oder einen Proxy-Server deaktivieren.

Der Befehl zum Konfigurieren von Updates für einen Proxy-Server und gibt dann die aktuellen Proxy-Einstellungen für den Management-Node zurück. Die Proxy-Einstellungen werden von Active IQ, dem NetApp Monitoring-Service und anderen Element Software Utilities verwendet, die auf dem Management-Node installiert sind. Hierzu zählen auch der Reverse-Support-Tunnel für NetApp Support.

Bevor Sie beginnen

- Sie sollten Host- und Anmeldeinformationen für den Proxyserver kennen, den Sie konfigurieren.
- Stellen Sie sicher, dass auf Ihrer Cluster-Version NetApp Element 11.3 oder höher ausgeführt wird.
- Stellen Sie sicher, dass Sie einen Management-Node mit Version 11.3 oder höher bereitgestellt haben.
- (Management-Node 12.0 und höher) vor der Konfiguration eines Proxy-Servers haben Sie die NetApp Hybrid Cloud Control auf die Managementservices Version 2.16 aktualisiert.

Schritte

1. Greifen Sie auf die REST-API-UI auf dem Management-Node zu, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode`:

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

2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie **PUT /settings**.
4. Wählen Sie **Probieren Sie es aus**.
5. Um einen Proxyserver zu aktivieren, müssen Sie festlegen `use_proxy` Um wahr zu sein. Geben Sie die IP- oder Host-Namen und Proxy-Port-Ziele ein.

   Der Proxy-Benutzername, das Proxy-Passwort und der SSH-Port sind optional und sollten bei Nichtverwendung weggelassen werden.

```
{
"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. Wählen Sie **Ausführen**.

Je nach Umgebung müssen Sie möglicherweise Ihren Management Node neu booten.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Überprüfen Sie die Betriebssystem- und Servicestversionen der Management-Nodes

Sie können die Versionsnummern des Management-Node-Betriebssystems, des Managementservices-Pakets und der einzelnen Services, die auf dem Management-Node ausgeführt werden, mithilfe der REST-API im Management-Node überprüfen.

Was Sie benötigen

- Auf dem Cluster wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.

Optionen

- API-Befehle
- SCHRITTE DER REST API-UI

API-Befehle

- Hier erhalten Sie Versionsinformationen zum Management-Node OS, zum Management-Services-Bundle und zum Management-Node-API-Service (mNode-API), der auf dem Management-Node ausgeführt wird:

```
curl -X GET "https://<ManagementNodeIP>/mnode/about" -H  "accept:
application/json"
```

- Abrufen der Versionsinformationen zu den einzelnen auf dem Management-Node ausgeführten Services:

```
curl -X GET "https://<ManagementNodeIP>/mnode/services?status=running"
-H  "accept: */*" -H  "Authorization: ${TOKEN}"
```

Ihr könnt den Träger finden `${TOKEN}` Wird von dem API-Befehl verwendet, wenn Sie "Autorisieren". Der Träger `${TOKEN}` Ist in der Curl-Antwort.

SCHRITTE DER REST API-UI

1. Rufen Sie die REST-API-UI für den Service auf, indem Sie die Management-Node-IP-Adresse, gefolgt von, eingeben `/mnode/`:

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

2. Führen Sie einen der folgenden Schritte aus:
   - Hier erhalten Sie Versionsinformationen zum Management-Node OS, zum Management-Services-Bundle und zum Management-Node-API-Service (mNode-API), der auf dem Management-Node ausgeführt wird:
     i. Wählen Sie **GET /about** aus.
     ii. Wählen Sie **Probieren Sie es aus**.
     iii. Wählen Sie **Ausführen**.

     Die Bundle-Version der Managementservices (`"mnode_bundle_version"`), Version des Management-Node-Betriebssystems (`"os_version"`) Und der Version der Management-Node-API (`"version"`) Sind im Antwortkörper angegeben.
   - Abrufen der Versionsinformationen zu den einzelnen auf dem Management-Node ausgeführten Services:
     i. Wählen Sie **GET /Services**.
     ii. Wählen Sie **Probieren Sie es aus**.
     iii. Wählen Sie den Status als **läuft** aus.
     iv. Wählen Sie **Ausführen**.

     Die Dienste, die auf dem Management-Knoten ausgeführt werden, werden im Response Body angezeigt.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Abrufen von Protokollen von Managementservices

Sie können mithilfe der REST API Protokolle von den Services abrufen, die auf dem Management-Node ausgeführt werden. Sie können Protokolle aus allen öffentlichen

Diensten abrufen oder bestimmte Dienste angeben und Abfrageparameter verwenden, um die Rückgabeergebnisse besser zu definieren.

Was Sie benötigen

- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.

Schritte

1. Öffnen Sie die REST-API-UI auf dem Managementknoten.
   - Ab Management Services 2.21.61:

     ```
     https://<ManagementNodeIP>/mnode/4/
     ```

   - Für Managementservices ab Version 2.20.69:

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

2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als mNode-Client ein, wenn der Wert nicht bereits gefüllt ist.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie **GET /logs**.
4. Wählen Sie **Probieren Sie es aus**.
5. Geben Sie die folgenden Parameter an:
   - `Lines`: Geben Sie die Anzahl der Zeilen ein, die das Protokoll zurückgeben soll. Bei diesem Parameter handelt es sich um eine Ganzzahl, die standardmäßig auf 1000 gesetzt ist.

     Vermeiden Sie es, den gesamten Verlauf des Protokollinhalts anzufragen, indem Sie Zeilen auf 0 setzen.

   - `since`: Fügt einen ISO-8601-Zeitstempel für den Startpunkt der Service-Protokolle hinzu.

     Machen Sie einen vernünftigen Rahmen `since` Parameter beim Sammeln von Protokollen mit größeren Zeitpfannen.

   - `service-name`: Geben Sie einen Dienstnamen ein.

     Verwenden Sie die `GET /services` Befehl zum Auflisten von Services auf dem Management-Node.

   - `stopped`: Auf eingestellt `true` Um Protokolle von angehalten Diensten abzurufen.
6. Wählen Sie **Ausführen**.

7. Wählen Sie im Antwortkörper **Download** aus, um die Protokollausgabe zu speichern.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Managen von Supportverbindungen

Zugriff auf Storage-Nodes mithilfe von SSH für die grundlegende Fehlerbehebung

Ab Element 12.5 können Sie das sfReadonly System-Konto auf den Storage-Nodes für eine grundlegende Fehlerbehebung nutzen. Sie können außerdem den Zugriff auf den Remote-Support-Tunnel für eine erweiterte Fehlerbehebung aktivieren und öffnen.

Das sfReadonly Systemkonto ermöglicht den Zugriff auf die Ausführung grundlegender Befehle zur Fehlerbehebung im Linux-System und Netzwerk, einschließlich `ping`.

> Sofern nicht vom NetApp Support beraten, werden Änderungen an diesem System nicht unterstützt, sodass Sie Ihren Support-Vertrag aufgeben und möglicherweise die Daten instabil oder unzugänglich machen können.

Bevor Sie beginnen

- **Schreibberechtigungen**: Stellen Sie sicher, dass Sie Schreibberechtigungen in das aktuelle Arbeitsverzeichnis haben.
- **(Optional) Generieren Sie Ihr eigenes Schlüsselpaar**: Laufen `ssh-keygen` Aus Windows 10, MacOS oder Linux-Distribution. Dies ist eine einmalige Aktion, um ein Benutzerschlüsselpaar zu erstellen und kann für zukünftige Fehlerbehebungssitzungen verwendet werden. Möglicherweise möchten Sie Zertifikate verwenden, die mit Mitarbeiterkonten verknüpft sind, was auch in diesem Modell funktionieren würde.
- **SSH-Funktion auf dem Management-Node aktivieren**: Um die Remote-Zugriffsfunktion im Verwaltungsmodus zu aktivieren, siehe "Diesem Thema". Für Managementservices ab Version 2.18 ist die Möglichkeit für den Remote-Zugriff auf dem Management-Node standardmäßig deaktiviert.
- **SSH-Funktion auf dem Storage-Cluster aktivieren**: Um die Remote-Zugriffsfunktion auf den Storage-Cluster-Knoten zu aktivieren, siehe "Diesem Thema".
- **Firewall-Konfiguration**: Wenn sich Ihr Management-Knoten hinter einem Proxy-Server befindet, sind die folgenden TCP-Ports in der Datei sshd.config erforderlich:

TCP-Port	Beschreibung	Verbindungsrichtung
443	API-Aufrufe/HTTPS zur Umkehrung der Port-Weiterleitung über offenen Support-Tunnel zur Web-UI	Management-Node zu Storage-Nodes
22	SSH-Login-Zugriff	Management-Node zu Storage-Nodes oder von Storage-Nodes zum Management-Node

Fehlerbehebungsoptionen

- Fehlerbehebung für einen Cluster-Node
- Fehlerbehebung für einen Cluster Node mit NetApp Support
- der nicht zum Cluster gehört

Fehlerbehebung für einen Cluster-Node

Sie können grundlegende Fehlerbehebungsmaßnahmen mit dem sfReadonly Systemkonto durchführen:

Schritte

1. SSH zum Management-Node mit Ihren Account-Anmeldedaten, die Sie beim Installieren der Management-Node-VM ausgewählt haben.
2. Wechseln Sie am Management-Node zu `/sf/bin`.
3. Suchen Sie das passende Skript für Ihr System:
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

   > SignSshKeys.ps1 ist abhängig von PowerShell 7 oder höher und SignSshKeys.py ist abhängig von Python 3.6.0 oder höher und dem "Anträgen-Modul".
   >
   > Der `SignSshKeys` Skript-Schreibvorgänge `user`, `user.pub`, und `user-cert.pub` Dateien in das aktuelle Arbeitsverzeichnis, die später vom verwendet werden `ssh` Befehl. Wenn dem Skript jedoch eine öffentliche Schlüsseldatei zur Verfügung gestellt wird, ist nur a verfügbar `<public_key>` Datei (mit `<public_key>` Ersetzt durch das Präfix der in das Skript übergebenen öffentlichen Schlüsseldatei) wird in das Verzeichnis geschrieben.

4. Führen Sie das Skript auf dem Management-Node aus, um die SSH-Schlüsselkette zu generieren. Das Skript ermöglicht den SSH-Zugriff über das sfReadonly Systemkonto über alle Nodes im Cluster hinweg.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--publickey [public key path]
```

   a. Ersetzen Sie den Wert in [ ] Klammern (einschließlich der Klammern) für jeden der folgenden Parameter:

      > Sie können entweder den abgekürzten oder den vollständigen Parameter verwenden.

      - **--ip: -i [ip-Adresse]**: IP-Adresse des Ziel-Knotens für die API, gegen die ausgeführt werden soll.
      - *--user: Cluster-Benutzer verwendet, um den API-Aufruf auszuführen.
      - **(Optional) --duration -d [hours]**: Die Dauer eines signierten Schlüssels sollte als Ganzzahl in Stunden gültig sein. Die Standardeinstellung ist 24 Stunden.
      - **(Optional) --publickey (öffentlicher Schlüsselpfad)**: Der Weg zu einem öffentlichen Schlüssel, wenn der Benutzer sich entscheidet, einen zu liefern.

   b. Vergleichen Sie Ihre Angaben mit dem folgenden Beispielbefehl. In diesem Beispiel `10.116.139.195` Die IP des Storage-Nodes `admin` Ist der Cluster-Benutzername und die Dauer der Schlüsselgültigkeit

zwei Stunden:

```
sh /sf/bin/SignSshKeys.sh --ip 10.116.139.195 --user admin --duration
2
```

c. Führen Sie den Befehl aus.

5. SSH an die Node-IPs:

```
ssh -i user sfreadonly@[node_ip]
```

Sie können grundlegende Linux-System- und Netzwerk-Fehlerbehebungsbefehle wie ausführen `ping`, Und anderen schreibgeschützten Befehlen.

6. (Optional) Deaktivieren "Remote-Zugriffsfunktion" Nach Abschluss der Fehlerbehebung erneut.

> SSH bleibt auf dem Management-Node aktiviert, wenn Sie ihn nicht deaktivieren. Die SSH-fähige Konfiguration bleibt auf dem Management-Node durch Updates und Upgrades bestehen, bis sie manuell deaktiviert ist.

Fehlerbehebung für einen Cluster Node mit NetApp Support

NetApp Support kann bei einer Systemkonto eine erweiterte Fehlerbehebung durchführen, sodass Techniker eine umfassendere Elementdiagnose durchführen können.

Schritte

1. SSH zum Management-Node mit Ihren Account-Anmeldedaten, die Sie beim Installieren der Management-Node-VM ausgewählt haben.
2. Führen Sie den rst-Befehl mit der Port-Nummer aus, die von NetApp Support gesendet wurde, um den Support-Tunnel zu öffnen:

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

   Der NetApp Support meldet sich mithilfe des Support-Tunnels am Management-Node an.

3. Wechseln Sie am Management-Node zu `/sf/bin`.
4. Suchen Sie das passende Skript für Ihr System:
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

SignSshKeys.ps1 ist abhängig von PowerShell 7 oder höher und SignSshKeys.py ist abhängig von Python 3.6.0 oder höher und dem "Anträgen-Modul".

Der `SignSshKeys` Skript-Schreibvorgänge `user`, `user.pub`, und `user-cert.pub` Dateien in das aktuelle Arbeitsverzeichnis, die später vom verwendet werden `ssh` Befehl. Wenn dem Skript jedoch eine öffentliche Schlüsseldatei zur Verfügung gestellt wird, ist nur a verfügbar `<public_key>` Datei (mit `<public_key>` Ersetzt durch das Präfix der in das Skript übergebenen öffentlichen Schlüsseldatei) wird in das Verzeichnis geschrieben.

5. Führen Sie das Skript aus, um die SSH-Schlüsselkette mit dem zu generieren `--sfadmin` Flagge. Das Skript ermöglicht SSH über alle Nodes hinweg.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--sfadmin
```

Für SSH als `--sfadmin` Um einen Cluster-Knoten zu erhalten, müssen Sie die SSH-Schlüsselanhänger mit einem generieren `--user` Mit `supportAdmin` Zugriff auf das Cluster.

Zu konfigurieren `supportAdmin` Zugriff für Cluster-Administratorkonten können Sie die Element UI oder die APIs verwenden:

- "Konfigurieren Sie den Zugriff auf „SupportAdmin“ über die Element UI"
- Konfigurieren `supportAdmin` Zugriff über APIs und Hinzufügen `"supportAdmin"` Als der `"access"` Geben Sie die API-Anforderung ein:
  - "Konfigurieren Sie den Zugriff auf „SupportAdmin“ für ein neues Konto"
  - "Konfigurieren Sie den Zugriff auf „SupportAdmin“ für ein vorhandenes Konto"

    Um die zu bekommen `clusterAdminID`, Sie können die verwenden "ListenClusteradministratoren" API:

Hinzufügen `supportAdmin` Zugriff: Sie müssen über Cluster-Administrator- oder Administratorrechte verfügen.

a. Ersetzen Sie den Wert in [ ] Klammern (einschließlich der Klammern) für jeden der folgenden Parameter:

   Sie können entweder den abgekürzten oder den vollständigen Parameter verwenden.

   - **--ip: -i [ip-Adresse]**: IP-Adresse des Ziel-Knotens für die API, gegen die ausgeführt werden soll.
   - *--user: Cluster-Benutzer verwendet, um den API-Aufruf auszuführen.
   - **(Optional) --duration -d [hours]**: Die Dauer eines signierten Schlüssels sollte als Ganzzahl in Stunden gültig sein. Die Standardeinstellung ist 24 Stunden.

b. Vergleichen Sie Ihre Angaben mit dem folgenden Beispielbefehl. In diesem Beispiel `192.168.0.1` Die IP des Storage-Nodes `admin` Ist der Cluster-Benutzername, die Schlüsseldauer beträgt zwei Stunden, und `--sfadmin` Ermöglicht NetApp Support Node-Zugriff zur Fehlerbehebung:

```
sh /sf/bin/SignSshKeys.sh --ip 192.168.0.1 --user admin --duration 2
--sfadmin
```

c. Führen Sie den Befehl aus.

6. SSH an die Node-IPs:

```
ssh -i user sfadmin@[node_ip]
```

7. Um den Remote Support-Tunnel zu schließen, geben Sie Folgendes ein:

```
rst --killall
```

8. (Optional) Deaktivieren "Remote-Zugriffsfunktion" Nach Abschluss der Fehlerbehebung erneut.

> SSH bleibt auf dem Management-Node aktiviert, wenn Sie ihn nicht deaktivieren. Die SSH-fähige Konfiguration bleibt auf dem Management-Node durch Updates und Upgrades bestehen, bis sie manuell deaktiviert ist.

Fehlerbehebung für einen Node, der nicht zum Cluster gehört

Sie können grundlegende Fehlerbehebung für einen Node ausführen, der noch nicht zu einem Cluster hinzugefügt wurde. Sie können das sfReadonly System-Konto zu diesem Zweck mit oder ohne Hilfe von NetApp Unterstützung verwenden. Wenn ein Management-Node eingerichtet wurde, können Sie ihn für SSH verwenden und das angegebene Skript für diese Aufgabe ausführen.

1. Führen Sie auf einem Windows-, Linux- oder Mac-Computer mit installiertem SSH-Client das entsprechende Skript für Ihr von NetApp Support bereitgestellte System aus.
2. SSH an die Node-IP:

```
ssh -i user sfreadonly@[node_ip]
```

3. (Optional) Deaktivieren "Remote-Zugriffsfunktion" Nach Abschluss der Fehlerbehebung erneut.

> SSH bleibt auf dem Management-Node aktiviert, wenn Sie ihn nicht deaktivieren. Die SSH-fähige Konfiguration bleibt auf dem Management-Node durch Updates und Upgrades bestehen, bis sie manuell deaktiviert ist.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "NetApp HCI-Dokumentation"

Starten Sie eine Remote NetApp Support Sitzung

Falls Sie technischen Support für Ihr SolidFire All-Flash-Storage-System benötigen, kann

sich NetApp Support per Fernzugriff mit Ihrem System verbinden. Um eine Sitzung zu starten und Remote-Zugriff zu erhalten, kann der NetApp Support eine Reverse Secure Shell-(SSH)-Verbindung zu Ihrer Umgebung öffnen.

Sie können einen TCP-Port für eine SSH-Reverse-Tunnel-Verbindung mit NetApp Support öffnen. Über diese Verbindung kann sich NetApp Support beim Management Node einloggen.

Bevor Sie beginnen

- Für Managementservices ab Version 2.18 ist die Möglichkeit für den Remote-Zugriff auf dem Management-Node standardmäßig deaktiviert. Informationen zum Aktivieren der Fernzugriffsfunktionen finden Sie unter "Verwalten der SSH-Funktionalität auf dem Management-Node".
- Wenn sich der Managementknoten hinter einem Proxyserver befindet, sind die folgenden TCP-Ports in der Datei sshd.config erforderlich:

TCP-Port	Beschreibung	Verbindungsrichtung
443	API-Aufrufe/HTTPS zur Umkehrung der Port-Weiterleitung über offenen Support-Tunnel zur Web-UI	Management-Node zu Storage-Nodes
22	SSH-Login-Zugriff	Management-Node zu Storage-Nodes oder von Storage-Nodes zum Management-Node

Schritte

- Melden Sie sich bei Ihrem Management-Knoten an und öffnen Sie eine Terminalsitzung.
- Geben Sie an einer Eingabeaufforderung Folgendes ein:

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

- Um den Remote Support-Tunnel zu schließen, geben Sie Folgendes ein:

```
rst --killall
```

- (Optional) Deaktivieren "Remote-Zugriffsfunktion" Ein weiteres Jahr in der

> SSH bleibt auf dem Management-Node aktiviert, wenn Sie ihn nicht deaktivieren. Die SSH-fähige Konfiguration bleibt auf dem Management-Node durch Updates und Upgrades bestehen, bis sie manuell deaktiviert ist.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Verwalten der SSH-Funktionalität auf dem Management-Node

Sie können den Status der SSH-Funktion auf dem Management-Node (mNode) mithilfe der REST-API deaktivieren, neu aktivieren oder bestimmen. SSH-Funktion, die bietet

"Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist auf Management-Knoten, die Management-Services 2.18 oder höher ausführen, standardmäßig deaktiviert.

Ab Management Services 2.20.69 können Sie die SSH-Funktion auf dem Management-Node über die NetApp Hybrid Cloud Control UI aktivieren und deaktivieren.

Was Sie benötigen

- **NetApp Hybrid Cloud Control Berechtigungen**: Sie haben Berechtigungen als Administrator.
- **Cluster Administrator Berechtigungen**: Sie haben Berechtigungen als Administrator auf dem Speicher-Cluster.
- **Element Software**: Auf Ihrem Cluster läuft die NetApp Element Software 11.3 oder höher.
- **Management-Node**: Sie haben einen Management-Node mit Version 11.3 oder höher bereitgestellt.
- **Aktualisierungen von Managementservices**:
  - Um die NetApp Hybrid Cloud Control UI zu verwenden, haben Sie Ihr aktualisiert "Management Services-Bundle" Auf Version 2.20.69 oder höher.
  - Um die REST API-UI zu verwenden, haben Sie das aktualisiert "Management Services-Bundle" Auf Version 2.17.

Optionen

- Deaktivieren oder aktivieren Sie die SSH-Funktion auf dem Management-Node mithilfe der NetApp Hybrid Cloud Control UI

Nach der Durchführung können Sie eine der folgenden Aufgaben ausführen "Authentifizierung":

- Deaktiviert bzw. aktiviert die SSH-Funktion auf dem Management-Node mithilfe von APIs
- Ermitteln des Status der SSH-Funktion auf dem Management-Node mithilfe von APIs

Deaktivieren oder aktivieren Sie die SSH-Funktion auf dem Management-Node mithilfe der NetApp Hybrid Cloud Control UI

Sie können die SSH-Funktion auf dem Management-Node deaktivieren oder neu aktivieren. SSH-Funktion, die bietet "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist auf Management-Knoten, die Management-Services 2.18 oder höher ausführen, standardmäßig deaktiviert. Durch Deaktivieren von SSH werden vorhandene SSH-Client-Sessions nicht zum Management-Node beendet oder getrennt. Wenn Sie SSH deaktivieren und sich zu einem späteren Zeitpunkt erneut aktivieren, können Sie dazu die Benutzeroberfläche von NetApp Hybrid Cloud Control verwenden.

> Um den Support-Zugriff über SSH für ein Storage-Cluster zu aktivieren oder zu deaktivieren, müssen Sie die verwenden "Seite „Cluster-Einstellungen für Element UI“".

Schritte

1. Wählen Sie im Dashboard oben rechts das Optionsmenü aus und wählen Sie **Konfigurieren**.
2. Schalten Sie im Bildschirm **Support Access for Management Node** den Switch ein, um den Management-Node SSH zu aktivieren.
3. Nach Abschluss der Fehlerbehebung schalten Sie im Bildschirm **Support Access for Management Node** den Switch ein, um SSH des Management-Node zu deaktivieren.

Deaktiviert bzw. aktiviert die SSH-Funktion auf dem Management-Node mithilfe von APIs

Sie können die SSH-Funktion auf dem Management-Node deaktivieren oder neu aktivieren. SSH-Funktion, die bietet "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist auf Management-Knoten, die Management-Services 2.18 oder höher ausführen, standardmäßig deaktiviert. Durch Deaktivieren von SSH werden vorhandene SSH-Client-Sessions nicht zum Management-Node beendet oder getrennt. Wenn Sie SSH deaktivieren und sich für eine spätere erneute Aktivierung entscheiden, können Sie dies über dieselbe API tun.

API-Befehl

Für Management Services 2.18 oder höher:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Für Managementservices ab Version 2.17:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Ihr könnt den Träger finden `${TOKEN}` Wird von dem API-Befehl verwendet, wenn Sie "Autorisieren". Der Träger `${TOKEN}` Ist in der Curl-Antwort.

SCHRITTE DER REST API-UI

1. Rufen Sie die REST-API-UI für den API-Service des Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode/`:

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

2. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie in DER REST API-Benutzeroberfläche **PUT /settings/ssh** aus.
   a. Wählen Sie **Probieren Sie es aus**.
   b. Legen Sie den Parameter **Enabled** auf fest `false` Um SSH oder zu deaktivieren `true` Um die zuvor deaktivierte SSH-Funktion wieder zu aktivieren.
   c. Wählen Sie **Ausführen**.

Ermitteln des Status der SSH-Funktion auf dem Management-Node mithilfe von APIs

Sie können ermitteln, ob die SSH-Funktion auf dem Management-Node mithilfe einer Management-Node-Service-API aktiviert ist. SSH ist auf Management-Nodes, auf denen Management-Services 2.18 oder höher ausgeführt werden, standardmäßig deaktiviert.

API-Befehl

Für Management Services 2.18 oder höher:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Für Managementservices ab Version 2.17:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Ihr könnt den Träger finden `${TOKEN}` Wird von dem API-Befehl verwendet, wenn Sie "Autorisieren". Der Träger `${TOKEN}` Ist in der Curl-Antwort.

SCHRITTE DER REST API-UI

1. Rufen Sie die REST-API-UI für den API-Service des Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode/`:

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

2. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie in DER REST API UI **GET /settings/ssh** aus.
   a. Wählen Sie **Probieren Sie es aus**.
   b. Wählen Sie **Ausführen**.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Upgrade für Ihr NetApp SolidFire All-Flash-Storage-System

Übersicht der Aktualisierungssequenz

Sie können das SolidFire Element Storage-System nach der Implementierung immer auf dem neuesten Stand halten, indem Sie alle NetApp Storage-Komponenten sequenziell aktualisieren.

Zu diesen Komponenten gehören Managementservices, NetApp Hybrid Cloud Control, Element Software, Management-Node und (je nach Installation) das Element Plug-in für vCenter Server.

- Ab November 2023 können Sie kein Komponenten-Upgrade mehr über NetApp Hybrid Cloud Control oder die REST-API starten, da die Signaturschlüsselzertifikate (privat und öffentlich) am 5. November 2023 abgelaufen sind. Dieses Problem lässt sich umgehen, indem man"Durchführen eines in-Place-Upgrades des Management-Node" Vor der Verwendung der NetApp Hybrid Cloud Control oder REST-API zum Aktualisieren der Management-Services, der Element-Software und der Speicher-Firmware muss auf Version 12.8 oder höher aktualisiert werden.

  Wenn Sie einen neuen Management-Knoten mit Version 12.8 oder höher bereitstellen, können Sie die NetApp Hybrid Cloud Control oder die REST-API verwenden, um Komponenten-Upgrades in der unten aufgeführten Reihenfolge durchzuführen.Systemaktualisierungssequenz Die

- Die folgenden Nodes werden nicht unterstützt. Wenn Sie versuchen, einen dieser Knoten auf eine nicht unterstützte Elementversion zu aktualisieren, wird eine Fehlermeldung angezeigt, die besagt, dass der Knoten nicht von Element 12.x unterstützt wird:
  - Ab Element 12.8, SF4805, SF9605, SF19210 und SF38410 Storage-Nodes
  - Ab Element 12.7, SF2405 und SF9608 Storage-Nodes und FC-Nodes FC0025 und SF-FCN-01
- Ab Element 12.5 werden NetApp HealthTools bei Upgrades der Element Software nicht mehr unterstützt. Wenn Sie Element 11.0 oder 11.1 ausführen, müssen Sie zuerst "Upgrade auf Element 12.3 mit HealthTools" Und dann upgraden Sie mithilfe von NetApp Hybrid Cloud Control auf Element 12.5 oder höher.

Der Systemaktualisierungssequenz Inhalt beschreibt die Aufgaben, die zum Abschluss eines Upgrades eines SolidFire All-Flash-Storage-Systems erforderlich sind. Idealerweise werden diese Verfahren als Teil der größeren Aufrüstsequenz und nicht isoliert durchgeführt. Wenn ein komponentenbasiertes Upgrade oder eine Aktualisierung erforderlich ist, lesen Sie die Verfahrensvoraussetzungen, um sicherzustellen, dass zusätzliche Komplexität bewältigt wird.

Der "VSphere-Upgrade-Sequenz" Der Inhalt des Element Plug-ins für vCenter Server enthält zusätzliche Schritte vor und nach dem Upgrade, die zur Neuinstallation des Element Plug-ins für vCenter Server erforderlich sind.

Bevor Sie beginnen

- Sie führen Management-Node 11.3 oder höher aus. Neuere Versionen des Management-Node verfügen über eine modulare Architektur, die individuelle Services zur Verfügung stellt.

Um die Version zu überprüfen, melden Sie sich bei Ihrem Management-Node an, und zeigen Sie die Versionsnummer des Elements im Anmeldebanner an. Wenn Sie keine 11.3 haben, lesen Sie "Upgrade Ihres Management-Node".

- Sie haben Ihre Managementservices auf mindestens Version 2.1.326 aktualisiert.

  Upgrades mit NetApp Hybrid Cloud Control sind in früheren Service-Bundle-Versionen nicht verfügbar.

- Sie stellen sicher, dass die Systemzeit auf allen Knoten synchronisiert ist und dass NTP für den Speicher-Cluster und die Knoten korrekt konfiguriert ist. Jeder Node muss in der Web-UI pro Node mit einem DNS-Nameserver konfiguriert sein (`https://[IP address]:442`) Ohne ungelöste Cluster Fehler im Zusammenhang mit Zeitverzerrung.
- Sie haben genügend Zeit für Ihr geplant "Element Software" Und "Storage-Firmware" Upgrades: Bei einem Upgrade auf Element Software 12.5 oder höher variiert die Dauer des Upgradevorgangs je nach Version der Element Software und Firmware-Updates.

Systemaktualisierungssequenz

Mithilfe der folgenden Sequenz können Sie Ihr NetApp SolidFire All-Flash-Storage-System für Element 12.5 oder höher aktualisieren.

Schritte

1. "Führen Sie vor dem Upgrade des Speichers Integritätsprüfungen des Element-Speichers durch" .
2. "(Optional) Upgrade Ihres Management-Node".

   Sie müssen das Betriebssystem des Management-Knotens nicht mehr aktualisieren, um die Element-Software auf dem Speichercluster zu aktualisieren. Wenn der Management-Knoten die Version 11.3 oder höher aufweist, können Sie die Management-Dienste einfach auf die neueste Version aktualisieren, um Element-Upgrades mit NetApp Hybrid Cloud Control durchzuführen. Falls Sie das Betriebssystem des Management-Knotens aus anderen Gründen, wie z. B. zur Behebung von Sicherheitslücken, aktualisieren müssen, befolgen Sie die für Ihr Szenario vorgesehene Vorgehensweise zur Aktualisierung des Management-Knotens.

3. "Aktualisierung der Managementservices von Hybrid Cloud Control".

   - Das Management Services 2.27 Bundle enthält das Element Plug-in für vCenter Server 5.5, das nur mit Management Node 12.8 oder höher kompatibel ist. Wenn Sie auf Management Services 2.27 aktualisieren, müssen Sie die Upgrade-Reihenfolge ändern und das Management Services-Paket *nach* dem Upgrade auf Element 12.9 aktualisieren, um Kompatibilität zwischen dem Management-Knoten und den Management Services zu gewährleisten.
   - Wenn Sie auf die Verwaltungsdienste 2.21.61 bis 2.26.40 aktualisieren, müssen Sie das Verwaltungsdienstpaket *vor* dem Upgrade auf Element 12.9 aktualisieren.

   Wenn Sie die Verwaltungsdienste auf Version 2.16 oder höher aktualisieren und einen Verwaltungsknoten 11.3 bis 11.8 ausführen, müssen Sie den RAM Ihrer Verwaltungsknoten-VM erhöhen, bevor Sie die Verwaltungsdienste aktualisieren.

4. "Aktualisieren Sie die Element Software und die Storage-Firmware".

5. "(Optional) Aktualisieren Sie nur die Element Storage-Firmware".

   Möglicherweise führen Sie diese Aufgabe aus, wenn außerhalb einer Hauptversion ein neues Speicher-Firmware-Upgrade verfügbar wird.

6. "Aktualisieren Sie Ihr Element Plug-in für vCenter Server".

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Verfahren für System-Upgrades

Integritätsprüfungen von Element Storage vor einem Storage Upgrade durchführen

Vor dem Upgrade von Element Storage müssen Sie Zustandsprüfungen durchführen, um sicherzustellen, dass alle Storage-Nodes im Cluster für das nächste Element Storage Upgrade bereit sind.

Was Sie benötigen

- **Management Services**: Sie haben das neueste Management Services Bundle (2.10.27 oder höher) aktualisiert.

  Vor einem Upgrade der Element Software müssen Sie ein Upgrade auf das neueste Management Services Bundle durchführen.

- **Management-Node**:Sie führen Management-Node 11.3 oder höher aus.
- **Element Software**: Ihre Clusterversion wird mit der NetApp Element Software 11.3 oder höher ausgeführt.
- **Endbenutzer-Lizenzvereinbarung (EULA)**: Ab Management Services 2.20.69 müssen Sie die EULA akzeptieren und speichern, bevor Sie die NetApp Hybrid Cloud Control UI oder API verwenden, um die Integritätsprüfungen für Element Storage auszuführen:
  a. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

  b. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
  c. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.
  d. Die EULA erscheint. Scrollen Sie nach unten, wählen Sie **Ich akzeptiere aktuelle und alle zukünftigen Updates** und wählen Sie **Speichern**.

Optionen zur Zustandsprüfung

Mit der Benutzeroberfläche von NetApp Hybrid Cloud Control oder der NetApp Hybrid Cloud Control API lassen sich Systemchecks durchführen:

- NetApp Hybrid Cloud Control bietet Zustandsüberprüfungen für Element Storage vor Storage-Upgrades (Bevorzugte Methode)

Weitere Informationen zu den vom Service ausgeführten Storage-Zustandsprüfungen:

- die vom Service durchgeführt werden

NetApp Hybrid Cloud Control bietet Zustandsüberprüfungen für Element Storage vor Storage-Upgrades

Mit NetApp Hybrid Cloud Control können Sie überprüfen, ob ein Storage-Cluster aktualisiert werden kann.

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.
4. Wählen Sie auf der Seite **Upgrades** die Registerkarte **Storage** aus.
5. Wählen Sie die Integritätsprüfung aus Für den Cluster möchten Sie die Upgrade-Bereitschaft überprüfen.
6. Wählen Sie auf der Seite **Storage Health Check** die Option **Run Health Check**.
7. Gehen Sie bei Problemen wie folgt vor:
   a. Gehen Sie zu dem für jedes Problem angegebenen KB-Artikel oder führen Sie das angegebene Heilmittel aus.
   b. Wenn ein KB angegeben wird, führen Sie den im entsprechenden KB-Artikel beschriebenen Prozess aus.
   c. Wählen Sie nach der Behebung von Cluster-Problemen die Option **Integritätsprüfung erneut ausführen** aus.

Nachdem die Integritätsprüfung ohne Fehler abgeschlossen wurde, kann das Storage-Cluster aktualisiert werden. Siehe Upgrade des Storage-Node "Anweisungen" Fortfahren.

Nutzen Sie API zur Ausführung von Element Storage-Zustandsprüfungen vor einem Storage-Upgrade

Mithilfe DER REST-API können Sie überprüfen, ob ein Storage-Cluster aktualisiert werden kann. Bei der Zustandsprüfung werden keine Hindernisse für Upgrades beseitigt, z. B. ausstehende Nodes, Probleme mit Festplattenspeicher und Cluster-Fehler.

Schritte

1. Suchen Sie die Storage Cluster ID:

   a. Öffnen Sie die REST-API-UI für den Management-Node:

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

b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:

   i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.

   ii. Geben Sie die Client-ID als ein `mnode-client` Wenn der Wert nicht bereits ausgefüllt ist.

   iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

   iv. Schließen Sie das Autorisierungsfenster.

c. Wählen Sie in DER REST API-UI aus `GET /assets`.

d. Wählen Sie **Probieren Sie es aus**.

e. Wählen Sie **Ausführen**.

f. Kopieren Sie von der Antwort die `"id"` Von `"storage"` Abschnitt des Clusters, den Sie auf die Upgrade-Bereitschaft überprüfen möchten.

> Verwenden Sie das nicht `"parent"` Der Wert in diesem Abschnitt, da dies die ID des Management-Node und nicht die ID des Storage-Clusters ist.

```
"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. Führen Sie Zustandsprüfungen für das Storage Cluster durch:

a. Öffnen Sie die Storage REST API-UI auf dem Management-Node:

```
https://<ManagementNodeIP>/storage/1/
```

b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:

   i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.

   ii. Geben Sie die Client-ID als ein `mnode-client` Wenn der Wert nicht bereits ausgefüllt ist.

   iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

   iv. Schließen Sie das Autorisierungsfenster.

c. Wählen Sie **POST/Health-Checks**.

d. Wählen Sie **Probieren Sie es aus**.

e. Geben Sie im Feld Parameter die Storage-Cluster-ID ein, die in Schritt 1 erhalten wurde.

```
{
  "config": {},
  "storageId": "123a45b6-1a2b-12a3-1234-1a2b34c567d8"
}
```

f. Wählen Sie **Ausführen** aus, um eine Integritätsprüfung auf dem angegebenen Speichercluster auszuführen.

Die Antwort sollte Status als angeben `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. Kopieren Sie die `healthCheckID` Das ist Teil der Antwort.

3. Überprüfen Sie die Ergebnisse der Zustandsprüfungen:

a. Wählen Sie **GET /Health-checks/{healtCheckId}** aus.

b. Wählen Sie **Probieren Sie es aus**.

c. Geben Sie im Feld Parameter die ID für die Integritätsprüfung ein.

d. Wählen Sie **Ausführen**.

e. Blättern Sie zum unteren Rand des Antwortkörpers.

Wenn alle Zustandsprüfungen erfolgreich sind, ähnelt die Rückkehr dem folgenden Beispiel:

```
"message": "All checks completed successfully.",
"percent": 100,
"timestamp": "2020-03-06T00:03:16.321621Z"
```

4. Wenn der `message` „Return“ gibt an, dass im Hinblick auf den Cluster-Systemzustand Probleme aufgetreten sind. Führen Sie folgende Schritte aus:
   a. Wählen Sie **GET /Health-checks/{healtCheckId}/log** aus
   b. Wählen Sie **Probieren Sie es aus**.
   c. Geben Sie im Feld Parameter die ID für die Integritätsprüfung ein.
   d. Wählen Sie **Ausführen**.
   e. Überprüfen Sie alle bestimmten Fehler und erhalten Sie die zugehörigen KB-Artikellinks.
   f. Gehen Sie zu dem für jedes Problem angegebenen KB-Artikel oder führen Sie das angegebene Heilmittel aus.
   g. Wenn ein KB angegeben wird, führen Sie den im entsprechenden KB-Artikel beschriebenen Prozess aus.
   h. Nachdem Sie Cluster-Probleme behoben haben, führen Sie wieder **GET /Health-checks /{healtCheckId}/log** aus.

Storage-Systemprüfungen, die vom Service durchgeführt werden

Bei den Storage-Zustandsprüfungen werden die folgenden Prüfungen pro Cluster durchgeführt.

Prüfen Sie Den Namen	Node/Cluster	Beschreibung
Check_async_Results	Cluster	Überprüft, ob die Anzahl der asynchronen Ergebnisse in der Datenbank unter einer Schwellennummer liegt.
„Check_Cluster_Fehlerbeseitigung“	Cluster	Stellt sicher, dass keine Fehler beim Blockieren von Cluster beim Upgrade auftreten (wie in Element Source definiert)
Check_Upload_Speed	Knoten	Misst die Upload-Geschwindigkeit zwischen dem Storage-Node und dem Management-Node.
Connection_Speed_Check	Knoten	Stellt sicher, dass Nodes mit dem Management-Node verbunden sind, der Upgrade-Pakete bereitstellt, und schätzt die Verbindungsgeschwindigkeit.
Check_Cores	Knoten	Überprüft auf den Kernel Crash Dump und die Core-Dateien auf dem Node. Die Prüfung schlägt bei Abstürzen in einem der letzten Zeit (Schwellenwert 7 Tage) fehl.
Prüfen Sie_root_Disk_space	Knoten	Überprüft, ob das Root-Dateisystem über genügend freien Speicherplatz verfügt, um ein Upgrade durchzuführen.

Prüfen Sie Den Namen	Node/Cluster	Beschreibung
Überprüfen Sie_var_log_Disk_space	Knoten	Überprüft das `/var/log` Freier Speicherplatz entspricht einem prozentualen freien Schwellenwert. Wenn dies nicht der Fall ist, dreht sich die Prüfung und löscht ältere Protokolle, um unter den Schwellenwert zu fallen. Die Prüfung schlägt fehl, wenn die Erstellung von ausreichend freiem Speicherplatz nicht erfolgreich ist.
Prüfung_ausstehend_Knoten	Cluster	Stellt sicher, dass keine ausstehenden Nodes im Cluster vorhanden sind.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Upgrade eines Management-Node

Sie können Ihren Management-Node ab Version 12.3.x oder höher auf den Management-Node 12.5 oder höher aktualisieren.

Zum Upgrade der Element Software auf dem Storage-Cluster ist kein Upgrade des Betriebssystems des Management-Node mehr erforderlich. Die Managementservices können einfach auf die neueste Version aktualisiert werden, um Element-Upgrades mit NetApp Hybrid Cloud Control durchzuführen. Befolgen Sie für Ihr Szenario die Vorgehensweise zum Upgrade des Management-Node, wenn Sie aus anderen Gründen, wie z. B. Sicherheitsbehebungsmaßnahmen, ein Upgrade des Betriebssystems des Management-Node durchführen möchten.

Wenn Sie Informationen zum Upgrade von Management-Knoten 12.2 oder älter benötigen, lesen Sie den "Upgrade-Dokumentation für Element 12.3.x Management-Node".

Schritt: Upgrade der VM-Hardwareversion auf einem Management-Node

Wenn Sie ein In-Place-Upgrade eines bestehenden Management-Knotens auf Element 12.9 durchführen, müssen Sie vor dem Upgrade sicherstellen, dass die VM-Hardwareversion auf dem Management-Knoten mit ESXi 6.7 (VM-Hardwareversion 14) oder höher kompatibel ist, abhängig von Ihrer Umgebung.

Schritte

1. Melden Sie sich beim vSphere Web Client als vCenter Administrator an.
2. Wählen Sie im vSphere Client-Menü **VMs und Vorlagen** aus.
3. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine (VM), und wählen Sie **Power** > **Gastbetriebssystem herunterfahren**.

   Warten Sie, bis die VM ausgeschaltet ist.

4. Klicken Sie mit der rechten Maustaste auf die VM, und wählen Sie **Kompatibilität** > **VM-Kompatibilität**

aktualisieren.

5. Wählen Sie **Ja**.
6. Wählen Sie je nach Version Ihrer vSphere-Umgebung ESXi 6.7 oder eine höhere Version aus.
7. Wählen Sie **OK**.
8. Klicken Sie nach Abschluss des Upgrades mit der rechten Maustaste auf die VM, und wählen Sie **Power** > **Power On**.
9. Wählen Sie **vSphere Client refresh** aus, und überprüfen Sie, ob die VM-Kompatibilität die gewünschte Version hat.

Schritt 2: Aktualisieren Sie einen Management-Node auf Element 12.5 oder höher

Wählen Sie eine der folgenden Upgrade-Optionen:

- Aktualisieren Sie einen Management-Node von Version 12.3.x oder höher auf Version 12.5 oder höher
- Konfigurieren Sie die Authentifizierung mithilfe der REST-API des Management-Node neu

  Wählen Sie diese Option, wenn Sie **sequenziell** aktualisiert haben (1) die Version der Managementservices und (2) Ihre Element Speicherversion und Ihren vorhandenen Management-Node **beibehalten** möchten:

Wenn Sie Ihre Managementservices, gefolgt vom Element Storage, nicht nacheinander aktualisieren, können Sie die erneute Authentifizierung mit diesem Verfahren nicht neu konfigurieren. Befolgen Sie stattdessen das entsprechende Upgrade-Verfahren.

Aktualisieren Sie einen Management-Node von Version 12.3.x oder höher auf Version 12.5 oder höher

Sie können ein in-Place-Upgrade des Management-Node von Version 12.3.x oder höher auf Version 12.5 oder höher durchführen, ohne eine neue Management-Node-VM bereitstellen zu müssen.

Der Element 12.5 oder höher ist ein optionales Upgrade. Bei bestehenden Implementierungen wird dieser Bedarf nicht benötigt.

Bevor Sie beginnen

- Der RAM der Management-Node-VM ist 24 GB.
- Der Management-Node, den Sie aktualisieren möchten, ist die Version 12.0 und verwendet IPv4-Netzwerke. Der Management-Node Version 12.5 oder höher unterstützt IPv6 nicht.

Um die Version Ihres Management-Node zu überprüfen, melden Sie sich bei Ihrem Management-Node an, und zeigen Sie die Versionsnummer des Elements im Anmeldebanner an.

- Sie haben das Management-Services-Bundle mit NetApp Hybrid Cloud Control auf die neueste Version aktualisiert. NetApp Hybrid Cloud Control kann über folgende IP-Adresse darauf zugreifen: `https://<ManagementNodeIP>`
- Wenn Sie Ihren Managementknoten auf Version 12.5 oder höher aktualisieren, benötigen Sie Managementdienste 2.21.61 oder höher, um fortzufahren.
- Sie haben (falls erforderlich) einen zusätzlichen Netzwerkadapter mit den Anweisungen für konfiguriert "Konfigurieren einer zusätzlichen Speicher-NIC".

Für persistente Volumes ist möglicherweise ein zusätzlicher Netzwerkadapter erforderlich, wenn eth0 nicht an das SVIP weitergeleitet werden kann. Konfigurieren Sie einen neuen Netzwerkadapter im iSCSI-Speichernetzwerk zur Konfiguration von persistenten Volumes.

- Auf Storage-Nodes ist Element 12.3.x oder höher ausgeführt.

Schritte

1. Melden Sie sich bei der Management-Node-VM über SSH oder Konsolenzugriff an.
2. Laden Sie die for Element Software von der NetApp Support-Website auf die Management-Node-VM herunter "ISO für den Management-Node".

   Der Name der ISO ist ähnlich wie `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Prüfen Sie die Integrität des Downloads, indem Sie md5sum auf der heruntergeladenen Datei ausführen und vergleichen Sie die Ausgabe mit den verfügbaren Ressourcen der NetApp Support Site für Element Software wie im folgenden Beispiel:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

4. Mounten Sie das Management-Node-ISO-Image und kopieren Sie den Inhalt auf das Dateisystem mit den folgenden Befehlen:

   ```
   sudo mkdir -p /upgrade
   ```

   ```
   sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso> /mnt
   ```

   ```
   sudo cp -r /mnt/* /upgrade
   ```

5. Wechseln Sie in das Home-Verzeichnis, und heben Sie die Bereitstellung der ISO-Datei von ab `/mnt`:

   ```
   sudo umount /mnt
   ```

6. Löschen Sie die ISO, um Speicherplatz auf dem Management-Node einzusparen:

   ```
   sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

7. Führen Sie auf dem Management-Node, den Sie aktualisieren, den folgenden Befehl aus, um die Version des Management-Node-Betriebssystems zu aktualisieren. Das Skript speichert alle erforderlichen Konfigurationsdateien nach dem Upgrade, wie z. B. Active IQ-Collector- und Proxy-Einstellungen.

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

Der Management-Node wird nach Abschluss des Upgrades mit einem neuen OS neu gebootet.

> Nachdem Sie den in diesem Schritt beschriebenen Sudo-Befehl ausgeführt haben, wird die SSH-Sitzung abgebrochen. Für kontinuierliches Monitoring ist ein Konsolenzugriff erforderlich. Wenn während des Upgrades kein Konsolenzugriff verfügbar ist, versuchen Sie die SSH-Anmeldung erneut, und überprüfen Sie die Verbindung nach 15 bis 30 Minuten. Nach der Anmeldung können Sie die neue Betriebssystemversion im SSH-Banner bestätigen, die angibt, dass das Upgrade erfolgreich war.

8. Führen Sie auf dem Management-Node den aus `redeploy-mnode` Skript zur Beibehaltung der Konfigurationseinstellungen für frühere Managementservices:

> Das Skript behält die vorherige Konfiguration der Managementservices bei, einschließlich der Konfiguration über den Active IQ Collector Service, Controller (vCenters) oder Proxy, je nach Ihren Einstellungen.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

> Wenn Sie die SSH-Funktion zuvor auf dem Management-Node deaktiviert hatten, müssen Sie dies ausführen "Deaktivieren Sie SSH erneut" Auf dem wiederhergestellten Management-Node. SSH-Funktion, die bietet "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist standardmäßig auf dem Management-Node aktiviert.

Konfigurieren Sie die Authentifizierung mithilfe der REST-API des Management-Node neu

Bei einem sequenziell aktualisierten Management-Service (1) und (2) Element Storage können bestehende Management-Node weiterhin verwendet werden. Wenn Sie eine andere Upgrade-Reihenfolge eingehalten haben, lesen Sie die Verfahren für Upgrades von vorhandenen Management-Nodes.

Bevor Sie beginnen

- Sie haben Ihre Managementservices auf Version 2.20.69 oder höher aktualisiert.
- Im Storage Cluster wird Element 12.3 oder höher ausgeführt.
- Sie haben Ihre Managementservices sequenziell aktualisiert und anschließend den Element Storage aktualisiert. Mit diesem Verfahren können Sie die Authentifizierung erst neu konfigurieren, wenn Sie Upgrades in der beschriebenen Reihenfolge durchgeführt haben.

Schritte

1. Öffnen Sie die REST-API-UI für den Management-Node:

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

2. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:

a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.

b. Geben Sie die Client-ID als ein `mnode-client` Wenn der Wert nicht bereits ausgefüllt ist.

c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

3. Wählen Sie in DER REST API-Benutzeroberfläche **POST /Services/rekonfigurieren-auth** aus.
4. Wählen Sie **Probieren Sie es aus**.
5. Wählen Sie für den Parameter **load_images** `true`.
6. Wählen Sie **Ausführen**.

   Der Antwortkörper zeigt an, dass die Neukonfiguration erfolgreich war.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Managementservices aktualisieren

Sie können Ihre Managementservices nach der Installation des Management Node 11.3 oder höher auf die neueste Bundle-Version aktualisieren.

Seit der Version für Element 11.3 Management-Nodes wurde das Design der Management-Nodes auf Grundlage einer neuen modularen Architektur, die individuelle Services bietet, geändert. Diese modularen Services bieten zentrale und erweiterte Managementfunktionen für ein SolidFire All-Flash-Storage-System. Zu den Managementservices gehören Systemtelemetrie, Protokollierung und Update-Services, der QoSSIOC-Service für das Element Plug-in für vCenter Server, NetApp Hybrid Cloud Control und vieles mehr.

Über diese Aufgabe

Das Management Services 2.27 Bundle enthält das Element Plug-in für vCenter Server 5.5, das nur mit Management Node 12.8 oder höher kompatibel ist. Wenn Sie auf Management Services 2.27 aktualisieren, müssen Sie die Upgrade-Reihenfolge ändern und das Management Services-Paket *nach* dem Upgrade auf Element 12.9 aktualisieren, um Kompatibilität zwischen dem Management-Knoten und den Management Services zu gewährleisten.

Wenn Sie auf die Verwaltungsdienste 2.21.61 bis 2.26.40 aktualisieren, müssen Sie das Verwaltungsdienstpaket *vor* dem Upgrade auf Element 12.9 aktualisieren.

- Die Management Services 2.22.7 enthalten das Element-Plug-in für vCenter Server 5.0, welches das Remote-Plug-in umfasst. Wenn Sie das Element-Plug-in verwenden, sollten Sie auf Management Services 2.22.7 oder höher aktualisieren, um der VMware-Richtlinie zu entsprechen, die die Unterstützung für lokale Plug-ins einstellt. "Weitere Informationen ."Die
- Die neuesten Versionshinweise für Management-Services zu wichtigen Services, neuen Funktionen, Bug Fixes und Behelfslösungen für jedes Service Bundle finden Sie unter "Die Versionshinweise für Managementservices"

Was Sie benötigen

Ab Management Services 2.20.69 müssen Sie die Endbenutzer-Lizenzvereinbarung (Endbenutzer License Agreement, EULA) akzeptieren und speichern, bevor Sie die NetApp Hybrid Cloud Control UI oder -API für Upgrade-Managementservices verwenden:

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.
4. Die EULA erscheint. Scrollen Sie nach unten, wählen Sie **Ich akzeptiere aktuelle und alle zukünftigen Updates** und wählen Sie **Speichern**.

Update-Optionen

Die Managementservices können mit der NetApp Hybrid Cloud Control UI oder DER REST-API des Management-Node aktualisiert werden:

- Aktualisieren von Managementservices mit Hybrid Cloud Control (Empfohlene Methode)
- Aktualisieren Sie Managementservices mit der Management-Node-API

Aktualisieren von Managementservices mit Hybrid Cloud Control

Sie können Ihre NetApp Managementservices mit NetApp Hybrid Cloud Control aktualisieren.

Management-Service-Bundles bieten erweiterte Funktionen und Korrekturen an Ihrer Installation außerhalb der größeren Versionen.

Bevor Sie beginnen

- Sie führen Management-Node 11.3 oder höher aus.
- Wenn Sie Managementservices auf Version 2.16 oder höher aktualisieren und einen Management-Node 11.3 bis 11.8 ausführen, müssen Sie vor der Aktualisierung der Managementservices den RAM der Management-Node-VM erhöhen:
  a. Schalten Sie die Management-Node-VM aus.
  b. Ändern Sie den RAM der Management-Node-VM von 12 GB in 24 GB RAM.
  c. Schalten Sie die Management-Node-VM ein.
- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben Ihre Managementservices auf mindestens Version 2.1.326 aktualisiert. Upgrades der NetApp Hybrid Cloud Control sind in früheren Servicepaketen nicht verfügbar.

Eine Liste der verfügbaren Services für jede Service-Bundle-Version finden Sie unter "Versionshinweise Für Management Services".

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.

3. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.
4. Wählen Sie auf der Seite Upgrades die Registerkarte **Management Services** aus.
5. Befolgen Sie die Anweisungen auf der Seite, um ein Upgrade-Paket für Verwaltungsdienste auf Ihrem Computer herunterzuladen und zu speichern.
6. Wählen Sie **Durchsuchen**, um das gespeicherte Paket zu finden und hochzuladen.

   Nach dem Hochladen des Pakets wird das Upgrade automatisch gestartet.

   Nach Beginn des Upgrades sehen Sie den Aktualisierungsstatus auf dieser Seite. Während des Upgrades besteht unter Umständen keine Verbindung zu NetApp Hybrid Cloud Control und muss sich erneut anmelden, um die Ergebnisse des Upgrades anzuzeigen.

Aktualisieren Sie Managementservices mit der Management-Node-API

Benutzer sollten idealerweise Management-Services-Updates von NetApp Hybrid Cloud Control durchführen. Sie können jedoch ein Service Bundle-Update für Managementservices manuell über die REST-API hochladen, extrahieren und implementieren. Sie können jeden Befehl für den Management-Node von DER REST-API-UI ausführen.

Bevor Sie beginnen

- Sie haben einen NetApp Element Software-Management-Node 11.3 oder höher implementiert.
- Wenn Sie Managementservices auf Version 2.16 oder höher aktualisieren und einen Management-Node 11.3 bis 11.8 ausführen, müssen Sie vor der Aktualisierung der Managementservices den RAM der Management-Node-VM erhöhen:
  a. Schalten Sie die Management-Node-VM aus.
  b. Ändern Sie den RAM der Management-Node-VM von 12 GB in 24 GB RAM.
  c. Schalten Sie die Management-Node-VM ein.
- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben Ihre Managementservices auf mindestens Version 2.1.326 aktualisiert. Upgrades der NetApp Hybrid Cloud Control sind in früheren Servicepaketen nicht verfügbar.

> Eine Liste der verfügbaren Services für jede Service-Bundle-Version finden Sie unter "Versionshinweise Für Management Services".

Schritte

1. Öffnen Sie die REST API-UI auf dem Managementknoten: `https://<ManagementNodeIP>/mnode`
2. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client` Wenn der Wert nicht bereits ausgefüllt ist.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Laden Sie das Service-Bundle mit diesem Befehl auf den Management-Node hoch und extrahieren Sie es. `PUT /services/upload`
4. Implementieren der Managementservices auf dem Management-Node: `PUT /services/deploy`

5. Überwachen Sie den Status der Aktualisierung: `GET /services/update/status`

   Ein erfolgreiches Update liefert ein Ergebnis, das dem folgenden Beispiel ähnelt:

```
{
"current_version": "2.10.29",
"details": "Updated to version 2.17.52",
"status": "success"
}
```

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Upgrade der Element Software

Für ein Upgrade der NetApp Element Software kann die NetApp Hybrid Cloud Control UI oder DIE REST-API verwendet werden. Bestimmte Vorgänge werden bei einem Upgrade der Element Software unterdrückt, z. B. beim Hinzufügen und Entfernen von Nodes, beim Hinzufügen und Entfernen von Laufwerken sowie Befehle, die unter anderem mit Initiatoren, Volume-Zugriffsgruppen und virtuellen Netzwerken verbunden sind.

> Das Management Services 2.27 Bundle enthält das Element Plug-in für vCenter Server 5.5, das nur mit Management Node 12.8 oder höher kompatibel ist. Wenn Sie auf Management Services 2.27 aktualisieren, müssen Sie die Upgrade-Reihenfolge ändern und das Management Services-Paket *nach* dem Upgrade auf Element 12.9 aktualisieren, um Kompatibilität zwischen dem Management-Knoten und den Management Services zu gewährleisten.
>
> Wenn Sie auf die Verwaltungsdienste 2.21.61 bis 2.26.40 aktualisieren, müssen Sie das Verwaltungsdienstpaket *vor* dem Upgrade auf Element 12.9 aktualisieren.

Bevor Sie beginnen

- **Administratorrechte**: Sie haben Berechtigungen für den Storage Cluster Administrator, um das Upgrade durchzuführen.
- **Gültiger Upgrade-Pfad**: Sie haben die Upgrade-Pfadinformationen für die Element-Version, auf die Sie aktualisieren, überprüft und bestätigt, dass der Upgrade-Pfad gültig ist.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: Upgrade-Matrix für Storage Cluster mit NetApp Element Software"^]

  Ab Element 12.5 werden NetApp HealthTools bei Upgrades der Element Software nicht mehr unterstützt. Wenn Sie Element 11.0 oder 11.1 ausführen, müssen Sie zuerst "Upgrade auf Element 12.3.x mit HealthTools" Und dann upgraden Sie mithilfe von NetApp Hybrid Cloud Control auf Element 12.5 oder höher.

- **System Time SYNC**: Sie haben sichergestellt, dass die Systemzeit auf allen Knoten synchronisiert ist und NTP für den Speicher-Cluster und die Knoten korrekt konfiguriert ist. Jeder Node muss in der Web-UI pro

Node mit einem DNS-Nameserver konfiguriert sein (`https://[IP address]:442`) Ohne ungelöste Cluster Fehler im Zusammenhang mit Zeitverzerrung.

- **System-Ports**: Bei Upgrade-Nutzung von NetApp Hybrid Cloud Control haben Sie sichergestellt, dass die erforderlichen Ports geöffnet sind. Siehe "Netzwerkports" Finden Sie weitere Informationen.
- **Management-Node**: Für NetApp Hybrid Cloud Control UI und API wird der Management-Node in Ihrer Umgebung mit Version 11.3 ausgeführt.
- **Cluster Health**: Sie haben überprüft, dass der Cluster bereit ist, aktualisiert zu werden. Siehe "Integritätsprüfungen von Element Storage vor einem Storage Upgrade durchführen".
- **Aktualisierter Baseboard Management Controller (BMC) für H610S Storage Nodes**: Sie haben die BMC-Version für Ihre H610S-Knoten aktualisiert. Siehe "Versionshinweise und Upgrade-Anweisungen".
- **Aktualisierungszeit**: Sie haben genügend Zeit für die Durchführung Ihres Upgrades eingeplant. Bei einem Upgrade auf Element Software 12.5 oder höher variiert die Dauer des Upgradevorgangs je nach aktueller Element Softwareversion und Firmware-Updates.

Storage-Node	Aktuelle Version der Element Software	Ungefähre Installationszeit für Software und Firmware pro Node[1]	Ungefähre Synchronisierung szeit pro Knoten[2]	Ungefähre gesamte Upgrade-Zeit pro Node
Alle SolidFire und NetApp H-Series Nodes mit aktueller Firmware[3]	12.x	15 Minuten	10 bis 15 Minuten	20 bis 30 Minuten
H610S und H410S	12.x und 11.8	60 Minuten	30 bis 60 Minuten	90 bis 120 Minuten
H610S	11.7 und früher	90 Minuten	40 bis 70 Minuten	130 bis 160 Minuten müssen Sie auch "Führen Sie ein komplettes Herunterfahren des Node durch, und trennen Sie die Stromversorgung" Für jeden H610S Node.

[1]eine vollständige Matrix von Firmware und Treiber-Firmware für Ihre Hardware finden Sie unter "Unterstützte Storage-Firmware-Versionen für SolidFire Storage-Nodes".

[2]Wenn Sie ein Cluster mit einer hohen Lese-IOPS-Last und einer längeren Firmware-Update-Zeit kombinieren, erhöht sich die Zeit für die Datensynchronisierung.

[3] die folgenden Nodes werden nicht unterstützt. Wenn Sie versuchen, einen dieser Knoten auf eine nicht unterstützte Elementversion zu aktualisieren, wird eine Fehlermeldung angezeigt, die besagt, dass der Knoten nicht von Element 12.x unterstützt wird:

  - Ab Element 12.8, SF4805, SF9605, SF19210 und SF38410 Storage-Nodes
  - Ab Element 12.7, SF2405 und SF9608 Storage-Nodes und FC-Nodes FC0025 und SF-FCN-01

- **Endbenutzer-Lizenzvereinbarung (EULA)**: Ab Management Services 2.20.69 müssen Sie die EULA akzeptieren und speichern, bevor Sie die NetApp Hybrid Cloud Control UI oder API zum Upgrade von

Element Software verwenden:

a. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

b. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.

c. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.

d. Die EULA erscheint. Scrollen Sie nach unten, wählen Sie **Ich akzeptiere aktuelle und alle zukünftigen Updates** und wählen Sie **Speichern**.

Upgrade-Optionen

Wählen Sie eine der folgenden Upgrade-Optionen für Element Software:

- Verwendung der NetApp Hybrid Cloud Control UI für das Upgrade von Element Storage
- Nutzen Sie die NetApp Hybrid Cloud Control API für das Upgrade von Element Storage

Wenn Sie einen Node der H610S-Serie auf Element 12.5 oder höher aktualisieren und auf dem Node eine Version von Element vor 11.8 ausgeführt wird, müssen Sie in diesem Fall die zusätzlichen Upgrade-Schritte durchführen "KB-Artikel" Für jeden Storage-Node. Wenn Sie Element 11.8 oder höher ausführen, sind keine weiteren Aktualisierungsschritte erforderlich.

Verwendung der NetApp Hybrid Cloud Control UI für das Upgrade von Element Storage

Über die Benutzeroberfläche von NetApp Hybrid Cloud Control können Sie ein Storage-Cluster-Upgrade durchführen.

Informationen zu potenziellen Problemen beim Upgrade von Storage-Clustern mit NetApp Hybrid Cloud Control und den zugehörigen Workarounds finden Sie in diesem Dokument "KB-Artikel".

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.
4. Wählen Sie auf der Seite **Upgrades** die Option **Speicherung**.

   Auf der Registerkarte **Storage** werden die Speichercluster aufgelistet, die Teil Ihrer Installation sind. Wenn durch NetApp Hybrid Cloud Control auf ein Cluster zugegriffen werden kann, wird es nicht auf der Seite **Upgrades** angezeigt.

5. Wählen Sie eine der folgenden Optionen aus und führen Sie die für das Cluster zutreffenden Schritte aus:

Option	Schritte
Alle Cluster laufen mit Element 11.8 und höher	a. Wählen Sie **Durchsuchen**, um das heruntergeladene Aktualisierungspaket hochzuladen. b. Warten Sie, bis der Upload abgeschlossen ist. In einer Statusleiste wird der Status des Uploads angezeigt. Der Datei-Upload geht verloren, wenn Sie vom Browser-Fenster wegnavigieren. Nach dem erfolgreichen Hochladen und Validierungen der Datei wird eine Meldung auf dem Bildschirm angezeigt. Die Validierung kann mehrere Minuten in Anspruch nehmen. Wenn Sie zu diesem Zeitpunkt vom Browser-Fenster weg navigieren, bleibt der Datei-Upload erhalten. c. Wählen Sie **Upgrade Starten**. Der **Upgrade-Status** ändert sich während des Upgrades, um den Status des Prozesses anzuzeigen. Es ändert sich auch in Reaktion auf Aktionen, die Sie ergreifen, z. B. die Unterbrechung des Upgrades oder wenn das Upgrade einen Fehler zurückgibt. Siehe Statusänderungen des Upgrades. Während das Upgrade läuft, können Sie die Seite verlassen und zu einem späteren Zeitpunkt zurückkehren, um den Fortschritt zu überwachen. Die Seite aktualisiert den Status und die aktuelle Version nicht dynamisch, wenn die Cluster-Zeile ausgeblendet ist. Die Cluster-Zeile muss erweitert werden, um die Tabelle zu aktualisieren, oder Sie können die Seite aktualisieren. Sie können Protokolle herunterladen, nachdem die Aktualisierung abgeschlossen ist.

Option	Schritte
Sie aktualisieren ein H610S Cluster mit Element Version vor 11.8.	a. Wählen Sie den Dropdown-Pfeil neben dem Cluster aus, das Sie aktualisieren möchten, und wählen Sie aus den verfügbaren Upgrade-Versionen aus. b. Wählen Sie **Upgrade Starten**. Nach Abschluss des Upgrades werden Sie von der Benutzeroberfläche aufgefordert, weitere Aktualisierungsschritte durchzuführen. c. Führen Sie die zusätzlichen Schritte aus, die im erforderlich sind "KB-Artikel", Und bestätigen Sie in der Benutzeroberfläche, dass Sie Phase 2 abgeschlossen haben. Sie können Protokolle herunterladen, nachdem die Aktualisierung abgeschlossen ist. Informationen zu den verschiedenen Änderungen des Aktualisierungsstatus finden Sie unter Statusänderungen des Upgrades.

Statusänderungen des Upgrades

Hier sind die verschiedenen Status, in denen die Spalte **Upgrade Status** in der UI vor, während und nach dem Upgrade-Prozess angezeigt wird:

Upgrade-Status	Beschreibung
Auf dem aktuellen Stand	Der Cluster wurde auf die aktuellste verfügbare Element Version aktualisiert.
Verfügbare Versionen	Neuere Versionen von Element und/oder Storage Firmware stehen für ein Upgrade zur Verfügung.
In Bearbeitung	Das Upgrade läuft. In einer Statusleiste wird der Aktualisierungsstatus angezeigt. Auf dem Bildschirm werden zudem Fehler auf Node-Ebene angezeigt und die Node-ID jedes Node im Cluster wird angezeigt, wenn das Upgrade fortschreitet. Sie können den Status jedes Knotens über die Element-UI oder das NetApp Element Plug-in für vCenter Server UI überwachen.
Anhalten Des Upgrades	Sie können das Upgrade anhalten. Je nach Status des Upgrade-Prozesses kann der Pause-Vorgang erfolgreich oder fehlgeschlagen sein. Es wird eine UI-Eingabeaufforderung angezeigt, in der Sie aufgefordert werden, den Pause-Vorgang zu bestätigen. Um sicherzustellen, dass sich das Cluster vor dem Anhalten eines Upgrades an einem sicheren Ort befindet, kann es bis zu zwei Stunden dauern, bis der Upgrade-Vorgang vollständig angehalten ist. Um das Upgrade fortzusetzen, wählen Sie **Fortsetzen**.

Upgrade-Status	Beschreibung
Angehalten	Sie haben das Upgrade angehalten. Wählen Sie **Fortsetzen**, um den Prozess fortzusetzen.
Fehler	Während des Upgrades ist ein Fehler aufgetreten. Sie können das Fehlerprotokoll herunterladen und an den NetApp Support senden. Nachdem Sie den Fehler behoben haben, können Sie zur Seite zurückkehren und **Fortsetzen** wählen. Wenn Sie das Upgrade fortsetzen, geht die Statusleiste einige Minuten lang zurück, während das System die Zustandsprüfung ausführt und den aktuellen Status des Upgrades überprüft.
Füllen Sie das Follow-up aus	Nur für H610S Nodes, die ein Upgrade von Element Version vor 11.8 durchführen. Nachdem Phase 1 des Upgrade-Vorgangs abgeschlossen ist, werden Sie in diesem Zustand aufgefordert, weitere Aktualisierungsschritte auszuführen (siehe "KB-Artikel"). Nachdem Sie Phase 2 abgeschlossen und bestätigt haben, dass Sie den Vorgang abgeschlossen haben, ändert sich der Status auf **bis Datum**.

Nutzen Sie die NetApp Hybrid Cloud Control API für das Upgrade von Element Storage

Mit APIs können Storage-Nodes in einem Cluster auf die neueste Element Softwareversion aktualisiert werden. Sie können ein Automatisierungstool Ihrer Wahl zum Ausführen der APIs verwenden. Der hier dokumentierte API-Workflow nutzt die REST-API-UI, die am Management-Node verfügbar ist.

Schritte

1. Laden Sie das Storage-Upgrade-Paket auf ein Gerät herunter, auf das der Management-Node zugreifen kann.

   Wechseln Sie zur Element Software "download-Seite" Und laden Sie das neueste Storage-Node-Image herunter.

2. Laden Sie das Storage-Upgrade-Paket auf den Management-Node hoch:
   a. Öffnen Sie die REST-API-UI für den Management-Node:

      ```
      https://<ManagementNodeIP>/package-repository/1/
      ```

   b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
      ii. Geben Sie die Client-ID als ein `mnode-client`.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Autorisierungsfenster.
   c. Wählen Sie in DER REST API-Benutzeroberfläche **POST /Packages** aus.
   d. Wählen Sie **Probieren Sie es aus**.

e. Wählen Sie **Durchsuchen** und wählen Sie das Aktualisierungspaket aus.
f. Wählen Sie **Ausführen**, um den Upload zu initiieren.
g. Kopieren Sie die Paket-ID aus der Antwort, und speichern Sie sie (`"id"`) Für den Einsatz in einem späteren Schritt.

3. Überprüfen Sie den Status des Uploads.
   a. Wählen Sie in DER REST-API-Benutzeroberfläche **GET /packages/{id}/Status** aus.
   b. Wählen Sie **Probieren Sie es aus**.
   c. Geben Sie die Paket-ID ein, die Sie im vorherigen Schritt in **id** kopiert haben.
   d. Wählen Sie **Ausführen**, um die Statusanforderung zu initiieren.

      Die Antwort zeigt an `state` Als `SUCCESS` Nach Abschluss.

4. Suchen Sie die Storage Cluster ID:
   a. Öffnen Sie die REST-API-UI für den Management-Node:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
      ii. Geben Sie die Client-ID als ein `mnode-client`.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Autorisierungsfenster.
   c. Wählen Sie in DER REST API-Benutzeroberfläche **GET /Installations** aus.
   d. Wählen Sie **Probieren Sie es aus**.
   e. Wählen Sie **Ausführen**.
   f. Kopieren Sie als Antwort die Installations-Asset-ID (`"id"`).
   g. Wählen Sie in DER REST-API-UI **GET /installations/{id}** aus.
   h. Wählen Sie **Probieren Sie es aus**.
   i. Fügen Sie die Installations-Asset-ID in das Feld **id** ein.
   j. Wählen Sie **Ausführen**.
   k. Kopieren Sie aus der Antwort die Storage-Cluster-ID und speichern Sie sie (`"id"`) Des Clusters Sie beabsichtigen, für die Verwendung in einem späteren Schritt zu aktualisieren.

5. Führen Sie das Storage-Upgrade aus:
   a. Öffnen Sie die Storage REST API-UI auf dem Management-Node:

      ```
      https://<ManagementNodeIP>/storage/1/
      ```

   b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:

i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.

ii. Geben Sie die Client-ID als ein `mnode-client`.

iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

iv. Schließen Sie das Autorisierungsfenster.

c. Wählen Sie **POST/Upgrades**.

d. Wählen Sie **Probieren Sie es aus**.

e. Geben Sie die Paket-ID des Upgrades in das Feld Parameter ein.

f. Geben Sie im Parameterfeld die Storage-Cluster-ID ein.

Die Nutzlast sollte wie im folgenden Beispiel aussehen:

```
{
  "config": {},
  "packageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4",
  "storageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4"
}
```

g. Wählen Sie **Ausführen**, um das Upgrade zu initiieren.

Die Antwort sollte den Status als angeben `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. Kopieren Sie die Upgrade-ID (`"upgradeId"`Das ist Teil der Antwort.

6. Überprüfen Sie den Aktualisierungsfortschritt und die Ergebnisse:

   a. Wählen Sie **GET /Upgrades/{upgradeId}** aus.

   b. Wählen Sie **Probieren Sie es aus**.

   c. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein.

   d. Wählen Sie **Ausführen**.

   e. Führen Sie einen der folgenden Schritte aus, wenn während des Upgrades Probleme oder besondere Anforderungen auftreten:

Option	Schritte
Sie müssen Probleme mit dem Cluster-Systemzustand aufgrund von korrigieren `failedHealthChecks` Nachricht im Antwortkörper.	i. Gehen Sie zu dem für jedes Problem angegebenen KB-Artikel oder führen Sie das angegebene Heilmittel aus. ii. Wenn ein KB angegeben wird, führen Sie den im entsprechenden KB-Artikel beschriebenen Prozess aus. iii. Nachdem Sie Clusterprobleme behoben haben, authentifizieren Sie sich bei Bedarf erneut und wählen Sie **PUT /Upgrades/{UpgradeId}** aus. iv. Wählen Sie **Probieren Sie es aus**. v. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein. vi. Eingabe `"action":"resume"` Im Anforderungsgremium. `{ "action": "resume" }` vii. Wählen Sie **Ausführen**.
Sie müssen das Upgrade unterbrechen, da das Wartungsfenster geschlossen wird oder aus einem anderen Grund.	i. Bei Bedarf erneut authentifizieren und **PUT /Upgrades/{UpgradeId}** auswählen. ii. Wählen Sie **Probieren Sie es aus**. iii. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein. iv. Eingabe `"action":"pause"` Im Anforderungsgremium. `{ "action": "pause" }` v. Wählen Sie **Ausführen**.

Option	Schritte
Wenn Sie ein H610S Cluster mit einer Elementversion vor 11.8 aktualisieren, wird der Status angezeigt `finishedNeedsAck` Im Antwortkörper.Sie müssen für jeden H610S Storage-Node zusätzliche Aktualisierungsschritte durchführen.	i. Führen Sie die weiteren Aktualisierungsschritte hier aus "KB-Artikel" Für jeden Node. ii. Bei Bedarf erneut authentifizieren und **PUT /Upgrades/{UpgradeId}** auswählen. iii. Wählen Sie **Probieren Sie es aus**. iv. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein. v. Eingabe `"action":"acknowledge"` Im Anforderungsgremium. `{ "action": "acknowledge" }` vi. Wählen Sie **Ausführen**.

f. Führen Sie die **GET /Upgrades/{upgradeId}** API nach Bedarf mehrmals aus, bis der Prozess abgeschlossen ist.

   Während des Upgrades, die `status` Zeigt an `running` Wenn keine Fehler aufgetreten sind. Wenn jeder Node aktualisiert wird, wird der `step` Wertänderungen an `NodeFinished`.

Das Upgrade wurde erfolgreich abgeschlossen, wenn der abgeschlossen wurde `percent` Wert ist `100` Und das `state` Zeigt an `finished`.

Was geschieht bei einem Upgrade mit NetApp Hybrid Cloud Control

Wenn während eines Upgrades ein Laufwerk oder ein Node ausfällt, zeigt die Element-UI Clusterfehler an. Der Upgrade-Prozess setzt nicht auf den nächsten Node fort und wartet auf die Behebung der Cluster-Fehler. Die Fortschrittsleiste in der UI zeigt an, dass das Upgrade auf die Behebung der Cluster-Fehler wartet. In dieser Phase funktioniert die Auswahl von **Pause** in der Benutzeroberfläche nicht, da das Upgrade wartet, bis der Cluster wieder gesund ist. Sie müssen NetApp Support beauftragen, die Fehleruntersuchung zu unterstützen.

NetApp Hybrid Cloud Control verfügt über eine festgelegte Wartezeit von drei Stunden. In diesem Fall kann es zu einem der folgenden Szenarien kommen:

- Die Behebung von Clusterfehlern erfolgt innerhalb des dreistündigen Zeitfensters und das Upgrade wird fortgesetzt. Sie müssen in diesem Szenario keine Maßnahmen ergreifen.
- Das Problem besteht nach drei Stunden weiter, und der Aktualisierungsstatus zeigt **Fehler** mit einem roten Banner an. Sie können das Upgrade fortsetzen, indem Sie nach der Behebung des Problems **Fortsetzen** auswählen.
- Der NetApp Support hat festgestellt, dass das Upgrade vorübergehend abgebrochen werden muss, damit Korrekturmaßnahmen vor dem dreistündigen Fenster durchgeführt werden können. Der Support verwendet die API, um das Upgrade abzubrechen.

Wenn das Cluster-Upgrade abgebrochen wird, während ein Node aktualisiert wird, kann dies dazu führen, dass die Laufwerke nicht ordnungsgemäß vom Node entfernt werden. Wenn die Laufwerke unnormal entfernt werden, muss das Hinzufügen der Laufwerke während eines Upgrades manuell durch den NetApp Support erfolgen. Der Node kann länger dauern, um Firmware-Updates durchzuführen oder Aktivitäten zur Synchronisierung nach dem Update durchzuführen. Wenn der Upgrade-Fortschritt blockiert wird, wenden Sie sich an den NetApp Support.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Firmware für Storage-Upgrades

Ab Element 12.0 und den Managementservices Version 2.14 können Sie mithilfe der NetApp Hybrid Cloud Control UI und DER REST-API Firmware-reine Upgrades auf Ihren Storage-Nodes durchführen. Dieses Verfahren führt keine Upgrades für Element Software durch und ermöglicht ein Upgrade der Storage-Firmware außerhalb einer größeren Version.

Was Sie benötigen

- **Administratorrechte**: Sie haben Berechtigungen für den Storage Cluster Administrator, um das Upgrade durchzuführen.
- **System Time SYNC**: Sie haben sichergestellt, dass die Systemzeit auf allen Knoten synchronisiert ist und NTP für den Speicher-Cluster und die Knoten korrekt konfiguriert ist. Jeder Node muss in der Web-UI pro Node mit einem DNS-Nameserver konfiguriert sein (`https://[IP address]:442`) Ohne ungelöste Cluster Fehler im Zusammenhang mit Zeitverzerrung.
- **System-Ports**: Bei Upgrade-Nutzung von NetApp Hybrid Cloud Control haben Sie sichergestellt, dass die erforderlichen Ports geöffnet sind. Siehe "Netzwerkports" Finden Sie weitere Informationen.
- **Management-Node**: Für NetApp Hybrid Cloud Control UI und API wird der Management-Node in Ihrer Umgebung mit Version 11.3 ausgeführt.
- **Management Services**: Sie haben Ihr Management Services Bundle auf die neueste Version aktualisiert.

Bei H610S Storage-Nodes mit Element Softwareversion 12.0 sollten Sie D-Patch SUST-909 anwenden, bevor Sie ein Upgrade auf das Storage-Firmware-Bundle 2.27 durchführen. Wenden Sie sich an den NetApp Support, um den D-Patch vor dem Upgrade zu erhalten. Siehe "Versionshinweise Zum Speicher-Firmware-Bundle 2.27".

Sie müssen ein Upgrade auf das neueste Management Services Bundle durchführen, bevor Sie die Firmware auf Ihren Storage-Nodes aktualisieren. Wenn Sie die Element Software auf Version 12.2 oder höher aktualisieren, benötigen Sie Managementdienste 2.14.60 oder höher, um fortfahren zu können.

- **Cluster Health**: Sie haben Health Checks durchgeführt. Siehe "Integritätsprüfungen von Element Storage vor einem Storage Upgrade durchführen".
- **Aktualisierter Baseboard Management Controller (BMC) für H610S-Knoten**: Sie haben die BMC-Version für Ihre H610S-Knoten aktualisiert. Siehe "Versionshinweise und Upgrade-Anweisungen".

Eine vollständige Matrix der Firmware und der Treiber-Firmware für Ihre Hardware finden Sie unter "Unterstützte Storage-Firmware-Versionen für SolidFire Storage-Nodes".

- **Aktualisierungszeit**: Sie haben genügend Zeit für die Durchführung Ihres Upgrades eingeplant. Bei einem Upgrade auf Element Software 12.5 oder höher variiert die Dauer des Upgradevorgangs je nach aktueller Element Softwareversion und Firmware-Updates.

Storage-Node	Aktuelle Version der Element Software	Ungefähre Installationszeit für Software und Firmware pro Node[1]	Ungefähre Synchronisierung szeit pro Knoten[2]	Ungefähre gesamte Upgrade-Zeit pro Node
Alle SolidFire und NetApp H-Series Nodes mit aktueller Firmware[3]	12.x	15 Minuten	10 bis 15 Minuten	20 bis 30 Minuten
H610S und H410S	12.x und 11.8	60 Minuten	30 bis 60 Minuten	90 bis 120 Minuten
H610S	11.7 und früher	90 Minuten	40 bis 70 Minuten	130 bis 160 Minuten müssen Sie auch "Führen Sie ein komplettes Herunterfahren des Node durch, und trennen Sie die Stromversorgung" Für jeden H610S Node.

[1]eine vollständige Matrix von Firmware und Treiber-Firmware für Ihre Hardware finden Sie unter "Unterstützte Storage-Firmware-Versionen für SolidFire Storage-Nodes".

[2]Wenn Sie ein Cluster mit einer hohen Lese-IOPS-Last und einer längeren Firmware-Update-Zeit kombinieren, erhöht sich die Zeit für die Datensynchronisierung.

[3] die folgenden Nodes werden nicht unterstützt. Wenn Sie versuchen, einen dieser Knoten auf eine nicht unterstützte Elementversion zu aktualisieren, wird eine Fehlermeldung angezeigt, die besagt, dass der Knoten nicht von Element 12.x unterstützt wird:

  - Ab Element 12.8, SF4805, SF9605, SF19210 und SF38410 Storage-Nodes
  - Ab Element 12.7, SF2405 und SF9608 Storage-Nodes und FC-Nodes FC0025 und SF-FCN-01

- **Endbenutzer-Lizenzvereinbarung (EULA)**: Ab Management Services 2.20.69 müssen Sie die EULA akzeptieren und speichern, bevor Sie die NetApp Hybrid Cloud Control UI oder API zum Upgrade der Storage-Firmware verwenden:

  a. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

  b. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.

c. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.

d. Die EULA erscheint. Scrollen Sie nach unten, wählen Sie **Ich akzeptiere aktuelle und alle zukünftigen Updates** und wählen Sie **Speichern**.

Upgrade-Optionen

Wählen Sie eine der folgenden Upgrade-Optionen für die Speicher-Firmware:

- Verwenden Sie die NetApp Hybrid Cloud Control UI für ein Upgrade der Storage-Firmware
- Verwenden Sie die NetApp Hybrid Cloud Control API für ein Upgrade der Storage-Firmware

Verwenden Sie die NetApp Hybrid Cloud Control UI für ein Upgrade der Storage-Firmware

Mit der NetApp Hybrid Cloud Control UI lässt sich die Firmware der Storage-Nodes in Ihrem Cluster aktualisieren.

Was Sie benötigen

- Wenn Ihr Management-Node nicht mit dem Internet verbunden ist, haben Sie den Zugriff "Das Storage-Firmware-Bundle heruntergeladen".

Informationen zu potenziellen Problemen beim Upgrade von Storage-Clustern mit NetApp Hybrid Cloud Control und den zugehörigen Workarounds finden Sie im "KB-Artikel".

Das Upgrade dauert etwa 30 Minuten pro Storage-Node. Wenn Sie ein Element Storage Cluster auf eine Storage-Firmware vor Version 2.76 aktualisieren, werden einzelne Storage-Nodes während des Upgrades nur neu gebootet, wenn neue Firmware auf den Node geschrieben wurde.

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.
4. Wählen Sie auf der Seite **Upgrades** die Option **Speicherung**.

Auf der Registerkarte **Storage** werden die Speichercluster aufgelistet, die Teil Ihrer Installation sind. Wenn durch NetApp Hybrid Cloud Control auf ein Cluster zugegriffen werden kann, wird es nicht auf der Seite **Upgrades** angezeigt. Wenn bei Clustern mit Element 12.0 oder höher die aktuelle Firmware-Bundle-Version für diese Cluster aufgeführt ist. Wenn die Knoten in einem einzelnen Cluster unterschiedliche Firmware-Versionen haben oder wenn das Upgrade fortschreitet, wird in der Spalte **Aktuelle Firmware Bundle Version Multiple** angezeigt. Sie können **multiple** auswählen, um zur Seite **Nodes** zu navigieren, um Firmware-Versionen zu vergleichen. Wenn auf allen Clustern Elementversionen vor 12.0 ausgeführt werden, werden Ihnen keine Informationen über die Versionsnummern der Firmware-Bundles angezeigt.

Wenn der Cluster aktuell ist und/oder keine Upgrade-Pakete verfügbar sind, werden die Registerkarten **Element** und **Firmware Only** nicht angezeigt. Diese Registerkarten werden auch nicht angezeigt, wenn ein Upgrade ausgeführt wird. Wenn die Registerkarte **Element** angezeigt wird, nicht jedoch die Registerkarte **Firmware only**, stehen keine Firmware-Pakete zur Verfügung.

5. Wählen Sie den Dropdown-Pfeil neben dem Cluster aus, das Sie aktualisieren möchten.
6. Wählen Sie **Durchsuchen**, um das heruntergeladene Aktualisierungspaket hochzuladen.
7. Warten Sie, bis der Upload abgeschlossen ist. In einer Statusleiste wird der Status des Uploads angezeigt.

   Der Datei-Upload geht verloren, wenn Sie vom Browser-Fenster wegnavigieren.

   Nach dem erfolgreichen Hochladen und Validierungen der Datei wird eine Meldung auf dem Bildschirm angezeigt. Die Validierung kann mehrere Minuten in Anspruch nehmen. Wenn Sie zu diesem Zeitpunkt vom Browser-Fenster weg navigieren, bleibt der Datei-Upload erhalten.

8. Wählen Sie **nur Firmware** aus, und wählen Sie aus den verfügbaren Upgrade-Versionen.
9. Wählen Sie **Upgrade Starten**.

Der **Upgrade-Status** ändert sich während des Upgrades, um den Status des Prozesses anzuzeigen. Es ändert sich auch in Reaktion auf Aktionen, die Sie ergreifen, z. B. die Unterbrechung des Upgrades oder wenn das Upgrade einen Fehler zurückgibt. Siehe Statusänderungen des Upgrades.

Während das Upgrade läuft, können Sie die Seite verlassen und zu einem späteren Zeitpunkt zurückkehren, um den Fortschritt zu überwachen. Die Seite aktualisiert den Status und die aktuelle Version nicht dynamisch, wenn die Cluster-Zeile ausgeblendet ist. Die Cluster-Zeile muss erweitert werden, um die Tabelle zu aktualisieren, oder Sie können die Seite aktualisieren.

Sie können Protokolle herunterladen, nachdem die Aktualisierung abgeschlossen ist.

Statusänderungen des Upgrades

Hier sind die verschiedenen Status, in denen die Spalte **Upgrade Status** in der UI vor, während und nach dem Upgrade-Prozess angezeigt wird:

Upgrade-Status	Beschreibung
Auf dem aktuellen Stand	Das Cluster wurde auf die neueste verfügbare Element-Version aktualisiert oder die Firmware wurde auf die neueste Version aktualisiert.
Erkennung nicht möglich	Dieser Status wird angezeigt, wenn die Speicherdienst-API einen Upgrade-Status zurückgibt, der nicht in der aufgezählten Liste möglicher Upgrade-Status aufgeführt ist.
Verfügbare Versionen	Neuere Versionen von Element und/oder Storage Firmware stehen für ein Upgrade zur Verfügung.
In Bearbeitung	Das Upgrade läuft. In einer Statusleiste wird der Aktualisierungsstatus angezeigt. Auf dem Bildschirm werden zudem Fehler auf Node-Ebene angezeigt und die Node-ID jedes Node im Cluster wird angezeigt, wenn das Upgrade fortschreitet. Sie können den Status jedes Knotens über die Element-UI oder das NetApp Element Plug-in für vCenter Server UI überwachen.
Anhalten Des Upgrades	Sie können das Upgrade anhalten. Je nach Status des Upgrade-Prozesses kann der Pause-Vorgang erfolgreich oder fehlgeschlagen sein. Es wird eine UI-Eingabeaufforderung angezeigt, in der Sie aufgefordert werden, den Pause-Vorgang zu bestätigen. Um sicherzustellen, dass sich das Cluster vor dem Anhalten eines Upgrades an einem sicheren Ort befindet, kann es bis zu zwei Stunden dauern, bis der Upgrade-Vorgang vollständig angehalten ist. Um das Upgrade fortzusetzen, wählen Sie **Fortsetzen**.
Angehalten	Sie haben das Upgrade angehalten. Wählen Sie **Fortsetzen**, um den Prozess fortzusetzen.
Fehler	Während des Upgrades ist ein Fehler aufgetreten. Sie können das Fehlerprotokoll herunterladen und an den NetApp Support senden. Nachdem Sie den Fehler behoben haben, können Sie zur Seite zurückkehren und **Fortsetzen** wählen. Wenn Sie das Upgrade fortsetzen, geht die Statusleiste einige Minuten lang zurück, während das System die Zustandsprüfung ausführt und den aktuellen Status des Upgrades überprüft.

Was geschieht bei einem Upgrade mit NetApp Hybrid Cloud Control

Wenn während eines Upgrades ein Laufwerk oder ein Node ausfällt, zeigt die Element-UI Clusterfehler an. Der Upgrade-Prozess setzt nicht auf den nächsten Node fort und wartet auf die Behebung der Cluster-Fehler. Die Fortschrittsleiste in der UI zeigt an, dass das Upgrade auf die Behebung der Cluster-Fehler wartet. In dieser Phase funktioniert die Auswahl von **Pause** in der Benutzeroberfläche nicht, da das Upgrade wartet, bis der Cluster wieder gesund ist. Sie müssen NetApp Support beauftragen, die Fehleruntersuchung zu unterstützen.

NetApp Hybrid Cloud Control verfügt über eine festgelegte Wartezeit von drei Stunden. In diesem Fall kann es zu einem der folgenden Szenarien kommen:

- Die Behebung von Clusterfehlern erfolgt innerhalb des dreistündigen Zeitfensters und das Upgrade wird fortgesetzt. Sie müssen in diesem Szenario keine Maßnahmen ergreifen.
- Das Problem besteht nach drei Stunden weiter, und der Aktualisierungsstatus zeigt **Fehler** mit einem roten Banner an. Sie können das Upgrade fortsetzen, indem Sie nach der Behebung des Problems **Fortsetzen** auswählen.
- Der NetApp Support hat festgestellt, dass das Upgrade vorübergehend abgebrochen werden muss, damit Korrekturmaßnahmen vor dem dreistündigen Fenster durchgeführt werden können. Der Support verwendet die API, um das Upgrade abzubrechen.

> Wenn das Cluster-Upgrade abgebrochen wird, während ein Node aktualisiert wird, kann dies dazu führen, dass die Laufwerke nicht ordnungsgemäß vom Node entfernt werden. Wenn die Laufwerke unnormal entfernt werden, muss das Hinzufügen der Laufwerke während eines Upgrades manuell durch den NetApp Support erfolgen. Der Node kann länger dauern, um Firmware-Updates durchzuführen oder Aktivitäten zur Synchronisierung nach dem Update durchzuführen. Wenn der Upgrade-Fortschritt blockiert wird, wenden Sie sich an den NetApp Support.

Verwenden Sie die NetApp Hybrid Cloud Control API für ein Upgrade der Storage-Firmware

Mit APIs können Storage-Nodes in einem Cluster auf die neueste Element Softwareversion aktualisiert werden. Sie können ein Automatisierungstool Ihrer Wahl zum Ausführen der APIs verwenden. Der hier dokumentierte API-Workflow nutzt die REST-API-UI, die am Management-Node verfügbar ist.

Schritte

1. Laden Sie das Storage-Firmware-Upgrade-Paket auf ein Gerät herunter, auf das der Management-Node zugreifen kann. Gehen Sie zu Element Software "download-Seite" Und laden Sie das neueste Speicher-Firmware-Image herunter.
2. Laden Sie das Upgrade-Paket für die Speicher-Firmware auf den Management-Node hoch:
   a. Öffnen Sie die REST-API-UI für den Management-Node:

      ```
      https://<ManagementNodeIP>/package-repository/1/
      ```

   b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
      ii. Geben Sie die Client-ID als ein `mnode-client`.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Autorisierungsfenster.
   c. Wählen Sie in DER REST API-Benutzeroberfläche **POST /Packages** aus.
   d. Wählen Sie **Probieren Sie es aus**.
   e. Wählen Sie **Durchsuchen** und wählen Sie das Aktualisierungspaket aus.
   f. Wählen Sie **Ausführen**, um den Upload zu initiieren.
   g. Kopieren Sie die Paket-ID aus der Antwort, und speichern Sie sie (`"id"`) Für den Einsatz in einem späteren Schritt.
3. Überprüfen Sie den Status des Uploads.

a. Wählen Sie in DER REST-API-Benutzeroberfläche **GET /packages/{id}/Status** aus.
b. Wählen Sie **Probieren Sie es aus**.
c. Geben Sie die Firmware-Paket-ID ein, die Sie im vorherigen Schritt in **id** kopiert haben.
d. Wählen Sie **Ausführen**, um die Statusanforderung zu initiieren.

   Die Antwort zeigt an `state` Als `SUCCESS` Nach Abschluss.

4. Suchen Sie die Installations-Asset-ID:
   a. Öffnen Sie die REST-API-UI für den Management-Node:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
      ii. Geben Sie die Client-ID als ein `mnode-client`.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Autorisierungsfenster.
   c. Wählen Sie in DER REST API-Benutzeroberfläche **GET /Installations** aus.
   d. Wählen Sie **Probieren Sie es aus**.
   e. Wählen Sie **Ausführen**.
   f. Kopieren Sie als Antwort die Installations-Asset-ID (`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. Wählen Sie in DER REST-API-UI **GET /installations/{id}** aus.
   h. Wählen Sie **Probieren Sie es aus**.
   i. Fügen Sie die Installations-Asset-ID in das Feld **id** ein.
   j. Wählen Sie **Ausführen**.
   k. Kopieren Sie aus der Antwort die Storage-Cluster-ID und speichern Sie sie (`"id"`) Des Clusters Sie beabsichtigen, für die Verwendung in einem späteren Schritt zu aktualisieren.

```
"storage": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterUuid": "a1bd1111-4f1e-46zz-ab6f-0a1111b1111x",
        "id": "a1bd1111-4f1e-46zz-ab6f-a1a1a111b012",
```

5. Führen Sie das Speicher-Firmware-Upgrade aus:

   a. Öffnen Sie die Storage REST API-UI auf dem Management-Node:

   ```
   https://<ManagementNodeIP>/storage/1/
   ```

   b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:

      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.

      ii. Geben Sie die Client-ID als ein `mnode-client`.

      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

      iv. Schließen Sie das Fenster.

   c. Wählen Sie **POST/Upgrades**.

   d. Wählen Sie **Probieren Sie es aus**.

   e. Geben Sie die Paket-ID des Upgrades in das Feld Parameter ein.

   f. Geben Sie im Parameterfeld die Storage-Cluster-ID ein.

   g. Wählen Sie **Ausführen**, um das Upgrade zu initiieren.

   Die Antwort sollte Status als angeben `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. Kopieren Sie die Upgrade-ID (`"upgradeId"`Das ist Teil der Antwort.

6. Überprüfen Sie den Aktualisierungsfortschritt und die Ergebnisse:

   a. Wählen Sie **GET /Upgrades/{upgradeId}** aus.

   b. Wählen Sie **Probieren Sie es aus**.

   c. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein.

   d. Wählen Sie **Ausführen**.

   e. Führen Sie einen der folgenden Schritte aus, wenn während des Upgrades Probleme oder besondere Anforderungen auftreten:

Option	Schritte
Sie müssen Probleme mit dem Cluster-Systemzustand aufgrund von korrigieren `failedHealthChecks` Nachricht im Antwortkörper.	i. Gehen Sie zu dem für jedes Problem angegebenen KB-Artikel oder führen Sie das angegebene Heilmittel aus. ii. Wenn ein KB angegeben wird, führen Sie den im entsprechenden KB-Artikel beschriebenen Prozess aus. iii. Nachdem Sie Clusterprobleme behoben haben, authentifizieren Sie sich bei Bedarf erneut und wählen Sie **PUT /Upgrades/{UpgradeId}** aus. iv. Wählen Sie **Probieren Sie es aus**. v. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein. vi. Eingabe `"action":"resume"` Im Anforderungsgremium. `{ "action": "resume" }` vii. Wählen Sie **Ausführen**.
Sie müssen das Upgrade unterbrechen, da das Wartungsfenster geschlossen wird oder aus einem anderen Grund.	i. Bei Bedarf erneut authentifizieren und **PUT /Upgrades/{UpgradeId}** auswählen. ii. Wählen Sie **Probieren Sie es aus**. iii. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein. iv. Eingabe `"action":"pause"` Im Anforderungsgremium. `{ "action": "pause" }` v. Wählen Sie **Ausführen**.

f. Führen Sie die **GET /Upgrades/{upgradeId}** API nach Bedarf mehrmals aus, bis der Prozess abgeschlossen ist.

   Während des Upgrades, die `status` Zeigt an `running` Wenn keine Fehler aufgetreten sind. Wenn jeder Node aktualisiert wird, wird der `step` Wertänderungen an `NodeFinished`.

Das Upgrade wurde erfolgreich abgeschlossen, wenn der abgeschlossen wurde `percent` Wert ist `100`

Und das `state` Zeigt an `finished`.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Aktualisieren Sie das Element Plug-in für vCenter Server

Bei bestehenden vSphere Umgebungen mit einem registrierten NetApp Element Plug-in für VMware vCenter Server können Sie Ihre Plug-in-Registrierung aktualisieren, nachdem Sie das Management-Services-Paket, das den Plug-in-Service enthält, aktualisiert haben.

Sie können die Plug-in-Registrierung auf der vCenter Server Virtual Appliance (vCSA) oder Windows mithilfe des Registrierungsprogramms aktualisieren. Sie müssen Ihre Registrierung für das vCenter Plug-in auf jedem vCenter Server ändern, auf dem Sie das Plug-in verwenden müssen.

Das Management Services 2.27 Bundle enthält das Element Plug-in für vCenter Server 5.5, das nur mit Management Node 12.8 oder höher kompatibel ist. Wenn Sie auf Management Services 2.27 aktualisieren, müssen Sie die Upgrade-Reihenfolge ändern und das Management Services-Paket *nach* dem Upgrade auf Element 12.9 aktualisieren, um Kompatibilität zwischen dem Management-Knoten und den Management Services zu gewährleisten.

Das Management Services-Paket 2.22.7 enthält das Element-Plug-in für vCenter Server 5.0, welches das Remote-Plug-in beinhaltet. Wenn Sie das Element-Plug-in verwenden, sollten Sie auf Management Services 2.22.7 oder höher aktualisieren, um der VMware-Richtlinie zu entsprechen, die die Unterstützung für lokale Plug-ins einstellt. "Weitere Informationen ."Die

Element vCenter Plug-in 5.0 oder höher

Dieses Upgrade-Verfahren umfasst die folgenden Upgrade-Szenarien:

- Sie führen ein Upgrade auf das Element Plug-in für vCenter Server 5.5, 5.4, 5.3, 5.2, 5.1 oder 5.0 durch.
- Sie aktualisieren gerade auf einen 8.0 oder 7.0 HTML5 vSphere Web Client.

Das Element Plug-in für vCenter 5.0 oder höher ist nicht mit vCenter Server 6.7 und 6.5 kompatibel.

Wenn Sie von Element Plug-in für vCenter Server 4.x auf 5.x aktualisieren, gehen die bereits mit dem Plug-in konfigurierten Cluster verloren, da die Daten nicht von einer vCenter-Instanz in ein Remote-Plug-in kopiert werden können. Sie müssen die Cluster dem Remote-Plug-in erneut hinzufügen. Dies ist eine einmalige Aktivität beim Upgrade von einem lokalen Plug-in auf ein Remote-Plug-in.

Element vCenter Plug-in 4.10 oder früher

Dieses Upgrade-Verfahren umfasst die folgenden Upgrade-Szenarien:

- Sie aktualisieren gerade auf Element Plug-in für vCenter Server 4.10, 4.9, 4.8, 4.7, 4.6 4.5, oder 4.4.
- Sie aktualisieren gerade auf einen 7.0, 6.7 oder 6.5 HTML5 vSphere Web Client.

- Das Plug-in ist nicht kompatibel mit VMware vCenter Server 8.0 für Element Plug-in für VMware vCenter Server 4.x
- Das Plug-in ist nicht mit VMware vCenter Server 6.5 für Element Plug-in für VMware vCenter Server 4.6, 4.7 und 4.8 kompatibel.

- Sie aktualisieren gerade auf einen 6.7 Flash vSphere Web Client.

Das Plug-in ist kompatibel mit vSphere Web Client Version 6.7 U2 für Flash, 6.7 U3 (Flash und HTML5) und 7.0 U1. Das Plug-in ist nicht kompatibel mit Version 6.7 U2 Build 13007421 des HTML5 vSphere Web Client und anderen 6.7 U2 Builds, die vor dem Update 2a (Build 13643870) veröffentlicht wurden. Weitere Informationen zu unterstützten vSphere-Versionen finden Sie in den Versionshinweisen zu "Ihre Version des Plug-ins".

Was Sie benötigen

- **Admin-Berechtigungen**: Sie haben vCenter Administrator-Rollenberechtigungen, um ein Plug-in zu installieren.
- **VSphere Upgrades**: Sie haben alle erforderlichen vCenter Upgrades vor dem Upgrade des NetApp Element Plug-ins für vCenter Server durchgeführt. Bei diesem Verfahren wird vorausgesetzt, dass vCenter Upgrades bereits abgeschlossen wurden.
- **VCenter Server**: Ihr vCenter Plug-in Version 4.x oder 5.x ist mit einem vCenter Server registriert. Über das Registrierungsdienstprogramm (`https://<ManagementNodeIP>:9443`Wählen Sie **Registrierungsstatus**, füllen Sie die erforderlichen Felder aus und wählen Sie **Prüfstatus** aus, um zu überprüfen, ob das vCenter

Plug-in bereits registriert ist und die Versionsnummer der aktuellen Installation.

- **Management Services-Updates**: Sie haben Ihre aktualisiert "Management Services-Bundle" Zur aktuellen Version wechseln. Updates für das vCenter Plug-in werden mithilfe von Management-Services-Updates veröffentlicht, die außerhalb der wichtigsten Produktversionen für NetApp SolidFire All-Flash-Storage veröffentlicht werden.
- **Management-Knoten-Upgrades**:

  Element vCenter Plug-in 5.0 oder höher

  Sie führen einen Management-Node aus, der bereits ausgeführt wurde "Upgrade durchgeführt" Auf Version 12.3.x oder höher.

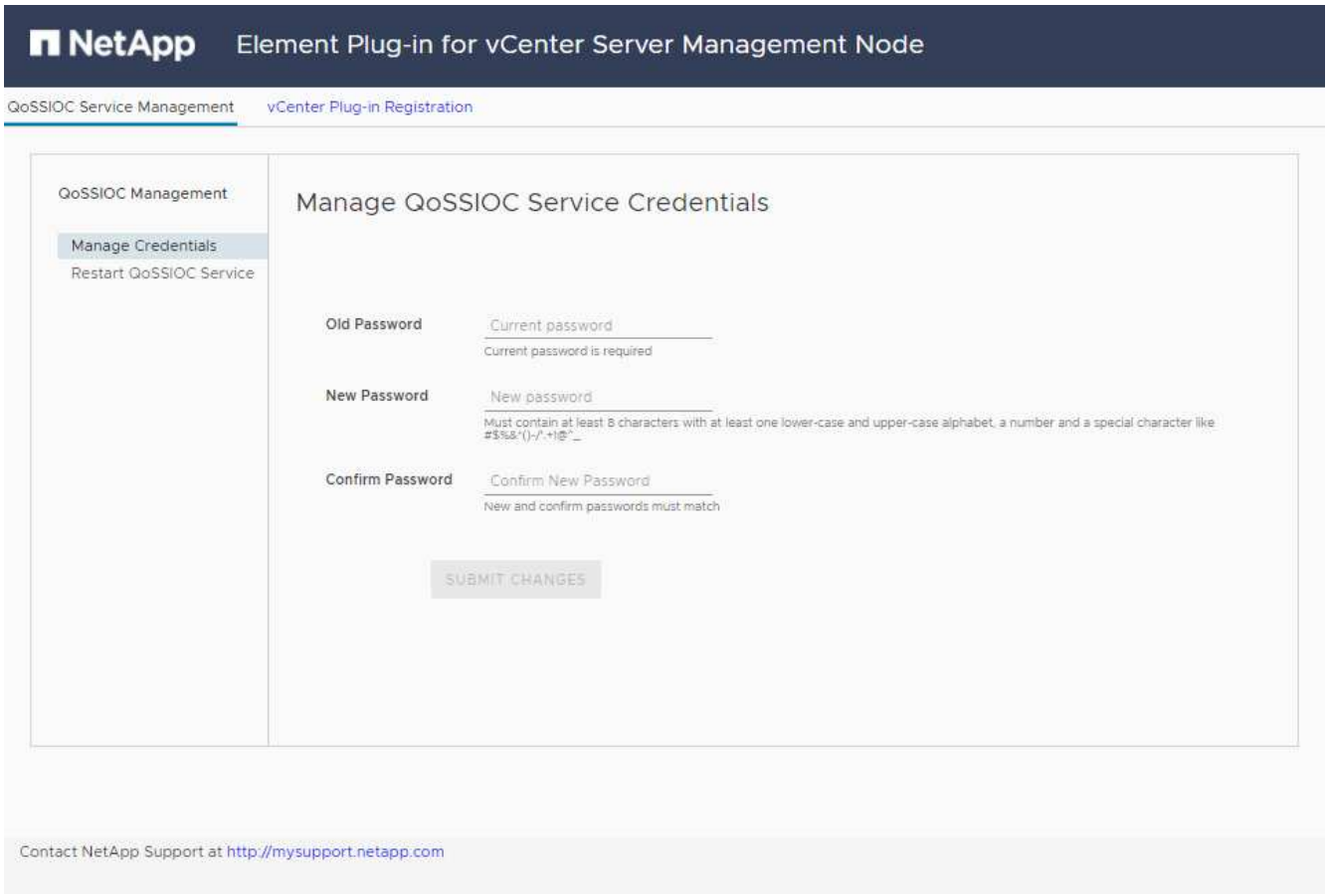
  Element vCenter Plug-in 4.10 oder früher

  Für Element vCenter Plug-in 4.4 bis 4.10 führen Sie einen Management-Node aus, der schon einmal verwendet wurde "Upgrade durchgeführt" Auf Version 11.3 oder höher. VCenter Plug-in 4.4 oder höher erfordert einen Management-Node mit mindestens 11.3 Versionen und einer modularen Architektur, die individuelle Services bietet. Der Management-Node muss mit seiner IP-Adresse oder der konfigurierten DHCP-Adresse eingeschaltet werden.

- * Element Storage-Upgrades*:
  - Ab dem Element vCenter Plug-in 5.0 verfügen Sie über einen Cluster, auf dem die NetApp Element Software 12.3.x oder höher ausgeführt wird.
  - Für Element vCenter Plug-in 4.10 oder eine frühere Version verfügen Sie über einen Cluster mit der NetApp Element Software 11.3 oder höher.
- **VSphere Web Client**: Sie haben sich vom vSphere Web Client abgemeldet, bevor Sie ein Plug-in-Upgrade starten. Der Web-Client erkennt Updates, die während dieses Prozesses an Ihrem Plug-in vorgenommen wurden, wenn Sie sich nicht abmelden.

Schritte

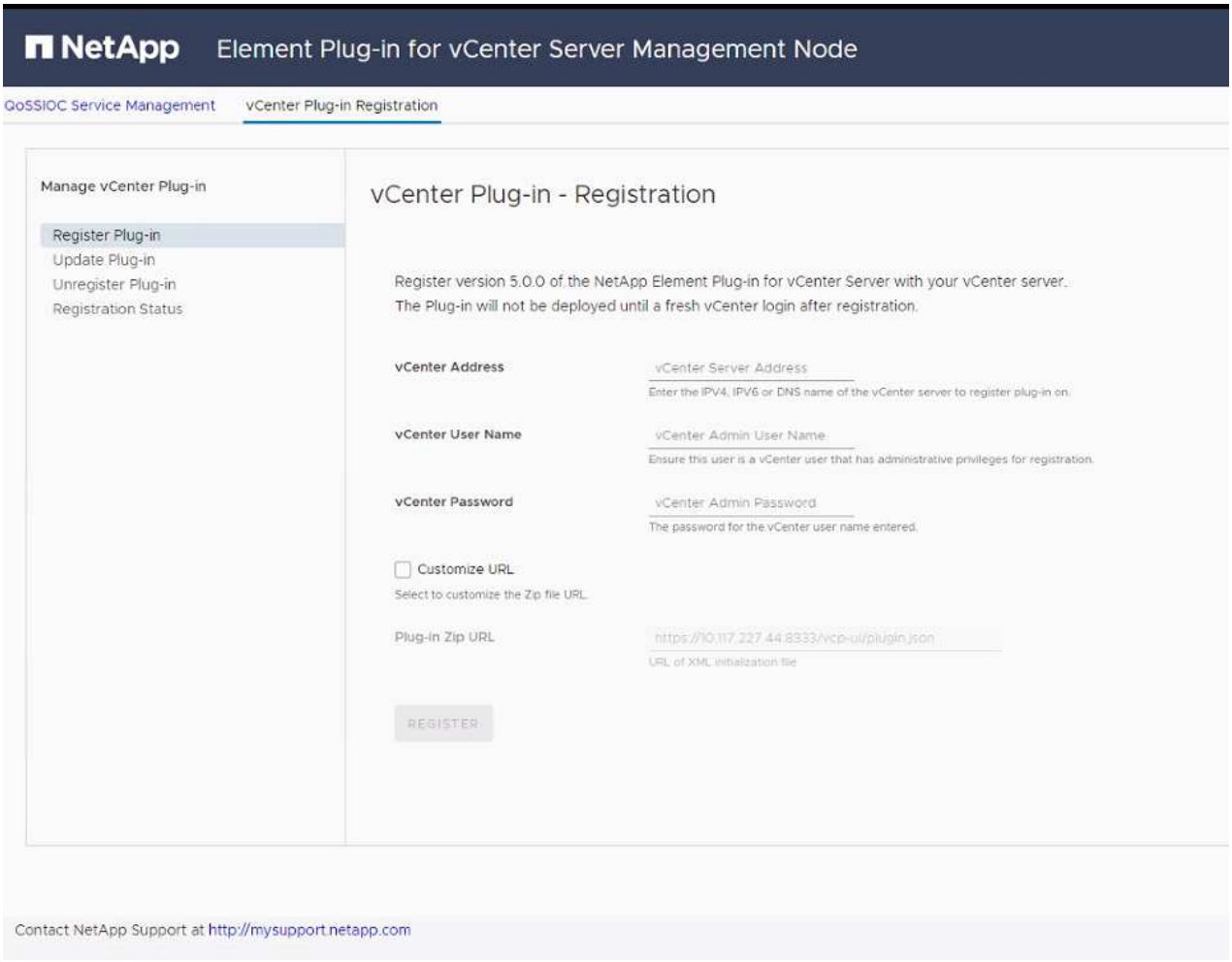
1. Geben Sie die IP-Adresse für den Management-Node in einem Browser ein, einschließlich des TCP-Ports für die Registrierung: `https://<ManagementNodeIP>:9443`Die Registrierungs-Utility-Benutzeroberfläche wird auf der Seite * QoSSIOC Service Credentials* verwalten für das Plug-in geöffnet.



2. Wählen Sie **vCenter Plug-in Registrierung**.

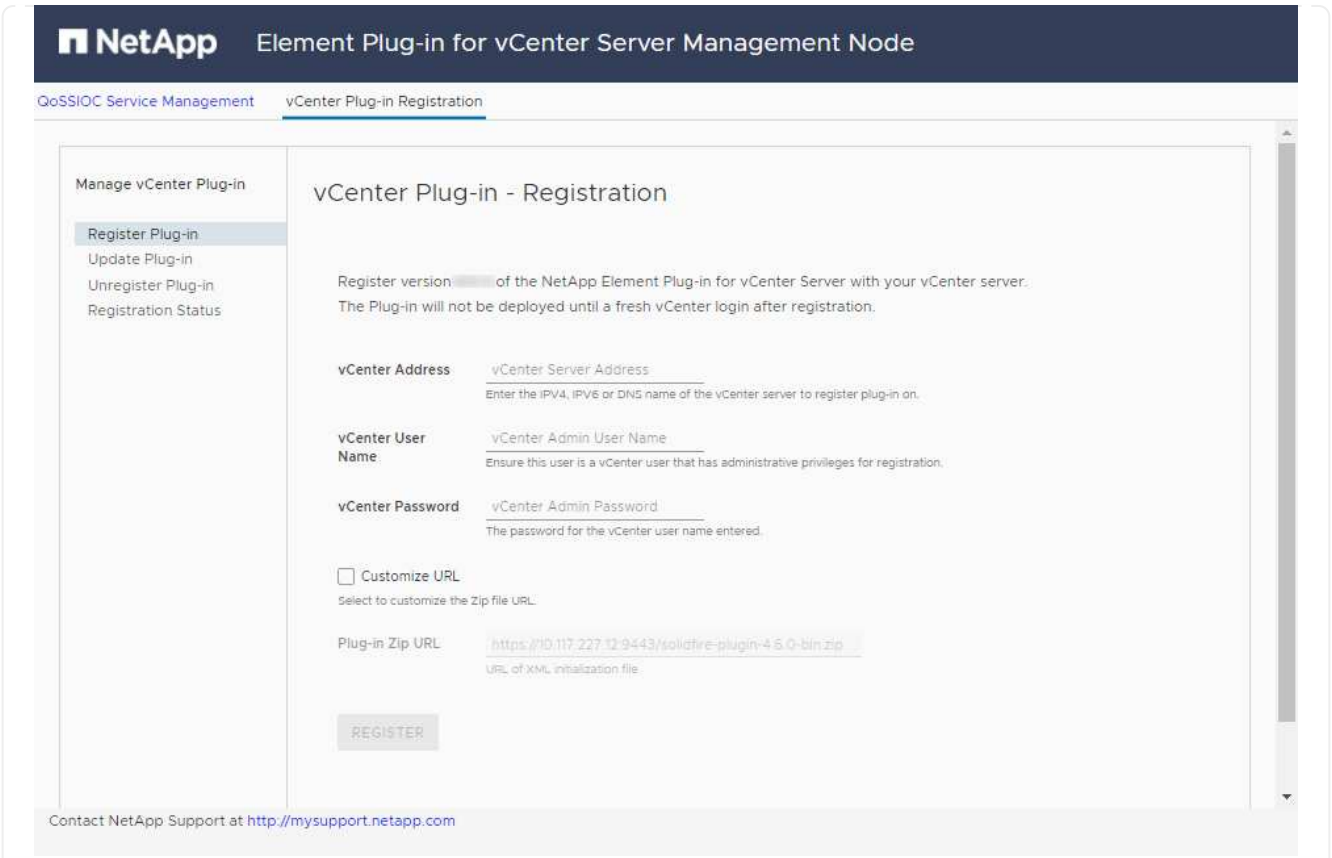
Element vCenter Plug-in 5.0 oder höher

Die Seite vCenter Plug-in Registration wird angezeigt:



Element vCenter Plug-in 4.10 oder früher

Die Seite vCenter Plug-in Registration wird angezeigt:



3. Wählen Sie in **vCenter-Plug-in verwalten** die Option **Update Plug-in** aus.
4. Bestätigen oder aktualisieren Sie die folgenden Informationen:
   a. Die IPv4-Adresse oder der FQDN des vCenter-Dienstes, auf dem Sie Ihr Plug-in registrieren.
   b. Der vCenter Administrator-Benutzername.

      Der von Ihnen eingegebene Benutzername und das Kennwort müssen für einen Benutzer mit den Berechtigungen der vCenter Administrator-Rolle verwendet werden.

   c. Das vCenter Administrator-Passwort.
   d. (Für interne Server/dunkle Sites) je nach Element Plug-in für vCenter Version, eine benutzerdefinierte URL für die Plug-in-JSON-Datei oder Plug-in ZIP:

Element vCenter Plug-in 5.0 oder höher

Eine benutzerdefinierte URL für die JSON-Plug-in-Datei.

> Sie können **Benutzerdefinierte URL** wählen, um die URL anzupassen, wenn Sie einen HTTP- oder HTTPS-Server (dunkle Site) verwenden oder den JSON-Dateinamen oder die Netzwerkeinstellungen geändert haben. Weitere Konfigurationsschritte, wenn Sie eine URL anpassen möchten, finden Sie in der Dokumentation zum Element Plug-in für vCenter Server zum Ändern von vCenter-Eigenschaften für einen internen HTTP-Server (Dark Site).

Element vCenter Plug-in 4.10 oder früher

Eine benutzerdefinierte URL für die Plug-in-ZIP.

> Sie können **Benutzerdefinierte URL** wählen, um die URL anzupassen, wenn Sie einen HTTP- oder HTTPS-Server (dunkle Site) verwenden oder den ZIP-Dateinamen oder die Netzwerkeinstellungen geändert haben. Weitere Konfigurationsschritte, wenn Sie eine URL anpassen möchten, finden Sie in der Dokumentation zum Element Plug-in für vCenter Server zum Ändern von vCenter-Eigenschaften für einen internen HTTP-Server (Dark Site).

5. Wählen Sie **Aktualisieren**.

   Ein Banner erscheint in der Benutzeroberfläche des Registrierungsprogramms, wenn die Registrierung erfolgreich ist.

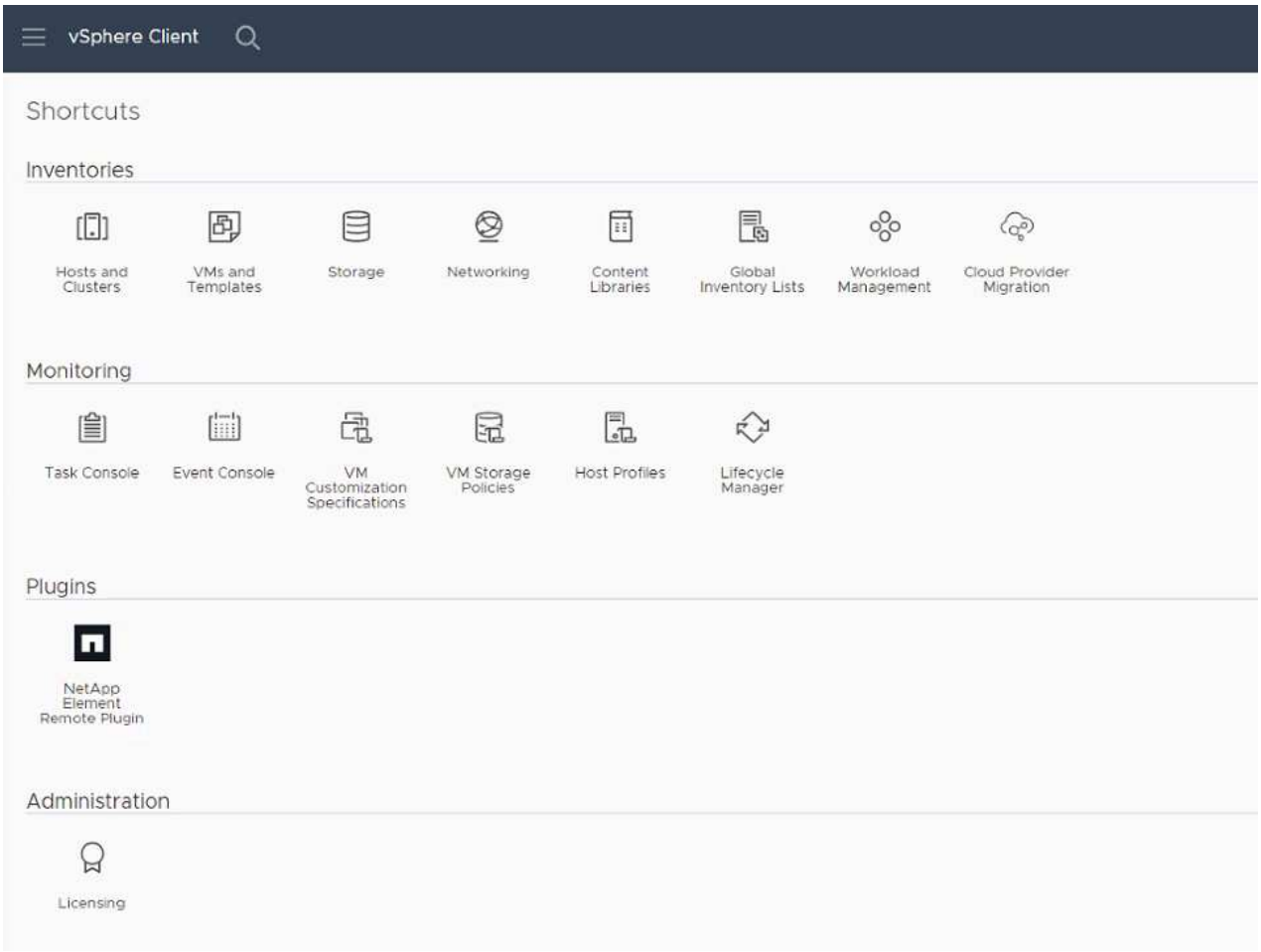
6. Melden Sie sich beim vSphere Web Client als vCenter Administrator an. Wenn Sie bereits beim vSphere Web Client angemeldet sind, müssen Sie sich zuerst abmelden, zwei bis drei Minuten warten und sich erneut anmelden.

   > Durch diese Aktion wird eine neue Datenbank erstellt und die Installation im vSphere Web Client abgeschlossen.

7. Suchen Sie im vSphere Web Client nach den folgenden abgeschlossenen Aufgaben im Task Monitor, um sicherzustellen, dass die Installation abgeschlossen wurde: `Download plug-in` Und `Deploy plug-in`.
8. Überprüfen Sie, ob die Plug-in-Erweiterungspunkte auf der Registerkarte **Shortcuts** des vSphere Web Clients und im Seitenfenster angezeigt werden.

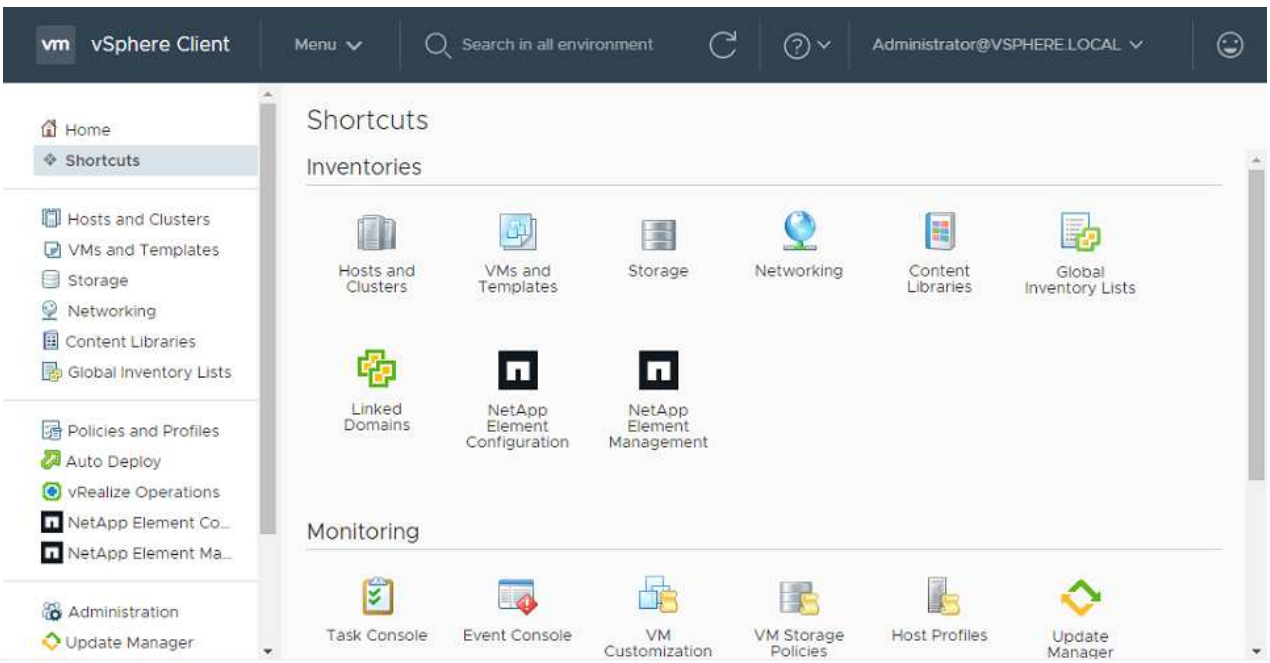
Element vCenter Plug-in 5.0 oder höher

Der Erweiterungspunkt für das Remote-Plugin von NetApp Element wird angezeigt:



Element vCenter Plug-in 4.10 oder früher

Die Erweiterungspunkte der NetApp Element-Konfiguration und -Verwaltung werden angezeigt:



Wenn die vCenter-Plug-in-Symbole nicht angezeigt werden, lesen Sie "Element Plug-in für vCenter Server" Dokumentation zur Fehlerbehebung beim Plug-in.

Nach dem Upgrade auf NetApp Element Plug-in für vCenter Server 4.8 oder höher mit VMware vCenter Server 6.7U1, wenn die Speicher-Cluster nicht aufgeführt sind oder ein Serverfehler in den Abschnitten **Cluster** und **QoSSIOC-Einstellungen** der NetApp Element-Konfiguration angezeigt wird, siehe "Element Plug-in für vCenter Server" Dokumentation über die Fehlerbehebung bei diesen Fehlern.

9. Überprüfen Sie die Versionsänderung auf der Registerkarte **über** im Erweiterungspunkt * NetApp Element Konfiguration* des Plug-ins.

   Sie sollten die folgenden Versionsdetails sehen:

   ```
   NetApp Element Plug-in Version: 5.5
   NetApp Element Plug-in Build Number: 16
   ```

Das vCenter Plug-in enthält Online-Hilfeinhalte. Um sicherzustellen, dass Ihre Hilfe die neuesten Inhalte enthält, löschen Sie Ihren Browser-Cache, nachdem Sie Ihr Plug-in aktualisiert haben.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Aktualisieren Sie Ihre vSphere Komponenten für ein NetApp SolidFire Storage-System mit dem Element Plug-in für vCenter Server

Beim Upgrade von VMware vSphere-Komponenten sind zusätzliche Schritte erforderlich. Diese Schritte sind für Systeme mit dem Element-Plug-in für vCenter Server erforderlich.

Schritte

1. Bei vCSA Upgrades "Löschen" QoSSIOC-Einstellungen im Plug-in (**NetApp Element-Konfiguration > QoSSIOC-Einstellungen**). Das Feld * QoSSIOC Status* wird angezeigt `Not Configured` Nach Abschluss des Vorgangs.
2. Für Upgrades von vCSA und Windows "Deregistrieren" Das Plug-in vom vCenter Server, mit dem es über das Registrierungsprogramm verknüpft ist.
3. "Aktualisieren Sie vSphere einschließlich vCenter Server, ESXi, VMs und anderen VMware Komponenten".

Sie sollten ein Upgrade auf das NetApp Element Plug-in für vCenter Server 5.0 oder höher durchführen, damit Sie das Plug-in mit VMware vCenter 7.0 Update 3 bereitstellen können, ohne eine Problemumgehung anwenden zu müssen.

Beim Upgrade auf VMware vCenter Server 7.0 Update 3 schlägt die Bereitstellung des Element-Plug-ins für vCenter Server 4.x fehl. Um dieses Problem mit Spring Framework 4 zu beheben, siehe "Diesen KB-Artikel"Die

4. "Registrieren" Das Element Plug-in für vCenter Server erneut mit vCenter.
5. "Fügen Sie Cluster hinzu" Verwenden des Plug-ins.
6. "Konfigurieren Sie die QoSSIOC-Einstellungen" Verwenden des Plug-ins.
7. "QoSSIOC aktivieren" Bei allen durch das Plug-in kontrollierten Datenspeichern.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Frühere Versionen der Dokumentation zu SolidFire und NetApp Element

Die Dokumentation für vorherige Versionen steht auf der NetApp Support Site zur Verfügung.

- "Dokumentation zu Element 12.2.1"
- "Dokumentation zu Element 12.2"
- "Dokumentation zu Element 12.0.1"
- "Dokumentation zu Element 12.0"
- "Dokumentation zu Element 11.8.2"
- "Dokumentation zu Element 11.8.1"
- "Dokumentation zu Element 11.8"
- "Dokumentation zu Element 11.7"
- "Dokumentation zu Element 11.5.1"
- "Dokumentation zu Element 11.5"
- "Dokumentation zu Element 11.3P1"
- "Dokumentation zu Element 11.3.2"
- "Dokumentation zu Element 11.1 und frühere Versionen"

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

- "Hinweis für die Element-Software 12.9"
- "Hinweis zu Element Software 12.8"
- "Hinweis zu Element Software 12.7"
- "Hinweis für Ember OS 12.7"
- "Hinweis für Management-Node 12.7"
- "Hinweis zu Element Software 12.5"
- "Hinweis für Management-Node 12.5"
- "Hinweis zu Management Services 2.27.40 (NetApp Element Plug-in für VMware vCenter Server 5.5.16)"
- "Hinweis zu Managementservices 2.26.30 (NetApp Element-Plug-in für VMware vCenter Server 5.4.1)"
- "Hinweis zu Managementservices 2.25.42 (NetApp Element-Plug-in für VMware vCenter Server 5.3.9)"
- "Hinweis zu Managementservices 2.24.40 (NetApp Element-Plug-in für VMware vCenter Server 5.2.12)"
- "Hinweis zu Managementservices 2.23.64 (NetApp Element-Plug-in für VMware vCenter Server 5.1.12)"
- "Hinweis zu Management Services 2.22.7 (NetApp Element-Plug-in für VMware vCenter Server 5.0.37)"

- "Hinweis zu Management Services 2.21.61 (NetApp Element Plug-in für VMware vCenter Server 4.10.12)"
- "Hinweis zu Managementservices 2.20.69 (NetApp Element-Plug-in für vCenter Server 4.9.14)"
- "Hinweis zu Managementservices 2.19.48 (NetApp Element-Plug-in für vCenter Server 4.8.34)"
- "Hinweis zu Managementservices 2.18.91 (NetApp Element-Plug-in für vCenter Server 4.7.10)"
- "Hinweis zu Managementservices 2.17.56 (NetApp Element-Plug-in für vCenter Server 4.6.32)"
- "Hinweis zu Managementservices 2.17.52 (NetApp Element-Plug-in für vCenter Server 4.6.29)"
- "Hinweis zu Managementservices 2.16 (NetApp Element-Plug-in für vCenter Server 4.6.29)"
- "Hinweis zu Managementservices 2.14 (NetApp Element-Plug-in für vCenter Server 4.5.42)"
- "Hinweis zu Managementservices 2.13 (NetApp Element-Plug-in für vCenter Server 4.5.42)"
- "Hinweis zum Speicher-Firmware-Paket 2.182.0"
- "Hinweis zum Speicher-Firmware-Paket 2.175.0"
- "Hinweis zum Storage Firmware Bundle 2.164.0"
- "Hinweis zum Storage Firmware Bundle 2.150"
- "Hinweis zum Storage Firmware Bundle 2.146"
- "Hinweis zum Storage Firmware Bundle 2.99.2"
- "Hinweis zum Storage Firmware Bundle 2.76"
- "Hinweis zum Storage Firmware Bundle 2.27"

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.