Documentación de SolidFire y el software Element

Element Software

NetApp
November 19, 2025

This PDF was generated from https://docs.netapp.com/es-es/element-software-123/index.html on November 19, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Documentación de SolidFire y el software Element . . . 1
Información actual y anterior de la versión . . . 2
- Software NetApp Element . . . 2
- Servicios de gestión . . . 2
- Plugin de NetApp Element para vCenter Server . . . 2
- Firmware de almacenamiento . . . 3
- Obtenga más información . . . 3
- Lo nuevo . . . 3
  - NetApp Bugs Online contiene problemas conocidos y resueltos . . . 3
  - Elemento 12.3.2 . . . 4
  - Elemento 12.3.1 . . . 4
  - Compatibilidad con la clasificación dinámica de nodos de CPU para plataformas host de SolidFire eSDS . . . 5
  - Elemento 12.3 . . . 5

Conceptos . . . 8
- Obtenga más información . . . 8
- Información general del producto . . . 8
  - Funciones de SolidFire . . . 8
  - Puesta en marcha de SolidFire . . . 9
  - Obtenga más información . . . 9
- Información general de la arquitectura de SolidFire . . . 9
  - Direcciones URL comunes . . . 10
  - Obtenga más información . . . 11
  - Interfaces de software de SolidFire . . . 11
  - SolidFire Active IQ . . . 13
  - Nodo de gestión para el software Element . . . 13
  - Servicios de gestión para el almacenamiento all-flash de SolidFire . . . 14
- Nodos . . . 14
  - Nodo de gestión . . . 14
  - Nodo de almacenamiento . . . 15
  - Nodo Fibre Channel . . . 15
  - estados de funcionamiento del nodo . . . 15
  - Obtenga más información . . . 16
- De clúster . . . 16
  - Clústeres de almacenamiento autoritativos . . . 17
  - Regla de las terceras partes . . . 17
  - Capacidad desaprovechada . . . 17
  - Eficiencia del almacenamiento . . . 17
  - Quórum del clúster de almacenamiento . . . 18
- Seguridad . . . 18
  - Cifrado en reposo (hardware) . . . 18
  - Cifrado en reposo (software) . . . 18
  - Gestión de claves externas . . . 19

Autenticación de múltiples factores . . . 19
FIPS 140-2 para HTTPS y cifrado de datos en reposo . . . 19
Si quiere más información . . . 20
Cuentas y permisos . . . 20
Cuentas de administrador de clúster de almacenamiento . . . 20
Cuentas de usuario . . . 20
Cuentas de usuario de clúster autoritativas . . . 21
Cuentas de volumen . . . 21
Reducida . . . 21
Volúmenes . . . 22
Volúmenes virtuales (vVols) . . . 22
Los grupos de acceso de volúmenes . . . 24
Iniciadores . . . 24
Protección de datos . . . 24
Tipos de replicación remota . . . 25
Snapshots de volumen para proteger los datos . . . 27
Clones de volúmenes . . . 27
Información general del proceso de backup y restauración para el almacenamiento Element . . . 27
Dominios de protección . . . 28
Dominios de protección personalizados . . . 28
Alta disponibilidad de Double Helix . . . 29
Rendimiento y calidad del servicio . . . 29
Parámetros de calidad de servicio . . . 29
Límites de valor de calidad de servicio . . . 30
Rendimiento de la calidad de servicio . . . 30
Políticas de calidad de servicio . . . 31
Obtenga más información . . . 32
Requisitos . . . 33
Obtenga más información . . . 33
Redes . . . 33
Si quiere más información . . . 33
Configuración de switches para los clústeres que ejecutan el software Element . . . 33
Si quiere más información . . . 35
Requisitos de puerto de red . . . 35
Si quiere más información . . . 39
Pruébelo . . . 40
Obtenga más información . . . 40
Pruebe las funciones de almacenamiento usando Element Demo Node . . . 40
Funcionalidad compatible: . . . 40
Requisitos de equipos virtuales . . . 41
Requisitos del host . . . 41
Descargue el nodo de demostración de Element . . . 41
Instale el nodo de demostración de Element en VMware ESXi . . . 41
Cómo obtener soporte . . . 43
Obtenga más información . . . 43

Instale y mantenga el hardware . . . 44
Obtenga más información . . . 44
Información de hardware H410S y H610S . . . 44
Obtenga más información . . . 44
Instale los nodos de almacenamiento H-Series . . . 44
Sustituya un nodo H410S . . . 53
Sustituya un nodo H610S . . . 57
Sustituya las unidades . . . 60
Sustituya una unidad de fuente de alimentación . . . 63
Información sobre hardware de SF-Series . . . 66
Obtenga más información . . . 66
Sustituya un chasis . . . 66
Sustituya unidades para los nodos de almacenamiento SF-Series . . . 69
Sustituya una unidad de fuente de alimentación . . . 72
Vuelva a la información de la imagen de fábrica . . . 73
Configure el RTFI . . . 73
El proceso RTFI . . . 74
Menú de opciones de RTFI . . . 77
Información general de la configuración . . . 80
Obtenga más información . . . 80
Configure un clúster con nodos de almacenamiento Element . . . 80
Obtenga más información . . . 81
Configure un nodo de almacenamiento . . . 81
Cree un clúster de almacenamiento de . . . 83
Acceda a la interfaz de usuario del software Element . . . 85
Añada unidades a un clúster . . . 85
Configure un clúster con nodos Fibre Channel . . . 86
Configure un nodo Fibre Channel . . . 86
Cree un nuevo clúster con nodos Fibre Channel . . . 87
Añada nodos Fibre Channel a un clúster . . . 88
Configure zonas para los nodos Fibre Channel . . . 88
Cree un grupo de acceso de volúmenes para clientes Fibre Channel . . . 89
Determine qué componentes de SolidFire instalar . . . 89
Si quiere más información . . . 90
Configure un nodo de gestión . . . 90
Obtenga más información . . . 90
Configure el acceso completo a la interfaz de usuario web de Nombre de dominio . . . 91
Configure el acceso de interfaz de usuario web de FQDN mediante NetApp Hybrid Cloud Control . . . 91
Configure el acceso de interfaz de usuario web del FQDN mediante la API DE REST . . . 92
Elimine el acceso de interfaz de usuario web de FQDN mediante el control de cloud híbrido de NetApp . . . 93
Quite el acceso de interfaz de usuario web del FQDN mediante la API DE REST . . . 93
Resolución de problemas . . . 94
Obtenga más información . . . 95
Lo siguiente . . . 95

Obtenga más información . . . 95
Gestionar el almacenamiento con el software Element . . . 96
Obtenga más información . . . 96
Acceda a la interfaz de usuario del software Element . . . 96
Obtenga más información . . . 97
Configure las opciones del sistema SolidFire después de la implementación . . . 97
Obtenga más información . . . 97
Cambie las credenciales en NetApp HCI y SolidFire de NetApp . . . 97
Cambie el certificado SSL predeterminado del software Element . . . 101
Cambie la contraseña de IPMI predeterminada para los nodos . . . 102
Use las opciones básicas en la interfaz de usuario del software Element . . . 104
Si quiere más información . . . 104
Ver la actividad de la API . . . 104
Iconos en la interfaz de Element . . . 105
Enviar comentarios . . . 106
Gestionar cuentas . . . 106
Si quiere más información . . . 107
Trabaje con cuentas que utilicen CHAP . . . 107
Gestione cuentas de usuario administrador del clúster . . . 109
Gestione su sistema . . . 120
Si quiere más información . . . 121
Habilite la autenticación multifactor . . . 121
Configure las opciones del clúster . . . 122
Cree un clúster que admita unidades FIPS . . . 138
Habilite FIPS 140-2 para HTTPS en el clúster . . . 141
Comience con la gestión de claves externas . . . 144
Gestione volúmenes y volúmenes virtuales . . . 149
Si quiere más información . . . 149
Trabaje con volúmenes . . . 149
Trabaje con volúmenes virtuales . . . 158
Trabajar con iniciadores y grupos de acceso de volúmenes . . . 168
Proteja sus datos . . . 176
Si quiere más información . . . 177
Use copias Snapshot de volumen para la protección de datos . . . 177
Llevar a cabo la replicación remota entre los clústeres que ejecutan el software NetApp Element . . . 190
Use la replicación de SnapMirror entre clústeres de Element y ONTAP . . . 205
Realice backups y restaure volúmenes . . . 217
Solucionar los problemas del sistema . . . 221
Si quiere más información . . . 222
Ver información acerca de los eventos del sistema . . . 222
Ver el estado de las tareas en ejecución . . . 225
Ver las alertas del sistema . . . 226
Ver la actividad de rendimiento del nodo . . . 243
Ver el rendimiento del volumen . . . 243
Ver sesiones iSCSI . . . 245

Consulte las sesiones Fibre Channel . . . 246
Solucione problemas de unidades . . . 247
Solucione los problemas de los nodos . . . 251
Trabaje con utilidades por nodo para los nodos de almacenamiento . . . 252
Comprender los niveles de llenado de clústeres . . . 259
Gestione y supervise el almacenamiento con Hybrid Cloud Control de NetApp . . . 261
Añada y gestione clústeres de almacenamiento utilizando Hybrid Cloud Control de NetApp . . . 261
Añada un clúster de almacenamiento . . . 262
Confirmar el estado del clúster de almacenamiento . . . 262
Editar credenciales del clúster de almacenamiento . . . 263
Quite un clúster de almacenamiento de . . . 263
Habilite y deshabilite el modo de mantenimiento . . . 263
Cree y gestione cuentas de usuario con NetApp Hybrid Cloud Control . . . 265
Habilite LDAP . . . 266
Administrar cuentas de clúster autorizadas . . . 266
Permite gestionar cuentas de volumen . . . 268
Cree y gestione volúmenes mediante Hybrid Cloud Control de NetApp . . . 269
Cree un volumen . . . 270
Aplique una política de calidad de servicio en un volumen . . . 271
Editar un volumen . . . 271
Clonar volúmenes . . . 273
Añada volúmenes a un grupo de acceso de volúmenes . . . 274
Eliminar un volumen . . . 274
Restaurar un volumen eliminado . . . 275
Purgar un volumen eliminado . . . 275
Permite crear y gestionar grupos de acceso de volúmenes . . . 276
Añadir un grupo de acceso de volúmenes . . . 276
Edite un grupo de acceso de volúmenes . . . 277
Elimine un grupo de acceso de volúmenes . . . 277
Cree y gestione iniciadores . . . 278
Cree un iniciador . . . 278
Añada iniciadores a un grupo de acceso de volúmenes . . . 279
Cambie un alias de iniciador . . . 280
Elimine los iniciadores . . . 280
Cree y gestione políticas de calidad de servicio de volúmenes . . . 280
Cree una política de calidad de servicio . . . 281
Aplique una política de calidad de servicio en un volumen . . . 281
Cambie la asignación de políticas de calidad de servicio de un volumen . . . 282
Edite una política de calidad de servicio . . . 283
Elimine una política de calidad de servicio . . . 283
Supervise su sistema SolidFire con el control del cloud híbrido de NetApp . . . 284
Supervise los recursos de almacenamiento en la consola de control del cloud híbrido . . . 284
Consulte el inventario en la página Nodes . . . 289
Supervise los volúmenes en el clúster de almacenamiento de . . . 291
Recopile registros para solucionar problemas . . . 292

Gestione el almacenamiento con la API de Element . . . 297
Obtenga más información . . . 297
Acerca de la API del software Element . . . 298
Obtenga más información . . . 298
Solicitar miembros de objeto . . . 298
Miembros del objeto de respuesta . . . 299
Extremos de solicitudes . . . 300
Autenticación API . . . 300
Métodos asíncronos . . . 301
Atributos . . . 302
Objetos comunes . . . 302
Obtenga más información . . . 305
cuenta . . . 305
AuthSessionInfo . . . 306
BulkVolumeJob . . . 308
vinculación (volúmenes virtuales) . . . 309
Detalles del certificado . . . 310
clúster . . . 311
ClusterAdmin . . . 313
ClusterCapacity . . . 314
ClusterConfig . . . 316
ClusterInfo . . . 317
ClusterPair . . . 319
ClusterStats . . . 320
ClusterStructure . . . 323
unidad . . . 324
DriveStats . . . 327
error . . . 329
evento . . . 329
fallo . . . 331
Puerto de FiberChannelPort . . . 334
FipsErrorNodeReport . . . 335
FipsNodeReport . . . 336
FipsReport . . . 337
GroupSnapshot . . . 337
HardwareInfo . . . 338
host (volúmenes virtuales) . . . 340
IdpConfigInfo . . . 341
iniciador . . . 342
KeyProviderKmip . . . 343
KeyServerKmip . . . 344
LdapConfiguration . . . 346
LoggingServer . . . 347
red (interfaces unidas) . . . 348
red (todas las interfaces) . . . 353

Red (interfaces Ethernet) . . . 353
red (interfaces locales) . . . 355
Red (SNMP) . . . 357
NetworkInterface . . . 358
NetworkInterfaceStats . . . 359
nodo . . . 360
ProtectionDomains de nodo . . . 363
Estadísticas de nodos . . . 363
OntapVersionInfo . . . 364
PendingActiveNode . . . 365
PendingNode . . . 367
ProtectionDomain . . . 369
ProtectionDomainLevel . . . 369
ProtectionDomainResiliency . . . 370
ProtectionDomainTolerance . . . 371
ProtectionSchemeResiliency . . . 371
ProtectionSchemeTolerance . . . 372
ProtocolEndpoint . . . 373
Calidad de servicio . . . 374
QoSPolicy . . . 375
RemoteClusterSnapshotStatus . . . 376
programación . . . 377
Sesión (Fibre Channel) . . . 380
Sesión (iSCSI) . . . 381
SnapMirrorAggregate . . . 384
SnapMirrorClusterIdentity . . . 384
SnapMirrorEndpoint . . . 385
SnapMirrorJobScheduleCronInfo . . . 386
SnapMirrorLunInfo . . . 386
SnapMirrorNetworkInterface . . . 387
SnapMirrorNode . . . 388
SnapMirrorPolicy . . . 389
SnapMirrorPolicyRule . . . 390
SnapMirrorRelationship . . . 391
SnapMirrorVolume . . . 394
SnapMirrorVolumeInfo . . . 395
SnapMirrorVServer . . . 396
SnapMirrorVserveragregateInfo . . . 397
snapshot . . . 398
SnmpTrapRecipient . . . 401
Contenedor de almacenamiento . . . 401
SyncJob . . . 402
tarea (volúmenes virtuales) . . . 405
UsumUsuario . . . 407
VirtualNetwork . . . 408

- Volumen virtual . . . 409
- volumen . . . 411
- VolumeAccessGroup . . . 415
- Pareja de volúmenes . . . 416
- VolumeStats . . . 418

Métodos comunes . . . 424
- Obtenga más información . . . 425
- GetAPI . . . 425
- GetAsyncResult . . . 433
- GetCompleteStats . . . 437
- GetLimits . . . 437
- GetOrigin . . . 440
- GetRawStats . . . 441
- ListAsyncResults . . . 441

Métodos de API de cuenta . . . 444
- Obtenga más información . . . 444
- AddAccount . . . 444
- GetAccountByID . . . 447
- GetAccountByName . . . 448
- GetAccountEfficiency . . . 450
- Cuentas de lista . . . 452
- ModificyAccount . . . 454
- RemoveAccount . . . 457

Métodos API de administrador . . . 458
- Obtenga más información . . . 459
- AddClusterAdmin . . . 459
- GetCurrentClusterAdmin . . . 461
- GetLoginBanner . . . 462
- ListClusterAdmins . . . 463
- ModifyClusterAdmin . . . 466
- RemoveClusterAdmin . . . 467
- SetLoginBanner . . . 468

Métodos de API de clúster . . . 471
- Obtenga más información . . . 472
- AddNodes . . . 472
- ClearClusterFaults . . . 475
- CreateClusterInterfacePreference . . . 477
- DeleteClusterInterfacePreference . . . 478
- EnableFeature . . . 479
- GetClusterCapacity . . . 481
- GetClusterFullThreshold . . . 483
- GetClusterHardwareInfo . . . 490
- GetClusterInfo . . . 492
- GetClusterInterfacePreference . . . 494
- GetClusterMasterNodeID . . . 495

- GetClusterStats . . . 496
- GetClusterVersionInfo . . . 497
- GetFeatureStatus . . . 501
- GetLoginSessionInfo . . . 503
- GetNodeHardwareInfo . . . 505
- GetNodeStats . . . 506
- ListActiveNodes . . . 507
- ListAllNodes . . . 508
- ListClusterFaults . . . 510
- ListClusterInterfacePreferences . . . 514
- ListEvents . . . 515
- ListNodeStats . . . 518
- ListISCSISessions . . . 519
- Servicios de listas . . . 521
- ListPendingNodes . . . 524
- ListPendingActiveNodes . . . 526
- ModifyClusterFullThreshold . . . 527
- ModifyClusterInterfacePreference . . . 534
- RemoveNodes . . . 535
- SetLoginSessionInfo . . . 537
- Apagado . . . 539

Métodos API de creación de clúster . . . 540
- Obtenga más información . . . 540
- Clúster de propuesta de CheckedCluster . . . 541
- CreateCluster . . . 542
- GetBootstrapConfig . . . 545

Métodos de API de unidad . . . 549
- Obtenga más información . . . 549
- AddDrives . . . 549
- GetDriveHardwarwareInfo . . . 551
- GetDriveStats . . . 553
- ListDrives . . . 556
- ListDriveStats . . . 558
- RemoveDrives . . . 560
- SecureEraseDrives . . . 562

Métodos de API de Fibre Channel . . . 564
- Obtenga más información . . . 564
- GetVolumeAccessGroupLunAssignments . . . 564
- ListFiberChannelPortInfo . . . 565
- ListFiberChannelSessions . . . 569
- ListNodeFiberChannelPortInfo . . . 570
- ModifyVolumeAccessGroupLunAssignments . . . 573

Métodos de API del iniciador . . . 575
- Obtenga más información . . . 575
- CreateInitiators . . . 575

DeleteInitiators 579
ListInitiators 581
ModificyInitiators 582
Métodos de API de LDAP 586
Obtenga más información 587
AddLdapClusterAdmin 587
EnableLdapAuthentication 588
Autenticación DisableLdapAuthentication 593
GetLdapConfiguration 594
TestLdapAuthentication 596
Métodos de API de autenticación multifactor 598
Obtenga más información 598
AddIdpClusterAdmin 598
CreateIdpConfiguration 601
DeleteAuthSession 603
DeleteAuthSessionsByClusterAdmin 604
DeleteAuthSessionsByUsername 606
DeleteIdpConfiguration 609
DisableIdpAuthentication 610
EnableIdpAuthentication 611
GetIdpAuthenticationState 612
ListActiveAuthSessions 613
ListIdpConfigurations 614
UpdateIdpConfiguration 616
Métodos API de autenticación de sesión 619
Obtenga más información 619
ListAuthSessionsByClusterAdmin 619
ListAuthSessionsByUsername 621
Métodos de API de nodo 623
Obtenga más información 625
CheckPingOnVlan 625
CheckboedNodeAdditions 629
CreateClusterSupportBundle 632
CreateSupportBundle 635
DeleteAllSupportBundles 638
Modo de mantenimiento disableMaintenanceMode 638
DisableSsh 641
EnableMaintenanceMode 642
EnableSsh 645
GetClusterConfig 646
Estado GetClusterState 647
Getconfig 649
GetDriveConfig 650
GetHardwarConfig 652
GetHardwareInfo 654

GetIpmiConfig . . . 656
GetIpmiInfo . . . 661
GetNetworkConfig . . . 664
GetNetworkInterface . . . 665
GetNodeActiveTlsCiphers . . . 669
GetNodeFipsDrivesReport . . . 670
GetNodeSSLCertificate . . . 671
GetNodeSupportedTlsCiphers . . . 673
GetPatchInfo . . . 675
GetPendingOperation . . . 677
GetSshInfo . . . 678
ListDrivehardware . . . 679
ListNetworkinterfaces . . . 682
ListNetworkInterfaceStats . . . 684
ListTests . . . 686
ListUtilities . . . 687
RemoveNodeSSLCertificate . . . 688
ResetDrives . . . 689
ResetNode . . . 691
ResetNodeSupplementalTlsCiphers . . . 694
RestartNetworking . . . 695
Servicios de RestartServices . . . 696
SetClusterConfig . . . 697
Config . . . 699
SetNetworkConfig . . . 701
SetNodeSSLCertificate . . . 703
SetNodeSupplementalTlsCiphers . . . 706
Apagado . . . 707
TestConnectEnsemble . . . 709
TestConnectMvip . . . 711
TestConnectSvip . . . 715
TestDrives . . . 720
TestHardwarConfig . . . 721
TestLocateCluster . . . 723
TestLocalConnectivity . . . 724
TestNetworkConfig . . . 727
Pruebas de ping . . . 730
TestRemoteConnectivity . . . 734
Métodos de API de replicación . . . 736
Obtenga más información . . . 737
Orden de operaciones de emparejamiento de clústeres . . . 737
Orden de las operaciones de emparejamiento de volúmenes . . . 738
Modos de replicación compatibles para clústeres emparejados . . . 738
CompleteClusterPairing . . . 738
CompleteVolumePairing . . . 740

ListClusterPairs . . . 741
ListActivePairedVolumes . . . 743
ModifyVolumePair . . . 746
RemoveClusterPair . . . 748
RemoveVolumePair . . . 749
StartClusterPairing . . . 750
StartVolumePairing . . . 751
Métodos de API de seguridad . . . 755
Obtenga más información . . . 755
AddKeyServerToProviderKmip . . . 755
CreateKeyProviderKmip . . . 757
CreateKeyServerKmip . . . 758
CreatePublicPrivateKeyPair . . . 761
DeleteKeyProviderKmip . . . 763
DeleteKeyServerKmip . . . 764
DisableEncryptionAtest . . . 765
EnableEncryptionAtest . . . 766
GetClientCertificateSignRequest . . . 768
GetKeyProviderKmip . . . 770
GetKeyServerKmip . . . 771
GetSoftwareEncryptionAtRestInfo . . . 772
ListKeyProvidersKmip . . . 774
ListKeyServersKmip . . . 777
ModifyKeyServerKmip . . . 780
RekeySoftwareEncryptionAtRestMasterKey . . . 783
RemoveKeyServerFromProviderKmip . . . 786
TestKeyProviderKmip . . . 787
TestKeyServerKmip . . . 788
Métodos de API de SnapMirror . . . 789
Obtenga más información . . . 790
AbrortSnapMirrorRelationship . . . 790
SnapBreakMirrorRelationship . . . 791
SnapBreakMirrorVolume . . . 792
CreateSnapMirrorEndpoint . . . 794
CreateSnapMirrorEndpointUnmanaged . . . 795
CreateSnapMirrorRelationship . . . 796
CreateSnapMirrorVolume . . . 798
DeleteSnapMirrorEndpoints . . . 800
DeleteSnapMirrorrelationships . . . 800
GetOntapVersionInfo . . . 801
GetSnapMirrorClusterIdentity . . . 802
InitializeSnapMirrorRelationship . . . 803
ListSnapMirrorAggregates . . . 804
ListSnapMirrorEndpoints . . . 804
ListSnapMirrorLuns . . . 805

ListSnapMirrorNetworkinterfaces 806
ListSnapMirrorNodes 807
ListSnapMirrorPolicies 808
ListSnapMirrorSchedules 809
ListSnapMirrorRelationship 809
ListSnapMirrorVolumes 811
ListSnapMirrorservidores 812
ModificySnapMirrorEndpoint 814
ModificySnapMirrorEndpoint (no administrado) 814
ModificySnapMirrorRelationship 815
UpdateSnapMirrorRelationship 817
QuiesceSnapMirrorRelationship 818
ReumeSnapMirrorRelationship 819
ResyncSnapMirrorRelationship 820
Métodos de la API de configuración del sistema 822
Obtenga más información 823
DisablebmcColdReset 823
DisableClusterSsh 824
DisableSnmp 825
EnablebmcColdReset 826
EnableClusterSsh 827
EnableSnmp 829
GetBinAssignmentProperties 830
GetClusterSshInfo 833
GetClusterStructure 834
GetFipsReport 835
GetLldpConfig 837
GetLldpInfo 838
GetNodeFipsDrivesReport 839
GetNtpInfo 840
GetNvramInfo 842
GetProtectionDomainLayout 843
GetRemoteLoggingHosts 845
GetSnmpACL 846
GetSnmpInfo 847
GetSnmpState 849
GetSnmpTrapInfo 851
GetSSLCertificate 852
ListProtectionDomainLevels 854
RemoveSSLCertificate 856
ResetNetworkConfig 857
ResetSupplementalTlsCiphers 858
SetClusterStructure 859
SetLldpConfig 860
SetNtpInfo 861

SetProtectionDomainLayout . . . 863
SetRemoteLoggingHosts . . . 866
SetSnmpACL . . . 867
SetSnmpInfo . . . 869
SetSnmpTrapInfo . . . 872
SetSSLCertificate . . . 874
SnmpSendTestTraps . . . 876
TestAddressAvailability . . . 877
Métodos de API de redes múltiples inquilinos . . . 879
Requisitos previos para configurar una red virtual multitenant . . . 879
Orden de operaciones de red virtual . . . 879
Obtenga más información . . . 879
Convenciones de nomenclatura de redes virtuales . . . 879
AddVirtualNetwork . . . 880
ModificyVirtualNetwork . . . 883
ListVirtualNetworks . . . 886
RemoveVirtualNetwork . . . 889
Métodos de API de volumen . . . 890
Obtenga más información . . . 891
CancelClone . . . 892
CancelGroupClone . . . 893
CloneMultipleVolumes . . . 894
CloneVolume . . . 898
CopyVolume . . . 903
QoCreateSPolicy . . . 905
CreateVolume . . . 907
CreateBackupTarget . . . 915
QoDeleteSPolicy . . . 916
DeleteVolume . . . 917
DeleteVolumes . . . 920
GetBackupTarget . . . 923
GetVolumeStats . . . 925
GetDefaultQoS . . . 928
GetQoSPolicy . . . 929
GetVolumeCount . . . 931
GetVolumeEffect . . . 932
ListActiveVolumes . . . 934
ListBackupTargets . . . 936
ListBulkVolumeJobs . . . 937
ListDeletedVolumes . . . 939
ListQoSPolicies . . . 942
ListSyncJobs . . . 944
ListVolumeQoSHistogramas . . . 946
ListVolumes . . . 948
ListVolumeStats . . . 953

ListVolumesForAccount . . . 955
ListVolumeStatsByAccount . . . 958
ListVolumeStatsByVirtualVolume . . . 960
ListVolumeStatsByVolume . . . 962
ListVolumeStatsByVolumeAccessGroup . . . 964
ModifyBackupTarget . . . 966
ModifyQoSPolicy . . . 968
Volumen ModificíoVolume . . . 970
ModificyVolumes . . . 979
PurgeDeletedVolume . . . 988
PurgeDeletedVolumes . . . 989
RemoveBackupTarget . . . 990
RestoreDeletedVolume . . . 991
SetDefaultQoS . . . 992
StartBulkVolumeRead . . . 994
StartBulkVolumeWrite . . . 997
UpdateBulkVolumeStatus . . . 1000
Métodos API de grupo de acceso de volúmenes . . . 1003
Obtenga más información . . . 1003
AddInitiatorsToVolumeAccessGroup . . . 1003
AddVolumesToVolumeAccessGroup . . . 1006
CreateVolumeAccessGroup . . . 1007
DeleteVolumeAccessGroup . . . 1010
ListVolumeAccessGroups . . . 1013
RemoveVolumesFromVolumeAccessGroup . . . 1015
RemoveInitiatorsFromVolumeAccessGroup . . . 1017
ModifyVolumeAccessGroup . . . 1019
GetVolumeAccessGroupEfficency . . . 1023
Métodos de API de Snapshot de volumen . . . 1025
Obtenga más información . . . 1025
Información general de Snapshot . . . 1025
CreateGroupSnapshot . . . 1026
CreateSchedule . . . 1033
CreateSnapshot . . . 1046
DeleteGroupSnapshot . . . 1052
DeleteSnapshot . . . 1054
GetSchedule . . . 1055
ListGroupSnapshots . . . 1057
ListSchedules . . . 1060
ListSnapshots . . . 1062
ModifiyGroupSnapshot . . . 1064
ModificySchedule . . . 1068
ModificySnapshot . . . 1075
RollbackToGroupSnapshot . . . 1079
RollbackToSnapshot . . . 1084

Métodos de API para volúmenes virtuales 1087
Obtenga más información 1087
CreateStorageContainer 1087
DeleteStorageContainers 1089
GetStorageContainerEfficiency 1090
GetVirtualVolumeCount 1092
ListProtocolEndpoints 1093
ListStorageContainers 1096
ListVirtualVolumeBindings 1097
ListVirtualVolumeHosts 1099
ListVirtualVolumes 1101
ListVirtualVolumeTasks 1105
ModificyStorageContainer 1106
Control de acceso 1108
cuentas 1108
administrador 1109
ClusterAdmin 1109
unidades 1112
nodos 1112
lea 1113
creación de informes 1114
repositorios 1116
volúmenes 1116
escritura 1117
Ejemplos de respuestas 1118
Obtenga más información 1119
Getconfig 1119
GetClusterHardwareInfo 1121
GetLldpInfo 1135
GetNetworkConfig 1164
GetNodeHardwareInfo (salida para iSCSI) 1169
GetNodeHardwareInfo (salida para nodos Fibre Channel) 1171
GetNvramInfo 1178
ListActiveNodes 1187
ListActiveVolumes 1190
TestHardwarConfig 1199
Plugin de NetApp Element para vCenter Server 1205
Si quiere más información 1205
Supervise el almacenamiento con SolidFire Active IQ 1206
Si quiere más información 1206
Trabaje con el nodo de gestión 1207
Información general sobre los nodos de gestión 1207
Instale o recupere un nodo de gestión 1208
Instale un nodo de gestión 1208
Configurar una controladora de interfaz de red (NIC) de almacenamiento 1214

Recupere un nodo de gestión . . . 1217
Acceda al nodo de gestión . . . 1221
Acceda a la interfaz de usuario de cada nodo de gestión . . . 1222
Acceda a la interfaz de usuario de API DE REST del nodo de gestión . . . 1223
Trabaje con la interfaz de usuario del nodo de gestión . . . 1224
Información general de la interfaz de usuario del nodo de gestión . . . 1224
Configure la supervisión de alertas . . . 1224
Modifique y pruebe la red, el clúster y la configuración del sistema de los nodos de gestión . . . 1224
Ejecute las utilidades del sistema desde el nodo de gestión . . . 1226
Trabaje con la API DE REST del nodo de gestión . . . 1228
Información general de la interfaz de usuario de la API DE REST del nodo de . . . 1228
Obtenga autorización para utilizar las API de REST . . . 1228
Habilite la supervisión de Active IQ y NetApp . . . 1229
Configure Cloud Control de NetApp híbrido para varias instancias de vCenter . . . 1232
Añada un activo de controladora al nodo de gestión . . . 1233
Crear y gestionar activos de clúster de almacenamiento . . . 1235
Ver o editar activos de controladora existentes . . . 1240
Configure un servidor proxy . . . 1242
Verifique el sistema operativo del nodo de gestión y las versiones de servicios . . . 1243
Obtener registros de los servicios de gestión . . . 1245
Gestión de conexiones de soporte . . . 1246
Inicie una sesión de soporte remota de NetApp . . . 1246
Gestione la funcionalidad SSH en el nodo de gestión . . . 1247
Actualice la versión Element 12,3.x de su sistema de almacenamiento all-flash NetApp SolidFire . . . 1251
Información general sobre la secuencia de actualización . . . 1251
secuencia de actualización del sistema . . . 1252
Procedimientos de actualización del sistema . . . 1252
Actualice los servicios de gestión . . . 1253
Actualice a la versión más reciente de HealthTools . . . 1255
Ejecute comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento . . . 1257
Actualice el software Element . . . 1266
Actualizar el firmware de almacenamiento . . . 1283
Actualice un nodo de gestión . . . 1293
Actualice el plugin de Element para vCenter Server . . . 1307
Actualice los componentes de vSphere para un sistema de almacenamiento SolidFire de NetApp con el plugin de Element para vCenter Server . . . 1314
Obtenga más información . . . 1314
Versiones anteriores de la documentación sobre el software SolidFire y NetApp Element . . . 1315
Si quiere más información . . . 1315
Avisos legales . . . 1316
Derechos de autor . . . 1316
Marcas comerciales . . . 1316
Estadounidenses . . . 1316
Política de privacidad . . . 1316

Código abierto 1316

Documentación de SolidFire y el software Element

Información actual y anterior de la versión

Es posible encontrar enlaces a las notas de la versión más reciente y anteriores para varios componentes del entorno de almacenamiento de Element.

Se le pedirá que inicie sesión con sus credenciales de soporte de NetApp.

Software NetApp Element

- "Notas de la versión del software NetApp Element 12.3.2"
- "Notas de la versión del software NetApp Element 12.3.1"
- "Notas de la versión del software NetApp Element 12.3"
- "Notas de la versión del software NetApp Element 12.2.1"
- "Notas de la versión del software NetApp Element 12.2"
- "Notas de la versión del software NetApp Element 12.0.1"
- "Notas de la versión del software NetApp Element 12.0"
- "Notas de la versión del software NetApp Element 11.8.2"
- "Notas de la versión del software NetApp Element 11.8.1"
- "Notas de la versión del software NetApp Element 11.8"
- "Notas de la versión del software NetApp Element 11.7"
- "Notas de la versión del software NetApp Element 11.5.1"
- "Notas de la versión del software NetApp Element 11.3P1"

Servicios de gestión

- "Notas de la versión de los servicios de gestión"

Plugin de NetApp Element para vCenter Server

- "Notas de la versión del plugin de vCenter 5,3" *NEW*
- "Notas de la versión del plugin de vCenter 5,2"
- "Notas de la versión del plugin de vCenter 5.1"
- "Notas de la versión del plugin de vCenter 5.0"
- "Notas de la versión del plugin de vCenter 4.10"
- "Notas de la versión del plugin de vCenter 4.9"
- "Notas de la versión del plugin de vCenter 4.8"
- "Notas de la versión del plugin de vCenter 4.7"
- "Notas de la versión del plugin de vCenter 4.6"
- "Notas de la versión del plugin de vCenter 4.5"
- "Notas de la versión del plugin de vCenter 4.4"

- "Notas de la versión del plugin de vCenter 4.3"

Firmware de almacenamiento

- "Notas de la versión del paquete de firmware de almacenamiento 2.146 (última)"
- "Notas de la versión del paquete de firmware de almacenamiento 2.99.2"
- "Notas de la versión del paquete de firmware de almacenamiento 2.76"
- "Notas de la versión del paquete de firmware de almacenamiento 2.27"
- "Notas de la versión de H610S BMC 3.84.07"

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"
- "Información general sobre el almacenamiento all-flash de SolidFire"

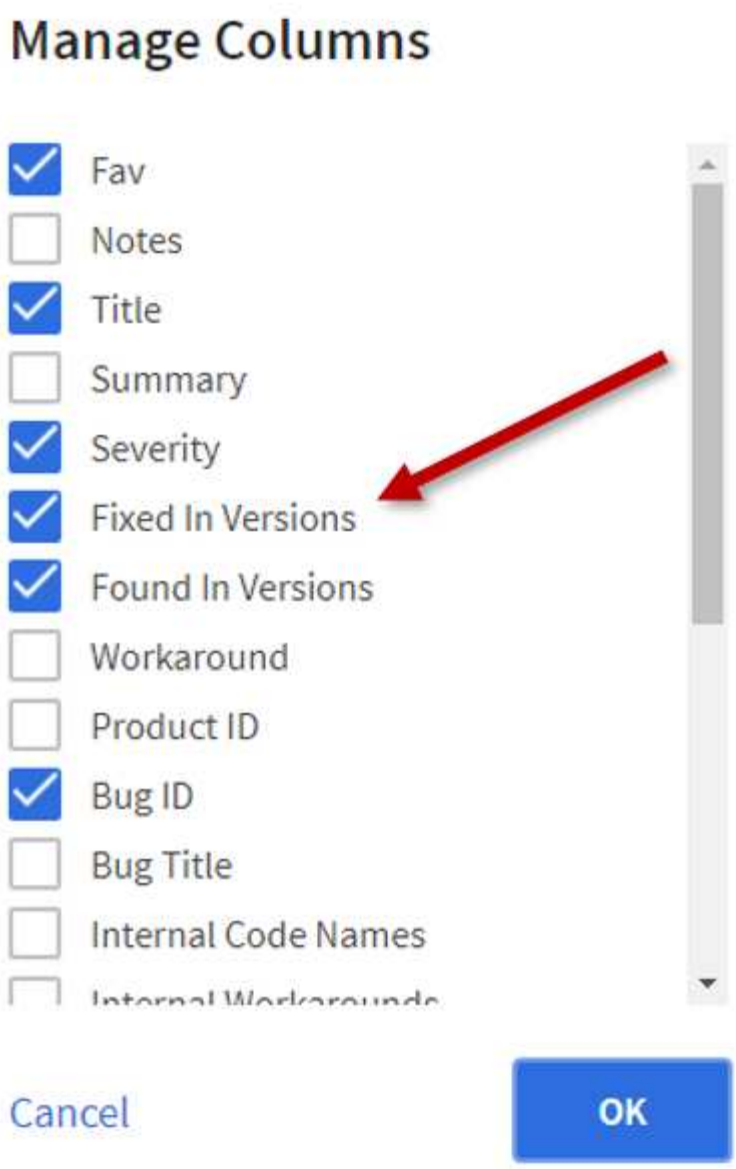
Lo nuevo

NetApp actualiza periódicamente el software SolidFire y Element para incorporar nuevas funciones, mejoras y correcciones de errores. Element 12.3 presenta el cifrado de software en reposo mejoras, mejoras en la seguridad, actualizaciones del firmware de almacenamiento, funcionalidad de copias Snapshot mejorada y comportamiento mejorado para unidades con fallos.

NetApp Bugs Online contiene problemas conocidos y resueltos

Los problemas conocidos y resueltos, ahora se incluyen en la herramienta NetApp Bugs Online. Puede examinar estos problemas para Element y otros productos.

1. Vaya a. "NetApp Bugs Online".
2. Escriba el nombre del producto, por ejemplo "elemento", en el campo **Buscar por palabra clave**.
3. Seleccione la Seleccione **Fixed in Versions** y seleccione **OK**.



4. Para filtrar por versión, escriba la versión en el campo **Fixed in Versions**.

Elemento 12.3.2

Obtenga más información sobre las novedades de la versión 12.3.2.

La versión 12.3.2 del software Element contiene la mitigación que cierra la exposición del software Element a la vulnerabilidad Apache Log4j. Los clústeres de almacenamiento de SolidFire de NetApp con la función Virtual Volumes (VVol) habilitada se exponen a esta vulnerabilidad.

Elemento 12.3.1

Obtenga más información sobre las novedades de la versión 12.3.1.

Paquete de firmware de almacenamiento 2.99.2

La versión 12.3.1 de Element incluye la versión 2.99.2 del paquete de firmware de almacenamiento. Si el clúster de almacenamiento ya está en Element 12.3, tiene la opción de instalar simplemente el nuevo paquete

de firmware 2.99.2.

Compatibilidad con la clasificación dinámica de nodos de CPU para plataformas host de SolidFire eSDS

SolidFire eSDS ahora puede admitir toda la gama de CPU de generación de lagos en cascada Intel Gold y Silver, una gama de 24 modelos. La función Dynamic Node Rating asigna una clasificación de IOPS de calidad de servicio entre 50.000 y 100K al servidor host en función de la CPU.

Número de núcleos de CPU	Clasificación de IOPS de nodos ESDS
8	50 000
10	60 000
12	75 000
16 o posterior	100 000

Compatibilidad con la configuración de red de enlace único para SolidFire eSDS

Ahora puede utilizar una configuración de red de enlace único para el host con SolidFire eSDS.

Nueva compatibilidad de servidores en SolidFire Enterprise SDS

SolidFire eSDS ya está disponible en los servidores HPE DL380. Consulte "Herramienta de matriz de interoperabilidad de NetApp (IMT)" para obtener más información sobre la configuración compatible.

Elemento 12.3

Obtenga más información sobre las novedades de la versión 12.3.

Compatibilidad con cola de instantáneas FIFO

Element 12.3 permite crear una cola de entrada primera salida (FIFO) para snapshots de volúmenes. Con la API de Element, es posible especificar el número mínimo y máximo de ranuras de snapshot FIFO que se deben reservar al crear un volumen. Cuando la cola de snapshot FIFO de un volumen está llena, la próxima snapshot que se crea para ese volumen quita la snapshot más antigua de ese volumen del sistema. Tanto las instantáneas FIFO como las que no lo son utilizan el mismo pool de ranuras Snapshot disponibles en un volumen.

Los siguientes métodos API de Element están relacionados con las instantáneas FIFO (consulte "Documentación de la API de Element" Para obtener detalles acerca de cada método de API):

- CreateGroupSnapshot
- CreateSchedule
- CreateSnapshot
- CreateVolume
- ModifiyGroupSnapshot

- ModificySchedule
- ModificySnapshot
- Volumen ModificíoVolume
- ModificyVolumes

Compatibilidad con la serialización de instantáneas

Element 12.3 admite la creación de snapshots serializada. Al crear una nueva copia de Snapshot con la API de Element, es posible especificar que no se debe crear la copia de Snapshot si aún hay una replicación de Snapshot anterior en curso.

Los siguientes métodos API de Element se relacionan con la serialización de snapshots (consulte "Documentación de la API de Element" Para obtener detalles acerca de cada método de API):

- CreateGroupSnapshot
- CreateSchedule
- CreateSnapshot
- ModificySchedule

Compatibilidad con retención de snapshots

Element 12.3 permite especificar el tiempo de retención de copias de Snapshot. Si no especifica un tiempo de retención o un tiempo de caducidad para una copia Snapshot, se conserva para siempre.

Los siguientes métodos API de Element están relacionados con la retención de copias de Snapshot (consulte "Documentación de la API de Element" Para obtener detalles acerca de cada método de API):

- CreateGroupSnapshot
- CreateSchedule
- CreateSnapshot
- ModifiyGroupSnapshot
- ModificySchedule
- ModificySnapshot

Mejoras en el cifrado de software en reposo

Para la función de cifrado de software en reposo, Element 12.3 presenta External Key Management (EKM) y la capacidad para volver a establecer la clave maestra de cifrado de software. Puede habilitar el cifrado de software en reposo cuando crea un clúster de almacenamiento. Cuando crea un clúster de almacenamiento SDS empresarial de SolidFire, el cifrado de software en reposo se habilita de forma predeterminada. Esta función cifra todos los datos almacenados en las unidades SSD de los nodos de almacenamiento y provoca que solo un impacto en el rendimiento de I/o del cliente muy pequeño (~2 %).

Los siguientes métodos API de Element están relacionados con el cifrado de software en reposo (consulte "Documentación de la API de Element" Para obtener detalles acerca de cada método de API):

- CreateCluster
- DisableEncryptionAtest

- EnableEncryptionAtest
- GetSoftwareEncryptionAtRestInfo
- RekeySoftwareEncryptionAtRestMasterKey

Actualizaciones del firmware del nodo de almacenamiento

Element 12.3 incluye actualizaciones de firmware para los nodos de almacenamiento. "Leer más".

Mejoras de seguridad

Element 12.3 resuelve las vulnerabilidades de seguridad de los nodos de almacenamiento y el nodo de gestión. "Leer más" acerca de estas mejoras de seguridad.

Comportamiento mejorado para unidades con fallos

Element 12.3 realiza comprobaciones periódicas del estado en las unidades del dispositivo SolidFire mediante datos INTELIGENTES de estado de las unidades. Una unidad que no supera la comprobación DEL estado INTELIGENTE puede estar cerca de un fallo. Si una unidad falla la comprobación DE estado INTELIGENTE, la unidad pasa al estado **con error** y aparece un error en el clúster de gravedad crítica: `Drive with serial: <serial number> in slot: <node slot><drive slot> has failed the SMART overall health check. To resolve this fault, replace the drive.`

Nueva compatibilidad de servidores en SolidFire Enterprise SDS

SolidFire eSDS ya está disponible en los servidores Dell R640. Consulte "Herramienta de matriz de interoperabilidad de NetApp (IMT)" para obtener más información sobre la configuración compatible.

Nueva ubicación para problemas conocidos de SolidFire eSDS

Ahora puede buscar problemas conocidos en "Herramienta bugs Online (se requiere inicio de sesión)".

Obtenga más información

- "Notas de la versión de los servicios de gestión y control del cloud híbrido de NetApp"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"
- "Documentación de SolidFire y el software Element"
- "Centro de documentación de SolidFire y el software Element para versiones anteriores"
- "Recursos de NetApp HCI"
- "Versiones de firmware de almacenamiento compatibles para los nodos de almacenamiento de SolidFire" *NEW*

Conceptos

Conozca los conceptos básicos relacionados con el software Element.

- "Información general del producto"
- Información general de la arquitectura de SolidFire
- Nodos
- De clúster
- "Seguridad"
- Cuentas y permisos
- "Volúmenes"
- Protección de datos
- Rendimiento y calidad del servicio

Obtenga más información

- "Información general sobre el almacenamiento all-flash de SolidFire"
- "Documentación de SolidFire y el software Element"

Información general del producto

Un sistema de almacenamiento all-flash de SolidFire consta de componentes de hardware diferenciados (unidad y nodos) que se combinan en un pool de recursos de almacenamiento único. Este clúster unificado se presenta como un único sistema de almacenamiento para que lo utilicen clientes externos y se gestiona con el software NetApp Element.

Mediante la interfaz de Element, la API u otras herramientas de gestión, puede supervisar el rendimiento y la capacidad de almacenamiento del clúster de SolidFire y gestionar la actividad de almacenamiento en una infraestructura multi-tenant.

Funciones de SolidFire

Un sistema SolidFire ofrece las siguientes funciones:

- Ofrece almacenamiento de alto rendimiento para su infraestructura de cloud privado a gran escala
- Ofrece una escala flexible que le permite satisfacer las cambiantes necesidades de almacenamiento
- Utiliza una interfaz de software Element de gestión de almacenamiento condicionada por la API
- Garantiza el rendimiento utilizando políticas de calidad de servicio
- Incluye equilibrio de carga automático en todos los nodos del clúster
- Los clústeres se reequilibran automáticamente cuando se agregan o se quitan nodos

Puesta en marcha de SolidFire

Utilice los nodos de almacenamiento que proporciona NetApp e integrados con el software NetApp Element.

"Información general de la arquitectura de almacenamiento all-flash de SolidFire"

Obtenga más información

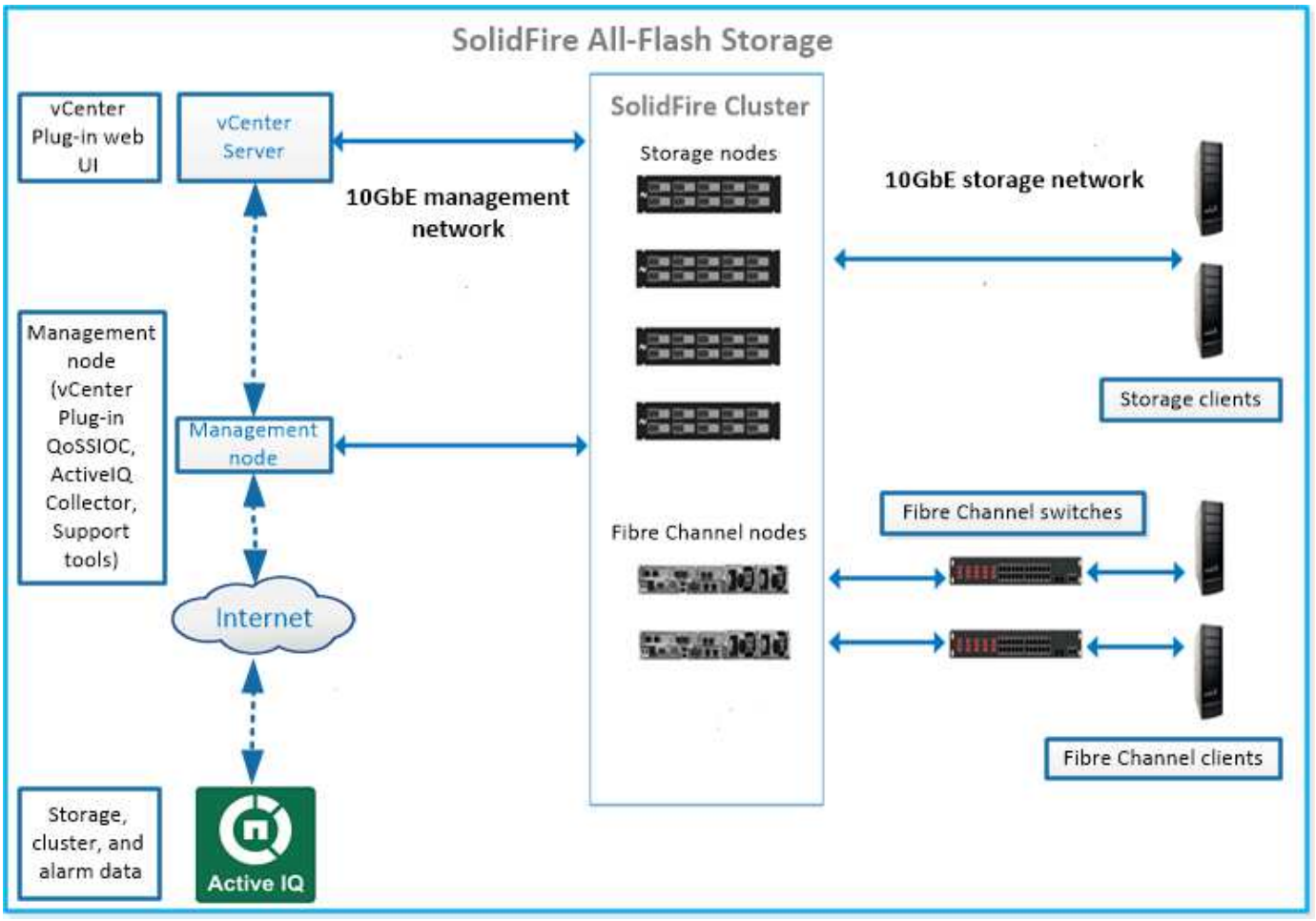
- "Información general sobre el almacenamiento all-flash de SolidFire"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Información general de la arquitectura de SolidFire

Un sistema de almacenamiento all-flash SolidFire consta de componentes de hardware diferenciados (unidad y nodos) que se combinan en un pool de recursos de almacenamiento con el software NetApp Element que se ejecuta de manera independiente en cada nodo. Este único sistema de almacenamiento se gestiona como una única entidad utilizando la interfaz de usuario del software Element, la API y otras herramientas de gestión.

Un sistema de almacenamiento SolidFire incluye los siguientes componentes de hardware:

- **Cluster**: El concentrador del sistema de almacenamiento SolidFire que es una colección de nodos.
- **Nodes**: Los componentes de hardware agrupados en un cluster. Existen dos tipos de nodos:
  - Nodos de almacenamiento, que son servidores que contienen una colección de unidades
  - Nodos Fibre Channel (FC), que se utilizan para conectarse a clientes FC
- **Drives**: Se utiliza en los nodos de almacenamiento para almacenar datos para el clúster. Un nodo de almacenamiento contiene dos tipos de unidades:
  - Las unidades de metadatos de volúmenes almacenan información que define los volúmenes y otros objetos dentro de un clúster.
  - Las unidades de bloques almacenan bloques de datos para los volúmenes.



Puede gestionar, supervisar y actualizar el sistema mediante la interfaz de usuario web de Element y otras herramientas compatibles:

- "Interfaces de software de SolidFire"
- "SolidFire Active IQ"
- "Nodo de gestión para el software Element"
- "Servicios de gestión"

Direcciones URL comunes

Estas son las URL comunes que utiliza con un sistema de almacenamiento all-flash de SolidFire:

URL	Descripción
`https://[storage cluster MVIP address]`	Acceda a la interfaz de usuario del software NetApp Element.
`https://activeiq.solidfire.com`	Supervise los datos y reciba alertas sobre los cuellos de botella de rendimiento o los problemas potenciales del sistema.
`https://[management node IP address]`	Acceda a Hybrid Cloud Control de NetApp para actualizar sus servicios de gestión de actualizaciones e instalación del almacenamiento.

URL	Descripción
`https://[IP address]:442`	Desde la interfaz de usuario por nodo, acceda a la configuración de red y clúster y utilice pruebas y utilidades del sistema. "Leer más."
`https://[management node IP address]/mnode`	Utilice la API DE REST de los servicios de gestión y otras funcionalidades desde el nodo de gestión."Leer más."
`https://[management node IP address]:9443`	Registre el paquete del plugin de vCenter en vSphere Web Client."Leer más."

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Interfaces de software de SolidFire

Puede gestionar un sistema de almacenamiento SolidFire mediante diferentes interfaces de software de NetApp Element y utilidades de integración.

Opciones

- Interfaz de usuario de software NetApp Element
- API de software NetApp Element
- Plugin de NetApp Element para vCenter Server
- Control del cloud híbrido de NetApp
- Las interfaces de usuario de los nodos de gestión
- Utilidades y herramientas de integración adicionales

Interfaz de usuario de software NetApp Element

Permite configurar el almacenamiento Element, supervisar la capacidad y el rendimiento del clúster y gestionar la actividad de almacenamiento en una infraestructura multi-tenant. Element es el sistema operativo de almacenamiento como pieza central de un clúster de SolidFire. El software Element se ejecuta de forma independiente en todos los nodos del clúster y permite que los nodos del clúster combinen los recursos que se presentan como un único sistema de almacenamiento a clientes externos. El software Element es responsable de toda la coordinación, escalado y gestión del clúster en su conjunto. La interfaz de software se creó sobre la API de Element.

"Gestionar el almacenamiento con el software Element"

API de software NetApp Element

Permite utilizar un conjunto de objetos, métodos y rutinas para gestionar el almacenamiento Element. La API de Element se basa en el protocolo JSON-RPC a través de HTTPS. Puede supervisar las operaciones de API en la interfaz de usuario de Element mediante la habilitación del registro de API, lo cual permite ver los métodos que se emiten al sistema. Puede activar tanto las solicitudes como las respuestas para ver cómo responde el sistema a los métodos que se emiten.

"Gestione el almacenamiento con la API de Element"

Plugin de NetApp Element para vCenter Server

Permite configurar y gestionar clústeres de almacenamiento que ejecutan el software Element mediante una interfaz alternativa para la interfaz de usuario de Element en VMware vSphere.

"Plugin de NetApp Element para vCenter Server"

Control del cloud híbrido de NetApp

Permite actualizar los servicios de gestión y almacenamiento de Element y gestionar los activos de almacenamiento mediante la interfaz de NetApp Hybrid Cloud Control.

"Gestione y supervise el almacenamiento con la información general de Hybrid Cloud Control de NetApp"

Las interfaces de usuario de los nodos de gestión

El nodo de gestión contiene dos interfaces de usuario: Una interfaz de usuario para gestionar los servicios basados en REST y una interfaz de usuario por nodo para gestionar la configuración de red y clúster, así como las pruebas y utilidades del sistema operativo. Desde la interfaz de usuario de la API DE REST, puede acceder a un menú de API relacionadas con el servicio que controlan las funcionalidades del sistema basadas en el servicio desde el nodo de gestión.

Utilidades y herramientas de integración adicionales

Si bien generalmente se gestiona el almacenamiento con NetApp Element, la API de NetApp Element y el plugin de NetApp Element para vCenter Server, puede usar utilidades y herramientas de integración adicionales para acceder al almacenamiento.

CLI de Element

"CLI de Element" Permite controlar un sistema de almacenamiento SolidFire mediante una interfaz de línea de comandos sin tener que utilizar la API de Element.

Herramientas de Element PowerShell

"Herramientas de Element PowerShell" Habilite usar una colección de funciones de Microsoft Windows PowerShell que utilizan la API de Element para gestionar un sistema de almacenamiento de SolidFire.

SDK de Element

"SDK de Element" Le permiten administrar el clúster de SolidFire mediante las siguientes herramientas:

- Element Java SDK: Permite a los programadores integrar la API de Element con el lenguaje de programación Java.
- Element .NET SDK: Permite a los programadores integrar la API de Element con la plataforma de programación .NET.
- Element Python SDK: Permite a los programadores integrar la API de elementos con el lenguaje de programación Python.

Suite de prueba de la API de SolidFire Postman

Permite a los programadores utilizar una colección de "Postman" Funciones que prueban las llamadas API de

Element.

Adaptador de replicación de almacenamiento de SolidFire

"Adaptador de replicación de almacenamiento de SolidFire" Se integra con VMware Site Recovery Manager (SRM) para permitir la comunicación con clústeres de almacenamiento de SolidFire replicados y ejecutar flujos de trabajo compatibles.

SolidFire Vro

"SolidFire Vro" Proporciona una forma cómoda de usar la API de Element para administrar su sistema de almacenamiento de SolidFire con VMware vRealize Orchestrator.

Proveedor VSS de SolidFire

"Proveedor VSS de SolidFire" Integra copias de sombra de VSS con copias de Snapshot de Element y clones.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

SolidFire Active IQ

"SolidFire Active IQ" es una herramienta web que proporciona vistas históricas actualizadas continuamente de los datos de todo el clúster. Es posible configurar alertas para eventos, umbrales o métricas específicos. SolidFire Active IQ le permite supervisar la capacidad y el rendimiento del sistema, así como mantenerse informado sobre el estado del clúster.

Puede encontrar la siguiente información sobre su sistema en SolidFire Active IQ:

- Número de nodos y estado de los nodos: En buen estado, sin conexión o fallo
- Representación gráfica de la CPU, el uso de memoria y la limitación de nodos
- Los detalles sobre el nodo, como el número de serie, la ubicación de la ranura en el chasis, el modelo y la versión del software NetApp Element que se ejecuta en el nodo de almacenamiento
- Información relacionada con la CPU y el almacenamiento sobre los equipos virtuales

Para obtener más información sobre SolidFire Active IQ, consulte "Documentación de SolidFire Active IQ".

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"
- "Herramientas del del sitio de soporte de NetApp para Active IQ"

Nodo de gestión para el software Element

La "Nodo de gestión (mNode)" Es una máquina virtual que se ejecuta en paralelo con uno o varios clústeres de almacenamiento basados en el software Element. Se utiliza

para actualizar y proporcionar servicios del sistema como supervisión y telemetría, gestionar activos y configuraciones del clúster, ejecutar pruebas y utilidades del sistema y habilitar el acceso al soporte de NetApp para la solución de problemas.

El nodo de gestión interactúa con un clúster de almacenamiento para realizar acciones de gestión, pero no es miembro del clúster de almacenamiento. Los nodos de gestión recopilan información periódicamente sobre el clúster a través de llamadas API e informan a Active IQ para la supervisión remota (si está habilitada). Los nodos de gestión también son responsables de coordinar las actualizaciones de software de los nodos del clúster.

A partir del lanzamiento de Element 11.3, el nodo de gestión funciona como host de microservicio, lo que permite actualizar más rápidamente los servicios de software seleccionados que no se incluyen en las principales versiones. Estos microservicios o. "servicios de gestión" se actualizan con frecuencia como paquetes de servicio.

Servicios de gestión para el almacenamiento all-flash de SolidFire

A partir de la versión Element 11.3, **servicios de administración** se alojan en el "nodo de gestión", permitiendo actualizaciones más rápidas de determinados servicios de software fuera de las versiones principales.

Los servicios de gestión proporcionan una funcionalidad de gestión centralizada y ampliada para el almacenamiento all-flash de SolidFire. Estos servicios incluyen "Control del cloud híbrido de NetApp", Telemetría del sistema de Active IQ, registro y actualizaciones de servicio, así como el servicio QoSSIOC para el plugin de Element para vCenter.

Más información acerca de "lanzamientos de servicios de gestión".

Nodos

Los nodos son recursos virtuales o de hardware que se agrupan en un clúster para proporcionar funcionalidades de computación y almacenamiento basado en bloques.

El software NetApp Element define varios roles de nodo para un clúster. Los tipos de roles de nodo son los siguientes:

- Nodo de gestión
- Nodo de almacenamiento
- Nodo Fibre Channel

estados de los nodos varía en función de la asociación del clúster.

Nodo de gestión

Un nodo de gestión es una máquina virtual que se usa para actualizar y proporcionar servicios del sistema, incluidos la supervisión y la telemetría, gestionar los activos y la configuración del clúster, ejecutar las pruebas y utilidades del sistema y habilitar el acceso al soporte de NetApp para la solución de problemas."Leer más"

Nodo de almacenamiento

Un nodo de almacenamiento SolidFire es un servidor que contiene una colección de unidades que se comunican entre sí a través de la interfaz de red Bond10G. Las unidades de cada nodo contienen espacio de bloques y metadatos para almacenar y gestionar los datos. Cada nodo contiene una imagen de fábrica de software NetApp Element.

Los nodos de almacenamiento tienen las siguientes características:

- Cada nodo tiene un nombre único. Si un administrador no especifica un nombre de nodo, se usa el predeterminado, SF-XXXX, donde XXXX representa cuatro caracteres aleatorios generados por el sistema.
- Cada nodo tiene su propia caché de escritura de alto rendimiento de memoria de acceso aleatorio no volátil (NVRAM) con la que se mejora el rendimiento general del sistema y se reduce la latencia de escritura.
- Cada nodo está conectado a dos redes, almacenamiento y gestión, cada una con dos enlaces independientes por motivos de redundancia y rendimiento. Cada nodo requiere una dirección IP en cada red.
- Es posible crear un clúster con nodos de almacenamiento nuevos o añadir nodos de almacenamiento a un clúster existente para aumentar el rendimiento y la capacidad del almacenamiento.
- En cualquier momento que desee, se pueden añadir nodos al clúster o quitarlos sin tener que interrumpir el servicio.

Nodo Fibre Channel

Los nodos Fibre Channel de SolidFire proporcionan conectividad a un switch Fibre Channel, que puede conectarse a clientes Fibre Channel. Los nodos Fibre Channel funcionan como un conversor de protocolo entre los protocolos de iSCSI y Fibre Channel. Esto permite añadir conectividad de Fibre Channel a un clúster de SolidFire nuevo o actual.

Los nodos Fibre Channel tienen las siguientes características:

- Los switches Fibre Channel gestionan el estado de la estructura para proporcionar interconexiones optimizadas.
- El tráfico entre dos puertos solo fluye por los switches; no se transmite a ningún otro puerto.
- Un error en un puerto es un hecho aislado y no afecta al funcionamiento de otros puertos.
- Varias parejas de puertos pueden comunicarse de forma simultánea en una estructura.

estados de funcionamiento del nodo

Un nodo se puede encontrar en alguno de varios estados en función del nivel de configuración.

- **Disponible**

  El nodo no tiene ningún nombre de clúster asociado y aún no forma parte de un clúster.

- **Pendiente**

  El nodo está configurado y se puede añadir a un clúster designado.

  No es necesario autenticarse para acceder al nodo.

- **Activo pendiente**

  El sistema está instalando el software Element compatible en el nodo. Cuando finalice, el nodo se moverá al estado Active.

- **Activo**

  El nodo participa en un clúster.

  Es necesario autenticarse para modificar el nodo.

En cada uno de estos estados, algunos campos son de solo lectura.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

De clúster

Un clúster es el concentrador de un sistema de almacenamiento SolidFire y se compone de una colección de nodos. Debe haber al menos cuatro nodos en un clúster para que se puedan aprovechar las eficiencias de almacenamiento de SolidFire. Un clúster aparece en la red como un grupo lógico y se puede acceder a él como almacenamiento basado en bloques.

La creación de un nuevo clúster inicializa un nodo como propietario de comunicaciones para un clúster y establece comunicaciones de red para cada nodo del clúster. Este proceso solo se realiza una vez por cada clúster nuevo. Un clúster se puede crear con la API o la interfaz de usuario de Element.

Un clúster se puede escalar horizontalmente si se añaden otros nodos. Cuando se añade un nodo nuevo, no se produce ninguna interrupción del servicio y el clúster utiliza automáticamente el rendimiento y la capacidad del nodo nuevo.

Los administradores y los hosts pueden acceder al clúster mediante las direcciones IP virtuales. Las direcciones IP virtuales se pueden alojar en cualquier nodo del clúster. La IP virtual de gestión (MVIP) permite administrar el clúster a través de una conexión de 1 GbE, mientras que la IP virtual de almacenamiento (SVIP) permite acceder al host para realizar tareas de almacenamiento a través de una conexión de 10 GbE. Estas direcciones IP virtuales permiten conexiones coherentes independientemente del tamaño o la composición de un clúster de SolidFire. Cuando un nodo que aloja una dirección IP virtual falla, otro nodo del clúster comienza a alojar la dirección IP virtual.

> A partir de la versión 11.0 de Element, los nodos se pueden configurar con IPv4, IPv6 o ambas direcciones para su red de gestión. Esto se aplica a los nodos de almacenamiento y de gestión, excepto el nodo de gestión 11.3 y una versión posterior que no admite IPv6. Cuando se crea un clúster, solo se puede usar una dirección IPv4 o IPv6 única para la dirección MVIP y el tipo de dirección correspondiente se debe configurar en todos los nodos.

Más sobre los clústeres

- Clústeres de almacenamiento autoritativos

- Regla de las terceras partes
- Capacidad desaprovechada
- Eficiencia del almacenamiento
- Quórum del clúster de almacenamiento

Clústeres de almacenamiento autoritativos

El clúster de almacenamiento autorizado es el clúster de almacenamiento que utiliza Hybrid Cloud Control de NetApp para autenticar usuarios.

Si su nodo de gestión solo tiene un clúster de almacenamiento, es el clúster autorizado. Si su nodo de gestión tiene dos o más clústeres de almacenamiento, uno de esos clústeres se asigna como un clúster autorizado y solo los usuarios de ese clúster pueden iniciar sesión en Hybrid Cloud Control de NetApp. Para averiguar qué clúster es el clúster autorizado, puede utilizar `GET /mnode/about` API. En la respuesta, la dirección IP de la `token_url` Field es la dirección IP virtual de gestión (MVIP) del clúster de almacenamiento autorizado. Si intenta iniciar sesión en NetApp Hybrid Cloud Control como usuario que no está en el clúster autorizado, el intento de inicio de sesión fallará.

Muchas funciones de control de cloud híbrido de NetApp están diseñadas para funcionar con varios clústeres de almacenamiento, pero la autenticación y la autorización tienen limitaciones. La limitación de la autenticación y la autorización consiste en que el usuario del clúster autorizado puede ejecutar acciones en otros clústeres vinculados a Hybrid Cloud Control de NetApp incluso si no son usuarios en otros clústeres de almacenamiento.

Antes de continuar con la gestión de varios clústeres de almacenamiento, debe asegurarse de que los usuarios definidos en los clústeres autorizados se hayan definido en todos los demás clústeres de almacenamiento con los mismos permisos. Puede gestionar usuarios desde "Interfaz de usuario del software Element".

Consulte "crear y gestionar activos de clúster de almacenamiento" para obtener más información sobre el trabajo con activos de clústeres de almacenamiento del nodo de gestión.

Regla de las terceras partes

Cuando se mezclan los tipos de nodo de almacenamiento en un clúster de almacenamiento SolidFire de NetApp, ningún nodo de almacenamiento puede contener más del 33 % de la capacidad total de clúster de almacenamiento.

Capacidad desaprovechada

Si un nodo que se acaba de añadir supone más del 50 % de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("trenzado"), de modo que cumpla con la regla de capacidad. Este sigue siendo el caso hasta que se añada más capacidad de almacenamiento. Si se añade un nodo muy grande que también desobedece la regla de capacidad, el nodo que antes se había abandonado ya no se quedará abandonado, mientras el nodo recién añadido se vuelve abandonado. La capacidad debe añadirse siempre por parejas para evitar que esto ocurra. Cuando un nodo se queda sin poner en cadena, se produce un error del clúster adecuado.

Eficiencia del almacenamiento

Los clústeres de almacenamiento SolidFire de NetApp utilizan la deduplicación, la compresión y el thin provisioning para reducir la cantidad de almacenamiento físico necesario para almacenar un volumen.

- **Compresión**

  La compresión reduce la cantidad de almacenamiento físico necesario en un volumen al combinar bloques de datos en grupos de compresión, cada uno de los cuales se almacena como un único bloque.

- **Deduplicación**

  La deduplicación reduce la cantidad de almacenamiento físico necesario en un volumen al eliminar los bloques de datos duplicados.

- **Thin Provisioning**

  Un volumen o LUN con thin provisioning es uno para el cual no se reserva almacenamiento por adelantado. En su lugar, el almacenamiento se asigna de forma dinámica conforme se necesita. El espacio libre se libera de nuevo al sistema de almacenamiento cuando se eliminan datos en el volumen o LUN

Quórum del clúster de almacenamiento

El software Element crea un clúster de almacenamiento a partir de los nodos seleccionados, que mantiene una base de datos replicada de la configuración de clúster. Se necesita un mínimo de tres nodos para participar en el conjunto de clústeres a fin de mantener el quórum para la resiliencia del clúster.

Seguridad

Al utilizar su sistema de almacenamiento all-flash SolidFire, sus datos están protegidos por protocolos de seguridad estándares del sector.

Cifrado en reposo (hardware)

Todas las unidades de los nodos de almacenamiento pueden cifrar AES de 256 bits a nivel de la unidad. Cada unidad tiene su propia clave de cifrado, que se crea cuando la unidad se inicializa por primera vez. Cuando habilita la función de cifrado, se crea una contraseña para todo el clúster y los fragmentos de la contraseña se distribuyen a todos los nodos del clúster. Ningún nodo almacena la contraseña completa. La contraseña se utiliza para proteger todo el acceso a las unidades. La contraseña se necesita para desbloquear la unidad y, a menos que se quite la alimentación de la unidad o que la unidad esté bloqueada.

"Habilitar la función de cifrado de hardware en reposo" no afecta al rendimiento o la eficiencia del clúster. Si un nodo o una unidad habilitados para el cifrado se quitan de la configuración del clúster con la API de Element o la interfaz de usuario de Element, se deshabilitará el cifrado en reposo en las unidades. Una vez que se quita la unidad, esta se puede borrar de forma segura mediante el `SecureEraseDrives` Método API. Si se elimina por la fuerza un nodo o una unidad física, los datos permanecen protegidos por la contraseña del clúster y las claves de cifrado individuales de la unidad.

Cifrado en reposo (software)

Otro tipo de cifrado en reposo, el cifrado por software en reposo permite cifrar todos los datos que se escriben en los SSD de un clúster de almacenamiento. "Si está habilitada", cifra todos los datos escritos y descifra todos los datos leídos automáticamente en el software. El cifrado por software en reposo refleja la implementación de la unidad de cifrado automático (SED) en el hardware para proporcionar seguridad de datos en ausencia de SED.

En los clústeres de almacenamiento all-flash de SolidFire, el cifrado del software en reposo debe habilitarse durante la creación del clúster y no se puede deshabilitar una vez que se ha creado el clúster.

Tanto el cifrado en reposo basado en software como en hardware pueden utilizarse de forma independiente o en combinación con uno al otro.

Gestión de claves externas

Es posible configurar el software Element para utilizar un servicio de gestión de claves (KMS) compatible con KMIP de terceros para gestionar las claves de cifrado de los clústeres de almacenamiento. Cuando habilita esta función, la clave de cifrado de contraseña de acceso a unidades para todo el clúster de almacenamiento se gestiona mediante un KMS que especifique.

Element puede usar los siguientes servicios de gestión de claves:

- SafeNet KeySecure de Gemalto
- SafeNet en KeySecure
- Control de claves HyTrust
- Administrador de seguridad de datos de VorMetric
- Administrador de ciclo de vida de claves de seguridad de IBM

Para obtener más información sobre la configuración de la gestión de claves externas, consulte "la puesta en marcha con la gestión de claves externas" documentación.

Autenticación de múltiples factores

La autenticación multifactor (MFA) permite requerir que los usuarios presenten múltiples tipos de pruebas para autenticar con la interfaz de usuario web de NetApp Element o la interfaz de usuario del nodo de almacenamiento después del inicio de sesión. Puede configurar el elemento para que acepte sólo la autenticación de múltiples factores para los inicios de sesión que se integran con el sistema de administración de usuarios y el proveedor de identidades existentes. Es posible configurar Element para que se integre con un proveedor de identidades SAML 2.0 existente que pueda aplicar múltiples esquemas de autenticación, como mensajes de texto y contraseña, mensajes de correo electrónico y contraseña, u otros métodos.

Puede emparejar la autenticación de múltiples factores con proveedores de identidades (PDI) compatibles con SAML 2.0 comunes, como Microsoft Active Directory Federation Services (ADFS) y Shibboleth.

Para configurar la MFA, consulte "la activación de la autenticación multifactor" documentación.

FIPS 140-2 para HTTPS y cifrado de datos en reposo

Los clústeres de almacenamiento SolidFire de NetApp admiten el cifrado, conforme a los requisitos del estándar de procesamiento de información federal (FIPS) 140-2 para módulos criptográficos. Es posible habilitar el cumplimiento de la normativa FIPS 140-2 en el clúster de SolidFire para las comunicaciones HTTPS y el cifrado de unidades.

Cuando habilita el modo operativo FIPS 140-2 en el clúster, el clúster activa el módulo de seguridad de criptografía de NetApp (NCSM) y utiliza el cifrado certificado FIPS 140-2 de nivel 1 para todas las comunicaciones a través de HTTPS a la interfaz de usuario y la API de NetApp Element. Utilice la `EnableFeature` La API de Element con la `fips` Para habilitar el cifrado HTTPS FIPS 140-2. En los clústeres de almacenamiento con hardware compatible con FIPS, también es posible habilitar el cifrado de unidades

FIPS para datos en reposo mediante el `EnableFeature` La API de Element con la `FipsDrives` parámetro.

Para obtener más información sobre cómo preparar un nuevo clúster de almacenamiento para el cifrado FIPS 140-2-2, consulte "Cree un clúster que admita unidades FIPS".

Para obtener más información sobre cómo habilitar FIPS 140-2 en un clúster existente y preparado, consulte "La API del elemento EnableFeature".

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Cuentas y permisos

Para administrar y proporcionar acceso a los recursos de almacenamiento del sistema, debe configurar cuentas para los recursos del sistema.

El almacenamiento de Element se puede crear y gestionar los siguientes tipos de cuentas:

- Cuentas de usuario de administrador para el clúster de almacenamiento de
- Las cuentas de usuario para acceder al volumen de almacenamiento
- Cuentas de usuario de clúster autorizadas sobre Hybrid Cloud Control de NetApp

Cuentas de administrador de clúster de almacenamiento

Existen dos tipos de cuentas de administrador que se pueden encontrar en un clúster de almacenamiento donde se ejecuta el software NetApp Element:

- **Cuenta de administrador del clúster principal**: Esta cuenta de administrador se crea cuando se crea el clúster. Es la cuenta administrativa principal con el nivel de acceso al clúster más alto. Esta cuenta es similar a un usuario raíz en un sistema Linux. Puede cambiar la contraseña de esta cuenta de administrador.
- **Cuenta de administrador de clúster**: Puede otorgar a una cuenta de administrador de clúster un rango limitado de acceso administrativo para realizar tareas específicas dentro de un clúster. Las credenciales que se asignan a cada cuenta de administrador de clúster sirven para autenticar las solicitudes de la API y la interfaz de usuario de Element dentro del sistema de almacenamiento.

Se necesita una cuenta de administrador de clúster local (que no sea LDAP) para acceder a los nodos activos en un clúster a través de la interfaz de usuario por nodo. No se necesitan credenciales de cuenta para acceder a un nodo que aún no forme parte de un clúster.

Puede hacerlo "gestione cuentas de administrador de clúster" Para crear, eliminar y editar cuentas de administrador de clúster, cambiar la contraseña de administrador de clúster y configurar los ajustes de LDAP para gestionar el acceso al sistema de los usuarios.

Cuentas de usuario

Las cuentas de usuario se utilizan para controlar el acceso a los recursos de almacenamiento en una red basada en software de NetApp Element. Se requiere al menos una cuenta de usuario para poder crear un volumen.

Cuando crea un volumen, este se asigna a una cuenta. Si creó un volumen virtual, la cuenta será el contenedor de almacenamiento.

A continuación, se indican algunas consideraciones adicionales:

- La cuenta contiene la autenticación CHAP que se necesita para acceder a los volúmenes que tiene asignados.
- Una cuenta puede tener hasta 2000 volúmenes asignados, pero un volumen solo puede pertenecer a una cuenta.
- Las cuentas de usuario se pueden gestionar desde el punto de extensión NetApp Element Management.

Cuentas de usuario de clúster autoritativas

Las cuentas de usuario de clúster autorizadas pueden autenticarse en cualquier activo de almacenamiento asociado con la instancia de Cloud Control de NetApp de los nodos y los clústeres. Con esta cuenta, puede gestionar volúmenes, cuentas, grupos de acceso y mucho más en todos los clústeres.

Las cuentas de usuario autorizadas se gestionan desde la opción de gestión de usuarios del menú superior derecho del control de cloud híbrido de NetApp.

La "clúster de almacenamiento fiable" Es el clúster de almacenamiento que utiliza el control del cloud híbrido de NetApp para autenticar usuarios.

Todos los usuarios que se creen en el clúster de almacenamiento autorizado pueden iniciar sesión en Hybrid Cloud Control de NetApp. Los usuarios creados en otros clústeres de almacenamiento *no se pueden* iniciar sesión en Hybrid Cloud Control.

- Si su nodo de gestión solo tiene un clúster de almacenamiento, es el clúster autorizado.
- Si su nodo de gestión tiene dos o más clústeres de almacenamiento, uno de esos clústeres se asigna como un clúster autorizado y solo los usuarios de ese clúster pueden iniciar sesión en Hybrid Cloud Control de NetApp.

Aunque muchas de las funciones de control de cloud híbrido de NetApp funcionan con varios clústeres de almacenamiento, la autenticación y la autorización tienen las limitaciones necesarias. La limitación de la autenticación y la autorización consiste en que los usuarios del clúster autorizado pueden ejecutar acciones en otros clústeres vinculados a Hybrid Cloud Control de NetApp incluso si no son usuarios en otros clústeres de almacenamiento. Antes de continuar con la gestión de varios clústeres de almacenamiento, debe asegurarse de que los usuarios definidos en los clústeres autorizados se hayan definido en todos los demás clústeres de almacenamiento con los mismos permisos. Puede gestionar usuarios desde NetApp Hybrid Cloud Control.

Cuentas de volumen

Las cuentas específicas de cada volumen solo son específicas del clúster de almacenamiento en el que se crearon. Estas cuentas permiten establecer permisos en volúmenes específicos de la red, pero no afectan fuera de dichos volúmenes.

Las cuentas de volumen se gestionan en la tabla volúmenes de control de cloud híbrido de NetApp.

Reducida

Volúmenes

El sistema de almacenamiento NetApp Element aprovisiona el almacenamiento mediante volúmenes. Los volúmenes son dispositivos de bloque a los que los clientes iSCSI o Fibre Channel acceden a través de la red.

El almacenamiento de Element permite crear, ver, editar, eliminar, clonar, realice backups o restaure volúmenes para cuentas de usuario. También es posible gestionar cada volumen en un clúster, así como añadir o quitar volúmenes en grupos de acceso de volúmenes.

Volúmenes persistentes

Los volúmenes persistentes permiten que los datos de configuración del nodo de gestión se almacenen en un clúster de almacenamiento especificado, en lugar de localmente con una máquina virtual, de modo que los datos se puedan conservar en caso de pérdida o eliminación del nodo de gestión. Los volúmenes persistentes son una configuración de nodos de gestión opcional pero recomendada.

Cuando se incluye una opción para habilitar volúmenes persistentes, se incluye en los scripts de instalación y actualización "implementar un nodo de gestión nuevo". Los volúmenes persistentes son volúmenes en un clúster de almacenamiento basado en software Element que contienen información de configuración del nodo de gestión para la máquina virtual del nodo de gestión de host que permanece más allá de la vida útil de la máquina virtual. Si se pierde el nodo de gestión, una máquina virtual del nodo de gestión de reemplazo puede volver a conectarse y recuperar los datos de configuración de la máquina virtual perdida.

La funcionalidad de volúmenes persistentes, si se habilita durante la instalación o la actualización, crea automáticamente varios volúmenes. Estos volúmenes, como cualquier volumen basado en el software Element, se pueden ver mediante la interfaz de usuario web del software Element, el plugin de NetApp Element para vCenter Server o la API, según sus preferencias e instalación. Los volúmenes persistentes deben estar activos y en ejecución con una conexión iSCSI al nodo de gestión para mantener los datos de configuración actuales que se pueden usar para la recuperación.

> Los volúmenes persistentes asociados con servicios de gestión se crean y se asignan a una nueva cuenta durante la instalación o la actualización. Si utiliza volúmenes persistentes, no modifique o elimine los volúmenes o su cuenta asociada

Volúmenes virtuales (vVols)

Los volúmenes virtuales de vSphere son un paradigma de almacenamiento para VMware que mueve gran parte de la gestión de almacenamiento de vSphere del sistema de almacenamiento a VMware vCenter. Con Virtual Volumes (vVols), puede asignar almacenamiento de acuerdo con los requisitos de cada equipo virtual.

Vinculaciones

El clúster de NetApp Element elige un extremo de protocolo adecuado, crea una vinculación que asocia el host ESXi y el volumen virtual con el extremo del protocolo, y devuelve la vinculación al host ESXi. Una vez enlazados, el host ESXi puede llevar a cabo operaciones de I/o con el volumen virtual vinculado.

Extremos de protocolo

Los hosts ESXi de VMware utilizan proxies lógicos de I/o, que se conocen como extremos de protocolo, para comunicarse con los volúmenes virtuales. Los hosts ESXi enlazan volúmenes virtuales con extremos de

protocolo para realizar operaciones de I/O. Cuando una máquina virtual en el host realiza una operación de I/o, el extremo de protocolo asociado dirige el I/o al volumen virtual con el que está enlazado.

Los extremos de protocolo de un clúster de NetApp Element funcionan como unidades lógicas administrativas SCSI. El clúster crea automáticamente cada extremo de protocolo. Para cada nodo de un clúster, se crea un extremo de protocolo correspondiente. Por ejemplo, un clúster de cuatro nodos tendrá cuatro extremos de protocolo.

ISCSI es el único protocolo compatible con el software NetApp Element. No se admite el protocolo Fibre Channel. Los usuarios no pueden eliminar ni modificar los extremos de protocolo. Tampoco se pueden asociar con una cuenta ni se pueden añadir a un grupo de acceso de volúmenes.

Contenedores de almacenamiento

Los contenedores de almacenamiento son construcciones lógicas que se asignan a cuentas de NetApp Element y se usan para crear informes y asignar recursos. Estos aprovechan la capacidad de almacenamiento sin configurar o añaden capacidades de almacenamiento que el sistema de almacenamiento puede ofrecer a los volúmenes virtuales. Un almacén de datos VVol que se crea en vSphere se asigna a un contenedor de almacenamiento individual. De forma predeterminada, un único contenedor de almacenamiento contiene todos los recursos disponibles del clúster de NetApp Element. Sin embargo, si se precisa una gestión granular para el multi-tenancy, se pueden crear varios contenedores.

Los contenedores de almacenamiento funcionan como cuentas tradicionales, y pueden contener volúmenes virtuales y volúmenes tradicionales a la vez. Se permite un máximo de cuatro contenedores de almacenamiento por clúster. Se requiere un mínimo de un contenedor de almacenamiento para habilitar la funcionalidad de VVol. Durante la creación de VVol, se pueden detectar contenedores de almacenamiento en vCenter.

Proveedor de VASA

Para que vSphere esté al tanto de la función VVol en el clúster de NetApp Element, el administrador de vSphere debe registrar el proveedor VASA de NetApp Element en vCenter. El proveedor de VASA es la ruta de control fuera de banda entre vSphere y el clúster de Element. Es responsable de ejecutar solicitudes en el clúster de Element en nombre de vSphere, como la creación de máquinas virtuales, la puesta a disposición de vSphere de máquinas virtuales y la publicidad de funcionalidades de almacenamiento para vSphere.

El proveedor de VASA se ejecuta como parte del maestro de clústeres en el software Element. El maestro de clústeres es un servicio de alta disponibilidad que se conmuta por error a cualquier nodo del clúster según sea necesario. Si el maestro del clúster se conmuta al nodo de respaldo, el proveedor de VASA se mueve con él, garantizando que el proveedor de VASA tiene una alta disponibilidad. Todas las tareas de aprovisionamiento y gestión de almacenamiento utilizan el proveedor VASA, que gestiona los cambios necesarios en el clúster de Element.

> No se deben registrar más de un proveedor de VASA de NetApp Element en una sola instancia de vCenter. Cuando se añade un segundo proveedor de VASA NetApp Element, esto hace que no se pueda acceder a todos los almacenes de datos DE VVOL.

> La compatibilidad CON VASA de hasta 10 vCenter está disponible como revisión de actualización si ya se registró un proveedor de VASA en el para vCenter. Para instalar, siga las instrucciones del manifiesto VASA39 y descargue el archivo .tar.gz desde el "Descargas de software de NetApp" sitio. El proveedor VASA de NetApp Element utiliza un certificado de NetApp. Con este parche, vCenter utiliza el certificado sin modificar para admitir varias instancias de vCenter para que usen VASA y VVol. No modifique el certificado. VASA no admite los certificados SSL personalizados.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Los grupos de acceso de volúmenes

Mediante la creación y el uso de grupos de acceso de volúmenes, se puede controlar el acceso a un conjunto de volúmenes. Cuando se asocia un conjunto de volúmenes y un conjunto de iniciadores a un grupo de acceso de volúmenes, el grupo de acceso otorga a esos iniciadores acceso al conjunto de volúmenes.

Los grupos de acceso de volúmenes del almacenamiento SolidFire de NetApp permiten que los IQN de iniciadores de iSCSI o WWPN de Fibre Channel accedan a una colección de volúmenes. Cada IQN que se añade a un grupo de acceso puede acceder a cada volumen del grupo sin utilizar autenticación CHAP. Cada WWPN que se añade a un grupo de acceso habilita el acceso a la red de Fibre Channel a los volúmenes del grupo de acceso.

Los grupos de acceso de volúmenes presentan los siguientes límites:

- Un máximo de 128 iniciadores por grupo de acceso de volúmenes.
- Un máximo de 64 grupos de acceso por volumen.
- Un grupo de acceso puede estar formado por un máximo de 2000 volúmenes.
- Un IQN o un WWPN solo pueden pertenecer a un grupo de acceso de volúmenes.
- Para los clústeres Fibre Channel, un solo volumen puede pertenecer a hasta cuatro grupos de acceso.

Iniciadores

Los iniciadores permiten que los clientes externos accedan a los volúmenes de un clúster. Se utilizan como el punto de entrada de la comunicación entre clientes y volúmenes. Es posible usar iniciadores para el acceso basado en CHAP en lugar de acceso basado en la cuenta a los volúmenes de almacenamiento. Cuando se añade un iniciador único a un grupo de acceso de volúmenes, permite que los miembros del grupo de acceso de volúmenes accedan a todos los volúmenes de almacenamiento añadidos al grupo sin necesidad de autenticación. Un iniciador solo puede pertenecer a un grupo de acceso.

Protección de datos

Las funcionalidades de protección de datos incluyen replicación remota, snapshots de volúmenes, clonado de volúmenes, Protection Domains y alta disponibilidad con la tecnología Double Helix.

La protección de datos de almacenamiento de Element incluye los siguientes conceptos:

- Tipos de replicación remota
- Snapshots de volumen para proteger los datos

- Clones de volúmenes
- Información general del proceso de backup y restauración para el almacenamiento Element
- Dominios de protección
- Dominios de protección personalizados
- Alta disponibilidad de Double Helix

Tipos de replicación remota

La replicación remota de datos puede adoptar las siguientes formas:

- Replicación síncrona y asíncrona entre clústeres
- Replicación solo de Snapshot
- Replicación entre clústeres de Element y ONTAP mediante SnapMirror

Para obtener más información, consulte "TR-4741: Replicación remota del software NetApp Element".

Replicación síncrona y asíncrona entre clústeres

En los clústeres que ejecutan el software NetApp Element, la replicación en tiempo real permite la creación rápida de copias remotas de datos de volumen.

Un clúster de almacenamiento se puede emparejar con hasta otros cuatro clústeres de almacenamiento. Es posible replicar datos de volúmenes de forma síncrona o asíncrona desde un clúster de una pareja de clústeres para escenarios de conmutación por error y conmutación tras recuperación.

Replicación síncrona

La replicación síncrona replica continuamente datos del clúster de origen al clúster de destino y se ve afectada por la latencia, la pérdida de paquetes, la fluctuación y el ancho de banda.

La replicación síncrona es adecuada para las siguientes situaciones:

- Replicación de varios sistemas a corta distancia
- Sitio de recuperación ante desastres que sea geográficamente local en el origen
- Las aplicaciones más urgentes y la protección de las bases de datos
- Aplicaciones de continuidad del negocio que requieren que el sitio secundario actúe como el sitio principal cuando el sitio principal esté inactivo

Replicación asíncrona

La replicación asíncrona replica continuamente datos de un clúster de origen a un clúster de destino sin esperar los reconocimientos del clúster de destino. Durante la replicación asíncrona, las escrituras se reconocen en el cliente (aplicación) después de que se aplican en el clúster de origen.

La replicación asíncrona es apropiada para las siguientes situaciones:

- El sitio de recuperación ante desastres está lejos del origen y la aplicación no tolera latencias inducidas por la red.
- La red que conecta los clústeres de origen y destino tiene limitaciones de ancho de banda.

Replicación solo de Snapshot

La protección de datos con Snapshot replica los datos modificados en momentos específicos a un clúster remoto. Solo se replican las copias de Snapshot que se crean en el clúster de origen. No se producen las escrituras activas del volumen de origen.

Puede establecer la frecuencia de las replicaciones de snapshots.

La replicación Snapshot no afecta a la replicación asíncrona o síncrona.

Replicación entre clústeres de Element y ONTAP mediante SnapMirror

Con la tecnología SnapMirror de NetApp, puede replicar copias snapshot realizadas mediante el software NetApp Element en ONTAP con fines de recuperación ante desastres. En una relación de SnapMirror, Element es un extremo y ONTAP es el otro.

SnapMirror es la tecnología de replicación Snapshot de NetApp que facilita la recuperación ante desastres, diseñada para la conmutación por error del almacenamiento principal al almacenamiento secundario en un centro geográficamente remoto. La tecnología SnapMirror crea una réplica, o réplica, de los datos del trabajo en almacenamiento secundario desde el cual puede seguir proporcionando datos si se produce una interrupción del servicio en el sitio principal. Los datos se reflejan en el nivel de volumen.

La relación entre el volumen de origen en el almacenamiento primario y el volumen de destino en el almacenamiento secundario se denomina relación de protección de datos. Los clústeres se denominan extremos en los que residen los volúmenes y los volúmenes que contienen los datos replicados deben tener una relación entre iguales. Una relación entre iguales permite que clústeres y volúmenes intercambien datos de forma segura.

SnapMirror se ejecuta de forma nativa en las controladoras ONTAP de NetApp y está integrado en Element, que se ejecuta en clústeres de NetApp HCI y SolidFire. La lógica para controlar SnapMirror reside en el software ONTAP; por tanto, todas las relaciones de SnapMirror deben implicar al menos un sistema ONTAP para realizar las tareas de coordinación. Los usuarios gestionan las relaciones entre los clústeres de Element y ONTAP principalmente mediante la interfaz de usuario de Element; no obstante, algunas tareas de gestión residen en ONTAP System Manager de NetApp. Los usuarios también pueden gestionar SnapMirror mediante la CLI y la API, que están disponibles en ONTAP y Element.

Consulte "TR-4651: Arquitectura y configuración de SnapMirror para SolidFire de NetApp" (se requiere inicio de sesión)

Es necesario habilitar manualmente la funcionalidad SnapMirror en el nivel de clúster mediante el software Element. La funcionalidad SnapMirror está deshabilitada de forma predeterminada y no se habilita automáticamente como parte de una nueva instalación o actualización.

Después de habilitar SnapMirror, es posible crear relaciones de SnapMirror desde la pestaña Data Protection del software Element.

El software NetApp Element 10.1 y versiones posteriores admite la funcionalidad de SnapMirror para copiar y restaurar copias Snapshot con sistemas ONTAP.

Los sistemas que ejecutan Element 10.1 y versiones posteriores incluyen el código que puede comunicarse directamente con SnapMirror en sistemas ONTAP que ejecutan 9.3 o posterior. La API de Element proporciona métodos para habilitar la funcionalidad de SnapMirror en clústeres, volúmenes y copias de Snapshot. Además, la interfaz de usuario de Element incluye la funcionalidad para gestionar las relaciones de SnapMirror entre el software Element y los sistemas ONTAP.

A partir de los sistemas Element 10.3 y ONTAP 9.4, es posible replicar volúmenes originados por ONTAP en volúmenes de Element en casos de uso específicos con funcionalidad limitada.

Para obtener más información, consulte la documentación de ONTAP.

Snapshots de volumen para proteger los datos

Una copia de Snapshot de volumen es una copia de un momento específico de un volumen que se puede utilizar más adelante para restaurar un volumen a ese momento específico.

Aunque las copias de Snapshot son similares a los clones de volúmenes, las copias de Snapshot son réplicas de los metadatos del volumen, por lo que no se pueden montar ni escribir en ellas. Además, para crear una copia de Snapshot de volumen, solo se requiere una pequeña cantidad de espacio y recursos del sistema, lo cual es más rápido crear una copia de Snapshot que clonar.

Las snapshots se pueden replicar en un clúster de remoto y usarlas como copia de backup del volumen. Gracias a ello, es posible revertir un volumen a un momento específico mediante la copia de Snapshot replicada, así como crear un clon de un volumen a partir de esta copia de Snapshot replicada.

Es posible realizar backups de copias de Snapshot de un clúster de Element en un almacén de objetos externo o en otro clúster de Element. Cuando se crea un backup de una copia de Snapshot en un almacén de objetos externo, debe haber una conexión con el almacén de objetos que permita realizar operaciones de lectura y escritura.

Es posible realizar una copia Snapshot de un volumen individual o varias para la protección de datos.

Clones de volúmenes

Un clon de un solo volumen o de varios volúmenes es una copia puntual de los datos. Cuando se clona un volumen, el sistema crea una copia de Snapshot del volumen y, a continuación, crea una copia de los datos que se indican en la copia de Snapshot.

Este es un proceso asíncrono, y la cantidad de tiempo que requiere el proceso depende del tamaño del volumen que se clona y de la carga del clúster actual.

El clúster admite hasta dos solicitudes de clones en ejecución por volumen a la vez y hasta ocho operaciones de clones de volúmenes activos a la vez. Las solicitudes que superen este límite se pondrán en cola para procesarlas más adelante.

Información general del proceso de backup y restauración para el almacenamiento Element

Es posible realizar backups y restaurar volúmenes en otro almacenamiento de SolidFire, así como en almacenes de objetos secundarios que sean compatibles con OpenStack Swift o Amazon S3.

Es posible realizar un backup de un volumen en los siguientes casos:

- Un clúster de almacenamiento de SolidFire
- Un almacén de objetos Amazon S3
- Un almacén de objetos OpenStack Swift

Cuando se restauran volúmenes desde OpenStack Swift o Amazon S3, se necesita información de manifiesto desde el proceso de backup original. Si desea restaurar un volumen de del cual se había realizado un backup en un sistema de almacenamiento de SolidFire, no será necesaria ninguna información de manifiesto.

Dominios de protección

Un dominio de protección es un nodo o un conjunto de nodos agrupados, de modo que cualquier parte o incluso todos fallen, al tiempo que se mantiene la disponibilidad de los datos. Los dominios de protección permiten que un clúster de almacenamiento se repare automáticamente de la pérdida de un chasis (afinidad de chasis) o de todo un dominio (grupo de chasis).

Es posible habilitar manualmente la supervisión de dominios de protección mediante el punto de extensión NetApp Element Configuration en el plugin de NetApp Element para vCenter Server. Puede seleccionar un umbral para Protection Domain a partir de dominios de nodo o de chasis. También es posible habilitar la supervisión de Protection Domain mediante la API o la interfaz de usuario web de Element.

Un diseño de Protection Domain asigna cada nodo a un dominio de protección específico.

Se admiten dos diseños diferentes de Protection Domain, denominados niveles de Protection Domain.

- En el nivel de nodo, cada nodo está en su propio dominio de protección.
- En el nivel del chasis, solo los nodos que comparten un chasis se encuentran en el mismo dominio de protección.
  - La distribución del nivel de chasis se determina automáticamente desde el hardware cuando el nodo se añade al clúster.
  - En un clúster en el que cada nodo se encuentra en un chasis independiente, estos dos niveles son funcionalmente idénticos.

Cuando crea un clúster nuevo, si utiliza nodos de almacenamiento que residen en un chasis compartido, puede que desee considerar diseñar la protección contra fallos en el nivel del chasis mediante la función Protection Domains.

Dominios de protección personalizados

Puede definir un diseño personalizado de Protection Domain que coincida con el diseño de nodo y chasis específicos, y donde cada nodo está asociado a un y solo un dominio de protección personalizado. De manera predeterminada, cada nodo se asigna al mismo dominio de protección personalizado predeterminado.

Si no se asignan dominios de protección personalizados:

- El funcionamiento del clúster no se ve afectado.
- El nivel personalizado no es tolerante ni resiliente.

Cuando se configuran los dominios de protección personalizados de un clúster, se pueden ver tres niveles posibles de protección en la consola de la interfaz de usuario web de Element:

- No protegido: El clúster de almacenamiento no está protegido ante el fallo de uno de sus dominios de protección personalizados. Para solucionarlo, añada más capacidad de almacenamiento al clúster o vuelva a configurar los dominios de protección personalizados del clúster para proteger el clúster de una posible pérdida de datos.
- Tolerancia a fallos: El clúster de almacenamiento tiene suficiente capacidad libre para evitar la pérdida de datos tras el fallo de uno de sus dominios de protección personalizados.
- Fault resiliente: El clúster de almacenamiento tiene suficiente capacidad libre para recuperarse tras el fallo de uno de sus dominios de protección personalizados. Una vez completado el proceso de reparación, el clúster se protegerá de la pérdida de datos si otros dominios fallan.

Si se asigna más de un dominio de protección personalizado, cada subsistema asignará duplicados a dominios de protección personalizados separados. Si esto no es posible, se revierte a la asignación de duplicados a nodos separados. Cada subsistema (por ejemplo, bandejas, segmentos, proveedores de extremo de protocolo y conjunto) realiza esto de forma independiente.

Puede configurar dominios de protección personalizados mediante los siguientes métodos API:

- "GetProtectionDomainLayout" - Muestra en qué chasis y en qué dominio de protección personalizado se encuentra cada nodo.
- "SetProtectionDomainLayout" - Permite asignar un dominio de protección personalizado a cada nodo.

Alta disponibilidad de Double Helix

La protección de datos de Double Helix es un método de replicación que expande al menos dos copias de datos redundantes en todas las unidades de un sistema. El enfoque “sin RAID” permite que un sistema absorba múltiples fallos simultáneos en todos los niveles del sistema de almacenamiento y los repare rápidamente.

Rendimiento y calidad del servicio

Un clúster de almacenamiento de SolidFire puede proporcionar parámetros de calidad de servicio (QoS) por volumen. Puede garantizar el rendimiento del clúster medido en entradas y salidas por segundo (IOPS) utilizando tres parámetros configurables que definen la calidad de servicio: Min IOPS, Max IOPS y Burst IOPS.

SolidFire Active IQ tiene una página de recomendaciones de calidad de servicio que ofrece asesoramiento sobre la configuración óptima y la configuración de las opciones de calidad de servicio.

Parámetros de calidad de servicio

Los parámetros de IOPS se definen de las siguientes formas:

- **Mínimo de IOPS**: El número mínimo de entradas y salidas sostenidas por segundo (IOPS) que el clúster de almacenamiento proporciona a un volumen. El valor de Min IOPS configurado para un volumen es el nivel garantizado de rendimiento de un volumen. El rendimiento nunca es inferior a este nivel.
- **Maximum IOPS**: El número máximo de IOPS sostenidas que el clúster de almacenamiento proporciona a un volumen. Cuando los niveles de IOPS del clúster son extremadamente altos, este nivel de rendimiento de IOPS nunca se supera.
- **Burst IOPS**: El número máximo de IOPS permitidas en un escenario de ráfaga breve. Si un volumen se ejecuta por debajo del valor Max IOPS, se acumulan créditos de ráfaga. Cuando los niveles de rendimiento llegan a ser muy altos e incluso alcanzan los niveles máximos, se permiten ráfagas breves de IOPS en el volumen.

  El software Element usa Burst IOPS cuando un clúster se ejecuta en un estado de bajo uso de IOPS de clúster.

  Un solo volumen puede acumular Burst IOPS y usar los créditos para superar su Max IOPS en ráfagas hasta su nivel de Burst IOPS durante un "período de ráfaga" establecido. Un volumen puede usar ráfagas durante hasta 60 segundos si el clúster tiene la capacidad de acomodar la ráfaga. Un volumen acumula un segundo de crédito de ráfaga (hasta un máximo de 60 segundos) por cada segundo que se ejecuta el

volumen por debajo de su límite de Max IOPS.

Burst IOPS se limita de dos formas:

- Un volumen puede usar ráfagas por encima de su Max IOPS durante un número de segundos que sea igual al número de créditos de ráfaga que ha acumulado el volumen.
- Cuando un volumen usa ráfagas por encima de su configuración de Max IOPS, estará limitado por su valor de Burst IOPS. Por ello, la IOPS de ráfaga nunca supera el valor de Burst IOPS del volumen.

- **Ancho de banda máximo efectivo**: El ancho de banda máximo se calcula multiplicando el número de IOPS (en función de la curva QoS) por el tamaño de E/S.

  Ejemplo: Una configuración del parámetro de calidad de servicio de 100 Min IOPS, 1000 Max IOPS y 1500 Burst IOPS afectan a la calidad del rendimiento de la siguiente manera:

  - Las cargas de trabajo pueden alcanzar y sostener un máximo de 1000 IOPS hasta que la condición de contención de carga de trabajo de IOPS se hace evidente en el clúster. Las IOPS se reducen de forma incremental hasta que las IOPS de todos los volúmenes estén dentro de los rangos de calidad de servicio designados y la contención para el rendimiento mejore.
  - El rendimiento de todos los volúmenes se empuja hasta el valor de Min IOPS de 100. Los niveles no se sitúan por debajo del valor de Min IOPS, pero podrían ser superiores a los 100 IOPS cuando la contención de carga de trabajo mejora.
  - El rendimiento nunca supera las 1000 IOPS ni es inferior a 100 IOPS durante un período sostenido. Se permite el rendimiento de 1500 IOPS (Burst IOPS), pero solo para esos volúmenes que hayan acumulado créditos de ráfaga al ejecutarse por debajo del valor de Max IOPS y solo se permite durante breves periodos de tiempo. Los niveles de ráfaga nunca son sostenidos.

Límites de valor de calidad de servicio

Estos son los posibles valores mínimos y máximos de la calidad de servicio.

Parámetros	Valor mínimo	Predeterminado	4 4 KB	5 8 KB	6 16 KB	262 KB
IOPS mín	50	50	15,000	9,375*	5556*	385*
Tasa máx. De IOPS	100	15,000	200,000**	125,000	74,074	5128
IOPS de ráfaga	100	15,000	200,000**	125,000	74.074	5128

*Estas estimaciones son aproximadas. **Max IOPS y Burst IOPS se pueden establecer con un valor máximo de 200,000 000; sin embargo, este valor solo se permite para destapar de forma efectiva el rendimiento de un volumen. El rendimiento máximo en el mundo real de un volumen está limitado por el uso del clúster y el rendimiento por cada nodo.

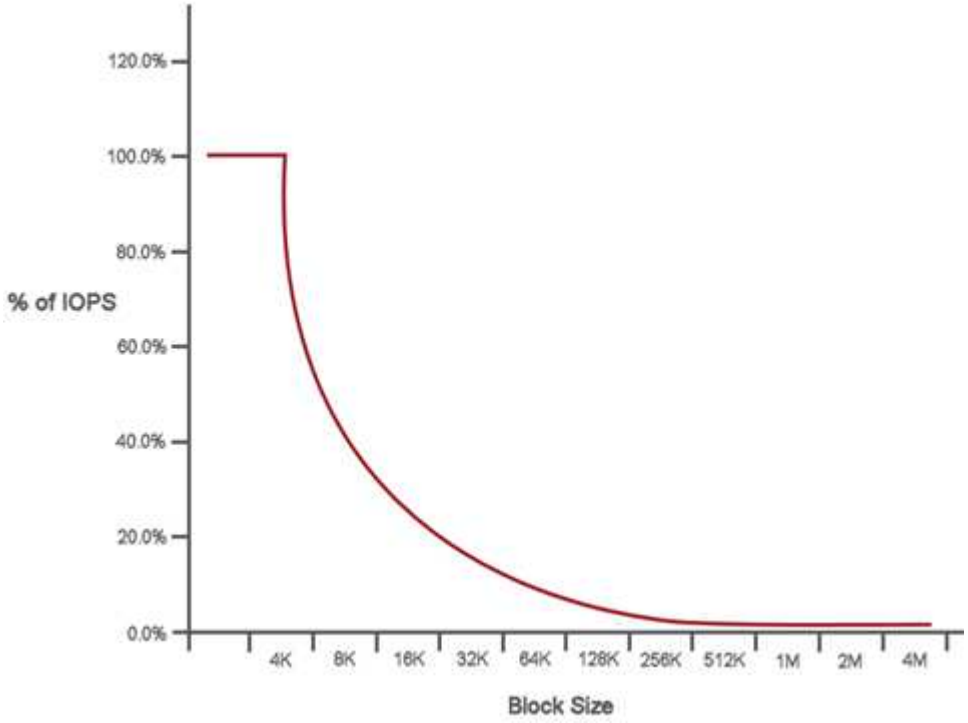
Rendimiento de la calidad de servicio

La curva de rendimiento de calidad de servicio muestra la relación entre el tamaño de bloque y el porcentaje de IOPS.

El tamaño de bloque y el ancho de banda repercuten directamente en el número de IOPS que puede obtener una aplicación. El software Element toma en cuenta los tamaños de bloque que recibe definiendo de forma

general el tamaño de los bloques en 4k. En función de la carga de trabajo, el sistema podría aumentar los tamaños de bloque. A medida que estos aumenten, el sistema aumentará el ancho de banda hasta el nivel que necesite para procesar los tamaños de bloque más grandes. A medida que aumenta el ancho de banda, se reduce el número de IOPS que el sistema es capaz de conseguir.

La curva de rendimiento de calidad de servicio muestra la relación entre el aumento de los tamaños de bloque y el porcentaje de IOPS en disminución:



A modo de ejemplo, si el tamaño de los bloques es de 4k y el ancho de banda es de 4000 kbps, la IOPS será de 1000. Si el tamaño de los bloques aumenta hasta 8k, el ancho de banda aumentará también hasta los 5000 kbps y la IOPS se reducirá hasta 625. Al tener en cuenta el tamaño de bloque, el sistema garantiza que las cargas de trabajo con prioridad más baja que utilizan tamaños de bloque más altos, como backups y actividades del hipervisor, no necesiten demasiado del rendimiento que necesita el tráfico de mayor prioridad utilizando tamaños de bloque más pequeños.

Políticas de calidad de servicio

Una política de calidad de servicio permite crear y guardar un ajuste de calidad de servicio estandarizado que se puede aplicar a muchos volúmenes.

Las políticas de calidad de servicio son mejores para los entornos de servicio, por ejemplo, con servidores de bases de datos, aplicaciones o infraestructuras que rara vez se reinician y necesitan igual acceso constante al almacenamiento. La calidad de servicio de un volumen individual es la mejor opción para equipos virtuales de uso reducido, como escritorios virtuales o equipos virtuales especializados de tipo quiosco, que pueden reiniciarse, encenderse o apagarse a diario o varias veces al día.

Las políticas de calidad de servicio y calidad de servicio no se deben utilizar juntas. Si utiliza políticas de calidad de servicio, no use la calidad de servicio personalizada en un volumen. La calidad de servicio personalizada anulará y ajustará los valores de las políticas de calidad de servicio de los volúmenes.

El clúster seleccionado debe ser Element 10.0 o posterior para usar políticas de calidad de servicio; de lo contrario, las funciones de las políticas de calidad de servicio no estarán disponibles.

Obtenga más información

- "Documentación de SolidFire y el software Element"

Requisitos

Antes de empezar, debe revisar los requisitos previos para implementar el software NetApp Element, incluidos los requisitos de red y puerto.

- "Requisitos de red"
- "Configuración de switches"
- "Requisitos de puerto de red"

Obtenga más información

- "Documentación de SolidFire y el software Element"

Redes

La configuración de red para un sistema SolidFire consta de requisitos de switch y puerto. La implementación de estos depende de su sistema.

Si quiere más información

- "Configuración de switches para los clústeres que ejecutan el software Element"
- "Requisitos de puerto de red"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Configuración de switches para los clústeres que ejecutan el software Element

El sistema de software NetApp Element tiene ciertos requisitos de switch y prácticas recomendadas para un rendimiento óptimo del almacenamiento.

Los nodos de almacenamiento requieren switches Ethernet de 10 GbE o 25GbE, en función del hardware de nodos específicos para la comunicación de los servicios de almacenamiento iSCSI y los servicios de nodo dentro del clúster. Los switches de 1 GbE se pueden usar para estos tipos de tráfico:

- Gestión del clúster y los nodos
- Tráfico de gestión dentro del clúster entre los nodos
- Tráfico entre los nodos del clúster y la máquina virtual del nodo de gestión

Práctica recomendada: debe implementar las siguientes prácticas recomendadas al configurar los conmutadores Ethernet para el tráfico de clúster:

- Para el tráfico que no sea de almacenamiento en el clúster, implemente un par de switches de 1 GbE para proporcionar alta disponibilidad y uso compartido de la carga.
- En los switches de red de almacenamiento, implemente switches en parejas y configure y utilice tramas gigantes (un tamaño de MTU de 9216 bytes). Esto garantiza una instalación correcta y elimina los errores de red de almacenamiento debidos a paquetes fragmentados.

La implementación de Element requiere al menos dos segmentos de red, uno para cada tipo de tráfico siguiente:

- Gestión
- Almacenamiento/datos

Según los modelos de nodos de almacenamiento de NetApp H-Series y la configuración de cableado planificada, estas redes se pueden separar mediante switches distintos, o bien mediante VLAN. Para la mayoría de las implementaciones, sin embargo, es necesario separar lógicamente estas redes mediante VLAN.

Los nodos de almacenamiento deben poder comunicarse antes, durante y después de la implementación.

Si va a implementar redes de gestión independientes para los nodos de almacenamiento, asegúrese de que estas redes de gestión tengan rutas de red entre ellas. Estas redes deben tener puertas de enlace asignadas, y debe existir una ruta entre las puertas de enlace. Asegúrese de que cada nodo nuevo tenga asignada una puerta de enlace para facilitar la comunicación entre nodos y redes de gestión.

NetApp Element requiere lo siguiente:

- Todos los puertos de switch conectados a los nodos de almacenamiento H-Series de NetApp deben configurarse como puertos periféricos de árbol de expansión.
  - En los switches Cisco, en función del modelo del switch, la versión del software y el tipo de puerto, puede hacerlo con uno de los siguientes comandos:
    - `spanning-tree port type edge`
    - `spanning-tree port type edge trunk`
    - `spanning-tree portfast`
    - `spanning-tree portfast trunk`
  - En los switches Mellanox, puede hacerlo con `spanning-tree port type edge` comando.
- Los switches que controlan el tráfico de almacenamiento deben admitir velocidades de al menos 10 GbE por puerto (se admiten hasta 25 GbE por puerto).
- Los switches que controlan el tráfico de gestión deben admitir velocidades de al menos 1 GbE por puerto.
- Debe configurar tramas gigantes en los puertos del switch que controla el tráfico de almacenamiento. Los hosts deben poder enviar paquetes de 9000 bytes de extremo a extremo para una instalación correcta.
- La latencia de red de ida y vuelta entre todos los nodos de almacenamiento no debe exceder los 2 ms.

Algunos nodos proporcionan funcionalidades de gestión fuera de banda adicionales a través de un puerto de gestión dedicado. Los nodos NetApp H300S, H500S y H700S también permiten el acceso IPMI a través del

puerto A. Como práctica recomendada, debe facilitar la gestión remota mediante la configuración de la gestión fuera de banda para todos los nodos del entorno.

Si quiere más información

- "Requisitos de switch y red de NetApp HCI"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Requisitos de puerto de red

Es posible que tenga que permitir a los siguientes puertos TCP y UDP atravesar el firewall perimetral del centro de datos, de manera que pueda gestionar el sistema de forma remota y permitir a los clientes que estén fuera del centro de datos conectarse a los recursos. En función de la manera en la que se use el sistema, es posible que algunos puertos no sean necesarios.

Todos los puertos son TCP a menos que se especifique lo contrario, y todos los puertos TCP deben admitir la comunicación de apretón de manos tripartito entre el servidor de soporte de NetApp, el nodo de gestión y los nodos que ejecutan el software Element. Por ejemplo, el host de un origen del nodo de gestión se comunica con el host en un destino de MVIP del clúster de almacenamiento a través del puerto TCP 443, y el host de destino se vuelve a comunicar al host de origen a través de cualquier puerto.

Habilite ICMP entre el nodo de gestión, los nodos que ejecutan el software Element y la MVIP del clúster.

En la tabla se emplean las siguientes abreviaturas:

- MIP: Dirección IP de gestión, una dirección por nodo
- SIP: Dirección IP de almacenamiento, una dirección por nodo
- MVIP: Dirección IP virtual de gestión
- SVIP: Dirección IP virtual de almacenamiento

Origen	Destino	Puerto	Descripción
Clientes iSCSI	MVIP de clúster de almacenamiento	443	Acceso de interfaz de usuario y API (opcional)
Clientes iSCSI	SVIP de clúster de almacenamiento	3260	Comunicaciones de cliente iSCSI
Clientes iSCSI	SIP de nodo de almacenamiento	3260	Comunicaciones de cliente iSCSI
Nodo de gestión	`sfsupport.solidfire.com`	22	Túnel SSH inverso para acceso al soporte

Origen	Destino	Puerto	Descripción
Nodo de gestión	MIP de nodo de almacenamiento	22	Acceso SSH para soporte
Nodo de gestión	Servidores DNS	53 TCP/UDP	Búsqueda de DNS
Nodo de gestión	MIP de nodo de almacenamiento	442	Acceso de interfaz de usuario y de API al nodo de almacenamiento y actualizaciones del software Element
Nodo de gestión	MVIP de clúster de almacenamiento	442	Acceso de interfaz de usuario y de API al nodo de almacenamiento y actualizaciones del software Element
Nodo de gestión	`monitoring.solidfire.com`	443	Informes del clúster de almacenamiento a Active IQ
Nodo de gestión	MVIP de clúster de almacenamiento	443	Acceso de interfaz de usuario y de API al nodo de almacenamiento y actualizaciones del software Element
Nodo de gestión	repo.netapp.com	443	Proporciona acceso a los componentes necesarios para instalar/actualizar la puesta en marcha en las instalaciones.
Nodo de gestión	BMC/IPMI de nodo de almacenamiento	623 UDP	Puerto RMCP. Esto es necesario para gestionar los sistemas habilitados para IPMI.
Nodo de gestión	Nodo de testimonio	9442	Servicio API de configuración por nodo
Nodo de gestión	VCenter Server	9443	Registro del plugin de vCenter; El puerto se puede cerrar una vez que se completa el registro.
Servidor SNMP	MVIP de clúster de almacenamiento	161 UDP	Sondeo de SNMP
Servidor SNMP	MIP de nodo de almacenamiento	161 UDP	Sondeo de SNMP
BMC/IPMI de nodo de almacenamiento	Nodo de gestión	623 UDP	Puerto RMCP. Esto es necesario para gestionar los sistemas habilitados para IPMI.
MIP de nodo de almacenamiento	Servidores DNS	53 TCP/UDP	Búsqueda de DNS

Origen	Destino	Puerto	Descripción
MIP de nodo de almacenamiento	Nodo de gestión	80	Actualizaciones del software Element
MIP de nodo de almacenamiento	Extremo de S3/Swift	80	Comunicación HTTP con el extremo de S3/Swift para backup y recuperación (opcional)
MIP de nodo de almacenamiento	Servidor NTP	123 UDP	NTP
MIP de nodo de almacenamiento	Nodo de gestión	162 UDP	(Opcional) capturas SNMP
MIP de nodo de almacenamiento	Servidor SNMP	162 UDP	(Opcional) capturas SNMP
MIP de nodo de almacenamiento	Servidor LDAP	389 TCP/UDP	Búsqueda de LDAP (opcional)
MIP de nodo de almacenamiento	Nodo de gestión	443	Actualizaciones del firmware de almacenamiento Element
MIP de nodo de almacenamiento	MVIP de clúster de almacenamiento remoto	443	Comunicación de emparejamiento de clústeres de replicación remota
MIP de nodo de almacenamiento	MIP de nodo de almacenamiento remoto	443	Comunicación de emparejamiento de clústeres de replicación remota
MIP de nodo de almacenamiento	Extremo de S3/Swift	443	Comunicación HTTPS con el extremo de S3/Swift para backup y recuperación (opcional)
MIP de nodo de almacenamiento	Nodo de gestión	514 TCP/UDP 10514 TCP/UDP	Reenvío de syslog
MIP de nodo de almacenamiento	Servidor de syslog	514 TCP/UDP 10514 TCP/UDP	Reenvío de syslog
MIP de nodo de almacenamiento	Servidor LDAPS	636 TCP/UDP	Búsqueda LDAPS

Origen	Destino	Puerto	Descripción
MIP de nodo de almacenamiento	MIP de nodo de almacenamiento remoto	2181	Comunicación entre clústeres para replicación remota
SIP de nodo de almacenamiento	SIP de nodo de almacenamiento remoto	2181	Comunicación entre clústeres para replicación remota
SIP de nodo de almacenamiento	SIP de nodo de almacenamiento	3260	ISCSI entre nodos
SIP de nodo de almacenamiento	SIP de nodo de almacenamiento remoto	4000 hasta 4020	Transferencia de datos nodo a nodo con replicación remota
PC del administrador de sistemas	Nodo de gestión	442	Acceso de interfaz de usuario de HTTPS a nodo de gestión
PC del administrador de sistemas	MIP de nodo de almacenamiento	442	Acceso de API e interfaz de usuario de HTTPS a nodo de almacenamiento
PC del administrador de sistemas	Nodo de gestión	443	Acceso HTTPS de interfaz de usuario y API al nodo de gestión
PC del administrador de sistemas	MVIP de clúster de almacenamiento	443	Acceso de API e interfaz de usuario de HTTPS a clúster de almacenamiento
PC del administrador de sistemas	Controlador de gestión en placa base del nodo de almacenamiento (BMC)/interfaz de gestión de plataforma inteligente (IPMI) serie H410 y H600	443	Acceso de API e interfaz de usuario de HTTPS a control remoto de nodos
PC del administrador de sistemas	MIP de nodo de almacenamiento	443	Creación de clúster de almacenamiento de HTTPS, acceso de interfaz de usuario al clúster de almacenamiento posterior a la implementación
PC del administrador de sistemas	Nodos de almacenamiento series BMC/IPMI H410 y H600	623 UDP	Puerto del protocolo de control de gestión remota. Esto es necesario para gestionar los sistemas habilitados para IPMI.
PC del administrador de sistemas	Nodo de testimonio	8080	Interfaz de usuario web de un nodo de testigos por nodo

Origen	Destino	Puerto	Descripción
VCenter Server	MVIP de clúster de almacenamiento	443	Acceso de API de plugin de vCenter
VCenter Server	Plugin remoto	8333	Servicio de complemento de vCenter remoto
VCenter Server	Nodo de gestión	8443	Servicio QoSSIOC del plugin de vCenter (opcional);
VCenter Server	MVIP de clúster de almacenamiento	8444	Acceso del proveedor VASA de vCenter (solo VVol)
VCenter Server	Nodo de gestión	9443	Registro del plugin de vCenter; El puerto se puede cerrar una vez que se completa el registro.

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Pruébelo

Obtenga información sobre recursos y herramientas para ayudar a comenzar a usar el software Element.

- "Flexibilidad del almacenamiento de Lab on Demand para el cloud privado con Element (se requiere inicio de sesión)": Este laboratorio presenta conceptos de escalado horizontal sin limitaciones, rendimiento garantizado de la carga de trabajo y automatización de la infraestructura de almacenamiento que se aplican a los sistemas de almacenamiento que ejecutan el software Element.
- "Pruebe las funciones de almacenamiento usando Element Demo Node": El nodo de demostración de Element es una versión de máquina virtual VMware del software Element, que proporciona una forma fácil de mostrar muchas de las características de almacenamiento clave de los productos NetApp HCI y SolidFire.

Obtenga más información

- "Documentación de SolidFire y el software Element"

Pruebe las funciones de almacenamiento usando Element Demo Node

"Nodo de demostración de Element" Es una versión de máquina virtual (VM) de VMware del software Element, que permite mostrar fácilmente muchas de las funciones de almacenamiento clave de los productos NetApp HCI y SolidFire. El nodo de demostración permite a los desarrolladores codificar la API de Element sin necesidad de contar con hardware físico. Se presenta como un archivo OVA para facilitar la puesta en marcha de VMware.

Funcionalidad compatible:

El nodo de demostración de Element sólo está diseñado para usarse como herramienta de demostración y desarrollo. Tenga en cuenta las siguientes limitaciones funcionales antes de utilizar el nodo de demostración:

- El nodo de demostración de Element no admite la agrupación en clústeres. Funciona solo como un clúster de un solo nodo.
- No admite actualizaciones de elementos. Para realizar una demostración posterior de Element, debe instalar una nueva máquina virtual del nodo de demostración.
- No pretende demostrar el rendimiento del almacenamiento. El rendimiento observado en el nodo de demostración no refleja de ningún modo el rendimiento en los clústeres físicos.
- No se pueden añadir nodos de demostración a clústeres de NetApp HCI o SolidFire.
- Las VLAN de VRF no son compatibles (se admiten las VLAN etiquetadas estándar).
- No se admite el servicio de segmentos de varias unidades (MDSS).
- El nodo de demostración de Element solo se admite con almacenes de datos VMFS. No se admiten VVol.
- La funcionalidad de supervisión y configuración basadas en hardware no funciona con el nodo de demostración.

- Admite un máximo de 10 copias Snapshot por volumen.
- Es compatible con un máximo de 20 cuentas por nodo/clúster.
- Admite un máximo de 100 volúmenes por cuenta.
- Soporta un máximo de 200 vVols por cuenta.
- Admite un tamaño de volumen máximo de 100 GIB.
- Admite un límite sostenido de 3000 000 IOPS.

Se aplican todas las demás limitaciones del software Element. Consulte las notas de la versión del software Element más reciente para obtener detalles.

Requisitos de equipos virtuales

- 240 GB de capacidad total (el tamaño y la cantidad de discos virtuales de la máquina virtual no se pueden cambiar. El sistema operativo invitado ignora cualquier almacenamiento adicional presentado a través del hipervisor).
- Disco raíz de 60 GB
- Thick provisioned/Eager Zeroed (una unidad de metadatos de 30 GB o tres unidades de bloque de 50 GB) o thin provisioning/Eager (**recomendado**) (una unidad de metadatos de 30 GB o tres unidades de bloque de 50 GB)
- Dos vCPU (totalmente reservado)
- 16 GB de RAM (totalmente reservado)
- HBA único para todos los discos, LSI Logic paralelo
- Dos NIC, tanto vmxnet3 (una gestión, un almacenamiento)

Requisitos del host

- ESXI 6.0 o 6.5 para el nodo de demostración de Element 11.7 VM
- ESXi 6.5 para los nodos de demostración de Element de 12.0 y 12.2
- ESXi 6.7 y 7.0 para el nodo de demostración de Element 12.3 VM
- Arquitectura Intel® multi-core de 64 bits

Descargue el nodo de demostración de Element

El software Element Demo Node es un conjunto de archivos de VMware que se empaquetaron en un archivo .ova.

Instale el nodo de demostración de Element en VMware ESXi

La instalación del nodo de demostración de Element en VMware ESXi implica las siguientes tareas:

- Configure las interfaces de red
- Registre el nodo de demostración en un servidor ESXi
- Inicie el nodo de demostración en un servidor ESXi

Configure las interfaces de red

El nodo de demostración de Element requiere dos redes de máquina virtual separadas. Una es para el tráfico de almacenamiento y la otra para el tráfico de gestión. Debe configurar la red de almacenamiento para que admita las tramas gigantes.

Registre el nodo de demostración en un servidor ESXi

Para registrar el nodo de demostración de Element en un servidor ESXi, debe implementar el archivo .ova del nodo de demostración mediante vSphere Client.

Pasos

1. Inicie sesión en vSphere Client y seleccione el host ESXi en el panel Inventory.
2. Seleccione **Archivo** > **despliegue de la plantilla OVF**.

   Se inicia el Asistente para implementar plantilla OVF.

3. En la página **Seleccionar plantilla**, busque el archivo OVA que ha descargado y seleccione **Abrir**.
4. Seleccione **Siguiente**.
5. En la página **Nombre y ubicación**, especifique un nombre y una ubicación para la plantilla desplegada y, a continuación, seleccione **Siguiente**.
6. En la página **Seleccionar un recurso**, busque la ubicación en la que desea ejecutar la plantilla y seleccione **Siguiente**.
7. Compruebe los detalles y seleccione **Siguiente**.
8. En la página Select Storage (Seleccionar almacenamiento), seleccione dónde desea almacenar los archivos de la máquina virtual y, a continuación, seleccione **Next** (Siguiente).
9. En la página **Seleccionar redes**, asigne la red utilizada en el archivo OVA a las dos redes de máquinas virtuales separadas del inventario y seleccione **Siguiente**.
10. En la página **preparado para completar**, compruebe los detalles de la máquina virtual que está creando y, a continuación, seleccione **Finalizar**.

> Es posible que la puesta en marcha del nodo de demostración demore unos minutos en completarse.

Inicie el nodo de demostración en un servidor ESXi

Debe iniciar la máquina virtual del nodo de demostración para acceder a Element mediante la consola de VMware ESXi.

Pasos

1. En vSphere Client, seleccione la máquina virtual del nodo de demostración que creó.
2. Seleccione la ficha **Resumen** para ver los detalles de este equipo virtual.
3. Seleccione **encendido** para iniciar la VM.
4. Seleccione **Iniciar Web Console**.
5. Con la TUI, configure el nodo de demostración. Para obtener más información, consulte "Configure un nodo de almacenamiento".

Cómo obtener soporte

El nodo de demostración de Element está disponible para voluntariado con el mejor esfuerzo. Para obtener soporte, envíe sus preguntas al "Foro de nodos de demostración de Element".

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Página de descarga del nodo de demostración de Element (se requiere inicio de sesión)"

Instale y mantenga el hardware

Conozca la instalación y el mantenimiento de hardware H-Series y SF-Series.

- Información de hardware H410S y H610S
- Información sobre hardware de SF-Series
- Vuelva a la información de la imagen de fábrica

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Información de hardware H410S y H610S

Encontrará información sobre la instalación y el mantenimiento de los nodos de almacenamiento H-Series.

A continuación encontrará los enlaces al contenido de instalación y mantenimiento:

- "Instale los nodos de almacenamiento H-Series"
- "Sustituya un nodo H410S"
- "Sustituya un nodo H610S"
- "Sustituya las unidades"
- "Sustituya una unidad de fuente de alimentación"

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Instale los nodos de almacenamiento H-Series

Antes de empezar a utilizar su sistema de almacenamiento all-flash, debe instalar y configurar los nodos de almacenamiento correctamente.

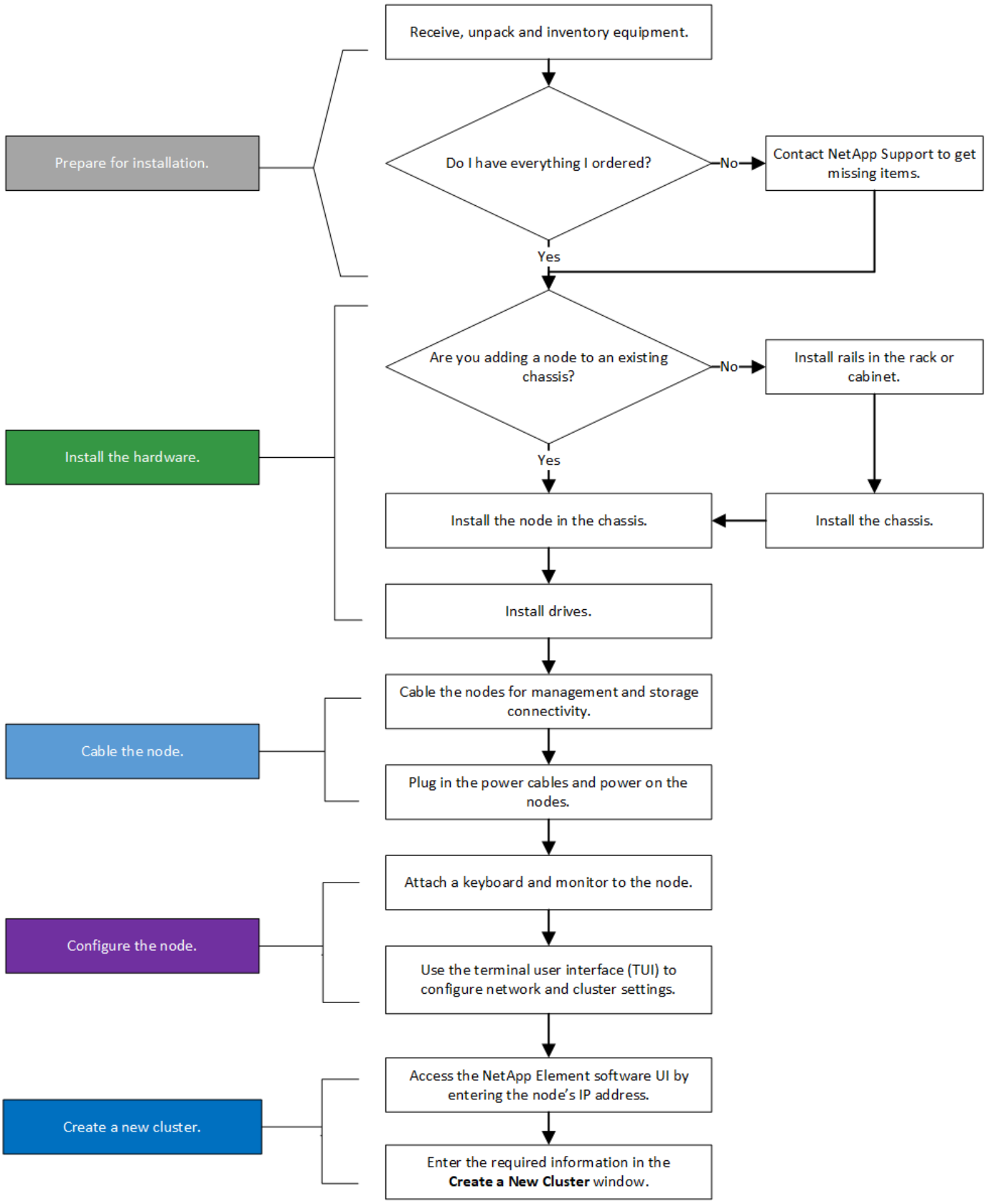
Consulte "cartel" para una representación visual de las instrucciones.

- Diagramas de flujo de trabajo
- Preparación de la instalación
- Instale los rieles
- Instale los nodos y cablee
- Configure los nodos
- Cree un clúster

Diagramas de flujo de trabajo

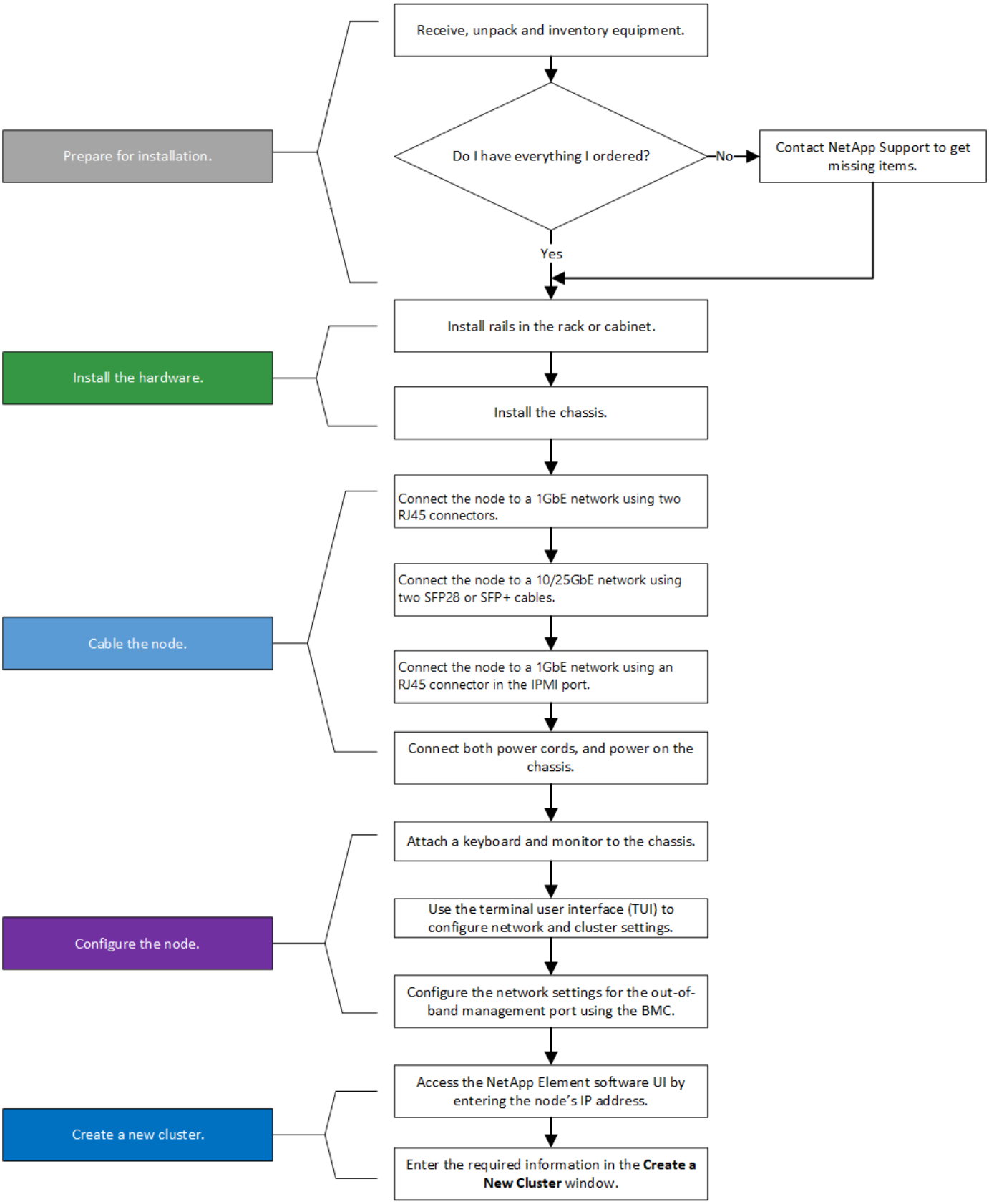
Los diagramas de flujo de trabajo aquí proporcionan una descripción general de alto nivel de los pasos de la instalación. Los pasos varían ligeramente según el modelo de la serie H.

H410S


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

H610S

Los términos "nodo" y "chasis" se usan indistintamente en el caso de H610S, ya que el nodo y el chasis no son componentes separados a diferencia de lo que sucede en el caso de un chasis 2U de cuatro nodos.



Preparación de la instalación

Durante la preparación para la instalación, realice el inventario del hardware que recibió y póngase en contacto con el soporte de NetApp en caso de que falte algún artículo.

Asegúrese de tener los siguientes elementos en su ubicación de instalación:

- Espacio en rack para el sistema.

Tipo de nodo	Espacio de rack
Nodos H410S	Dos unidades de rack (2U)
Nodos H610S	Una unidad de rack (1U)

- Cables o transceptores de conexión directa SFP28/SFP+
- Cables CAT5e o superiores con conector RJ45
- Un switch de teclado, vídeo y ratón (KVM) para configurar el sistema
- Stick USB (opcional)

El hardware que se le envía depende de lo que realice su pedido. Un nuevo pedido de 2U de cuatro nodos incluye el chasis, el panel frontal, el kit de rieles deslizantes, unidades, nodos de almacenamiento, y los cables de alimentación (dos por chasis). Si solicita nodos de almacenamiento H610S, las unidades se instalan en el chasis.

Durante la instalación de la tornillería, asegúrese de retirar todo el material de embalaje y el embalaje de la unidad. Esto evitará que los nodos se sobrecalienten y se apaguen.

Instale los rieles

El orden de hardware que se le envió incluye un conjunto de rieles deslizantes. Necesitará un destornillador para completar la instalación del riel. Los pasos de instalación varían ligeramente para cada modelo de nodo.

Instale la tornillería desde la parte inferior del bastidor hasta la parte superior para evitar que el equipo se caiga. Si el rack incluye dispositivos estabilizadores, instálelos antes de instalar el hardware.

- H410S
- H610S

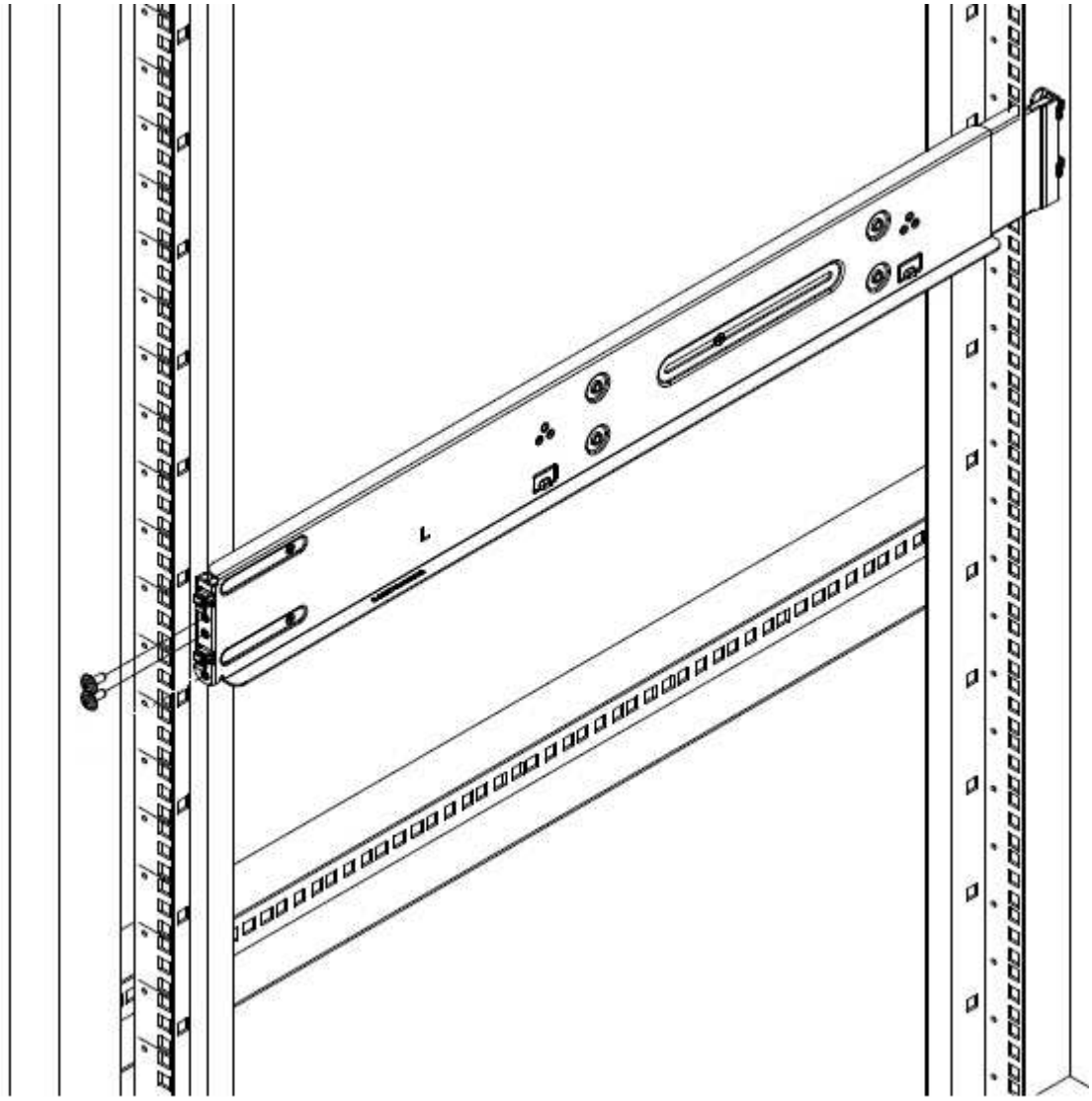
H410S

Los nodos H410S se instalan en chasis 2U de cuatro nodos H-Series, que se envía con dos conjuntos de adaptadores. Si desea instalar el chasis en un rack con orificios redondos, utilice los adaptadores adecuados para un rack con orificios redondos. Los rieles para nodos H410S colocan un rack de entre 29 pulgadas y 33.5 pulgadas de profundidad. Cuando el riel está totalmente contrapuesto, tiene 28 pulgadas de largo, y las secciones delantera y trasera del riel se mantienen Unidas sólo con un tornillo.

Si instala el chasis en un riel totalmente contratado, es posible que las secciones delantera y trasera del riel se separen.

Pasos

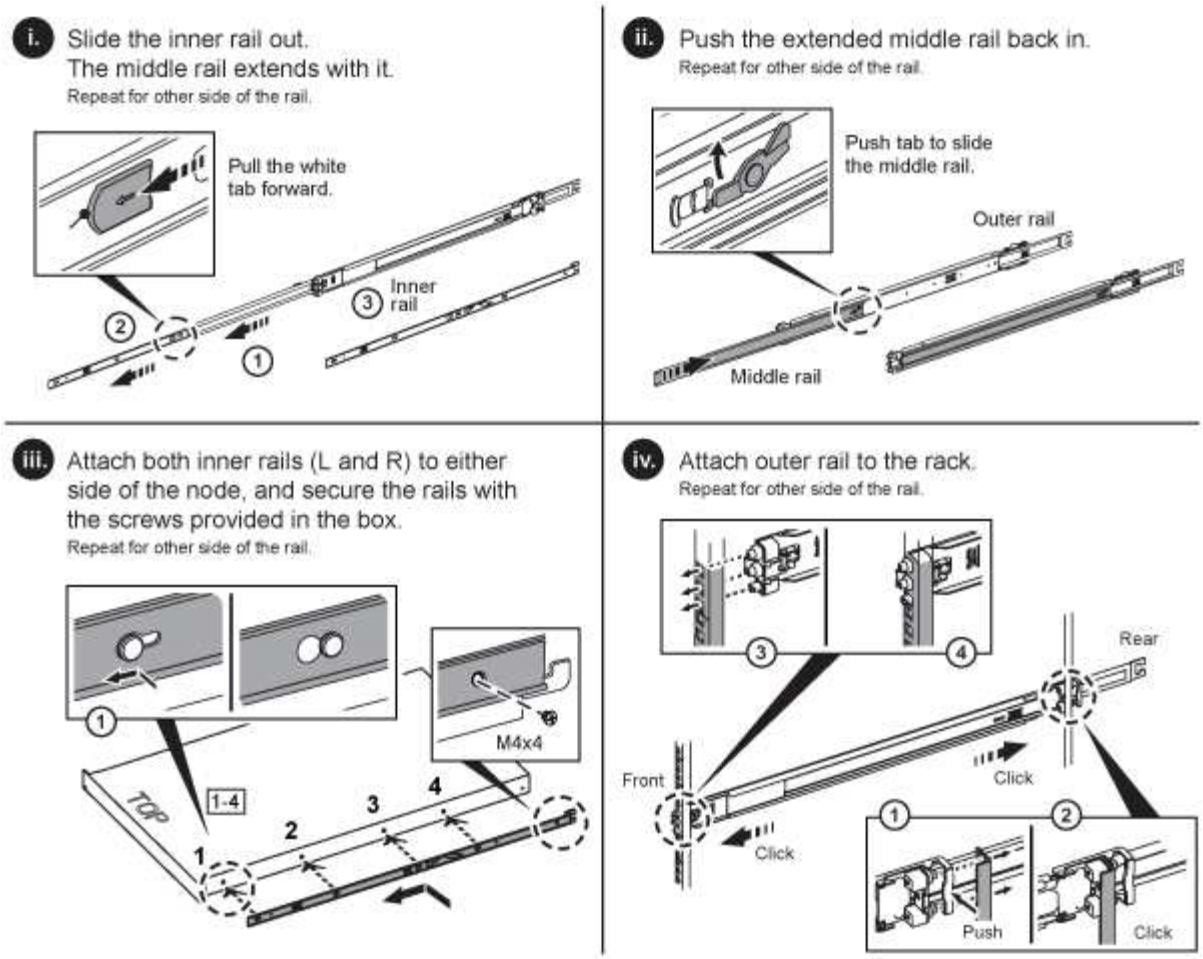
1. Alinee la parte frontal del raíl con los orificios del poste delantero del rack.
2. Empuje los ganchos de la parte frontal del raíl hacia los orificios del poste delantero del rack y, a continuación, hacia abajo hasta que las clavijas cargadas por resorte encajen en los orificios del rack.
3. Fije el riel al rack con tornillos. A continuación, se muestra una ilustración del raíl izquierdo conectado a la parte frontal del rack:



4. Extienda la sección trasera del raíl al poste trasero del bastidor.
5. Alinee los ganchos de la parte trasera del raíl con los orificios adecuados del poste trasero, asegurándose de que la parte delantera y posterior del raíl estén al mismo nivel.
6. Monte la parte posterior del raíl en el rack y fije el riel con tornillos.
7. Realice todos los pasos anteriores para el otro lado del rack.

H610S

A continuación encontrará una ilustración de la instalación de rieles para un nodo de almacenamiento H610S:



Hay rieles izquierdo y derecho en la H610S. Coloque el orificio roscado hacia la parte inferior de manera que el tornillo de mariposa H610S pueda fijar el chasis al raíl.

Instale los nodos y cablee

Debe instalar el nodo de almacenamiento H410S en un chasis 2U de cuatro nodos. Para H610S, instale el chasis/nodo directamente en los rieles del rack.

Retire todo el material de embalaje y el embalaje de la unidad. Esto evita que los nodos se sobrecalienten y se apaguen.

- H410S
- H610S

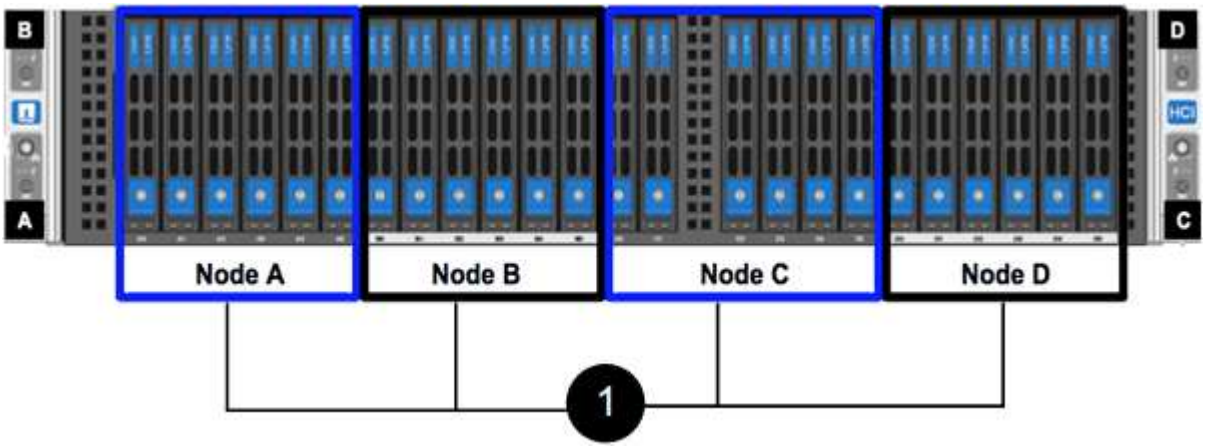
H410S

Pasos

1. Instale los nodos H410S en el chasis. A continuación, se muestra un ejemplo de vista posterior de un chasis con cuatro nodos instalados:

Sea cauteloso al levantar el hardware e instalarlo en el rack. Un chasis vacío de dos unidades en rack (2U) de cuatro nodos pesa 54.45 lb (24.7 kg) y un nodo pesa 8.0 lb (3.6 kg).

2. Instale las unidades.



3. Cablee los nodos.

Si la apertura de flujo de aire de la parte trasera del chasis está bloqueada con cables o etiquetas, puede provocar fallos prematuros en los componentes debido al sobrecalentamiento.

   - Conecte dos cables CAT5e o superiores en los puertos A y B para conectividad de gestión.
   - Conecte dos cables o transceptores SFP28/SFP+ en los puertos C y D para conectividad de almacenamiento.
   - (Opcional, recomendado) Conecte un cableCAT5e en el puerto IPMI para conectividad de gestión fuera de banda.

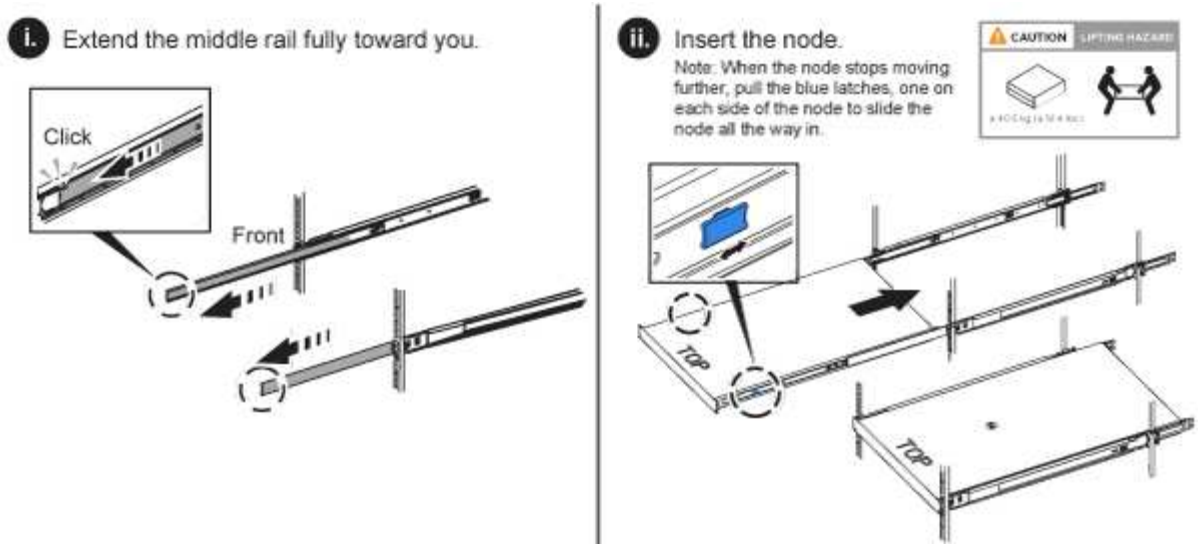
4. Conecte los cables de alimentación a las dos unidades de suministro de alimentación por chasis y enchúfelos en un PDU o tomacorriente de 240 V.
5. Encienda los nodos.

El nodo tarda aproximadamente seis minutos en arrancar.

H610S

Pasos

1. Instale el chasis H610S. A continuación se muestra una ilustración de la instalación del nodo/chasis en el rack:



Sea cauteloso al levantar el hardware e instalarlo en el rack. Un chasis H610S pesa 40.5 lb (18.4 kg).

2. Cablee los nodos.

Si la apertura de flujo de aire de la parte trasera del chasis está bloqueada con cables o etiquetas, puede provocar fallos prematuros en los componentes debido al sobrecalentamiento.

   - Conecte el nodo a una red de 10 GbE mediante dos cables SFP28 o SFP+.
   - Conecte el nodo a una red de 1 GbE mediante dos conectores RJ45.
   - Conecte el nodo a una red de 1 GbE mediante un conector RJ-45 en el puerto IPMI.
   - Conecte ambos cables de alimentación al nodo.

3. Encienda los nodos.

El nodo tarda aproximadamente cinco minutos y 30 segundos en arrancar.

Configure los nodos

Después de montar en rack y cablear el hardware, está listo para configurar el nuevo recurso de almacenamiento.

Pasos

1. Conecte un teclado y un monitor al nodo.
2. En la interfaz de usuario de terminal (TUI) que se muestra, configure la red y la configuración del clúster del nodo con la navegación en pantalla.

Debe obtener la dirección IP del nodo de la TUI. Lo necesita cuando añade el nodo a un clúster. Después de guardar la configuración, el nodo está en estado pendiente y se puede añadir a un clúster. Consulte la <insert link to Setup section>.

3. Configurar la administración fuera de banda mediante el controlador de administración de la placa base (BMC). Estos pasos se aplican **sólo a los nodos H610S**.
   a. Utilice un explorador Web y navegue hasta la dirección IP predeterminada del BMC: 192.168.0.120
   b. Inicie sesión utilizando **root** como nombre de usuario y **calvin** como contraseña.
   c. Desde la pantalla de administración de nodos, vaya a **Configuración** > **Configuración de red** y configure los parámetros de red para el puerto de administración fuera de banda.

Consulte "Este artículo de base de conocimientos (es necesario iniciar sesión)".

Cree un clúster

Después de añadir el nodo de almacenamiento a la instalación y de configurar el nuevo recurso de almacenamiento, estará listo para crear un nuevo clúster de almacenamiento

Pasos

1. Desde un cliente en la misma red que el nodo recién configurado, acceda a la interfaz de usuario del software NetApp Element introduciendo la dirección IP del nodo.
2. Introduzca la información necesaria en la ventana **Crear un nuevo clúster**. Consulte "información general de la configuración" si quiere más información.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

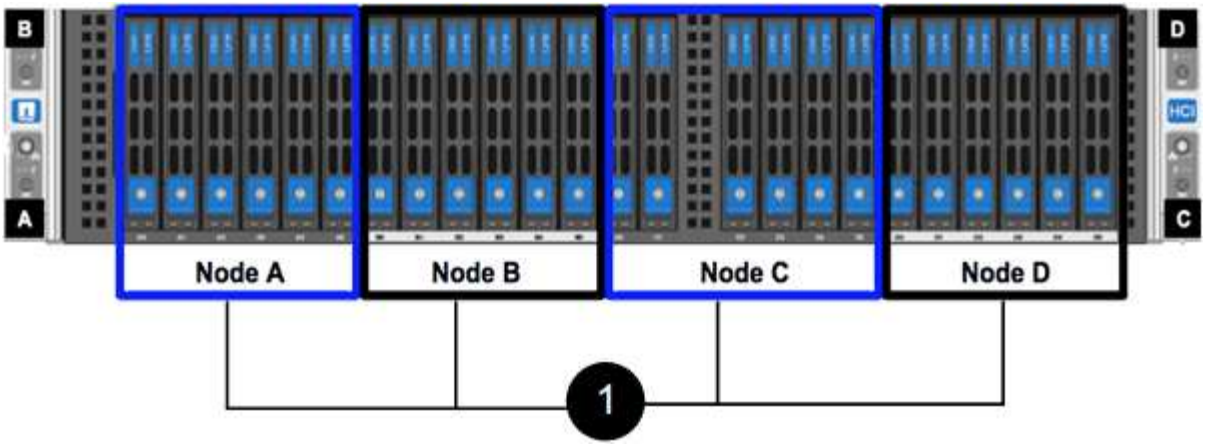
Sustituya un nodo H410S

Debe sustituir un nodo de almacenamiento en caso de que se produzca un fallo de CPU, problemas de tarjeta radial, otros problemas de la placa base o si no se enciende. Las instrucciones se aplican a los nodos de almacenamiento H410S.

Las alarmas en la interfaz de usuario del software NetApp Element le alertan de un nodo de almacenamiento. Debe usar la interfaz de usuario de Element para obtener el número de serie (etiqueta de servicio) del nodo con errores. Necesita esta información para localizar el nodo con errores en el clúster.

Aquí se encuentra la parte posterior de un chasis de dos racks (2U) de cuatro nodos con cuatro nodos de almacenamiento:

A continuación, se muestra la vista frontal de un chasis de cuatro nodos con nodos H410S, mostrando las bahías que corresponden a cada nodo:



Lo que necesitará

- Verificó que el nodo de almacenamiento está defectuoso y se debe sustituir.
- Obtuvo un nodo de almacenamiento de reemplazo.
- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otra protección antiestática.
- Ha etiquetado cada cable conectado al nodo de almacenamiento.

A continuación, se ofrece una descripción general de alto nivel de los pasos:

- Prepare para sustituir el nodo
- Sustituya el nodo en el chasis
- Añada el nodo al clúster

Prepare para sustituir el nodo

Debe quitar el nodo de almacenamiento defectuoso correctamente desde el clúster en la interfaz de usuario del software NetApp Element antes de instalar el nodo de reemplazo. Puede hacer esto sin causar ninguna interrupción del servicio. Debe obtener el número de serie del nodo de almacenamiento defectuoso en la interfaz de usuario de Element y relacionarlo con el número de serie de la etiqueta adhesiva en la parte posterior del nodo.

Pasos

1. En la interfaz de usuario de Element, seleccione **Cluster** > **Drives**.
2. Quite las unidades del nodo mediante uno de los siguientes métodos:

Opción	Pasos
Para quitar unidades individuales	a. Haga clic en **acciones** para la unidad que desea quitar. b. Haga clic en **Quitar**.
Para quitar varias unidades	a. Seleccione todas las unidades que desee quitar y haga clic en **acciones masivas**. b. Haga clic en **Quitar**.

3. Seleccione **Cluster** > **Nodes**.
4. Tenga en cuenta el número de serie (etiqueta de servicio) del nodo defectuoso. Debe coincidir con el número de serie de la etiqueta en la parte posterior del nodo.
5. Después de anotar el número de serie, quite el nodo del clúster del siguiente modo:
   a. Seleccione el botón **acciones** del nodo que desea quitar.
   b. Seleccione **Quitar**.

Sustituya el nodo en el chasis

Después de quitar el nodo defectuoso del clúster mediante la interfaz de usuario del software NetApp Element, estará listo para quitar físicamente el nodo del chasis. Debe instalar el nodo de reemplazo en la misma ranura del chasis desde el que quitó el nodo con errores.

Pasos

1. Use protección antiestática antes de continuar.
2. Desembale el nuevo nodo de almacenamiento y configúrelo en una superficie plana cerca del chasis.

   Mantenga el material de empaque durante el momento en que devuelve el nodo defectuoso a NetApp.

3. Etiquete cada cable que esté insertado en la parte posterior del nodo de almacenamiento que desea quitar.

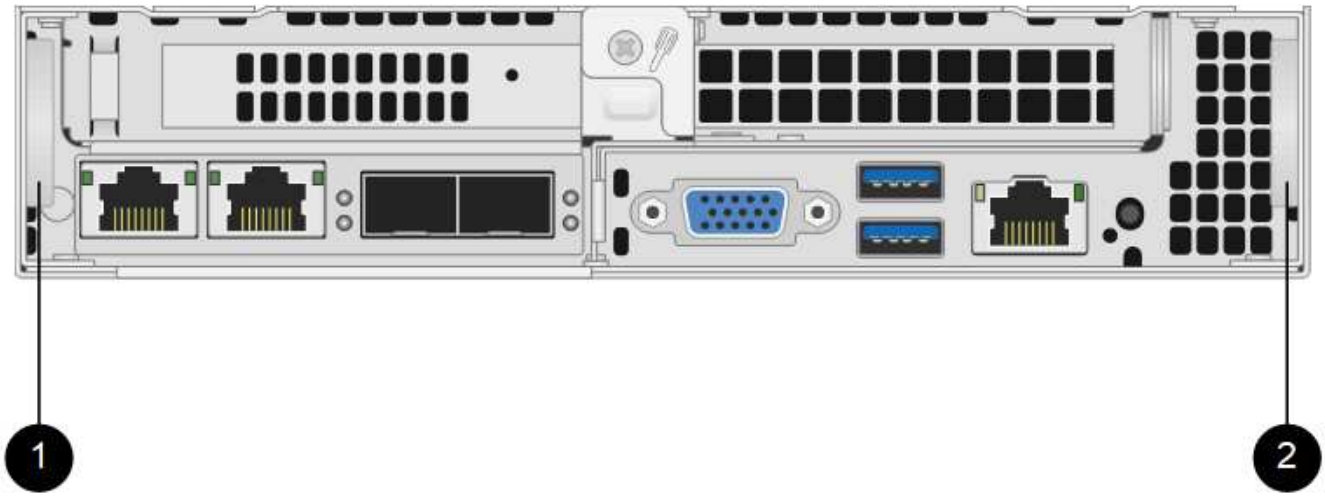
   Después de instalar el nodo de almacenamiento nuevo, debe insertar los cables en los puertos originales.

   Esta es una imagen que muestra la parte posterior de un nodo de almacenamiento:

Puerto	Detalles
Puerto A	Puerto 1/10 GbE RJ45
Puerto B	Puerto 1/10 GbE RJ45
Puerto C	Puerto SFP+ o SFP28 de 10 GbE
Puerto D	Puerto SFP+ o SFP28 de 10 GbE
IPMI	Puerto 1/10 GbE RJ45

4. Desconecte todos los cables del nodo de almacenamiento.
5. Tire hacia abajo del asa de leva en el lado derecho del nodo y tire del nodo para sacarlo con las dos asas de leva.

   El mango de leva que tira hacia abajo tiene una flecha sobre él para indicar la dirección en la que se mueve. El otro controlador de leva no se mueve y está allí para ayudarle a sacar el nodo.



Elemento	Descripción
1	Asa de leva para ayudarle a sacar el nodo.
2	Mango de leva que se tira hacia abajo antes de sacar el nodo.

Dé soporte al nodo con las dos manos cuando lo tire del chasis.

6. Coloque el nodo en una superficie nivelada.

   Debe empaquetar el nodo y devolverlo a NetApp.

7. Instale el nodo de repuesto en la misma ranura del chasis.

   Asegúrese de no utilizar una fuerza excesiva al deslizar el nodo en el chasis.

8. Mueva las unidades del nodo que quitó e insértelas en el nodo nuevo.
9. Vuelva a conectar los cables a los puertos desde los que se desconectaron originalmente.

   Las etiquetas que tenía en los cables cuando los desconectó le ayudarán a guiar.

   a. Si la apertura de flujo de aire de la parte trasera del chasis está bloqueada con cables o etiquetas, puede provocar fallos prematuros en los componentes debido al sobrecalentamiento.
   b. No fuerce los cables hacia los puertos, podría dañar los cables, los puertos o ambos.

   Asegúrese de que el nodo de reemplazo esté cableado de la misma manera que los otros nodos del chasis.

10. Pulse el botón situado en la parte frontal del nodo para encender el nodo.

Añada el nodo al clúster

Cuando se añade un nodo al clúster o se instalan unidades nuevas en un nodo existente, las unidades se

registran automáticamente como Available. Las unidades se deben añadir al clúster mediante la interfaz de usuario o la API de Element antes de que puedan participar en el clúster.

La versión de software de cada nodo en un clúster tiene que ser compatible. Cuando se añade un nodo a un clúster, el clúster instala la versión del clúster del software Element en el nuevo nodo según sea necesario.

Pasos

1. Seleccione **Cluster** > **Nodes**.
2. Seleccione **pendiente** para ver la lista de nodos pendientes.
3. Debe realizar una de las siguientes acciones:
   - Para agregar nodos individuales, seleccione el icono **acciones** del nodo que desea agregar.
   - Para añadir varios nodos, active la casilla de los nodos que desee agregar y, a continuación, **acciones masivas**.

   > Si el nodo que desea añadir tiene una versión de software Element diferente a la versión que se ejecuta en el clúster, el clúster actualiza de forma asíncrona el nodo a la versión del software Element que se ejecuta en el maestro de clústeres. Después de que se actualiza el nodo, se añade automáticamente al clúster. Durante este proceso asíncrono, el nodo estará en un `pendingActive` estado.

4. Seleccione **Agregar**.

   El nodo aparece en la lista de nodos activos.

5. En la interfaz de usuario de Element, seleccione **Cluster** > **Drives**.
6. Seleccione **Available** para ver la lista de unidades disponibles.
7. Debe realizar una de las siguientes acciones:
   - Para agregar unidades individuales, seleccione el icono **acciones** de la unidad que desea agregar y, a continuación, seleccione **Agregar**.
   - Para añadir varias unidades, active las casillas de verificación de las unidades que desee agregar, seleccione **acciones masivas** y, a continuación, seleccione **Agregar**.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Sustituya un nodo H610S

Puede que deba sustituir el chasis si falla el ventilador, la unidad de procesamiento central (CPU) o el módulo de memoria en línea doble (DIMM), o bien si resuelve problemas de sobrecalentamiento o problemas con el proceso de arranque. El LED ámbar parpadeante de la parte frontal del chasis indica la posible necesidad de sustituir el chasis. Debe comunicarse con el soporte de NetApp antes de continuar.

Consulte "Artículo de base de conocimientos" Para obtener información acerca de los requisitos de instalación para los nodos H610S. Los nodos de almacenamiento H610S nuevos y de repuesto pueden tener requisitos de instalación adicionales según la versión existente del software Element del clúster de almacenamiento. Póngase en contacto con el soporte de NetApp si desea obtener más información.

Los términos "nodo" y "chasis" se utilizan indistintamente en el caso de H610S, que es un chasis de unidad de rack (1U).

Prácticas recomendadas para agregar y quitar unidades

Debe seguir estas prácticas recomendadas para añadir unidades al clúster:

- Añada todas las unidades de bloques y asegúrese de que la sincronización de bloques se complete antes de añadir las unidades de segmentos.
- Para el software Element 10.x y versiones posteriores, añada todas las unidades de bloques a la vez. Asegúrese de no hacerlo para más de tres nodos a la vez.
- Para el software Element 9.x y versiones anteriores, añada tres unidades a la vez que le permitan sincronizarse completamente antes de añadir el siguiente grupo de tres.
- Quite la unidad de segmentos y asegúrese de que la sincronización de segmentos se complete antes de quitar las unidades de bloques.
- Quite todas las unidades de bloques de un único nodo a la vez. Asegúrese de que toda la sincronización de bloques esté completa antes de moverse al siguiente nodo.

Lo que necesitará

- Se ha puesto en contacto con el soporte de NetApp. Si solicita una sustitución, debe tener un caso abierto con el soporte de NetApp.
- Ha obtenido el nodo de sustitución.
- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otra protección antiestática.
- Si necesita realizar el proceso Volver a la imagen de fábrica (RTFI), ha obtenido la llave USB. El soporte de NetApp puede ayudarle a decidir si necesita llevar a cabo el proceso RTFI.
- Tiene un teclado y un monitor.
- Ha quitado el nodo con errores correctamente del clúster.
- Si un DIMM ha dado error, ha quitado las unidades antes de quitar el nodo del clúster.

Acerca de esta tarea

Las alarmas en la interfaz de usuario de Element se alertan de un error en un host. Debe coincidir con el número de serie del host con el error desde VMware vSphere Web Client con el número de serie en la etiqueta adhesiva que aparece en la parte posterior del nodo.

Pasos

1. Localice la etiqueta de servicio en la parte frontal del chasis con errores.

2. Compruebe que el número de serie de la etiqueta de servicio coincida con el número de caso de soporte de NetApp cuando solicitó el chasis de reemplazo.
3. Conecte el teclado y el monitor a la parte posterior del chasis con errores.
4. Compruebe el número de serie del nodo con errores con el soporte de NetApp.
5. Apague el chasis.
6. Etiquete las unidades frontales y los cables posteriores con sus ubicaciones, de modo que se puedan volver a colocar en las mismas ubicaciones después de la sustitución. Consulte la siguiente imagen para ver la colocación de las unidades en el chasis:

7. Quite los cables.
8. Retire el chasis desenroscando los tornillos de apriete manual de las orejas de montaje. Debe empaquetar y devolver el chasis con errores a NetApp.
9. Instale el chasis de repuesto.
10. Quite las unidades con cuidado del chasis que ha fallado e insértelas en el chasis de reemplazo.

> Debe insertar las unidades en las mismas ranuras en las que estaban antes de quitarlas.

11. Quite las unidades de suministro de alimentación del chasis con errores e insértelas en el chasis de reemplazo.
12. Inserte los cables de suministro de alimentación y los cables de red en sus puertos originales.
13. Es posible que se inserten transceptores de factor de forma pequeño conectable (SFP) en los puertos 10 GbE del nodo de reemplazo. Debe quitarlos antes de conectar los puertos 10 GbE.

> Consulte la documentación del proveedor del switch si el switch no reconoce los cables.

14. Encienda el chasis pulsando el botón de encendido situado en la parte frontal. El nodo tarda aproximadamente cinco minutos y 30 segundos en arrancar.
15. Realice los pasos de configuración.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Sustituya las unidades

Si una unidad está defectuosa o si el nivel de deterioro de la unidad está por debajo de un umbral, debe reemplazarla. Las alarmas en la interfaz de usuario del software Element se notifican cuando una unidad se produjo un error o se va a producir un fallo. Es posible cambiar en caliente una unidad con error.

Acerca de esta tarea

Este procedimiento permite reemplazar unidades en nodos de almacenamiento H610S y H410S. Al quitar una unidad, esta se desconecta. Los datos en la unidad se extraen y se migran a otras unidades del clúster. La migración de datos a otras unidades activas del sistema puede demorar desde algunos minutos hasta una hora según el uso de la capacidad y las operaciones de I/o activas en el clúster. Debe seguir las siguientes prácticas recomendadas para gestionar las unidades al tiempo que las quita y las reemplaza:

- Mantenga la unidad en la bolsa ESD hasta que esté listo para instalarla.
- Abra la bolsa ESD a mano o corte la parte superior con unas tijeras.
- Utilice siempre una muñequera ESD conectada a una superficie sin pintar en su chasis.
- Utilice siempre ambas manos cuando quite, instale o lleve una unidad.
- No fuerce nunca una unidad en el chasis.
- Utilice siempre paquetes aprobados cuando los lleve.
- No coloque las unidades entre sí.

Prácticas recomendadas para agregar y quitar unidades

- Añada todas las unidades de bloques y asegúrese de que la sincronización de bloques se complete antes de añadir las unidades de segmentos.
- Para el software Element 10.x y versiones posteriores, añada todas las unidades de bloques a la vez. Asegúrese de no hacerlo para más de tres nodos a la vez.
- Para el software Element 9.x y versiones anteriores, añada tres unidades a la vez que le permitan sincronizarse completamente antes de añadir el siguiente grupo de tres.
- Quite la unidad de segmentos y asegúrese de que la sincronización de segmentos se complete antes de quitar las unidades de bloques.
- Quite todas las unidades de bloques de un único nodo a la vez. Asegúrese de que toda la sincronización de bloques esté completa antes de moverse al siguiente nodo.

Pasos

1. Quite la unidad del clúster mediante la interfaz de usuario del software NetApp Element:
   a. En la interfaz de usuario de Element, seleccione **Cluster > Drives**.

b. Seleccione **error** para ver la lista de unidades con errores.

c. Anote el número de ranura de la unidad con error. Esta información se necesita para localizar la unidad con error en el chasis.

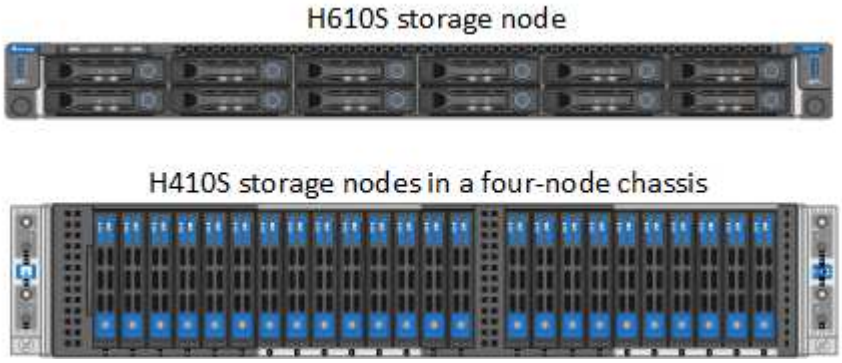
d. Seleccione **acciones** para la unidad que desea quitar.

e. Seleccione **Quitar**.

> Si no hay suficiente capacidad para quitar las unidades activas antes de quitar un nodo, se muestra un mensaje de error al confirmar la eliminación de la unidad. Después de resolver el error, ahora puede quitar físicamente la unidad del chasis.

2. Sustituya la unidad del chasis:

a. Desembale la unidad de repuesto y colóquela en una superficie plana y sin estática cerca del bastidor. Guarde los materiales de embalaje para cuando devuelva la unidad con error a NetApp. Aquí tiene la vista frontal de los nodos de almacenamiento H610S y H410S con las unidades:

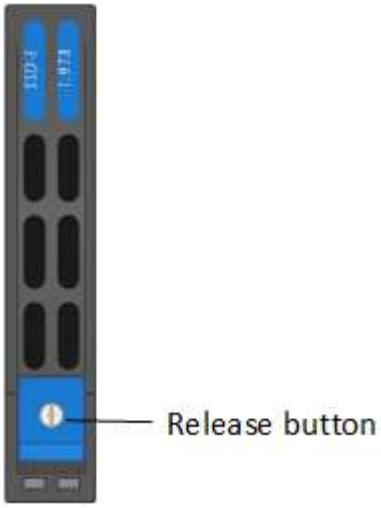


b. (**sólo H410S**) realice los siguientes pasos:

i. Identifique el nodo haciendo coincidir el número de serie (etiqueta de servicio) con el número que anotó abajo en la interfaz de usuario de Element. El número de serie está en una pegatina situada en la parte posterior de cada nodo. Después de identificar el nodo, se puede usar la información de ranura para identificar la ranura en la que está ubicada la unidad con error. Las unidades se ordenan alfabéticamente de La A a la D y del 0 al 5.

ii. Retire el bisel.

iii. Pulse el botón de liberación de la unidad con error:

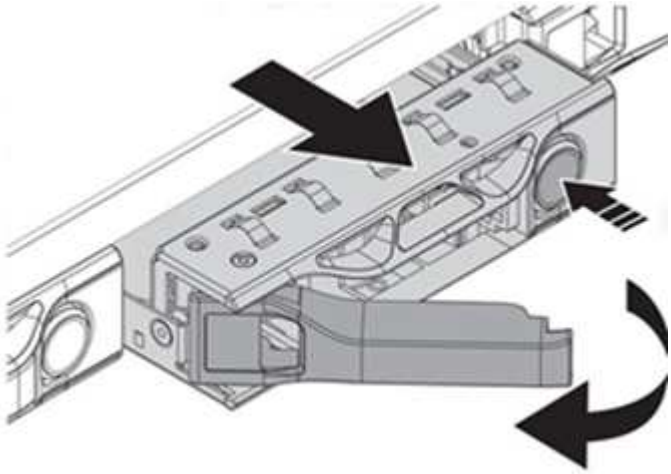


Al pulsar el botón de liberación, la palanca de leva de los resortes de accionamiento se abre parcialmente y la unidad se libera del plano medio.

i. Abra el mango de la leva y deslice la unidad con cuidado con ambas manos.
ii. Coloque la unidad sobre una superficie nivelada y antiestática.
iii. Inserte la unidad de sustitución en la ranura completamente en el chasis con ambas manos.
iv. Presione el asa de la leva hasta que haga clic.
v. Vuelva a instalar el bisel.
vi. Notifique al soporte de NetApp sobre el reemplazo de la unidad. El soporte de NetApp proporcionará instrucciones para la devolución de la unidad con error.

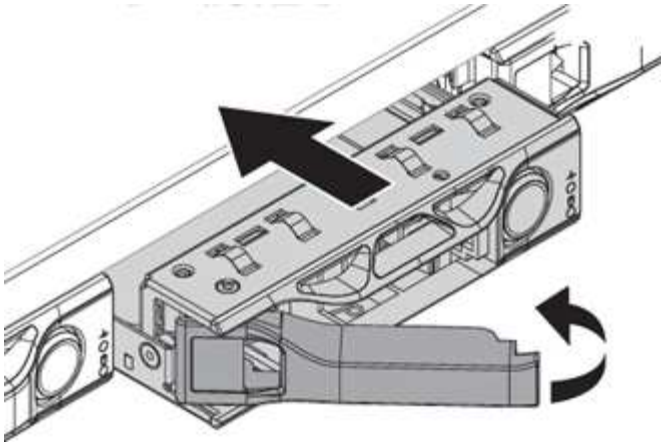
c. (**sólo H610S**) realice los siguientes pasos:

i. Coincida el número de ranura de la unidad con error desde la interfaz de usuario de Element con el número en el chasis. El LED de la unidad con error se ilumina en ámbar.
ii. Retire el bisel.
iii. Pulse el botón de liberación y quite la unidad con error como se muestra en la siguiente ilustración:



Asegúrese de que el asa de la bandeja está completamente abierto antes de intentar sacar la unidad del chasis.

i. Deslice la unidad hacia fuera y colóquela sobre una superficie nivelada y sin estática.
ii. Pulse el botón de liberación de la unidad de repuesto antes de insertarla en el compartimiento para unidades. Los muelles del mango de la bandeja de unidades se abren.



iii. Inserte la transmisión de sustitución sin aplicar demasiada fuerza. Cuando la unidad se inserta por completo, se oye un clic.

iv. Cierre Tratar con cuidado. del soporte de unidades

v. Vuelva a instalar el bisel.

vi. Notifique al soporte de NetApp sobre el reemplazo de la unidad. El soporte de NetApp proporcionará instrucciones para la devolución de la unidad con error.

3. Vuelva a añadir la unidad al clúster mediante la interfaz de usuario de Element.

> Al instalar una unidad nueva en un nodo existente, la unidad se registra automáticamente como **disponible** en la interfaz de usuario de Element. La unidad se debe añadir al clúster antes de que esta pueda participar en el clúster.

a. En la interfaz de usuario de Element, seleccione **Cluster > Drives**.

b. Seleccione **Available** para ver la lista de unidades disponibles.

c. Seleccione el icono acciones de la unidad que desea agregar y seleccione **Agregar**.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Sustituya una unidad de fuente de alimentación

Cada chasis incluye dos unidades de alimentación para redundancia de alimentación. Si una unidad de fuente de alimentación está defectuosa, debe sustituirla Lo antes posible. para garantizar que el chasis dispone de una fuente de alimentación redundante.

Lo que necesitará

- Ha determinado que la unidad de alimentación está defectuosa.
- Tiene una unidad de suministro de alimentación de repuesto.
- Ha comprobado que la segunda unidad de alimentación está en funcionamiento.
- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otras precauciones antiestáticas.

Acerca de esta tarea

El procedimiento de sustitución se aplica a los siguientes modelos de nodo:

- Chasis NetApp HCI de cuatro nodos y unidad rack doble (2U)
- Un chasis de almacenamiento H610S de unidad de rack (1U)

> En el caso de H610S, los términos "nodo" y "chasis" se utilizan indistintamente porque el nodo y el chasis no son componentes separados, a diferencia de lo que sucede en el chasis de 2U de cuatro nodos.

Las alarmas en la interfaz de usuario de Element proporcionan información sobre la unidad de suministro de alimentación que ha fallado, haciendo referencia a ella como PS1 o PS2. En un chasis NetApp HCI 2U de cuatro nodos, PS1 hace referencia a la unidad de la fila superior del chasis y PS2 hace referencia a la unidad de la fila inferior del chasis. Puede sustituir la unidad de fuente de alimentación defectuosa mientras el chasis está encendido y en funcionamiento, siempre que la unidad de fuente de alimentación redundante esté funcionando.

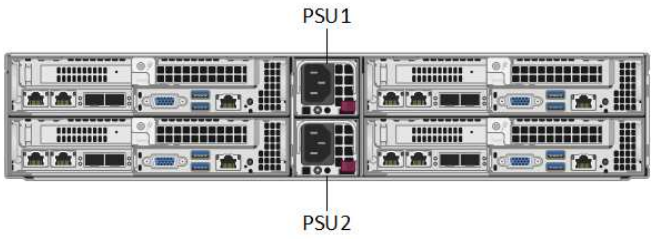
> Si va a sustituir ambas PSU en un nodo, las PSU deben tener el mismo número de pieza y el mismo vataje. Las PSU que no coinciden pueden dañar el sistema.

Pasos

1. Localice la unidad de alimentación defectuosa en el chasis. El indicador LED de la unidad defectuosa se ilumina en ámbar.

   > Las unidades de suministro de alimentación se encuentran de forma diferente según el tipo de chasis.

   Consulte las siguientes imágenes para conocer las ubicaciones de las unidades de alimentación:

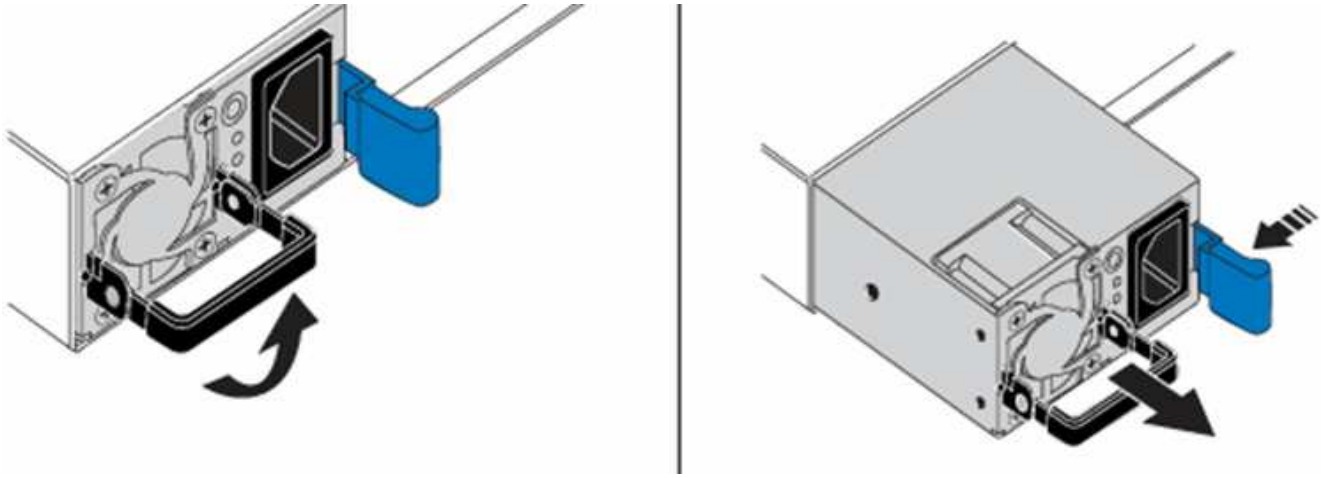
Modelo	Ubicación de las unidades de alimentación
Chasis de almacenamiento NetApp HCI 2U de cuatro nodos	 Los nodos del chasis pueden parecer diferentes según el tipo de nodos (almacenamiento o computación) que tenga.
Chasis H610S	

2. Identifique el nodo correcto mediante la etiqueta de extracción azul o el número de serie. La etiqueta desplegable azul indica el número de serie (S/N) y la distribución de la unidad. Confirme el número de

serie del nodo que se va a reparar.

- Si va a sustituir ambas unidades de suministro de alimentación, vaya al paso 3.
- Si sólo va a sustituir una unidad de alimentación, vaya al paso 4.

3. Confirme que el nodo se ha apagado o está listo para funcionar. Tenga en cuenta lo siguiente:
   - Un nodo que se ha apagado no muestra ningún LED de encendido azul de las unidades ni del botón de encendido.
   - Un nodo que aún no se ha apagado muestra LED azules en las unidades y el botón de encendido.
   - Un nodo que se ha apagado y está listo para el servicio muestra un LED de PSU que parpadea (verde) y se apaga (no hay color).
   - Un nodo que aún no se ha apagado muestra LED de verde fijo en las fuentes de alimentación.
4. Desenchufe el cable de alimentación de la unidad de alimentación o de ambos cables de alimentación, si va a sustituir ambas unidades.
5. Levante el asa de la leva y presione el pestillo azul para sacar la unidad de alimentación.



La ilustración es un ejemplo. La ubicación de las unidades de fuente de alimentación del chasis y el color del botón de liberación varían según el tipo de chasis que tenga.

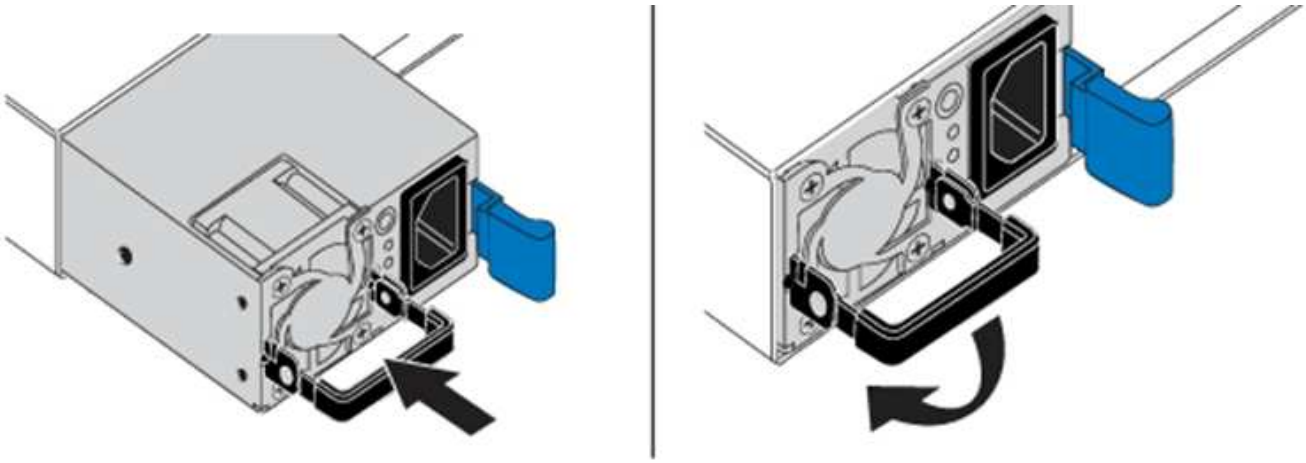
Asegúrese de utilizar ambas manos para soportar el peso de la unidad de alimentación.

Repita los pasos 3, 4 y 5 si sustituye una segunda unidad de alimentación.

6. Localice la etiqueta de la unidad de alimentación que ha retirado del chasis. La etiqueta contiene detalles del fabricante y el vataje de salida.

No sustituya la unidad de fuente de alimentación si el vataje de la fuente de alimentación de su RMA no coincide con el vataje de la fuente de alimentación extraída. Comuníquese con el soporte de NetApp para obtener los siguientes pasos.

7. Con ambas manos, alinee los bordes de la unidad de alimentación con la abertura del chasis, empuje suavemente la unidad hacia el chasis con el asa de leva hasta que encaje en su sitio y vuelva a colocar el mango de leva en la posición vertical.



8. Conecte uno o ambos cables de alimentación.
9. Si ha sustituido ambas unidades de suministro de alimentación, vaya a la parte frontal del nodo y pulse el botón de alimentación para encender los nodos. Después de encenderse, el LED del botón de encendido ilumina un color azul fijo. Los LED azules de las unidades y el botón de identificación comenzarán a parpadear.
10. Devuelva la unidad defectuosa a NetApp siguiendo las instrucciones de la caja que le ha enviado.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Información sobre hardware de SF-Series

Puede encontrar información sobre la instalación y el mantenimiento de los nodos de almacenamiento SF-Series.

A continuación encontrará los enlaces al contenido de instalación y mantenimiento:

- "Instalar y configurar nodos C-Series de SolidFire"
- "Instale y configure los nodos Fibre Channel"
- "Instalar y configurar nodos de almacenamiento SF-Series"
- "Sustituya un chasis"
- "Sustituya las unidades"
- "Sustituya una unidad de fuente de alimentación"

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Sustituya un chasis

Puede que deba sustituir el chasis si falla el ventilador, la unidad de procesamiento

central (CPU) o el módulo de memoria en línea doble (DIMM), o bien si resuelve problemas de sobrecalentamiento o problemas con el proceso de arranque. Los errores del clúster en la interfaz de usuario del software (UI) de NetApp Element y la luz ámbar intermitente en la parte frontal del chasis son indicios de una posible necesidad de sustituir el chasis. Debe comunicarse con el soporte de NetApp antes de continuar.

Lo que necesitará

- Se ha puesto en contacto con el soporte de NetApp.

  Si solicita una sustitución, debe tener un caso abierto con el soporte de NetApp.

- Ha obtenido el chasis de repuesto.
- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otra protección antiestática.
- Si necesita realizar el proceso Volver a la imagen de fábrica (RTFI), ha obtenido la llave USB.

  El soporte de NetApp le ayudará a decidir si se necesita RTFI. Consulte "Este artículo de base de conocimientos (se requiere inicio de sesión)".

- Tiene un teclado y un monitor.

Acerca de esta tarea

Las instrucciones de este documento se aplican si dispone de un chasis de unidad de rack única (1U) con cualquiera de los siguientes nodos:

- SF2405
- SF3010
- SF4805
- SF6010
- SF9605
- SF9608
- SF9010
- SF19210
- SF38410
- SF-FCN-01
- FC0025

Pasos

1. Localice la etiqueta de servicio del chasis con errores y compruebe que el número de serie coincide con el número de la incidencia que abrió con el soporte de NetApp cuando solicitó el reemplazo.

   Puede localizar la etiqueta de servicio desde la parte frontal del chasis.

   La siguiente figura muestra un ejemplo de la etiqueta de servicio:

La figura anterior es un ejemplo. La ubicación exacta de la etiqueta de servicio puede variar en función del modelo de hardware.

2. Conecte el teclado y el monitor a la parte posterior del chasis con errores.
3. Verificar la información del chasis con el soporte de NetApp.
4. Apague el chasis.
5. Etiquete las unidades en la parte frontal del chasis y los cables en la parte posterior.

   Los nodos Fibre Channel no tienen unidades en la parte frontal.

6. Retire las unidades de alimentación y los cables.
7. Retire las unidades con cuidado y colóquelas en una superficie nivelada y antiestática.

   Si tiene un nodo Fibre Channel, puede omitir este paso.

8. Retire el chasis presionando el pestillo o desenroscando el tornillo de mariposa, según su modelo de hardware.

   Debe empaquetar y devolver el chasis con errores a NetApp.

9. **Opcional**: Retire los rieles e instale los nuevos rieles que se enviaron con el chasis de repuesto.

   Puede optar por reutilizar los rieles existentes. Si está reutilizando los rieles existentes, puede omitir este paso.

10. Deslice el chasis de repuesto sobre los rieles.
11. En el caso de los nodos de almacenamiento, inserte las unidades del chasis con errores en el chasis de reemplazo.

    Debe insertar las unidades en las mismas ranuras que las que estaban en el chasis con errores.

12. Instale las unidades de la fuente de alimentación.
13. Inserte los cables de suministro de alimentación, y los cables 1 GbE y 10 GbE en sus puertos originales.

    Es posible que se inserten transceptores de factor de forma pequeño conectable (SFP) en los puertos 10 GbE del chasis de reemplazo. Debe quitarlos antes de conectar los puertos 10 GbE.

14. Si ha determinado que no necesita realizar el proceso RTFI en el nodo, arranque el nodo y espere hasta que aparezca la interfaz de usuario del terminal (TUI). Continúe con el paso 16 y permita que el clúster vuelva a crear la imagen del nodo automáticamente cuando lo añada mediante la interfaz de usuario de.
15. **Opcional**: Si la compatibilidad con NetApp recomienda volver a crear imágenes del nodo con una clave USB, lleve a cabo los siguientes pasos:
    a. Encienda el chasis. Arranca con la imagen clave de RTFI.
    b. En el primer símbolo del sistema, escriba **y** para obtener la imagen del nodo de almacenamiento.
    c. En el segundo indicador, escriba **N** para las comprobaciones de estado del hardware.

       Si la secuencia de comandos RTFI detecta un problema con un componente de hardware, muestra un

error en la consola. Si observa un error, póngase en contacto con el soporte de NetApp. Una vez completado el proceso RTFI, el nodo se apaga.

d. Extraiga la llave USB de la ranura USB.

e. Arranque el nodo que se acaba de exponer y espere a que aparezca la TUI.

16. Configure la información de red y del clúster de la TUI.

    Puede ponerse en contacto con el soporte de NetApp para obtener ayuda.

17. Añada el nodo nuevo al clúster con la TUI del clúster.

18. Empaque y devuelva el chasis con errores.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Sustituya unidades para los nodos de almacenamiento SF-Series

Una unidad de estado sólido con fallos se puede cambiar en caliente por una unidad de reemplazo.

Lo que necesitará

- Tiene una unidad de reemplazo.
- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otras precauciones antiestáticas.
- Usted se ha puesto en contacto con el soporte de NetApp para verificar que el SSD debe sustituirse y que para facilitar el procedimiento de resolución de problemas adecuado.

  Necesitará la etiqueta o el número de serie del servicio al llamar al soporte de NetApp. El equipo de soporte colaborará con usted para obtener una unidad de sustitución de acuerdo con su acuerdo de nivel de servicio.

Acerca de esta tarea

Las instrucciones se aplican a los siguientes modelos de nodos de almacenamiento SolidFire:

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

La siguiente figura muestra la colocación de las unidades en un chasis SF9605:

La figura anterior es un ejemplo. SF9608 tiene una distribución de unidades diferente que incluye solo ocho unidades numeradas de una a ocho, de izquierda a derecha.

La ranura 0 contiene la unidad de metadatos para el nodo. Si va a sustituir la unidad en la ranura 0, debe fijar la pegatina incluida en la caja de envío de la unidad de reemplazo, de modo que pueda identificarla por separado del resto. SF3010 es una excepción, ya que los metadatos se conservan en el módulo de memoria en línea dual (DIMM) de conexión de tecnología avanzada en serie interna (SATA).

Siga estas prácticas recomendadas al gestionar las unidades:

- Evite la descarga electrostática (ESD) manteniendo la unidad en la bolsa ESD hasta que esté listo para instalarla.
- No inserte una herramienta o cuchilla metálicas en la bolsa ESD.
- Abra la bolsa ESD a mano o corte la parte superior con unas tijeras.
- Guarde la bolsa ESD y cualquier material de embalaje en caso de que deba devolver una unidad más tarde.
- Utilice siempre una muñequera ESD conectada a una superficie sin pintar en su chasis.
- Utilice siempre ambas manos cuando quite, instale o lleve una unidad.
- No fuerce nunca una unidad en el chasis.
- No coloque las unidades entre sí.
- Utilice siempre paquetes aprobados cuando los lleve.

A continuación, se ofrece una descripción general de alto nivel de los pasos:

- Quite la unidad del clúster
- Sustituya la unidad del chasis
- Añada la unidad al clúster

Quite la unidad del clúster

El sistema SolidFire pone una unidad en estado de error cuando el sistema de autodiagnóstico de la unidad indica al nodo que se ha producido un error o cuando la comunicación con la unidad se detiene durante cinco minutos y medio o más. El sistema muestra una lista de las unidades con errores. Quite una unidad con error de la lista de unidades con errores en el software NetApp Element.

Pasos

1. En la interfaz de usuario de Element, seleccione **Cluster** > **Drives**.
2. Seleccione **error** para ver la lista de unidades con errores.
3. Anote el número de ranura de la unidad con error.

   Esta información se necesita para localizar la unidad con error en el chasis.

4. Quite la unidad con error mediante uno de los siguientes métodos:

Opción	Pasos
Para quitar unidades individuales	a. Seleccione **acciones** para la unidad que desea quitar. b. Seleccione **Quitar**.
Para quitar varias unidades	a. Seleccione todas las unidades que desee quitar y seleccione **acciones masivas**. b. Seleccione **Quitar**.

Sustituya la unidad del chasis

Después de quitar una unidad con error de la lista de unidades con errores en la interfaz de usuario de Element, está listo para sustituir físicamente la unidad con error del chasis.

Pasos

1. Desembale la unidad de repuesto y colóquela en una superficie plana y sin estática cerca del bastidor.

   Guarde los materiales de embalaje para cuando devuelva la unidad con error a NetApp.

2. Coincida el número de ranura de la unidad con error desde la interfaz de usuario de Element con el número en el chasis.

   La siguiente figura muestra un ejemplo para mostrar la numeración de las ranuras de unidad:

Elemento	Descripción
1	Números de ranura de unidad

3. Pulse el círculo rojo de la unidad que desea quitar para liberar la unidad.

   El pestillo hace clic en abierto.

4. Deslice la unidad fuera del chasis y colóquela sobre una superficie nivelada y sin estática.
5. Presione el círculo rojo en la unidad de repuesto antes de deslizarla en la ranura.
6. Inserte la unidad de sustitución y presione el círculo rojo para cerrar el pestillo.
7. Notifique al soporte de NetApp sobre el reemplazo de la unidad.

   El soporte de NetApp proporcionará instrucciones para la devolución de la unidad con error.

Añada la unidad al clúster

Después de instalar una unidad nueva en el chasis, se registra como disponible. Debe añadir la unidad al clúster mediante la interfaz de usuario de Element antes de que esta pueda participar en el clúster.

Pasos

1. En la interfaz de usuario de Element, haga clic en **Cluster** > **Drives**.

2. Haga clic en **disponible** para ver la lista de unidades disponibles.
3. Seleccione una de las siguientes opciones para añadir unidades:

Opción	Pasos
Para añadir unidades individuales	a. Seleccione el botón **acciones** de la unidad que desea agregar. b. Seleccione **Agregar**.
Para añadir varias unidades	a. Active las casillas de verificación de las unidades que desee agregar y, a continuación, seleccione **acciones masivas**. b. Seleccione **Agregar**.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Sustituya una unidad de fuente de alimentación

Cada chasis SolidFire incluye dos unidades de suministro de alimentación para redundancia de alimentación. Si falla una unidad de fuente de alimentación, debe sustituirla Lo antes posible. para garantizar que el chasis tiene una fuente de alimentación redundante.

Lo que necesitará

- Ha determinado que es necesario sustituir la unidad de alimentación.
- Tiene una unidad de suministro de alimentación de repuesto.
- Ha comprobado que la segunda unidad de alimentación está en funcionamiento.
- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otras precauciones antiestáticas.

Acerca de esta tarea

Las instrucciones se aplican si dispone de un chasis de unidad de rack individual (1U) con cualquiera de los siguientes nodos:

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

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

Pasos

1. Desconecte el cable de alimentación de la unidad de alimentación que va a sustituir.
2. Pulse el botón de liberación para extraer la unidad de alimentación del chasis.

   Asegúrese de utilizar ambas manos para soportar el peso de la unidad de alimentación.

3. Con ambas manos, alinee los bordes de la unidad de alimentación de repuesto con la abertura del chasis y empuje suavemente la unidad hacia dentro del chasis.

   No ejerza demasiada fuerza al deslizar la unidad de alimentación en el chasis para evitar daños en el hardware.

4. Enchufe el cable de alimentación.
5. Devuelva la unidad con el error a NetApp siguiendo las instrucciones de la caja que se le envió.

   Puede ponerse en contacto con el soporte de NetApp para obtener ayuda sobre el procedimiento de sustitución.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Vuelva a la información de la imagen de fábrica

Configure el RTFI

Los sistemas de almacenamiento SolidFire de NetApp utilizan el proceso Return to Factory Image (RTFI) para escribir una imagen de software en un nodo nuevo o restaurar un nodo a su estado original de fábrica. El proceso RTFI borra de forma segura todos los datos y configuraciones existentes (si los hubiera) e instala una imagen de software de NetApp Element sin configurar. El proceso RTFI está disponible para todos los nodos SolidFire.

Los sistemas SolidFire utilizan un proceso RTFI para todas las instalaciones de software Element. Esto incluye instalaciones manuales internas realizadas por desarrolladores, instalaciones automáticas mediante pruebas de marco automatizadas, instalaciones de campo realizadas por ingenieros de servicio y clientes e instalaciones realizadas por varios integradores y partners. Se utiliza el mismo proceso RTFI en todos los nodos SolidFire, independientemente del chasis o el tipo de nodo que se estén utilizando, para resolver automáticamente cualquier problema.

Los destinatarios de esta guía están integradores que instalan, configuran, usan o solucionan problemas relacionados con el almacenamiento.

- Linux: Tiene experiencia con sistemas Linux.
- Redes: Conoce bien la red del servidor y el almacenamiento en red, incluidas las direcciones IP, las máscaras de red y las puertas de enlace.

> El proceso RTFI es destructivo para los datos y borra todos los datos y detalles de configuración del nodo de forma segura e instala un nuevo sistema operativo. Compruebe que el nodo utilizado para el proceso RTFI no está activo como parte de un clúster.

Despliegue e instale la imagen de la Organización Internacional de Normalización (ISO) de RTFI y realice el proceso RTFI:

- Opciones de implementación e instalación de RTFI
- Realice el proceso RTFI
- Menú de opciones de RTFI

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

El proceso RTFI

Puede comenzar el proceso Volver a la imagen de fábrica (RTFI) interactuando con el nodo a través de las indicaciones de la consola de texto que aparecen antes de que arranque el sistema.

> El proceso RTFI es destructivo para los datos y borra todos los datos y detalles de configuración del nodo de forma segura e instala un nuevo sistema operativo. Compruebe que el nodo utilizado para el proceso RTFI no está activo como parte de un clúster.

El proceso RTFI realiza las siguientes operaciones de alto nivel:

1. Inicia la instalación tras la confirmación del usuario y valida la imagen.
2. Desbloquea todas las unidades de un nodo.
3. Valida y parpadea el firmware.
4. Comprueba la tornillería.
5. Prueba hardware.
6. Secure borra todas las unidades seleccionadas.
7. Crea particiones en la unidad raíz y crea sistemas de archivos.
8. Monta y descomprime la imagen.
9. Configura el nombre del host, la red (Protocolo de configuración dinámica de host), la configuración de clúster predeterminada y el gestor de arranque de GRUB.
10. Detiene todos los servicios, recopila registros y reinicia.

Para configurar el nodo una vez finalizado correctamente el proceso de RTFI, consulte "Documentación para la versión del software Element". Una vez que un nodo finaliza correctamente el proceso RTFI, pasa al estado *Available* (sin configurar) de forma predeterminada.

Realice el proceso RTFI

Utilice el siguiente procedimiento para restaurar el software Element en su nodo SolidFire.

Para obtener información sobre cómo crear una clave USB o utilizar el BMC para realizar el proceso RTFI, consulte Opciones de implementación e instalación de RTFI.

Antes de empezar

Compruebe que cumple los siguientes requisitos:

- Tiene acceso a una consola para el nodo SolidFire.
- El nodo en el que está realizando el proceso RTFI se enciende y se conecta a una red.
- El nodo en el que está realizando el proceso RTFI no forma parte de un clúster activo.
- Tiene acceso a medios de instalación de inicio que contienen la imagen de la versión de software Element correspondiente para la configuración.

Póngase en contacto con el soporte de NetApp si tiene alguna duda antes de realizar el proceso RTFI.

Pasos

1. Conecte un monitor y un teclado a la parte posterior del nodo, o conecte a la interfaz de usuario de IP de BMC, y active la consola **iKVM/HTML5** desde la ficha **Control remoto** de la interfaz de usuario.
2. Inserte una llave USB con la imagen adecuada en una de las dos ranuras USB de la parte posterior del nodo.
3. Encienda o restablezca el nodo. Durante el arranque, seleccione dispositivo de arranque seleccionando **F11**:

   Debe seleccionar **F11** varias veces en sucesión rápida porque la pantalla Boot Device (dispositivo de inicio) va rápidamente.

4. En el menú de selección Boot Device (dispositivo de inicio), resalte la opción USB (USB).

   Las opciones que aparecen dependen de la Marca USB que esté utilizando.

   Si no aparece ningún dispositivo USB en la lista, vaya al BIOS, compruebe que el USB aparece en el orden de inicio, reinicie y vuelva a intentarlo.

   Si eso no resuelve el problema, vaya al BIOS, vaya a la ficha **Guardar y salir**, seleccione **Restaurar valores predeterminados optimizados**, acepte y guarde la configuración y reinicie.

5. Aparece una lista de las imágenes que se encuentran en el dispositivo USB resaltado. Seleccione la versión deseada y seleccione ENTER para iniciar el proceso RTFI.

   Aparece el nombre y número de versión del software del elemento de imagen de RTFI.

6. En la solicitud inicial, se le notifica que el proceso eliminará todos los datos del nodo y que los datos no se podrán recuperar una vez que se inicie el proceso. Introduzca **Sí** para comenzar.

   Una vez iniciado el proceso, todos los datos y detalles de configuración se borran de forma permanente del nodo. Si opta por no continuar, se le dirigirá al Menú de opciones de RTFI.

   Si desea ver la consola durante el proceso de RTFI, puede presionar las teclas **ALT+F8** para cambiar a la consola de modo detallado. Presione **ALT+F7** para volver a la GUI principal.

7. Introduzca **no** cuando se le solicite que realice amplias pruebas de hardware a menos que tenga un motivo para sospechar que se trata de un error de hardware o que le indique que realice las pruebas realizadas por el soporte de NetApp.

   Un mensaje indica que el proceso RTFI ha finalizado y que el sistema se apaga.

8. Si es necesario, quite todos los medios de instalación de arranque después de que el nodo se apague.

   El nodo ahora está listo para estar encendido y configurado. Consulte "El software Element configura la documentación de almacenamiento" para configurar el nodo de almacenamiento.

   Si ha encontrado un mensaje de error durante el proceso de RTFI, consulte Menú de opciones de RTFI.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Menú de opciones de RTFI

El siguiente menú de opciones aparece si el proceso de RTFI no se realiza correctamente o si opta por no continuar en el indicador de proceso de RTFI inicial.

Póngase en contacto con el soporte de NetApp antes de utilizar cualquiera de las siguientes opciones de comando.

Opción	Descripción
Reinicie	Sale del proceso de RTFI y reinicia el nodo en su estado actual. No se realiza ninguna limpieza.
Apagado	Apaga el nodo con gracia en su estado actual. No se realiza ninguna limpieza.
Salga	Sale del proceso de RTFI y abre un símbolo del sistema.
UploadLogs	Recopila todos los registros del sistema y carga un único archivo de registro consolidado en una dirección URL especificada.

Cargar registros

Recopile todos los registros del sistema y cárguelos en una URL específica según el procedimiento siguiente.

Pasos

1. En el símbolo del sistema del menú de opciones de RTFI, introduzca **UploadLogs**.
2. Introduzca la información del directorio remoto:

   a. Escriba una dirección URL que incluya el protocolo. Por ejemplo: `ftp://,scp://,http://,orhttps://.`

   b. (Opcional) Agregue un nombre de usuario y una contraseña incorporados. Por ejemplo: `scp://user:password@URLaddress.com`.

   > Para obtener un rango completo de opciones de sintaxis, consulte "Rizo" manual de usuario.

   El archivo de registro se carga y se guarda en el directorio especificado como un `.tbz2` archivado.

Utilice el túnel de soporte

Si necesita soporte técnico para su sistema NetApp HCI o almacenamiento all-flash de SolidFire, el soporte de NetApp puede conectarse de forma remota con su sistema. Para iniciar una sesión y tener acceso remoto, el soporte de NetApp puede abrir una conexión de Secure Shell (SSH) inversa a su entorno.

Puede abrir un puerto TCP para una conexión de túnel SSH inverso con el soporte de NetApp. Gracias a esta conexión, el soporte de NetApp puede iniciar sesión en su nodo de gestión.

Antes de empezar

- Para los servicios de gestión 2.18 y posteriores, la funcionalidad para el acceso remoto se deshabilita en el nodo de gestión de manera predeterminada. Para activar la función de acceso remoto, consulte "Gestione la funcionalidad SSH en el nodo de gestión".
- Si el nodo de gestión está detrás de un servidor proxy, se necesitan los siguientes puertos TCP en el archivo sshd.config:

Puerto TCP	Descripción	Dirección de conexión
443	Llamadas API/HTTPS para un reenvío de puertos inverso a través de un túnel de soporte abierto a la interfaz de usuario web	Del nodo de gestión a los nodos de almacenamiento
22	Acceso de inicio de sesión SSH	Del nodo de gestión a los nodos de almacenamiento o desde los nodos de almacenamiento al nodo de gestión

Pasos

- Inicie sesión en su nodo de almacenamiento y abra una sesión de terminal.
- En un símbolo del sistema, introduzca lo siguiente:

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

- Para cerrar el túnel de soporte remoto, introduzca lo siguiente:

  ```
  rst --killall
  ```

- (Opcional) Deshabilitar "función de acceso remoto" de nuevo.

> SSH sigue estando habilitado en el nodo de gestión si no se la deshabilita. La configuración habilitada para SSH continúa en el nodo de gestión a través de actualizaciones y renovaciones hasta que se deshabilita manualmente.

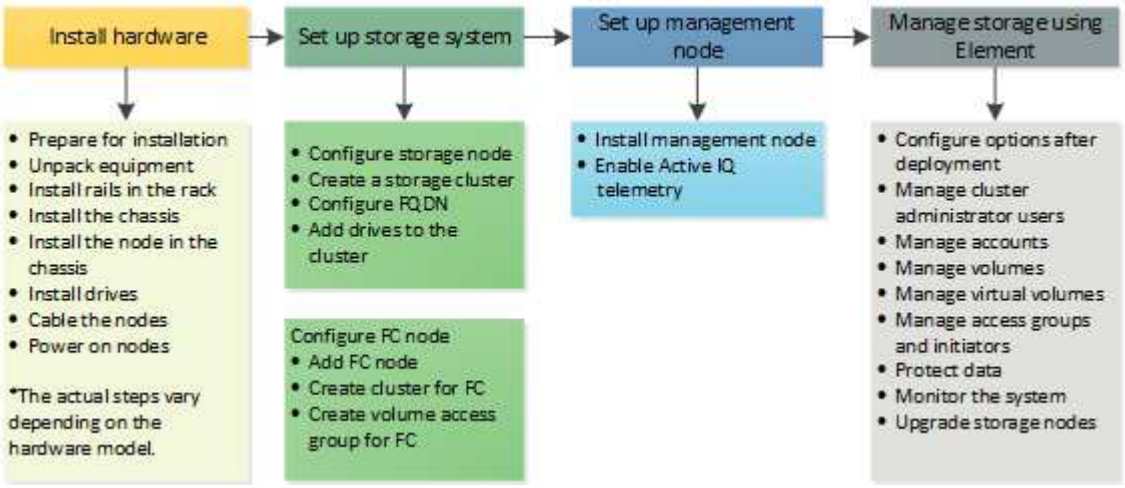
Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Información general de la configuración

En este momento, debería haber instalado el hardware. El hardware también incluye el software Element.

A continuación, tendrá que configurar el sistema de almacenamiento para su entorno. Es posible configurar un clúster con nodos de almacenamiento o Fibre Channel y gestionarlo mediante el software Element después de instalar los nodos de cable en una unidad de rack y conectarlos.



Pasos para configurar el almacenamiento

1. Seleccione una de las siguientes opciones:
   - "Configure el clúster con nodos de almacenamiento"
   - "Configure el clúster con los nodos Fibre Channel"
2. "Determine qué componentes de SolidFire instalar"
3. "Configure un nodo de gestión y habilite la telemetría Active IQ"

Obtenga más información

- "Descubra los siguientes pasos para usar el almacenamiento"
- "Documentación de SolidFire y el software Element"

Configure un clúster con nodos de almacenamiento Element

Es posible configurar un clúster con nodos de almacenamiento y gestionarlo mediante el software Element después de instalar y cablear los nodos en una unidad de rack y encender los. De esta forma, puede instalar y configurar componentes adicionales en el sistema de almacenamiento.

Pasos

1. "Configure un nodo de almacenamiento"
2. "Cree un clúster de almacenamiento de"

3. "Inicie sesión en la interfaz de usuario del software Element"
4. "Añada unidades al clúster"
5. "Determine qué componentes de SolidFire instalar"
6. "Configure un nodo de gestión"

Obtenga más información

- "Documentación de SolidFire y el software Element"

Configure un nodo de almacenamiento

Tiene que configurar nodos de individuales antes de poder añadirlos a un clúster. Después de instalar y cablear un nodo en una unidad de rack y encitarlo, puede configurar los ajustes de red del nodo con la interfaz de usuario por nodo o la interfaz de usuario de terminal (TUI) del nodo. Asegúrese de tener la información de configuración de red que necesita para el nodo antes de proceder.

La configuración de los nodos de almacenamiento es de dos opciones:

- IU por nodo: Utilice la interfaz de usuario por nodo para configurar los ajustes de red de los nodos.
- configure un nodo de almacenamiento,TUI: Utilice la interfaz de usuario del terminal (TUI) del nodo para configurar el nodo.

No es posible añadir a un clúster un nodo con direcciones IP asignadas por DHCP. Con la dirección IP de DHCP, puede usar la dirección IP de DHCP para configurar inicialmente el nodo en la interfaz de usuario, la TUI o la API por nodo. Durante esta configuración inicial, puede añadir la información de la dirección IP estática para que pueda añadir el nodo a un clúster.

Tras la configuración inicial, podrá acceder al nodo con la dirección IP de gestión del nodo. Después, podrá cambiar la configuración del nodo, añadirlo a un clúster o usarlo para crear un clúster. También es posible configurar un nodo nuevo con los métodos API del software Element.

> A partir de la versión 11.0 de Element, los nodos se pueden configurar con IPv4, IPv6 o ambas direcciones para su red de gestión. Esto se aplica a los nodos de almacenamiento y de gestión, excepto el nodo de gestión 11.3 y una versión posterior que no admite IPv6. Cuando crea un clúster, solo se puede usar una dirección IPv4 o IPv6 única para la MVIP y el tipo de dirección correspondiente se debe configurar en todos los nodos.

Configure un nodo de almacenamiento con la interfaz de usuario por nodo

Con la interfaz de usuario por nodo se pueden configurar nodos.

Acerca de esta tarea

- Puede configurar el nodo para que tenga una dirección IPv4 o IPv6.
- Con el fin de acceder a un nodo, es necesario que la dirección DHCP aparezca en la TUI. No se puede usar para añadir un nodo a un clúster.

Debe configurar las interfaces de gestión (Bond1G) y almacenamiento (Bond10G) para subredes independientes. Si las interfaces de Bond1G y Bond10G se configuran para la misma subred, podrían ocurrir problemas de enrutamiento cuando el tráfico de almacenamiento se envía a través de la interfaz de Bond1G. Si tiene que usar la misma subred para el tráfico de gestión y de almacenamiento, configure manualmente el tráfico de gestión para que use la interfaz de Bond10G. Puede hacer esto por cada nodo utilizando la página **Configuración de clúster** de la interfaz de usuario por nodo.

Pasos

1. En una ventana del navegador, introduzca la dirección IP de DHCP de un nodo.

   Se debe añadir la extensión `:442` para acceder al nodo; por ejemplo, https://172.25.103.6:442.

   La ficha **Configuración de red** se abre con la sección **Bond1G**.

2. Especifique las opciones de configuración de la red de gestión 1G.
3. Haga clic en **aplicar cambios**.
4. Haga clic en **Bond10G** para mostrar la configuración de la red de almacenamiento 10G.
5. Especifique las opciones de configuración de la red de almacenamiento 10G.
6. Haga clic en **aplicar cambios**.
7. Haga clic en **Configuración de clúster**.
8. Escriba el nombre de host de la red 10G.
9. Introduzca el nombre del clúster.

   Este nombre debe añadirse a la configuración de todos los nodos para poder crear un clúster. Todos los nodos de un clúster deben tener exactamente los mismos nombres en clúster. Los nombres de clúster distinguen mayúsculas de minúsculas.

10. Haga clic en **aplicar cambios**.

Con la TUI, configure un nodo de almacenamiento

La interfaz de usuario de terminal (TUI) se puede usar para realizar una configuración inicial de los nodos nuevos.

Debe configurar las interfaces de Bond1G (Management) y Bond10G (almacenamiento) para subredes independientes. Si las interfaces de Bond1G y Bond10G se configuran para la misma subred, podrían ocurrir problemas de enrutamiento cuando el tráfico de almacenamiento se envía a través de la interfaz de Bond1G. Si tiene que usar la misma subred para el tráfico de gestión y de almacenamiento, configure manualmente el tráfico de gestión para que use la interfaz de Bond10G. Puede hacer esto por cada nodo utilizando la página **Cluster** > **Nodes** de la interfaz de usuario de Element.

Pasos

1. Conecte un teclado y un monitor al nodo y, a continuación, active el nodo.

   El menú principal de la TUI de almacenamiento NetApp aparece en el terminal tty1.

Si el nodo no puede conectarse con el servidor de configuración, la TUI mostrará un mensaje de error. Compruebe la conexión del servidor de configuración o la conexión de red para solucionar el error.

2. Seleccione **Red** > **Configuración de red**.

Para desplazarse por el menú, pulse las teclas de flecha hacia arriba o hacia abajo. Para desplazarse a otro botón o a los campos desde los botones, pulse **Tab**. Para desplazarse por los campos, use las teclas de flecha arriba o abajo.

3. Seleccione **Bond1G (Gestión)** o **Bond10G (almacenamiento)** para configurar la configuración de red 1G y 10G para el nodo.
4. Para los campos modo Bond y Estado, pulse **TAB** para seleccionar el botón Ayuda e identificar las opciones disponibles.

   Todos los nodos de un clúster deben tener exactamente los mismos nombres en clúster. Los nombres de clúster distinguen mayúsculas de minúsculas. Si hay un servidor DHCP ejecutándose en la red con direcciones IP disponibles, aparecerá la dirección 1GbE en el campo Address.

5. Pulse **Tab** para seleccionar el botón **OK** y guardar los cambios.

   El nodo cambia al estado pendiente y puede añadirse a un clúster existente o a otro nuevo.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Cree un clúster de almacenamiento de

Es posible crear un clúster de almacenamiento después de configurar todos los nodos individuales. Cuando se crea un clúster, también se crea automáticamente una cuenta de usuario de administrador de clúster. El administrador de clúster tiene permiso para gestionar todos los atributos del clúster y crear otras cuentas de administrador de clúster.

Lo que necesitará

- Instaló el nodo de gestión.
- Configuró todos los nodos individuales.

Acerca de esta tarea

Durante la configuración de nodos nuevos, se asignan direcciones IP de gestión (MIP) 1G o 10G a cada nodo. Debe usar una de las direcciones IP de nodo que se han creado durante la configuración para abrir la página Create a New Cluster. La dirección IP que utilice dependerá de la red que haya elegido para la gestión del clúster.

Si desea habilitar toda la clúster "cifrado de software en reposo", debe crear el clúster mediante "CreateCluster" En su lugar, el método API y cambie el parámetro enableSoftwareEncryptionAtRest a. `true`. Después de habilitar el cifrado de software en reposo, no se puede deshabilitar en el clúster. El cifrado basado en hardware en reposo puede realizarse "activado y desactivado" tras crear el clúster.

Al crear un nuevo clúster, tenga en cuenta lo siguiente:

- Si se utilizan nodos de almacenamiento que residen en un chasis compartido, es posible que se desee considerar el diseño de la protección contra fallos en el nivel del chasis mediante la función de dominios de protección.
- Si un chasis compartido no está en uso, puede definir un diseño de dominio de protección personalizado.

Pasos

1. En una ventana del navegador, introduzca `https://MIP:443`, Donde MIP es la dirección IP del nodo de gestión.
2. En Create a New Cluster, introduzca la siguiente información:
   - Management VIP: IP virtual enrutable en una red 1GbE o 10GbE para tareas de gestión de red.

     Es posible crear un nuevo clúster mediante la dirección IPv4 o IPv6.

   - ISCSI (Storage) VIP: IP virtual en la red 10GbE para tareas de almacenamiento y detección iSCSI.

     No se puede cambiar la dirección MVIP, la SVIP o el nombre del clúster después de crear el clúster.

   - User name: El nombre de usuario del administrador de clúster principal para el acceso autenticado al clúster. Debe guardar el nombre de usuario para consultarlo más adelante.

     Se pueden utilizar letras mayúsculas y minúsculas, caracteres especiales y números para el nombre de usuario y la contraseña.

   - Password: Contraseña para el acceso autenticado al clúster. Debe guardar la contraseña para poder consultarla en el futuro. La protección de datos bidireccional está habilitada de forma predeterminada. No puede cambiar esta configuración.
3. Lea el contrato de licencia para usuario final y seleccione **Acepto**.
4. **Opcional**: En la lista Nodes, asegúrese de que las casillas de verificación de los nodos que no deben incluirse en el clúster no están seleccionadas.
5. Seleccione **Crear clúster**.

   En función del número de nodos que se incluyan, el sistema podría tardar varios minutos en crear el clúster. En una red que se haya configurado correctamente, la creación de un clúster pequeño de cinco nodos debería tardar menos de un minuto. Una vez que se haya creado el clúster, la ventana Create a New Cluster se redirige a la dirección URL de MVIP del clúster y muestra la interfaz de usuario de Element.

Si quiere más información

- "Gestionar el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Acceda a la interfaz de usuario del software Element

Es posible acceder a la interfaz de usuario de Element mediante la dirección IP virtual de gestión (MVIP) del nodo de clúster principal.

Debe asegurarse de que se hayan deshabilitado los bloqueadores de ventanas emergentes y la configuración de NoScript en el navegador.

Según la configuración durante la creación del clúster, es posible acceder a la interfaz de usuario mediante la dirección IPv4 o IPv6.

Pasos

1. Elija una de las siguientes opciones:
   - IPv6: Introduzca `https://[IPv6_MVIP_address]`. Por ejemplo:

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

   - IPv4: Introduzca `https://[IPv4 MVIP address]`. Por ejemplo:

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

2. En el caso de DNS, introduzca el nombre de host.
3. Haga clic en los mensajes de certificados de autenticación que aparezcan.

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Añada unidades a un clúster

Cuando se añade un nodo al clúster o se instalan unidades nuevas en un nodo existente, las unidades se registran automáticamente como Available. Las unidades se deben añadir al clúster mediante la interfaz de usuario o la API de Element antes de que puedan participar en el clúster.

Las unidades no se muestran en la lista Available Drives cuando se dan las siguientes condiciones:

- Las unidades se encuentran en el estado Active, Removing, Erasing o Failed.
- El estado del nodo del que forma parte la unidad es Pending.

Pasos

1. En la interfaz de usuario de Element, seleccione **Cluster** > **Drives**.
2. Haga clic en **disponible** para ver la lista de unidades disponibles.
3. Debe realizar una de las siguientes acciones:
   - Para agregar unidades individuales, haga clic en el icono **acciones** de la unidad que desea agregar y haga clic en **Agregar**.
   - Para añadir varias unidades, active las casillas de verificación de las unidades que desee agregar, haga clic en **acciones masivas** y haga clic en **Agregar**.

```
== 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^]
```

Configure un clúster con nodos Fibre Channel

Configure un nodo Fibre Channel

Los nodos Fibre Channel permiten conectar el clúster de a una estructura de red Fibre Channel. Los nodos Fibre Channel se añaden en parejas y funcionan en modo activo-activo (todos los nodos procesan de forma activa tráfico para el clúster). Los clústeres que ejecutan el software Element de la versión 9.0 y versiones posteriores admiten hasta cuatro nodos, mientras que los clústeres que ejecutan versiones anteriores admiten un máximo de dos nodos.

Antes de configurar un nodo Fibre Channel, debe asegurarse de que se cumplan las siguientes condiciones:

- Se conectan al menos dos nodos Fibre Channel a switches Fibre Channel.
- Todos los puertos Fibre Channel de SolidFire deben estar conectados a la estructura Fibre Channel. Las cuatro conexiones de red Bond10G de SolidFire se deben conectar en un grupo de vínculos LACP en el nivel del switch. Esto permitirá obtener el mejor rendimiento general de los sistemas Fibre Channel.
- Revise y valide las mejores prácticas para los clústeres de Fibre Channel incluidos en este artículo de la base de conocimientos de NetApp.

  "Mejores prácticas para el clúster FC de SolidFire"

Los pasos de configuración de red y clúster son los mismos para los nodos Fibre Channel y los nodos de almacenamiento.

Cuando crea un clúster nuevo con nodos Fibre Channel y nodos de almacenamiento SolidFire, las direcciones de nombre de puerto WWPN para los nodos están disponibles en la interfaz de usuario de Element. Puede usar las direcciones WWPN para dividir el switch de Fibre Channel en zonas.

Los WWPN se registran en el sistema cuando se crea un clúster nuevo con nodos. En la interfaz de usuario de Element, puede encontrar las direcciones WWPN desde la columna WWPN de la pestaña puertos FC, a la

que se accede desde la pestaña Cluster.

Obtenga más información

Añada nodos Fibre Channel a un clúster

Cree un nuevo clúster con nodos Fibre Channel

Cree un nuevo clúster con nodos Fibre Channel

Es posible crear un nuevo clúster de después de configurar los nodos Fibre Channel individuales. Cuando se crea un clúster, también se crea automáticamente una cuenta de usuario de administrador de clúster. El administrador de clúster tiene permiso para gestionar todos los atributos del clúster y crear otras cuentas de administrador de clúster.

Durante la configuración de nodos nuevos, se asignan direcciones IP de gestión (MIP) 1G o 10G a cada nodo. Debe usar una de las direcciones IP de nodo que se han creado durante la configuración para abrir la página Create a New Cluster. La dirección IP que utilice dependerá de la red que haya elegido para la gestión del clúster.

Lo que necesitará

Configuró los nodos Fibre Channel individuales.

Pasos

1. En una ventana del navegador, introduzca la dirección MIP de un nodo.
2. En Create a New Cluster, introduzca la siguiente información:
   - Management VIP: IP virtual enrutable en una red 1GbE o 10GbE para tareas de gestión de red.
   - ISCSI (Storage) VIP: IP virtual en la red 10GbE para tareas de almacenamiento y detección iSCSI.

     No se puede cambiar la SVIP una vez que se ha creado el clúster.

   - User name: El nombre de usuario del administrador de clúster principal para el acceso autenticado al clúster. Debe guardar el nombre de usuario para consultarlo más adelante.

     Se pueden utilizar letras mayúsculas y minúsculas, caracteres especiales y números para el nombre de usuario.

   - Password: Contraseña para el acceso autenticado al clúster. Debe guardar el nombre de usuario para consultarlo más adelante. La protección de datos bidireccional está habilitada de forma predeterminada. No puede cambiar esta configuración.
3. Lea el Contrato de licencia para el usuario final y haga clic en **Acepto**.
4. **Opcional**: En la lista Nodes, asegúrese de que las casillas de verificación de los nodos que no deben incluirse en el clúster no están seleccionadas.
5. Haga clic en **Crear clúster**.

   En función del número de nodos que se incluyan, el sistema podría tardar varios minutos en crear el clúster. En una red que se haya configurado correctamente, la creación de un clúster pequeño de cinco nodos debería tardar menos de un minuto. Una vez que se haya creado el clúster, la ventana Create a New Cluster se redirige a la dirección URL de MVIP del clúster y muestra la interfaz de usuario web de de.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Añada nodos Fibre Channel a un clúster

Es posible añadir nodos Fibre Channel a un clúster cuando se necesita más almacenamiento o durante la creación del clúster. Los nodos Fibre Channel requieren una configuración inicial cuando se conectan por primera vez. Una vez que se configura, aparece en la lista de nodos pendientes y puede añadirlos a un clúster.

La versión de software de cada nodo Fibre Channel en un clúster tiene que ser compatible. Cuando se añade un nodo Fibre Channel a un clúster, el clúster instala la versión del clúster de Element en el nodo nuevo según sea necesario.

Pasos

1. Seleccione **Cluster** > **Nodes**.
2. Haga clic en **pendiente** para ver la lista de nodos pendientes.
3. Debe realizar una de las siguientes acciones:
   - Para agregar nodos individuales, haga clic en el icono **acciones** del nodo que desea agregar.
   - Para añadir varios nodos, active la casilla de los nodos que desee agregar y, a continuación, **acciones masivas**.

   > Si el nodo que desea añadir tiene una versión de elemento diferente a la versión que se ejecuta en el clúster, el clúster actualiza de forma asíncrona el nodo a la versión de Element que se ejecuta en el maestro de clústeres. Después de que se actualiza el nodo, se añade automáticamente al clúster. Durante este proceso asíncrono, el nodo tendrá el estado pendingActive.

4. Haga clic en **Agregar**.

   El nodo aparece en la lista de nodos activos.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Configure zonas para los nodos Fibre Channel

Cuando crea un clúster de nuevo con nodos Fibre Channel y nodos de almacenamiento de SolidFire, las direcciones de nombre de puerto WWPN para los nodos están disponibles en la interfaz de usuario web de. Puede usar las direcciones WWPN para dividir el switch de Fibre Channel en zonas.

Los WWPN se registran en el sistema cuando se crea un clúster nuevo con nodos. En la interfaz de usuario de Element, puede encontrar las direcciones WWPN desde la columna WWPN de la pestaña puertos FC, a la que se accede desde la pestaña Cluster.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Cree un grupo de acceso de volúmenes para clientes Fibre Channel

Los grupos de acceso de volúmenes permiten la comunicación entre volúmenes y clientes de Fibre Channel en un sistema de almacenamiento SolidFire. La asignación de iniciadores de cliente Fibre Channel (WWPN) a los volúmenes en un grupo de acceso de volúmenes permite operaciones de E/S de datos seguras entre una red Fibre Channel y un volumen de SolidFire.

También se pueden añadir iniciadores iSCSI a un grupo de acceso de volúmenes para permitir el acceso de los iniciadores a los mismos volúmenes del grupo de acceso de volúmenes.

Pasos

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en **Crear grupo de acceso**.
3. Escriba un nombre para el grupo de acceso de volúmenes en el campo **Nombre**.
4. Seleccione y añada los iniciadores Fibre Channel de la lista **Unbound Fibre Channel Initiators**.

   Puede añadir o eliminar iniciadores más adelante.

5. **Opcional:** Seleccione y añada un iniciador iSCSI de la lista **Initiators**.
6. Para adjuntar volúmenes al grupo de acceso, realice los siguientes pasos:
   a. Seleccione un volumen de la lista **Volumes**.
   b. Haga clic en **Adjuntar volumen**.
7. Haga clic en **Crear grupo de acceso**.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Determine qué componentes de SolidFire instalar

Tal vez desee comprobar qué componentes de SolidFire, como el nodo de gestión, Active IQ y el agente de supervisión de NetApp (NMA), se debería instalar, en función de las opciones de configuración e implementación.

La siguiente tabla enumera los componentes adicionales e indica si debe instalarlos.

Componente	Clúster de almacenamiento de SolidFire independiente	Clúster de NetApp HCI
Nodo de gestión	Recomendado	Instalado de forma predeterminada, necesario
Active IQ	Recomendado*	Recomendado*
Agente de supervisión de NetApp	No admitido	Recomendado

*Se requiere Active IQ para los clústeres de almacenamiento SolidFire con licencia por capacidad.

Pasos

1. Determine qué componentes se deben instalar.
2. Complete la instalación de acuerdo con "instale el nodo de gestión" procedimiento.

> Para configurar Active IQ, utilice `--telemetry_active` Parámetro en el script de configuración para habilitar la recogida de datos para análisis por parte de Active IQ.

3. Para obtener información sobre el agente de supervisión de NetApp, consulte este tema "procedimiento".

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Configure un nodo de gestión

Puede instalar el nodo de gestión del software (mNode) de NetApp Element para actualizar y proporcionar servicios del sistema, gestionar activos y configuraciones del clúster, ejecutar pruebas y utilidades del sistema y habilitar el acceso de soporte de NetApp para la solución de problemas.

1. Consulte "instale el nodo de gestión" documentación.

> Para configurar Active IQ, utilice `--telemetry_active` Parámetro en el script de configuración para habilitar la recogida de datos para análisis por parte de Active IQ.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Configure el acceso completo a la interfaz de usuario web de Nombre de dominio

El almacenamiento all-flash de SolidFire con el software NetApp Element 12.2 o posterior le permite acceder a las interfaces web de los clústeres de almacenamiento usando el nombre de dominio completo (FQDN). Si desea usar el FQDN para acceder a interfaces de usuario web como la interfaz de usuario web de Element, la interfaz de usuario por nodo o la interfaz de usuario de nodo de gestión, primero debe añadir un ajuste de clúster de almacenamiento para identificar el FQDN que utiliza el clúster.

Este proceso permite al clúster redirigir correctamente una sesión de inicio de sesión y mejora la integración con servicios externos como gestores de claves y proveedores de identidades para la autenticación de múltiples factores.

Lo que necesitará

- Esta función requiere Element 12.2 o posterior.
- Para configurar esta función con las API REST de NetApp Hybrid Cloud Control, se requieren servicios de gestión 2.15 o posteriores.
- Para configurar esta función con la interfaz de usuario de control del cloud híbrido de NetApp se requieren servicios de gestión 2.19 o posteriores.
- Para utilizar las API DE REST, debe haber puesto en marcha un nodo de gestión que ejecuta la versión 11.5 o una versión posterior.
- Necesita nombres de dominio completos para el nodo de gestión y cada clúster de almacenamiento que se resuelven correctamente con la dirección IP del nodo de gestión y cada dirección IP de clúster de almacenamiento de.

Puede configurar o quitar el acceso de interfaz de usuario web FQDN de NetApp Hybrid Cloud Control y la API DE REST. También puede solucionar problemas de RFQ configuradas incorrectamente.

- Configure el acceso de interfaz de usuario web de FQDN mediante NetApp Hybrid Cloud Control
- Configure el acceso de interfaz de usuario web del FQDN mediante la API DE REST
- Elimine el acceso de interfaz de usuario web de FQDN mediante el control de cloud híbrido de NetApp
- Quite el acceso de interfaz de usuario web del FQDN mediante la API DE REST
- Resolución de problemas

Configure el acceso de interfaz de usuario web de FQDN mediante NetApp Hybrid Cloud Control

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

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

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.

3. Seleccione el icono de menú en la parte superior derecha de la página.
4. Seleccione **Configurar**.
5. En el panel **nombres de dominio completos**, seleccione **Configurar**.
6. En la ventana que aparece, introduzca las FQDN para el nodo de administración y cada clúster de almacenamiento.
7. Seleccione **Guardar**.

   El panel **nombres de dominio completos** enumera cada clúster de almacenamiento con su MVIP y FQDN asociados.

> En el panel **nombres de dominio completos** sólo aparecen los clústeres de almacenamiento conectados con el conjunto FQDN.

Configure el acceso de interfaz de usuario web del FQDN mediante la API DE REST

Pasos

1. Asegúrese de que los nodos de almacenamiento de Element y mNode tengan el DNS configurado correctamente para el entorno de red para que se puedan resolver las FQDN del entorno. Para establecer DNS, vaya a la interfaz de usuario por nodo para nodos de almacenamiento y al nodo de gestión y seleccione **Configuración de red** > **Red de administración**.
   a. IU por nodo para nodos de almacenamiento: `https://<storage_node_management_IP>:442`
   b. IU por nodo para el nodo de gestión: `https://<management_node_IP>:442`
2. Cambie la configuración del clúster de almacenamiento mediante la API de Element.
   a. Acceda a la API de Element y cree la siguiente preferencia de interfaz del clúster mediante el "CreateClusterInterfacePreference" Método API, inserte el FQDN de MVIP del clúster para el valor de preferencia:
      - Nombre: `mvip_fqdn`
      - Valor: `Fully Qualified Domain Name for the Cluster MVIP`

        En este ejemplo, FQDN=storagecluster.my.org:

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

3. Cambie la configuración del nodo de gestión con la API DE REST en el nodo de gestión:
   a. Acceda a la interfaz de usuario de API DE REST para el nodo de gestión. Para ello, introduzca la dirección IP del nodo de gestión seguida de `/mnode/2/`

      Por ejemplo:

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

   a. Haga clic en **autorizar** o en cualquier icono de bloqueo e introduzca el nombre de usuario y la

contraseña del clúster.

b. Introduzca el ID de cliente as `mnode-client`.

c. Haga clic en **autorizar** para iniciar la sesión y, a continuación, cerrar la ventana.

d. En la lista de servidores, seleccione `mnode2`.

e. Haga clic en **GET /settings**.

f. Haga clic en **probar**.

g. Haga clic en **Ejecutar**.

h. Registre cualquier configuración de proxy informada en el cuerpo de respuesta.

i. Haga clic en **PONER/configurar**.

j. Haga clic en **probar**.

k. En el área cuerpo de la solicitud, introduzca el nombre de dominio completo del nodo de gestión como valor para `mnode_fqdn` parámetro.

l. Introduzca los valores de configuración de proxy que haya registrado anteriormente en los parámetros restantes del cuerpo de la solicitud. Si deja vacíos los parámetros del proxy o no los incluye en el cuerpo de la solicitud, se eliminará la configuración del proxy existente.

m. Haga clic en **Ejecutar**.

Elimine el acceso de interfaz de usuario web de FQDN mediante el control de cloud híbrido de NetApp

Puede usar este procedimiento para quitar el acceso web FQDN para el nodo de gestión y los clústeres de almacenamiento.

Pasos

1. En el panel **nombres de dominio completos**, seleccione **Editar**.
2. En la ventana resultante, elimine el contenido en el campo de texto **FQDN**.
3. Seleccione **Guardar**.

La ventana se cierra y el FQDN ya no aparece en el panel **nombres de dominio completos**.

Quite el acceso de interfaz de usuario web del FQDN mediante la API DE REST

Pasos

1. Cambie la configuración del clúster de almacenamiento mediante la API de Element.

a. Acceda a la API de Element y elimine la siguiente preferencia de interfaz de clúster mediante el `DeleteClusterInterfacePreference` Método API:

- Nombre: `mvip_fqdn`

Por ejemplo:

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

2. Cambie la configuración del nodo de gestión con la API DE REST en el nodo de gestión:
   a. Acceda a la interfaz de usuario de API DE REST para el nodo de gestión. Para ello, introduzca la dirección IP del nodo de gestión seguida de `/mnode/2/`. Por ejemplo:

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

   b. Seleccione **autorizar** o cualquier icono de bloqueo e introduzca el nombre de usuario y la contraseña del clúster de elementos.
   c. Introduzca el ID de cliente as `mnode-client`.
   d. Seleccione **autorizar** para iniciar una sesión.
   e. Cierre la ventana.
   f. Seleccione **COLOCAR /settings**.
   g. Seleccione **probar**.
   h. En el área cuerpo de la solicitud, no introduzca un valor para `mnode_fqdn` parámetro. Especifique también si se debe utilizar el proxy (`true` o. `false`) para `use_proxy` parámetro.

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

   i. Seleccione **Ejecutar**.

Resolución de problemas

Si las FQDN están configuradas incorrectamente, es posible que tenga problemas para acceder al nodo de administración, a un clúster de almacenamiento o a ambos. Utilice la siguiente información como ayuda para solucionar el problema.

Problema	Causa	Resolución
• Se obtiene un error del explorador al intentar acceder al nodo de gestión o al clúster de almacenamiento mediante el FQDN. • No puede iniciar sesión en el nodo de gestión ni en el clúster de almacenamiento mediante una dirección IP.	El nombre de dominio completo del nodo de gestión y el nombre de dominio completo del clúster de almacenamiento están configurados incorrectamente.	Use las instrucciones de API DE REST que aparecen en esta página para quitar las opciones de FQDN del nodo de gestión y del clúster de almacenamiento y volver a configurarlos.

Problema	Causa	Resolución
• Se obtiene un error del explorador al intentar acceder al FQDN del clúster de almacenamiento. • No puede iniciar sesión en el nodo de gestión ni en el clúster de almacenamiento mediante una dirección IP.	El nombre de dominio completo del nodo de gestión está configurado correctamente, pero el nombre de dominio completo del clúster de almacenamiento está configurado incorrectamente.	Use las instrucciones de API DE REST que aparecen en esta página para quitar la configuración de FQDN del clúster de almacenamiento y volver a configurarlos
• Obtiene un error del explorador al intentar acceder al FQDN del nodo de gestión. • Puede iniciar sesión en el nodo de gestión y el clúster de almacenamiento con una dirección IP.	El nombre de dominio completo del nodo de gestión está configurado incorrectamente, pero el nombre de dominio completo del clúster de almacenamiento está configurado correctamente.	Inicie sesión en NetApp Hybrid Cloud Control para corregir los ajustes FQDN del nodo de gestión en la interfaz de usuario o utilice las instrucciones API DE REST en esta página para corregir los ajustes.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Lo siguiente

Después de configurar el software Element, es posible gestionar el almacenamiento completando algunas de las siguientes opciones:

- "Acceda a la interfaz de usuario del software Element"
- "Configure las opciones del sistema SolidFire después de la implementación"
- "Gestionar cuentas"
- "Gestione su sistema"
- "Gestione volúmenes y volúmenes virtuales"
- "Proteja sus datos"
- "Solucionar los problemas del sistema"

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"
- "Plugin de NetApp Element para vCenter Server"

Gestionar el almacenamiento con el software Element

Utilice el software Element para configurar almacenamiento SolidFire, supervisar la capacidad y el rendimiento del clúster y gestionar la actividad de almacenamiento en una infraestructura multi-tenant.

Element es el sistema operativo de almacenamiento como pieza central de un clúster de SolidFire. El software Element se ejecuta de forma independiente en todos los nodos del clúster y permite que los nodos del clúster combinen recursos y presenten como un único sistema de almacenamiento a clientes externos. El software Element es responsable de toda la coordinación, escalado y gestión del clúster en su conjunto.

La interfaz de software se creó sobre la API de Element.

- "Acceda a la interfaz de usuario del software Element"
- "Configure las opciones del sistema SolidFire después de la implementación"
- "Actualice los componentes del sistema de almacenamiento"
- "Use las opciones básicas en la interfaz de usuario del software Element"
- "Gestionar cuentas"
- "Gestione su sistema"
- "Gestione volúmenes y volúmenes virtuales"
- "Proteja sus datos"
- "Solucionar los problemas del sistema"

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Acceda a la interfaz de usuario del software Element

Es posible acceder a la interfaz de usuario de Element mediante la dirección IP virtual de gestión (MVIP) del nodo de clúster principal.

Debe asegurarse de que se hayan deshabilitado los bloqueadores de ventanas emergentes y la configuración de NoScript en el navegador.

Según la configuración durante la creación del clúster, es posible acceder a la interfaz de usuario mediante la dirección IPv4 o IPv6.

1. Elija una de las siguientes opciones:
   - IPv6: Introduzca la dirección https://[IPv6 MVIP] por ejemplo:

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

- IPv4: Introduzca la dirección https://[IPv4 MVIP] por ejemplo:

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

2. En el caso de DNS, introduzca el nombre de host.
3. Haga clic en los mensajes de certificados de autenticación que aparezcan.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Configure las opciones del sistema SolidFire después de la implementación

Después de configurar el sistema SolidFire, quizás desee ejecutar algunas tareas opcionales.

Si cambia las credenciales en el sistema, se recomienda conocer el impacto sobre otros componentes.

Además, es posible configurar la autenticación multifactor, la gestión de claves externa y la seguridad de estándar de procesamiento de información federal (FIPS). También debe revisar las contraseñas cuando sea necesario.

Obtenga más información

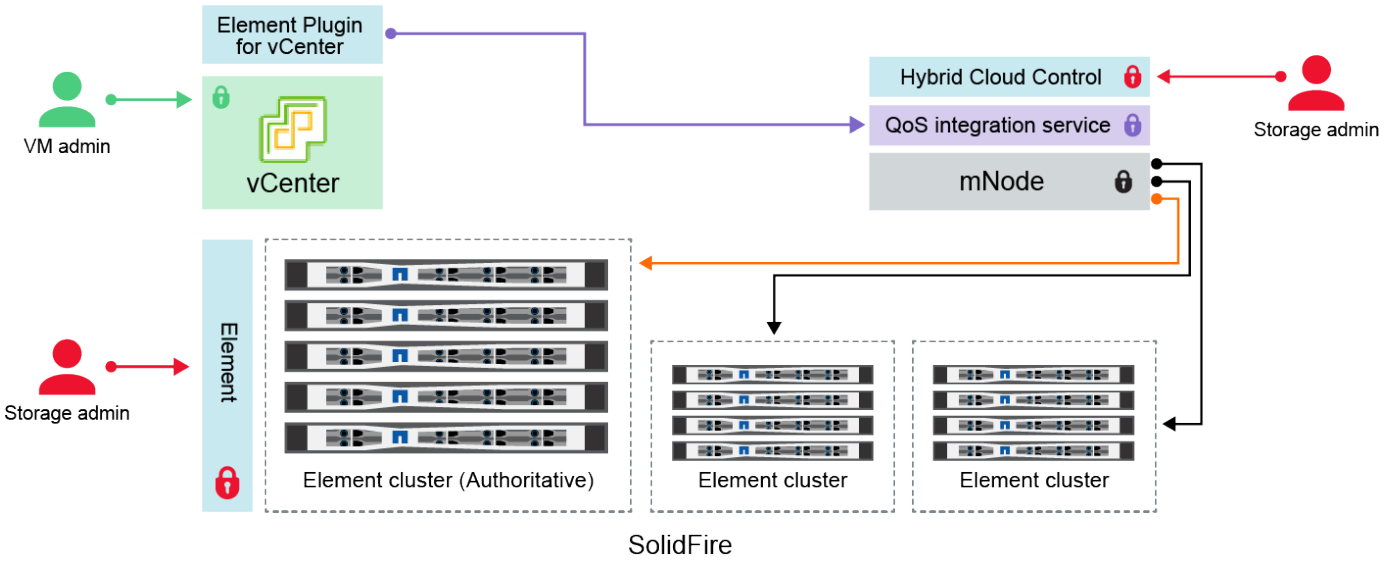
- "Cambie las credenciales en NetApp HCI y SolidFire de NetApp"
- "Cambie el certificado SSL predeterminado del software Element"
- "Cambie la contraseña de IPMI para los nodos"
- "Habilite la autenticación multifactor"
- "Comience con la gestión de claves externas"
- "Cree un clúster que admita unidades FIPS"

Cambie las credenciales en NetApp HCI y SolidFire de NetApp

Según las políticas de seguridad de la organización que implementó NetApp HCI o SolidFire de NetApp, los cambios de credenciales o contraseñas suelen formar parte de las prácticas de seguridad. Antes de cambiar las contraseñas, debe tener en cuenta el impacto sobre otros componentes de software en la implementación.

Si cambia las credenciales de un componente de una implementación de NetApp HCI o SolidFire de NetApp, la siguiente tabla proporciona directrices sobre el impacto en otros componentes.

Interacciones de componentes de NetApp
SolidFire:



Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
Credenciales de Element	**Se aplica a**: NetApp HCI y SolidFire Los administradores utilizan estas credenciales para iniciar sesión en: • La interfaz de usuario de Element en el clúster de almacenamiento de Element • Control del cloud híbrido en el nodo de gestión (mnode) Cuando Hybrid Cloud Control gestiona varios clústeres de almacenamiento, solo acepta las credenciales de administrador de los clústeres de almacenamiento, conocidas como el *autoritativo cluster* para el que se configuró mnode inicialmente. Para los clústeres de almacenamiento que se añadieron más adelante al control del cloud híbrido, el nodo mnode almacena de forma segura las credenciales de administración. Si se modifican las credenciales para clústeres de almacenamiento añadidos posteriormente, también se deben actualizar las credenciales en mnode con la API mnode.	• "Actualice las contraseñas de administrador del clúster de almacenamiento." • Actualice las credenciales de administrador del clúster de almacenamiento en el nodo mmediante el "API modifyclusteradmin".

Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
Credenciales de inicio de sesión único de vSphere 	**Se aplica a**: Sólo NetApp HCI Los administradores utilizan estas credenciales para iniciar sesión en VMware vSphere Client. Cuando vCenter forma parte de la instalación de NetApp HCI, las credenciales se configuran en el motor de implementación de NetApp como lo siguiente: • nombreusuario@vsphere.locloc l con la contraseña especificada, y. • administrator@vsphere.locloc l con la contraseña especificada. Cuando se usa una instancia existente de vCenter para poner en marcha NetApp HCI, los administradores DE TI de VMware gestionan las credenciales de inicio de sesión único de vSphere.	"Actualice las credenciales de vCenter y ESXi".
Credenciales del controlador de administración de la placa base (BMC) 	**Se aplica a**: Sólo NetApp HCI Los administradores utilizan estas credenciales para iniciar sesión en el BMC de los nodos de computación de NetApp en una implementación de NetApp HCI. El BMC proporciona funcionalidades básicas de supervisión de hardware y consola virtual. Las credenciales de BMC (denominadas en ocasiones *IPMI*) para cada nodo de computación de NetApp se almacenan de forma segura en el nodo men las puestas en marcha de NetApp HCI. Control de cloud híbrido de NetApp usa las credenciales de BMC en una capacidad de cuenta de servicio para comunicarse con el BMC en los nodos de computación durante las actualizaciones del firmware de los nodos de computación. Cuando se cambian las credenciales del BMC, también se deben actualizar las credenciales de los nodos de computación respectivos en el mnode para conservar todas las funciones de Hybrid Cloud Control.	• "Configure IPMI para cada nodo en NetApp HCI". • Para los nodos H410C, H610C y H615C, "Cambie la contraseña de IPMI predeterminada". • Para nodos H410S y H610S, "Cambiar la contraseña predeterminada de IPM". • "Cambie las credenciales de BMC en el nodo de gestión".

Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
Credenciales de ESXi	**Se aplica a**: Sólo NetApp HCI Los administradores pueden iniciar sesión en hosts ESXi mediante SSH o la DCUI local con una cuenta raíz local. En implementaciones de NetApp HCI, el nombre de usuario es "raíz" y la contraseña se especificó durante la instalación inicial de ese nodo de computación en el motor de puesta en marcha de NetApp. Las credenciales raíz de ESXi para cada nodo de computación de NetApp se almacenan de forma segura en mnode en puestas en marcha de NetApp HCI. Hybrid Cloud Control de NetApp utiliza las credenciales en una capacidad de cuenta de servicio para comunicarse con hosts ESXi directamente durante las actualizaciones del firmware de los nodos de computación y las comprobaciones del estado. Cuando un administrador de VMware cambia las credenciales raíz de ESXi, las credenciales de los nodos de computación respectivos deben actualizarse en el mnode para mantener la funcionalidad de control de cloud híbrido.	"Actualice las credenciales de para hosts ESXi y vCenter".
Contraseña de integración de la calidad de servicio	**Se aplica a**: NetApp HCI y opcional en SolidFire No se utiliza para inicios de sesión interactivos por parte de administradores. La integración de calidad de servicio entre VMware vSphere y el software Element se habilita mediante: • Plugin de Element para vCenter Server y. • Servicio QoS en el mnode. Para la autenticación, el servicio QoS utiliza una contraseña que se utiliza exclusivamente en este contexto. La contraseña de calidad de servicio se especifica durante la instalación inicial del plugin de Element para vCenter Server, o bien se genera automáticamente durante la implementación de NetApp HCI. Ningún impacto sobre otros componentes.	"Actualice las credenciales de QoSSIOC en el plugin de NetApp Element para vCenter Server". La contraseña de SIOC del plugin de NetApp Element para vCenter Server también se conoce como *QoSSIOC Password*. Revise el {URL-pico}[plugin de Element para vCenter Server KB].

Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
Credenciales de vCenter Service Appliance	**Se aplica a**: NetApp HCI solo si configura el motor de puesta en marcha de NetApp Los administradores pueden iniciar sesión en las máquinas virtuales del dispositivo de vCenter Server. En implementaciones de NetApp HCI, el nombre de usuario es "raíz" y la contraseña se especificó durante la instalación inicial de ese nodo de computación en el motor de puesta en marcha de NetApp. Según la versión de VMware vSphere implementada, algunos administradores del dominio de inicio de sesión único de vSphere también pueden iniciar sesión en el dispositivo. Ningún impacto sobre otros componentes.	No es necesario realizar cambios.
Credenciales de administrador del nodo de gestión de NetApp	**Se aplica a**: NetApp HCI y opcional en SolidFire Los administradores pueden iniciar sesión en las máquinas virtuales del nodo de gestión de NetApp para obtener una configuración avanzada y solucionar problemas. Según la versión del nodo de gestión puesta en marcha, el inicio de sesión a través de SSH no se habilita de forma predeterminada. En implementaciones de NetApp HCI, el usuario y la contraseña fueron especificados durante la instalación inicial de ese nodo de computación en el motor de puesta en marcha de NetApp. Ningún impacto sobre otros componentes.	No es necesario realizar cambios.

Obtenga más información

- "Cambie el certificado SSL predeterminado del software Element"
- "Cambie la contraseña de IPMI para los nodos"
- "Habilite la autenticación multifactor"
- "Comience con la gestión de claves externas"
- "Cree un clúster que admita unidades FIPS"

Cambie el certificado SSL predeterminado del software Element

Puede cambiar el certificado SSL predeterminado y la clave privada del nodo de almacenamiento del clúster mediante la API de NetApp Element.

Cuando se crea un clúster de software de NetApp Element, el clúster crea un certificado único de capa de sockets seguros (SSL) con firma automática y una clave privada que se utiliza para todas las comunicaciones HTTPS a través de la interfaz de usuario de Element, la interfaz de usuario por nodo o las API. El software Element admite certificados autofirmados, así como certificados que una entidad de certificación (CA) de confianza emite y verifica.

Puede utilizar los siguientes métodos API para obtener más información sobre el certificado SSL predeterminado y realizar cambios.

- **GetSSLCertificate**

  Puede utilizar el "Método GetSSLCertificate" Para recuperar información acerca del certificado SSL instalado actualmente, incluidos todos los detalles del certificado.

- **SetSSLCertificate**

  Puede utilizar el "Método SetSSLCertificate" Para establecer los certificados SSL por clúster y por nodo en el certificado y la clave privada que suministre. El sistema valida el certificado y la clave privada para evitar que se aplique un certificado no válido.

- **RemoveSSLCertificate**

  La "Método RemoveSSLCertificate" Quita el certificado SSL y la clave privada instalados actualmente. A continuación, el clúster genera un nuevo certificado autofirmado y una clave privada.

> El certificado SSL de clúster se aplica automáticamente a todos los nodos nuevos que se añaden al clúster. Cualquier nodo que se quite del clúster se revierte a un certificado autofirmado y toda la información de claves y certificados definidos por el usuario se elimina del nodo.

Obtenga más información

- "Cambie el certificado SSL predeterminado del nodo de gestión"
- "¿Cuáles son los requisitos para configurar certificados SSL personalizados en el software Element?"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Cambie la contraseña de IPMI predeterminada para los nodos

En cuanto tenga acceso IPMI remoto al nodo, puede cambiar la contraseña predeterminada del administrador de la interfaz de gestión de plataformas inteligentes (IPMI). Puede que desee hacerlo si se han actualizado alguna instalación.

Para obtener más información acerca de cómo configurar el acceso IPM para los nodos, consulte "Configure IPMI para cada nodo".

Puede cambiar la contraseña de IPM para estos nodos:

- Nodos H410S
- Nodos H610S

Cambie la contraseña de IPMI predeterminada para los nodos H410S

En cuanto configure el puerto de red IPMI, debe cambiar la contraseña predeterminada de la cuenta de administrador de IPMI en cada nodo de almacenamiento.

Lo que necesitará

Debe haber configurado la dirección IP de IPMI para cada nodo de almacenamiento.

Pasos

1. Abra un explorador web en un equipo que pueda acceder a la red de IPMI y vaya a la dirección IP de IPMI correspondiente al nodo.
2. Introduzca el nombre de usuario `ADMIN` y contraseña `ADMIN` en la solicitud de inicio de sesión de.
3. Después de iniciar sesión, haga clic en la ficha **Configuración**.
4. Haga clic en **usuarios**.
5. Seleccione la `ADMIN` Haga clic en **Modificar usuario**.
6. Seleccione la casilla de verificación **Cambiar contraseña**.
7. Introduzca una nueva contraseña en los campos **Contraseña** y **Confirmar contraseña**.
8. Haga clic en **Modificar** y, a continuación, haga clic en **Aceptar**.
9. Repita este procedimiento para todos los demás nodos H410S con contraseñas IPMI predeterminadas.

Cambie la contraseña de IPMI predeterminada para los nodos H610S

En cuanto configure el puerto de red IPMI, debe cambiar la contraseña predeterminada de la cuenta de administrador de IPMI en cada nodo de almacenamiento.

Lo que necesitará

Debe haber configurado la dirección IP de IPMI para cada nodo de almacenamiento.

Pasos

1. Abra un explorador web en un equipo que pueda acceder a la red de IPMI y vaya a la dirección IP de IPMI correspondiente al nodo.
2. Introduzca el nombre de usuario `root` y contraseña `calvin` en la solicitud de inicio de sesión de.
3. Después de iniciar sesión, haga clic en el icono de navegación del menú que aparece en la parte superior izquierda de la página para abrir el cajón de la barra lateral.
4. Haga clic en **Configuración**.
5. Haga clic en **Administración de usuarios**.
6. Seleccione el usuario **Administrador** de la lista.
7. Active la casilla de verificación **Cambiar contraseña**.
8. Introduzca una nueva contraseña segura en los campos **Contraseña** y **Confirmar contraseña**.
9. Haga clic en **Guardar** en la parte inferior de la página.
10. Repita este procedimiento para todos los demás nodos H610S con contraseñas de IPMI predeterminadas.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Use las opciones básicas en la interfaz de usuario del software Element

La interfaz de usuario web del software NetApp Element (interfaz de usuario de Element) permite supervisar y realizar tareas comunes en el sistema SolidFire.

Las opciones básicas incluyen ver comandos de API activados por actividad de la interfaz de usuario y proporcionar comentarios.

- "Ver la actividad de la API"
- "Iconos en la interfaz de Element"
- "Enviar comentarios"

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Ver la actividad de la API

El sistema Element usa la API de NetApp Element como base para sus funciones y funcionalidades. La interfaz de usuario de Element le permite ver diversos tipos de actividad de la API en tiempo real en el sistema conforme utiliza la interfaz. Con el registro de la API, puede ver la actividad de la API del sistema en segundo plano y la que ha iniciado el usuario, así como las llamadas API que se han hecho en la página que está viendo en ese momento.

Puede usar el registro de API para identificar qué métodos API se usan en determinadas tareas y cómo se usan los objetos y los métodos API para crear aplicaciones personalizadas.

Para obtener más información sobre cada método, consulte "Referencia de API del software Element".

1. En la barra de navegación de la interfaz de usuario de Element, haga clic en **API Log**.
2. Realice los siguientes pasos para modificar el tipo de actividad de API que se muestra en la ventana API Log:
   a. Seleccione **peticiones** para mostrar el tráfico de solicitud de API.
   b. Seleccione **respuestas** para mostrar el tráfico de respuesta de la API.
   c. Filtre los tipos de tráfico de API seleccionando una de las siguientes opciones:
      - **Usuario iniciado**: Tráfico API por sus actividades durante esta sesión de interfaz de usuario web.
      - * Sondeo de fondo*: Tráfico de API generado por la actividad del sistema en segundo plano.
      - **Página actual**: Tráfico de API generado por tareas en la página que está viendo actualmente.

Obtenga más información

- "Gestionar el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"

- "Plugin de NetApp Element para vCenter Server"

Tasa de actualización de la interfaz afectada por la carga del clúster

Dependiendo de los tiempos de respuesta de la API, el clúster podría ajustar automáticamente el intervalo de actualización de los datos para ciertas porciones de la página de software de NetApp Element que está viendo.

Los valores predeterminados del intervalo de actualización se restablecen cuando la página se vuelve a cargar en el navegador. El intervalo de actualización actual se puede ver si hace clic en el nombre del clúster en la parte superior derecha de la página. Hay que tener en cuenta que el intervalo determina la frecuencia con la que se realizan las solicitudes de API, no la rapidez con la que los datos regresan del servidor.

Cuando la carga del clúster es muy pesada, puede poner en cola las solicitudes de API de la interfaz de usuario de Element. En las pocas ocasiones, cuando la respuesta del sistema se retrasa significativamente, como una conexión de red lenta combinada con un clúster ocupado, puede optar por cerrar la sesión de la interfaz de usuario de Element si el sistema no responde a las solicitudes de API en cola con la suficiente rapidez. Si se le redirige a la pantalla de cierre de sesión, puede volver a iniciar sesión después de desactivar cualquier solicitud de autenticación inicial del navegador. Tras volver a la página de introducción, se le pueden pedir las credenciales del clúster si no las ha guardado en el navegador.

Iconos en la interfaz de Element

La interfaz del software de NetApp Element muestra iconos para representar las acciones que puede realizar sobre los recursos del sistema.

La tabla siguiente proporciona una referencia rápida:

.	Descripción
	Acciones
	Backup a.
	Clonar o copiar
	Eliminar o purgar
	Editar
	Filtro
	Emparejar

	Actualice
	Restaurar
	Restaurar desde
	Revertir
	Snapshot

Enviar comentarios

Es posible mejorar la interfaz de usuario web del software Element y solucionar cualquier problema con la interfaz de usuario mediante el formulario de comentarios al que se puede acceder en toda la interfaz de usuario.

1. En cualquier página de la interfaz de usuario del elemento, haga clic en el botón **Comentarios**.
2. Introduzca la información que corresponda en los campos Summary y Description.
3. Adjunte las capturas de pantalla que le ayuden.
4. Introduzca un nombre y una dirección de correo electrónico.
5. Active la casilla para incluir datos sobre su entorno actual.
6. Haga clic en **Enviar**.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Gestionar cuentas

En los sistemas de almacenamiento de SolidFire, los inquilinos pueden utilizar las cuentas para permitir que los clientes se conecten a volúmenes en un clúster. Cuando crea un volumen, este se asigna a una cuenta específica. También se pueden gestionar cuentas de administrador de clúster para un sistema de almacenamiento SolidFire.

- "Trabaje con cuentas que utilicen CHAP"
- "Gestione cuentas de usuario administrador del clúster"

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Trabaje con cuentas que utilicen CHAP

En los sistemas de almacenamiento de SolidFire, los inquilinos pueden utilizar las cuentas para permitir que los clientes se conecten a volúmenes en un clúster. Una cuenta contiene la autenticación mediante protocolo de autenticación por desafío mutuo (CHAP) que se necesita para acceder a los volúmenes que tiene asignados. Cuando crea un volumen, este se asigna a una cuenta específica.

Una cuenta puede tener hasta 2000 volúmenes asignados, pero un volumen solo puede pertenecer a una cuenta.

Crear una cuenta

Es posible crear una cuenta para permitir el acceso a los volúmenes.

Cada nombre de cuenta del sistema debe ser exclusivo.

1. Seleccione **Administración** > **Cuentas**.
2. Haga clic en **Crear cuenta**.
3. Introduzca un **Nombre de usuario**.
4. En la sección **Configuración CHAP**, introduzca la siguiente información:

   Puede dejar los campos de credenciales vacíos para que cualquier contraseña se genere automáticamente.

   - **Secreto de iniciador** para la autenticación de sesión de nodo CHAP.
   - **Secreto de destino** para la autenticación de sesión de nodo CHAP.
5. Haga clic en **Crear cuenta**.

Ver los detalles de la cuenta

La actividad de rendimiento de cada cuenta se puede ver como un gráfico.

El gráfico proporciona información de I/o y rendimiento de la cuenta. Los niveles de actividad promedio y pico se muestran en incrementos de períodos de informe de 10 segundos. Estas estadísticas incluyen la actividad de todos los volúmenes asignados a la cuenta.

1. Seleccione **Administración** > **Cuentas**.
2. Haga clic en el icono Actions de una cuenta.
3. Haga clic en **Ver detalles**.

Estos son algunos de los detalles:

- **Estado**: El estado de la cuenta. Los posibles valores son los siguientes:

- Active: Una cuenta activa.
- Locked: Una cuenta bloqueada.
- Deleted: Una cuenta que se ha eliminado y purgado.

- **Volúmenes activos**: Número de volúmenes activos asignados a la cuenta.
- **Compresión**: La puntuación de eficiencia de compresión para los volúmenes asignados a la cuenta.
- **Deduplicación**: La puntuación de eficiencia de deduplicación para los volúmenes asignados a la cuenta.
- **Thin Provisioning**: La puntuación de eficiencia de thin provisioning para los volúmenes asignados a la cuenta.
- **Eficiencia general**: La puntuación de eficiencia general para los volúmenes asignados a la cuenta.

Editar una cuenta

Una cuenta se puede editar para cambiar el estado, cambiar los secretos de CHAP o modificar el nombre de la cuenta.

Si se modifica la configuración de CHAP en una cuenta o se quitan los iniciadores o los volúmenes de un grupo de acceso, se podría interrumpir el acceso de los iniciadores a los volúmenes de forma inesperada. Para asegurarse de que no se interrumpirá el acceso a los volúmenes de forma inesperada, siempre debe cerrar las sesiones iSCSI afectadas por alguno de los cambios en la cuenta o en el grupo de acceso. Asimismo, compruebe que los iniciadores pueden volver a conectarse con los volúmenes una vez que se hayan realizado los cambios en la configuración del iniciador y la configuración del clúster.

> Los volúmenes persistentes asociados con servicios de gestión se asignan a una cuenta nueva que se crea durante la instalación o la actualización. Si utiliza volúmenes persistentes, no modifique o elimine su cuenta asociada.

1. Seleccione **Administración** > **Cuentas**.
2. Haga clic en el icono Actions de una cuenta.
3. En el menú que se abre, seleccione **Editar**.
4. **Opcional:** edite el **Nombre de usuario**.
5. **Opcional:** haga clic en la lista desplegable **Estado** y seleccione un estado diferente.

   > Al cambiar el estado a **Locked** se cierran todas las conexiones iSCSI a la cuenta y ya no se puede acceder a ella. Los volúmenes asociados con la cuenta se mantienen, pero ya no se podrán detectar los volúmenes con iSCSI.

6. **Opcional:** en **Configuración CHAP**, edite las credenciales **Secreto de iniciador** y **Secreto de destino** utilizadas para la autenticación de sesión de nodo.

   > Si no cambia las credenciales **Configuración CHAP**, seguirán siendo las mismas. Si deja vacíos los campos de las credenciales, el sistema generará contraseñas nuevas.

7. Haga clic en **Guardar cambios**.

Eliminar una cuenta

Una cuenta se puede eliminar cuando ya no se necesita.

Debe eliminar y purgar los volúmenes asociados con la cuenta antes de eliminarla.

> Los volúmenes persistentes asociados con servicios de gestión se asignan a una cuenta nueva que se crea durante la instalación o la actualización. Si utiliza volúmenes persistentes, no modifique o elimine su cuenta asociada.

1. Seleccione **Administración** > **Cuentas**.
2. Haga clic en el icono Actions de la cuenta que quiera eliminar.
3. En el menú que se abre, seleccione **Eliminar**.
4. Confirme la acción.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Gestione cuentas de usuario administrador del clúster

Para gestionar las cuentas de administrador de clúster correspondientes a un sistema de almacenamiento de SolidFire, debe crear, eliminar y editar cuentas de administrador de clúster, cambiar la contraseña de administrador de clúster y configurar las opciones de LDAP para gestionar el acceso a los usuarios al sistema.

Tipos de cuenta de administrador del clúster de almacenamiento

Existen dos tipos de cuentas de administrador que pueden existir en un clúster de almacenamiento que ejecuta el software NetApp Element: La cuenta de administrador de clúster principal y una cuenta de administrador de clúster.

- **Cuenta de administrador del clúster principal**

  Esta cuenta de administrador se crea cuando se crea el clúster. Es la cuenta administrativa principal con el nivel de acceso al clúster más alto. Esta cuenta es similar a un usuario raíz en un sistema Linux. Puede cambiar la contraseña de esta cuenta de administrador.

- **Cuenta de administrador de clúster**

  Puede conceder a una cuenta de administrador de clúster una gama limitada de accesos de administrador para realizar determinadas tareas dentro de un clúster. Las credenciales que se asignan a cada cuenta de administrador de clúster sirven para autenticar las solicitudes de la API y la interfaz de usuario de Element dentro del sistema de almacenamiento.

> Se necesita una cuenta de administrador de clúster local (que no sea LDAP) para acceder a los nodos activos en un clúster a través de la interfaz de usuario por nodo. No se necesitan credenciales de cuenta para acceder a un nodo que aún no forme parte de un clúster.

Ver los detalles de administrador del clúster

1. Si desea crear una cuenta de administrador de clúster (que no sea LDAP) para todo el clúster, realice las siguientes acciones:

a. Haga clic en **usuarios** > **Administradores de clúster**.

2. En la página Cluster Admins de la pestaña Users, puede ver la siguiente información.
   - **ID**: Número secuencial asignado a la cuenta de administrador del clúster.
   - **Nombre de usuario**: El nombre otorgado a la cuenta de administrador del clúster cuando se creó.
   - **Acceso**: Los permisos de usuario asignados a la cuenta de usuario. Los posibles valores son los siguientes:
     - lea
     - creación de informes
     - nodos
     - unidades
     - volúmenes
     - cuentas
     - Administradores de clústeres
     - administrador

     Todos los permisos están disponibles para el tipo de acceso del administrador.
   - **Tipo**: El tipo de administrador de clúster. Los posibles valores son los siguientes:
     - Clúster
     - LDAP
   - **Atributos**: Si la cuenta de administrador de clúster se creó mediante la API de elemento, esta columna muestra cualquier par nombre-valor que se haya establecido utilizando ese método.

     Consulte "Referencia de API del software NetApp Element".

Cree una cuenta de administrador de clúster

Es posible crear nuevas cuentas de administrador de clúster con permisos para conceder o restringir el acceso a determinadas áreas del sistema de almacenamiento. Cuando se configuran los permisos de la cuenta de administrador del clúster, el sistema otorga derechos de solo lectura a aquellos permisos que no se asignen al administrador del clúster.

Si desea crear una cuenta de administrador de clúster LDAP, asegúrese de que LDAP esté configurado en el clúster antes de comenzar.

"Habilite la autenticación de LDAP con la interfaz de usuario de Element"

Más adelante, los privilegios de la cuenta de administrador de clúster se pueden cambiar para crear informes, nodos, unidades, volúmenes, cuentas y acceso a nivel de clúster. Cuando habilita un permiso, el sistema asigna acceso de escritura para ese nivel. Para los niveles que no se seleccionan, el sistema concede al usuario administrador acceso de solo lectura.

También es posible quitar más adelante cualquier cuenta de usuario administrador de clúster que haya creado un administrador del sistema. Sin embargo, no es posible quitar la cuenta de administrador de clúster principal que se generó al crear el clúster.

1. Si desea crear una cuenta de administrador de clúster (que no sea LDAP) para todo el clúster, realice las

siguientes acciones:

a. Haga clic en **usuarios** > **Administradores de clúster**.
b. Haga clic en **Crear administrador de clúster**.
c. Seleccione el tipo de usuario **Cluster**.
d. Introduzca un nombre de usuario y una contraseña para la cuenta y confirme la contraseña.
e. Seleccione los permisos de usuario que se van a aplicar a la cuenta.
f. Active la casilla con la que se acepta el contrato de licencia para usuario final de.
g. Haga clic en **Crear administrador de clúster**.

2. Para crear una cuenta de administrador de clúster en el directorio LDAP, realice las siguientes acciones:

a. Haga clic en **Cluster** > **LDAP**.
b. Asegúrese de que la autenticación LDAP está habilitada.
c. Haga clic en **probar autenticación de usuario** y copie el nombre completo que aparece para el usuario o uno de los grupos de los que el usuario es miembro para poder pegarlo más tarde.
d. Haga clic en **usuarios** > **Administradores de clúster**.
e. Haga clic en **Crear administrador de clúster**.
f. Seleccione el tipo de usuario LDAP.
g. En el campo Nombre distintivo, siga el ejemplo del cuadro de texto para introducir un nombre completo distintivo para el usuario o grupo. Como alternativa, péguela desde el nombre distintivo que copió anteriormente.

   Si el nombre distintivo forma parte de un grupo, cualquier usuario que sea miembro de dicho grupo en el servidor LDAP tendrá permisos de esta cuenta de administrador.

Para agregar usuarios o grupos de administración de clúster LDAP, el formato general del nombre de usuario es "'LDAP:<Full Distinguished Name>'".

a. Seleccione los permisos de usuario que se van a aplicar a la cuenta.
b. Active la casilla con la que se acepta el contrato de licencia para usuario final de.
c. Haga clic en **Crear administrador de clúster**.

Edite los permisos de administrador del clúster

Los privilegios de la cuenta de administrador de clúster se pueden cambiar para crear informes, nodos, unidades, volúmenes y cuentas. y acceso a nivel de clúster. Cuando habilita un permiso, el sistema asigna acceso de escritura para ese nivel. Para los niveles que no se seleccionan, el sistema concede al usuario administrador acceso de solo lectura.

1. Haga clic en **usuarios** > **Administradores de clúster**.
2. Haga clic en el icono Actions del administrador de clúster que quiera editar.
3. Haga clic en **Editar**.
4. Seleccione los permisos de usuario que se van a aplicar a la cuenta.
5. Haga clic en **Guardar cambios**.

Cambiar contraseñas de las cuentas de administrador del clúster

Es posible usar la interfaz de usuario de Element para cambiar las contraseñas de administrador de clúster.

1. Haga clic en **usuarios** > **Administradores de clúster**.
2. Haga clic en el icono Actions del administrador de clúster que quiera editar.
3. Haga clic en **Editar**.
4. En el campo Change Password, introduzca una contraseña nueva y confírmela.
5. Haga clic en **Guardar cambios**.

Obtenga más información

- "Habilite la autenticación de LDAP con la interfaz de usuario de Element"
- "Deshabilite LDAP"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Gestione LDAP

Puede configurar el protocolo ligero de acceso a directorios (LDAP) para habilitar la funcionalidad de inicio de sesión seguro basado en directorios en el almacenamiento de SolidFire. Se puede configurar LDAP en el nivel del clúster y autorizar grupos y usuarios de LDAP.

La gestión de LDAP implica configurar la autenticación LDAP en un clúster de SolidFire mediante un entorno de Microsoft Active Directory existente y probar la configuración.

Es posible usar tanto direcciones IPv4 como IPv6.

Habilitar LDAP implica los siguientes pasos de alto nivel, descritos con detalle:

1. **Completar los pasos de preconfiguración para compatibilidad con LDAP**. Valide tener todos los detalles necesarios para configurar la autenticación LDAP.
2. **Activar autenticación LDAP**. Use la interfaz de usuario de Element o la API de Element.
3. **Validar la configuración LDAP**. De manera opcional, compruebe que el clúster se haya configurado con los valores correctos ejecutando el método API GetLdapConfiguration o comprobando la configuración LCAP mediante la interfaz de usuario de Element.
4. **Pruebe la autenticación LDAP** (con la `readonly` usuario). Compruebe que la configuración de LDAP sea correcta mediante la ejecución del método API TestLdapAuthentication o mediante la interfaz de usuario de Element. Para esta prueba inicial, utilice el nombre de usuario «sAMAccountName» del `readonly` usuario. Esto validará que su clúster esté configurado correctamente para la autenticación LDAP y también validará que el `readonly` las credenciales y el acceso son correctos. Si este paso falla, repita los pasos del 1 al 3.
5. **Pruebe la autenticación LDAP** (con una cuenta de usuario que desea agregar). Repita setp 4 con una cuenta de usuario que desee agregar como administrador de clúster de Element. Copie el `distinguished` Nombre (DN) o usuario (o grupo). Este DN se utilizará en el paso 6.
6. **Agregue el administrador del clúster LDAP** (copie y pegue el DN del paso probar autenticación LDAP). Mediante la interfaz de usuario de Element o el método API AddLdapClusterAdmin, cree un nuevo usuario

administrador de clúster con el nivel de acceso adecuado. Para el nombre de usuario, pegue el DN completo que ha copiado en el paso 5. Esto asegura que el DN está formateado correctamente.

7. **Pruebe el acceso de administrador del clúster**. Inicie sesión en el clúster con el usuario administrador del clúster LDAP recién creado. Si agregó un grupo LDAP, puede iniciar sesión como cualquier usuario de ese grupo.

Complete los pasos previos de configuración para ser compatible con LDAP

Antes de habilitar la compatibilidad con LDAP en Element, debe configurar un servidor de Windows Active Directory y realizar otras tareas previas a la configuración.

Pasos

1. Configure un servidor de Active Directory de Windows.
2. **Opcional:** Activar soporte LDAPS.
3. Crear usuarios y grupos.
4. Cree una cuenta de servicio de sólo lectura (como «sfreadonly») que se utilizará para buscar en el directorio LDAP.

Habilite la autenticación de LDAP con la interfaz de usuario de Element

Puede configurar la integración del sistema de almacenamiento con un servidor LDAP existente. De este modo, los administradores de LDAP pueden gestionar de forma centralizada el acceso al sistema de almacenamiento para los usuarios.

Es posible configurar LDAP con la interfaz de usuario de Element o la API de Element. Este procedimiento describe cómo configurar LDAP mediante la interfaz de usuario de Element.

Este ejemplo muestra cómo configurar la autenticación LDAP en SolidFire y utiliza `SearchAndBind` como tipo de autenticación. En el ejemplo se utiliza un solo servidor de Active Directory de Windows Server 2012 R2.

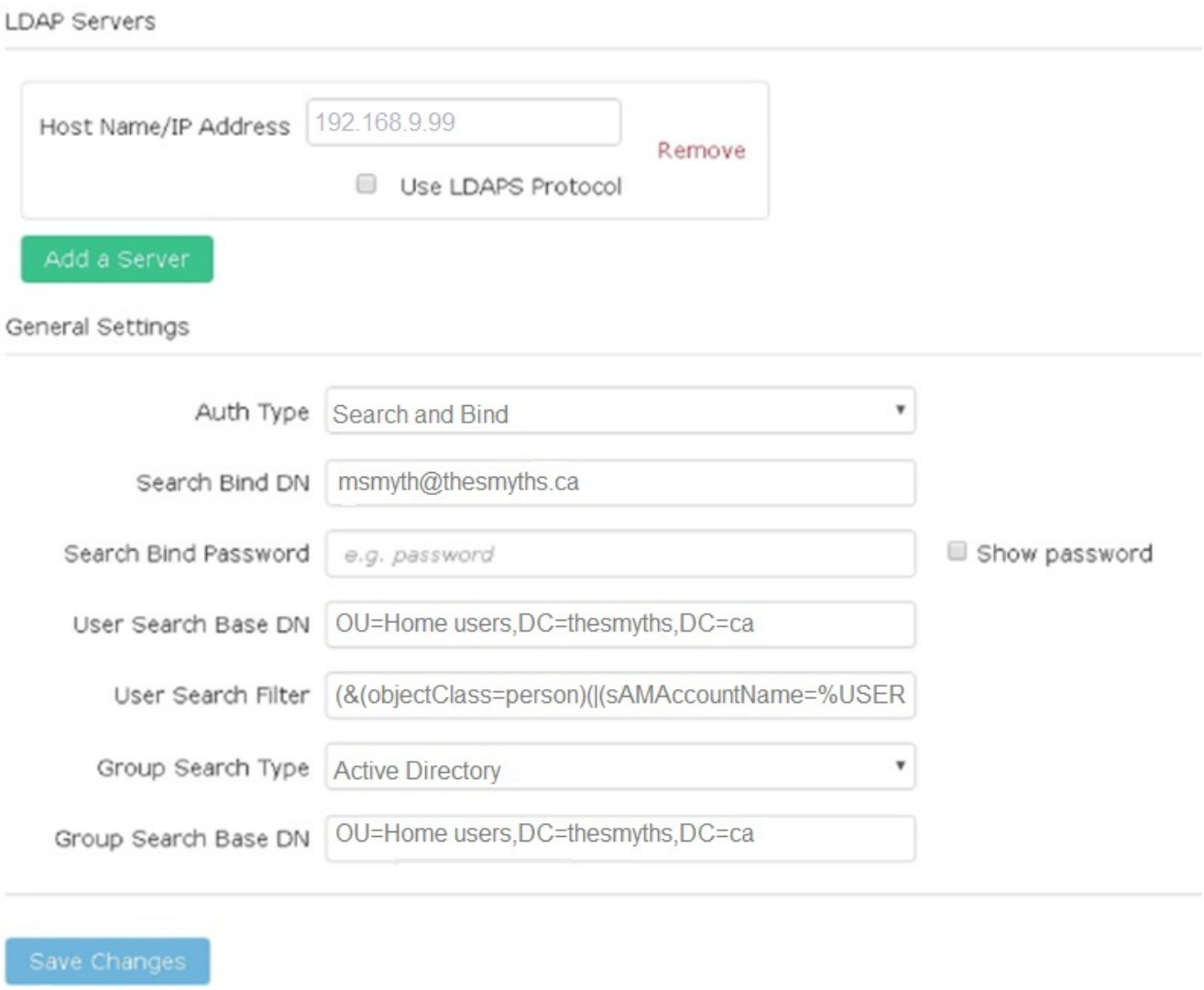
Pasos

1. Haga clic en **Cluster** > **LDAP**.
2. Haga clic en **Sí** para activar la autenticación LDAP.
3. Haga clic en **Agregar un servidor**.
4. Introduzca **Nombre de host/dirección IP**.

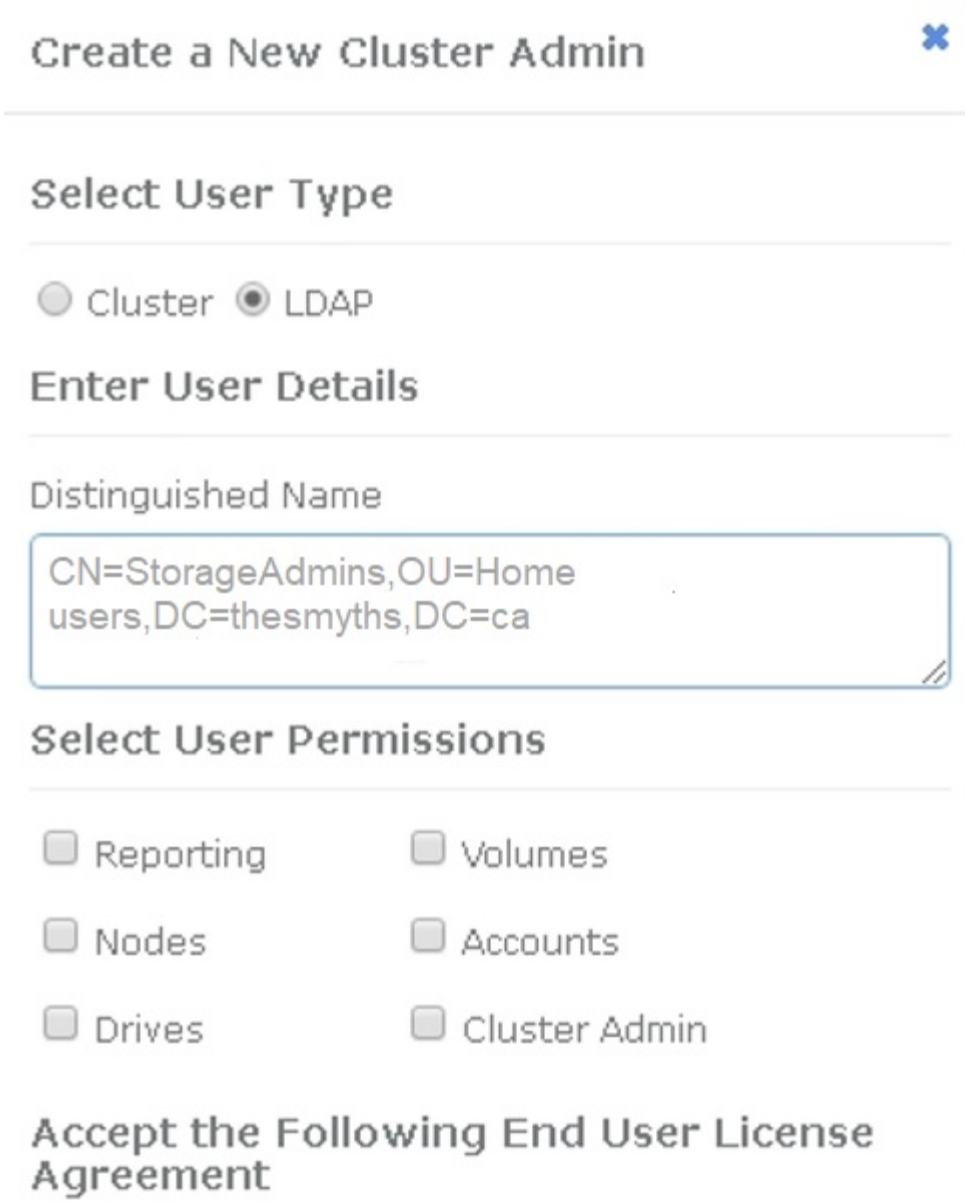
   También puede introducir un número de puerto personalizado opcional.

   Por ejemplo, para añadir un número de puerto personalizado, introduzca <host name or ip address>:<port number>

5. **Opcional:** Seleccione **Use LDAPS Protocol**.
6. Introduzca la información necesaria en **Ajustes generales**.



7. Haga clic en **Activar LDAP**.
8. Haga clic en **probar autenticación de usuario** si desea probar el acceso al servidor para un usuario.
9. Copie la información del nombre distintivo y del grupo de usuarios que aparece para usarla más adelante cuando se crean administradores de clúster.
10. Haga clic en **Guardar cambios** para guardar cualquier configuración nueva.
11. Para crear un usuario en este grupo de modo que cualquiera pueda iniciar sesión, realice lo siguiente:
    a. Haga clic en **Usuario** > **Ver**.



b. Para el nuevo usuario, haga clic en **LDAP** para el tipo de usuario y pegue el grupo que copió en el campo Nombre distintivo.
c. Seleccione los permisos, normalmente todos los permisos.
d. Desplácese hasta el Contrato de licencia para el usuario final y haga clic en **Acepto**.
e. Haga clic en **Crear administrador de clúster**.

   Ahora tiene un usuario con el valor de un grupo de Active Directory.

Para probarlo, cierre sesión en la interfaz de usuario del elemento y vuelva a iniciarla como usuario en ese grupo.

Habilite la autenticación de LDAP con la API de Element

Puede configurar la integración del sistema de almacenamiento con un servidor LDAP existente. De este modo, los administradores de LDAP pueden gestionar de forma centralizada el acceso al sistema de almacenamiento para los usuarios.

Es posible configurar LDAP con la interfaz de usuario de Element o la API de Element. Este procedimiento describe cómo configurar LDAP mediante la API de Element.

Para aprovechar la autenticación LDAP en un clúster de SolidFire, primero debe habilitar la autenticación LDAP en el clúster mediante el `EnableLdapAuthentication` Método API.

Pasos

1. Habilite la autenticación LDAP primero en el clúster de mediante el `EnableLdapAuthentication` Método API.
2. Especifique la información obligatoria.

```
{
     "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. Cambie los valores de los siguientes parámetros:

Parámetros utilizados	Descripción
AuthType: SearchAndBind	Dicta que el clúster utilizará la cuenta de servicio readonly para buscar primero el usuario que se va a autenticar y, a continuación, enlazar ese usuario si se encuentra y se autentica.
GroupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica la ubicación en el árbol LDAP para comenzar a buscar grupos. Para este ejemplo, hemos utilizado la raíz de nuestro árbol. Si su árbol LDAP es muy grande, quizás desee establecer este árbol en un subárbol más granular para reducir los tiempos de búsqueda.

Parámetros utilizados	Descripción
UserSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica la ubicación en el árbol LDAP para comenzar a buscar usuarios. Para este ejemplo, hemos utilizado la raíz de nuestro árbol. Si su árbol LDAP es muy grande, quizás desee establecer este árbol en un subárbol más granular para reducir los tiempos de búsqueda.
GroupSearchType: ActiveDirectory	Utiliza el servidor de Windows Active Directory como servidor LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Para utilizar userPrincipalName (dirección de correo electrónico para el inicio de sesión), puede cambiar userSearchFilter a:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
O bien, para buscar userPrincipalName y sAMAccountName, puede usar el siguiente usuarioSearchFilter:
 	
`"(&(objectClass=person)(`
	(SAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%))" ----

Utiliza sAMAccountName como nombre de usuario para iniciar sesión en el clúster de SolidFire. Esta configuración indica a LDAP que busque el nombre de usuario especificado durante el inicio de sesión en el atributo sAMAccountName y que también limite la búsqueda a entradas que tengan "'Person'" como valor en el atributo objectClass.	SearchBindDN
Es el nombre completo del usuario readonly que se utilizará para buscar en el directorio LDAP. Para un directorio activo suele ser más fácil utilizar userPrincipalName (formato de dirección de correo electrónico) para el usuario.	SearchBindPassword

Para probarlo, cierre sesión en la interfaz de usuario del elemento y vuelva a iniciarla como usuario en ese grupo.

Ver los detalles de LDAP

Consulte la información de LDAP en la página LDAP de la pestaña Cluster.

Debe habilitar LDAP para ver estas opciones de configuración de LDAP.

1. Para ver los detalles de LDAP con la interfaz de usuario de Element, haga clic en **Cluster** > **LDAP**.
   - **Nombre de host/Dirección IP**: Dirección de un servidor de directorio LDAP o LDAPS.
   - **Tipo de autenticación**: El método de autenticación de usuario. Los posibles valores son los siguientes:
     - Enlace directo
     - Búsqueda y vinculación
   - **Buscar Bind DN**: Un DN completo con el que conectarse para realizar una búsqueda LDAP del usuario (necesita acceso de nivel de enlace al directorio LDAP).
   - **Buscar Contraseña de enlace**: Contraseña utilizada para autenticar el acceso al servidor LDAP.
   - **User Search base DN**: El DN base del árbol utilizado para iniciar la búsqueda del usuario. El sistema busca el subárbol de la ubicación especificada.
   - **Filtro de búsqueda de usuario**: Introduzca lo siguiente utilizando su nombre de dominio:

     ```
     (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
     ```

   - **Tipo de búsqueda de grupo**: Tipo de búsqueda que controla el filtro de búsqueda de grupo predeterminado utilizado. Los posibles valores son los siguientes:
     - Active Directory: Pertenencia anidada de todos los grupos LDAP de un usuario.
     - No hay grupos: Ningún soporte de grupo.
     - DN de miembro: Grupos de tipo DN de miembro (un nivel).
   - **DN base de búsqueda de grupo**: El DN base del árbol utilizado para iniciar la búsqueda de grupo. El sistema busca el subárbol de la ubicación especificada.
   - **Probar autenticación de usuario**: Después de configurar LDAP, utilice esta opción para probar la autenticación de nombre de usuario y contraseña para el servidor LDAP. Introduzca una cuenta que ya existe para probarlo. Se muestra la información relacionada con el nombre distintivo y el grupo de usuarios, que se puede copiar para usarlo más adelante al crear administradores de clúster.

Pruebe la configuración de LDAP

Después de configurar LDAP, debe probarla mediante la interfaz de usuario de Element o la API de Element `TestLdapAuthentication` método.

Pasos

1. Para probar la configuración de LDAP con la interfaz de usuario de Element, haga lo siguiente:
   a. Haga clic en **Cluster** > **LDAP**.
   b. Haga clic en **probar autenticación LDAP**.
   c. Resuelva cualquier problema utilizando la información de la siguiente tabla:

Mensaje de error	Descripción
`xLDAPUserNotFound`	• El usuario que se está probando no se encontró en el configurado `userSearchBaseDN` subárbol. • La `userSearchFilter` está configurado incorrectamente.
`xLDAPBindFailed (Error: Invalid credentials)`	• El nombre de usuario que se está probando es un usuario LDAP válido, pero la contraseña proporcionada es incorrecta. • El nombre de usuario que se está probando es un usuario LDAP válido, pero la cuenta está deshabilitada actualmente.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	El URI del servidor LDAP es incorrecto.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	El nombre de usuario o la contraseña de solo lectura están configurados incorrectamente.
`xLDAPSearchFailed (Error: No such object)`	La `userSearchBaseDN` No es una ubicación válida dentro del árbol LDAP.
`xLDAPSearchFailed (Error: Referral)`	• La `userSearchBaseDN` No es una ubicación válida dentro del árbol LDAP. • La `userSearchBaseDN` y.. `groupSearchBaseDN` Están en una unidad organizativa anidada. Esto puede provocar problemas de permisos. La solución alternativa es incluir la unidad organizativa en las entradas DN base de usuario y grupo (por ejemplo: `ou=storage, cn=company, cn=com`)

2. Para probar la configuración de LDAP con la API de Element, haga lo siguiente:
   a. Llame al método TestLdapAuthentication.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

b. Revise los resultados. Si la llamada API es correcta, los resultados incluyen el nombre completo del usuario especificado y una lista de grupos en los que el usuario es miembro.

```
{
"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"
     }
}
```

Deshabilite LDAP

Es posible deshabilitar la integración de LDAP con la interfaz de usuario de Element.

Antes de comenzar, debe tener en cuenta todas las opciones de configuración, ya que al deshabilitar LDAP se borran todas las opciones.

Pasos

1. Haga clic en **Cluster** > **LDAP**.
2. Haga clic en **no**.
3. Haga clic en **Desactivar LDAP**.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Gestione su sistema

Puede gestionar el sistema en la interfaz de usuario de Element. Esto incluye habilitar la autenticación multifactor, gestionar la configuración de clústeres, admitir estándares de

procesamiento de información federal (FIPS) y el uso de gestión de claves externa.

- "Habilite la autenticación multifactor"
- "Configure las opciones del clúster"
- "Cree un clúster que admita unidades FIPS"
- "Comience con la gestión de claves externas"

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Habilite la autenticación multifactor

La autenticación multifactor (MFA) utiliza un proveedor de identidades (IDP) de terceros a través del lenguaje de marcado de aserción de seguridad (SAML) para gestionar las sesiones de usuario. La MFA permite a los administradores configurar factores adicionales de autenticación según sea necesario, como la contraseña y los mensajes de texto, y la contraseña y los mensajes de correo electrónico.

Configure la autenticación de múltiples factores

Es posible usar estos pasos básicos a través de la API de Element para configurar el clúster con el fin de utilizar la autenticación multifactor.

Puede encontrar más detalles de cada método de API en la "Referencia de la API de Element".

1. Cree una nueva configuración de un proveedor de identidades (IDP) de terceros para el clúster llamando al siguiente método de API y pasando los metadatos de IDP en formato JSON: `CreateIdpConfiguration`

   Los metadatos de IDP, en formato de texto sin formato, se recuperan del IDP de terceros. Estos metadatos se deben validar para asegurarse de que están formateados correctamente en JSON. Hay numerosas aplicaciones de formateador JSON disponibles que puede utilizar, por ejemplo:https://freeformatter.com/json-escape.html.

2. Recupere los metadatos del clúster, a través de spMetadataUrl, para copiar al IDP de terceros llamando al siguiente método API: `ListIdpConfigurations`

   SpMetadataUrl es una URL que se utiliza para recuperar metadatos del proveedor de servicios del clúster para el IDP con el fin de establecer una relación de confianza.

3. Configure las afirmaciones SAML en el IDP de terceros para incluir el atributo "'NameID'" para identificar de forma exclusiva a un usuario para el registro de auditorías y para que Single Logout funcione correctamente.
4. Cree una o varias cuentas de usuario administrador del clúster autenticadas por un IDP de terceros para su autorización, llamando al siguiente método API:`AddIdpClusterAdmin`

El nombre de usuario del administrador del clúster IDP debe coincidir con el mapa de nombre/valor del atributo SAML del efecto deseado, como se muestra en los siguientes ejemplos:

- Email=bob@company.com — donde el IDP está configurado para liberar una dirección de correo electrónico en los atributos SAML.
- Group=cluster-Administrator: Donde el IDP está configurado para liberar una propiedad de grupo en la que todos los usuarios deberían tener acceso. Tenga en cuenta que el emparejamiento nombre/valor del atributo SAML distingue mayúsculas y minúsculas por motivos de seguridad.

5. Habilite la MFA para el clúster llamando al siguiente método API: `EnableIdpAuthentication`

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Información adicional para la autenticación multifactor

Debe conocer las siguientes advertencias en relación con la autenticación de múltiples factores.

- Para actualizar los certificados de IDP que ya no son válidos, deberá usar un usuario administrador no IDP para llamar al siguiente método API: `UpdateIdpConfiguration`
- La MFA es incompatible con certificados con una longitud inferior a 2048 bits. De manera predeterminada, se crea un certificado SSL de 2048 bits en el clúster. Debe evitar establecer un certificado de menor tamaño cuando llame al método de API: `SetSSLCertificate`

Si el clúster utiliza un certificado que sea inferior a 2048 bits antes de la actualización, el certificado del clúster debe actualizarse con un certificado de 2048 bits o superior después de la actualización a Element 12.0 o una versión posterior.

- Los usuarios del administrador de IDP no pueden utilizarse para realizar llamadas de API directamente (por ejemplo, mediante SDK o Postman) o para otras integraciones (por ejemplo, OpenStack Cinder o el complemento vCenter). Si necesita crear usuarios que tengan estas capacidades, añada usuarios bien al administrador del clúster LDAP o usuarios de administrador del clúster local.

Obtenga más información

- "Gestionar el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Configure las opciones del clúster

Es posible ver y modificar la configuración de todo el clúster y realizar tareas específicas del clúster en la pestaña Cluster de la interfaz de usuario de Element.

Puede configurar ajustes como el umbral de ocupación del clúster, el acceso de soporte, el cifrado en reposo, los volúmenes virtuales, SnapMirror, Y el cliente de retransmisión NTP.

Opciones

- Trabaje con volúmenes virtuales
- Use la replicación de SnapMirror entre clústeres de Element y ONTAP
- Establezca el umbral de ocupación del clúster
- Habilite y deshabilite el acceso al soporte
- "Cómo se calculan los umbrales de blockSpace para el elemento"
- Habilite y deshabilite el cifrado de un clúster
- Gestione el banner de las condiciones de uso
- Configure los servidores de protocolo de tiempo de red para que el clúster consulte
- Gestionar SNMP
- Gestionar unidades
- Gestione los nodos
- Gestionar redes virtuales
- Ver detalles de los puertos Fibre Channel

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Habilite y deshabilite el cifrado en reposo para un clúster

Con los clústeres de SolidFire, puede cifrar todos los datos en reposo almacenados en unidades del clúster. Puede habilitar la protección en todo el clúster de unidades de autocifrado (SED) mediante cualquiera de los dos "cifrado basado en hardware o software en reposo".

Puede habilitar el cifrado de hardware en reposo mediante la interfaz de usuario o la API de Element. La habilitación de la función de cifrado de hardware en reposo no afecta al rendimiento o la eficiencia del clúster. Puede habilitar el cifrado de software en reposo únicamente mediante la API de Element.

El cifrado basado en hardware en reposo no está habilitado de forma predeterminada durante la creación de clústeres, y se puede habilitar o deshabilitar desde la interfaz de usuario de Element.

> En los clústeres de almacenamiento all-flash de SolidFire, el cifrado del software en reposo debe habilitarse durante la creación del clúster y no se puede deshabilitar una vez que se ha creado el clúster.

Lo que necesitará

- Tiene privilegios de administrador de clúster para habilitar o modificar la configuración de cifrado.
- Para el cifrado basado en hardware en reposo, se ha asegurado de que el clúster está en estado correcto antes de cambiar la configuración de cifrado.
- Si va a deshabilitar el cifrado, debe haber dos nodos participando en un clúster para acceder a la clave para deshabilitar el cifrado en una unidad.

Comprobar el cifrado en estado de reposo

Para ver el estado actual del cifrado en reposo y/o el cifrado de software en reposo en el clúster, use el "GetClusterInfo" método. Puede utilizar el "GetSoftwareEncryptionAtRestInfo" método para obtener información que utiliza el clúster para cifrar datos en reposo.

> La consola de interfaz de usuario del software Element en `https://<MVIP>/` actualmente, solo muestra el cifrado en estado de reposo para el cifrado basado en hardware.

Opciones

- Habilite el cifrado basado en hardware en reposo
- Habilite el cifrado basado en software en reposo
- Deshabilite el cifrado basado en hardware en reposo

Habilite el cifrado basado en hardware en reposo

> Para habilitar el cifrado en reposo mediante una configuración de gestión de claves externa, debe habilitar el cifrado en reposo a través de la "API". Al habilitar el uso del botón existente de la interfaz de usuario de Element, se revierten al uso de claves generadas internamente.

1. En la interfaz de usuario de Element, seleccione **Cluster** > **Settings**.
2. Seleccione **Activar cifrado en reposo**.

Habilite el cifrado basado en software en reposo

> El cifrado de software en reposo no se puede deshabilitar una vez que se habilita en el clúster.

1. Durante la creación del clúster, ejecute el "cree el método de clúster" con `enableSoftwareEncryptionAtRest` establezca en `true`.

Deshabilite el cifrado basado en hardware en reposo

1. En la interfaz de usuario de Element, seleccione **Cluster** > **Settings**.
2. Seleccione **Desactivar cifrado en reposo**.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Establezca el umbral de ocupación del clúster

Puede cambiar el nivel en el que el sistema genera una advertencia de ocupación de la capacidad del clúster de bloques mediante los pasos siguientes. Además, puede utilizar el método API ModifyClusterFullThreshold para cambiar el nivel en el que el sistema genera una advertencia de bloque o metadatos.

Lo que necesitará

Debe tener privilegios de administrador del clúster.

Pasos

1. Haga clic en **Cluster** > **Settings**.
2. En la sección Cluster Full Settings, introduzca un porcentaje en **Raise a warning alert when _% capacity remains before Helix could not recover from a node failure**.
3. Haga clic en **Guardar cambios**.

Obtenga más información

"Cómo se calculan los umbrales de blockSpace para el elemento"

Habilite y deshabilite el acceso al soporte

Es posible habilitar el acceso de soporte para permitir temporalmente el acceso del personal de soporte de NetApp a los nodos de almacenamiento a través de SSH para solucionar problemas.

Para modificar el acceso al soporte, debe tener privilegios de administrador de clúster.

1. Haga clic en **Cluster** > **Settings**.
2. En la sección Habilitar/deshabilitar acceso de soporte, introduzca la duración (en horas) que desea permitir que el soporte tenga acceso.
3. Haga clic en **Activar acceso de soporte**.
4. **Opcional:** para desactivar el acceso al soporte técnico, haga clic en **Desactivar acceso al soporte técnico**.

Gestione el banner de las condiciones de uso

Puede habilitar, editar o configurar un banner que contenga un mensaje para el usuario.

Opciones

Habilite el banner de las condiciones de uso
Edite el banner con las condiciones de uso
Deshabilite el banner con las condiciones de uso

Habilite el banner de las condiciones de uso

Si lo desea, se puede habilitar un banner con las condiciones de uso que aparece cuando un usuario inicia sesión en la interfaz de usuario de Element. Cuando el usuario haga clic en el banner, aparecerá un cuadro de diálogo de texto con el mensaje que haya configurado para el clúster. El banner se puede descartar cuando desee.

Para poder habilitar la funcionalidad de las condiciones de uso, debe tener privilegios de administrador del clúster.

1. Haga clic en **usuarios** > **Términos de uso**.
2. En el formulario **Términos de uso**, introduzca el texto que desea que aparezca en el cuadro de diálogo Términos de uso.

   No supere los 4096 caracteres.

3. Haga clic en **Activar**.

Edite el banner con las condiciones de uso

Se puede editar el texto que ven los usuarios cuando seleccionan el banner de inicio de sesión de las condiciones de uso.

Lo que necesitará

- Para poder configurar las condiciones de uso, debe tener privilegios de administrador del clúster.
- Asegúrese de que la función de las condiciones de uso esté habilitada.

Pasos

1. Haga clic en **usuarios** > **Términos de uso**.
2. En el cuadro de diálogo **Términos de uso**, edite el texto que desea que aparezca.

   No supere los 4096 caracteres.

3. Haga clic en **Guardar cambios**.

Deshabilite el banner con las condiciones de uso

El banner con las condiciones de uso se puede deshabilitar. Cuando se deshabilita el banner, se deja de solicitar al usuario que acepte las condiciones de uso cuando se usa la interfaz de usuario de Element.

Lo que necesitará

- Para poder configurar las condiciones de uso, debe tener privilegios de administrador del clúster.
- Asegúrese de que las condiciones de uso estén habilitadas.

Pasos

1. Haga clic en **usuarios** > **Términos de uso**.
2. Haga clic en **Desactivar**.

Establezca el protocolo de hora de red

La configuración del protocolo de tiempo de redes (NTP) se puede lograr de dos maneras: Indique a cada nodo de un clúster que escuche las difusiones o indique a cada nodo que consulte un servidor NTP para obtener actualizaciones.

El NTP se utiliza para sincronizar los relojes que hay en toda una red. La conexión con un servidor NTP interno o externo debe formar parte de la configuración inicial del clúster.

Configure los servidores de protocolo de tiempo de red para que el clúster consulte

Puede indicar a cada nodo de un clúster que consulte un servidor de protocolo de tiempo de redes (NTP) en busca de actualizaciones. El clúster solo contacta con los servidores configurados y solicita información NTP de ellos.

Configure el NTP en el clúster para que apunte a un servidor NTP local. Es posible usar la dirección IP o el nombre de host FQDN. El servidor NTP predeterminado en el momento de crear el clúster se establece en us.pool.ntp.org; sin embargo, no siempre es posible establecer una conexión con este sitio en función de la

ubicación física del clúster de SolidFire.

El uso del FQDN depende de si la configuración de DNS del nodo de almacenamiento individual está en su lugar y operativa. Para ello, revise la página requisitos de puerto de red para configurar los servidores DNS en cada nodo de almacenamiento y asegúrese de que los puertos estén abiertos.

Es posible introducir hasta cinco servidores NTP distintos.

Es posible usar tanto direcciones IPv4 como IPv6.

Lo que necesitará

Para poder configurar esta opción, debe tener privilegios de administrador del clúster.

Pasos

1. Configure una lista de IP y/o FQDN en la configuración del servidor.
2. Compruebe que DNS se haya configurado correctamente en los nodos.
3. Haga clic en **Cluster** > **Settings**.
4. En Configuración del protocolo de tiempo de redes, seleccione **no**, que utiliza la configuración NTP estándar.
5. Haga clic en **Guardar cambios**.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Configure el clúster para que escuche las transmisiones NTP

Con el modo de retransmisión, puede ordenar a cada nodo de un clúster que escuche en la red de mensajes de retransmisión de protocolo de tiempo de redes (NTP) de un servidor determinado.

Lo que necesitará

- Para poder configurar esta opción, debe tener privilegios de administrador del clúster.
- Debe configurar un servidor NTP en la red como servidor de retransmisión.

Pasos

1. Haga clic en **Cluster** > **Settings**.
2. Introduzca en la lista de servidores el servidor NTP o los servidores que utilizan el modo de retransmisión.
3. En Configuración del protocolo de tiempo de redes, seleccione **Sí** para utilizar un cliente de difusión.
4. Para establecer el cliente de difusión, en el campo **servidor**, introduzca el servidor NTP configurado en modo de difusión.
5. Haga clic en **Guardar cambios**.

Obtenga más información

- "Documentación de SolidFire y el software Element"

- "Plugin de NetApp Element para vCenter Server"

Gestionar SNMP

Puede configurar el protocolo simple de gestión de redes (SNMP) en el clúster.

Puede seleccionar un solicitante SNMP, seleccionar la versión de SNMP que desea usar, identificar el usuario de modelo de seguridad basado en usuario de SNMP (USM) y configurar las capturas para supervisar el clúster de SolidFire. También permite ver y acceder a los archivos de base de información de gestión.

Es posible usar tanto direcciones IPv4 como IPv6.

Detalles de SNMP

En la página SNMP de la pestaña Cluster, puede ver la siguiente información.

- **MIB SNMP**

  Los archivos MIB que hay disponibles para que pueda verlos o descargarlos.

- **Configuración general de SNMP**

  Es posible habilitar o deshabilitar SNMP. Después de habilitar SNMP, puede elegir qué versión quiere usar. Si utiliza la versión 2, puede añadir solicitantes y, si usa la versión 3, puede configurar usuarios USM.

- **Configuración de la captura SNMP**

  Puede identificar los retos que quiere recibir. Puede establecer el host, el puerto y la cadena de comunidad para cada destinatario de reto.

Configure un solicitante SNMP

Cuando se habilita la versión 2 de SNMP, puede habilitar o deshabilitar un solicitante, así como configurar solicitantes para que reciban solicitudes SNMP autorizadas.

1. Haga clic en MENU:Cluster[SNMP].
2. En **Configuración general de SNMP**, haga clic en **Sí** para activar SNMP.
3. En la lista **Versión**, seleccione **Versión 2**.
4. En la sección **Requestors**, introduzca la información **Community String** y **Network**.

   De forma predeterminada, la cadena de comunidad es public y la red es localhost. No obstante, puede cambiar estas opciones predeterminadas si lo necesita.

5. **Opcional:** para añadir otro solicitante, haga clic en **Añadir un solicitante** e introduzca la información **cadena de comunidad** y **Red**.
6. Haga clic en **Guardar cambios**.

Obtenga más información

- Configurar las capturas SNMP

- Se pueden ver los datos de objetos gestionados mediante los archivos de base de información de gestión

Configure un usuario USM en SNMP

Al habilitar la versión 3 de SNMP, tendrá que configurar un usuario USM para que reciba las solicitudes de SNMP autorizadas.

1. Haga clic en **Cluster** > **SNMP**.
2. En **Configuración general de SNMP**, haga clic en **Sí** para activar SNMP.
3. En la lista **Versión**, seleccione **Versión 3**.
4. En la sección **usuarios USM**, introduzca el nombre, la contraseña y la contraseña.
5. **Opcional:** para añadir otro usuario USM, haga clic en **Añadir usuario USM** e introduzca el nombre, la contraseña y la frase de paso.
6. Haga clic en **Guardar cambios**.

Configurar las capturas SNMP

Los administradores del sistema pueden utilizar capturas SNMP, también denominadas notificaciones, para supervisar el estado del clúster de SolidFire.

Cuando se habilitan los retos SNMP, el clúster de SolidFire genera retos asociados con las entradas del registro de eventos y las alertas del sistema. Para recibir notificaciones SNMP, tiene que elegir los retos que se tendrían que generar e identificar los destinatarios de la información del reto. De forma predeterminada, no se genera ningún reto.

1. Haga clic en **Cluster** > **SNMP**.
2. Seleccione uno o varios tipos de solapamientos en la sección **Configuración de solapamientos SNMP** que el sistema debe generar:
   - Retos de fallo de clúster
   - Retos de fallo resueltos del clúster
   - Retos de evento de clúster
3. En la sección **destinatarios de la captura**, introduzca la información de host, puerto y cadena de comunidad para un destinatario.
4. **Opcional**: Para agregar otro destinatario de captura, haga clic en **Agregar un destinatario de captura** e introduzca la información de host, puerto y cadena de comunidad.
5. Haga clic en **Guardar cambios**.

Se pueden ver los datos de objetos gestionados mediante los archivos de base de información de gestión

Es posible ver y descargar los archivos de la base de datos de información de administración (MIB) que se usan para definir cada uno de los objetos gestionados. La función SNMP admite el acceso de solo lectura a los objetos que se definen en SolidFire-StorageCluster-MIB.

Los datos estadísticos que se proporcionan en el archivo MIB muestran la actividad del sistema en relación a lo siguiente:

- Estadísticas de clúster
- Estadísticas de volumen
- Estadísticas de volúmenes por cuenta
- Estadísticas de nodo
- Otros datos, como informes, errores y eventos del sistema

El sistema también permite acceder al archivo MIB que contenga los puntos de acceso del nivel superior (OIDS) a los productos SF-Series.

Pasos

1. Haga clic en **Cluster** > **SNMP**.
2. En **MIB de SNMP**, haga clic en el archivo MIB que desee descargar.
3. En la ventana de descarga que aparece, abra o guarde el archivo MIB.

Gestionar unidades

Cada nodo contiene una o varias unidades físicas que se utilizan para almacenar una parte de los datos del clúster. El clúster utiliza la capacidad y el rendimiento de la unidad una vez que esta se ha añadido correctamente a un clúster. Es posible usar la interfaz de usuario de Element para gestionar las unidades.

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Detalles de unidades

En la página Drives de la pestaña Cluster, se proporciona una lista de las unidades activas del clúster. La página se puede filtrar si selecciona de las pestañas Active, Available, Removing, Erasing y Failed.

Cuando se inicializa un clúster por primera vez, la lista de unidades activas está vacía. Puede añadir unidades que no estén asignadas a un clúster y que aparezcan en la pestaña Available después de crear un clúster de SolidFire nuevo.

Los siguientes elementos se muestran en la lista de unidades activas.

- **ID de unidad**

  El número secuencial asignado a la unidad.

- **ID de nodo**

  El número de nodo asignado cuando el nodo se añade al clúster.

- **Nombre de nodo**

  El nombre del nodo que aloja la unidad.

- **Ranura**

  El número de ranura en la que la unidad se encuentra físicamente.

- **Capacidad**

  El tamaño de la unidad, en GB.

- **Serie**

  El número de serie de la unidad.

- **Desgaste restante**

  El indicador del nivel de desgaste.

  El sistema de almacenamiento informa de la cantidad aproximada de desgaste disponible en cada unidad de estado sólido (SSD) para escribir y borrar datos. Una unidad que ha consumido el 5% de los ciclos de escritura y borrado diseñados informa del 95% de desgaste restante. El sistema no actualiza automáticamente la información de desgaste de la unidad; se puede actualizar o cerrar y volver a cargar la página para actualizar la información.

- **Tipo**

  El tipo de unidad. El tipo puede ser de bloque o metadatos.

Gestione los nodos

Desde la página Nodes de la pestaña Cluster, se pueden gestionar los nodos de almacenamiento SolidFire y Fibre Channel.

Si un nodo que se acaba de añadir supone más del 50 % de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("trenzado"), de modo que cumpla con la regla de capacidad. Este sigue siendo el caso hasta que se añada más almacenamiento. Si se añade un nodo muy grande que también desobedece la regla de capacidad, el nodo que antes se había abandonado ya no se quedará abandonado, mientras el nodo recién añadido se vuelve abandonado. La capacidad debe añadirse siempre por parejas para evitar que esto suceda. Cuando un nodo se queda sin poner en cadena, se produce un error del clúster adecuado.

Obtenga más información

Añada un nodo a un clúster

Añada un nodo a un clúster

Es posible añadir nodos a un clúster cuando se necesita más almacenamiento o después de crear el clúster. Los nodos requieren una configuración inicial cuando se conectan por primera vez. Una vez que se configura, aparece en la lista de nodos pendientes y puede añadirlos a un clúster.

La versión de software de cada nodo en un clúster tiene que ser compatible. Cuando añade un nodo a un clúster, el clúster instala la versión del clúster del software NetApp Element en el nuevo nodo según sea necesario.

Es posible añadir nodos de capacidad inferior o superior a un clúster existente. Es posible añadir capacidades de nodos superiores a un clúster para aumentar su capacidad. Cuando se añaden nodos más grandes a un clúster con nodos más pequeños, debe hacerse en parejas. De este modo se le otorga suficiente espacio para que Double Helix pueda mover los datos en caso de que uno de los nodos superiores presente errores. Es posible añadir capacidades de nodos más pequeños a un clúster de nodos más grandes para mejorar el rendimiento.

> Si un nodo que se acaba de añadir supone más del 50 % de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("trenzado"), de modo que cumpla con la regla de capacidad. Este sigue siendo el caso hasta que se añada más almacenamiento. Si se añade un nodo muy grande que también desobedece la regla de capacidad, el nodo que antes se había abandonado ya no se quedará abandonado, mientras el nodo recién añadido se vuelve abandonado. La capacidad debe añadirse siempre por parejas para evitar que esto suceda. Cuando un nodo se convierte en abandonado, se produce el error del clúster strandedCapacity.

"Vídeo de NetApp: Escale según sus necesidades: Ampliar un clúster de SolidFire"

Puede añadir nodos a dispositivos NetApp HCI.

Pasos

1. Seleccione **Cluster** > **Nodes**.
2. Haga clic en **pendiente** para ver la lista de nodos pendientes.

   Una vez completado el proceso de adición de nodos, aparecen en la lista Active Nodes. Hasta entonces, los nodos pendientes aparecen en la lista Pending Active.

   SolidFire instala la versión del software Element del clúster en los nodos pendientes cuando se añaden a un clúster. Esto puede tardar varios minutos.

3. Debe realizar una de las siguientes acciones:
   - Para agregar nodos individuales, haga clic en el icono **acciones** del nodo que desea agregar.
   - Para añadir varios nodos, active la casilla de los nodos que desee agregar y, a continuación, **acciones masivas**. **Nota:** Si el nodo que está agregando tiene una versión diferente del software Element que la versión que se ejecuta en el clúster, el clúster actualiza de forma asíncrona el nodo a la versión del software Element que se ejecuta en el maestro de clústeres. Después de que se actualiza el nodo, se añade automáticamente al clúster. Durante este proceso asíncrono, el nodo tendrá el estado pendingActive.
4. Haga clic en **Agregar**.

   El nodo aparece en la lista de nodos activos.

Obtenga más información

Versiones y compatibilidad de nodos

Versiones y compatibilidad de nodos

La compatibilidad del nodo se basa en la versión del software Element instalada en un nodo. Los clústeres de almacenamiento basados en software Element crean automáticamente la imagen de un nodo en la versión de software Element en el clúster

cuando las versiones del nodo y el clúster no son compatibles.

En la siguiente lista, se describen los niveles de importancia de las versiones del software Element que conforman el número de versión del software Element:

- **Mayor**

  El primer número designa una versión de software. No es posible añadir un nodo con un número de componente principal a un clúster que contenga nodos de otro número de revisión principal ni se puede crear un clúster con nodos de versiones principales mixtas.

- **Menor**

  El segundo número designa mejoras o funciones de software más pequeñas que se aplican en funciones de software existentes que se han incorporado a una versión principal. Este componente aumenta dentro de un componente de versión principal para indicar que esta versión incremental no es compatible con otras versiones incrementales del software Element con un componente secundario distinto. Por ejemplo, 11.0 no es compatible con 11.1 y 11.1 no es compatible con 11.2.

- **Micro**

  El tercer número designa una revisión compatible (versión incremental) con la versión de software Element que representan los componentes principal.secundario. Por ejemplo, 11.0.1 es compatible con 11.0.2 y 11.0 es compatible con 11.0.3.

Los números de versión principal y secundario deben coincidir para ser compatibles. Los números micro no tienen que coincidir para ser compatibles.

Capacidad de clúster en un entorno de nodos mixtos

En un clúster se pueden combinar distintos tipos de nodos. SF-Series 2405, 3010, 4805, 6010, 9605 9010, 19210, 38410 y H-Series pueden coexistir en un clúster.

H-Series consta de nodos H610S-1, H610S-2, H610S-4 y H410S. Estos nodos son compatibles tanto con 10 GbE como con 25 GbE.

Es mejor no mezclar nodos no cifrados y no cifrados. En un clúster de nodos mixtos, ningún nodo puede superar el 33 % de la capacidad total del clúster. Por ejemplo, en un clúster con cuatro nodos SF-Series 4805, el nodo más grande que se puede añadir solo es un nodo SF-Series 9605. El umbral de capacidad del clúster se calcula en función de la pérdida potencial del nodo más grande en esta situación.

A partir de Element 12.0, los siguientes nodos de almacenamiento SF-Series no son compatibles:

- SF3010
- SF6010
- SF9010

Si actualiza uno de estos nodos de almacenamiento a Element 12.0, verá un error indicando que este nodo no es compatible con Element 12.0.

Ver los detalles del nodo

Puede ver detalles de nodos individuales, como etiquetas de servicio, detalles de

unidades y gráficos para la utilización y estadísticas de unidades. La página Nodes de la pestaña Cluster proporciona la columna Version donde puede ver la versión de software de cada nodo.

Pasos

1. Haga clic en **Cluster** > **Nodes**.
2. Para ver los detalles de un nodo específico, haga clic en el icono **acciones** de un nodo.
3. Haga clic en **Ver detalles**.
4. Revise los detalles del nodo:
   - **ID de nodo**: El ID generado por el sistema para el nodo.
   - **Nombre de nodo**: El nombre de host del nodo.
   - **iops 4k** disponible: IOPS configuradas para el nodo.
   - **Función de nodo**: La función que tiene el nodo en el clúster. Los posibles valores son los siguientes:
     - Cluster Master: El nodo que realiza tareas administrativas para todo el clúster y contiene la MVIP y la SVIP.
     - Ensemble Node: Un nodo que participa en el clúster. Hay nodos de 3 o 5 conjuntos, según el tamaño del clúster.
     - Fibre Channel: Un nodo del clúster.
   - **Tipo de nodo**: Tipo de modelo del nodo.
   - **Active Drives**: Número de unidades activas en el nodo.
   - **IP de administración**: La dirección IP de administración (MIP) asignada al nodo para las tareas de administración de red de 1 GbE o 10 GbE.
   - **IP de clúster**: La dirección IP de clúster (CIP) asignada al nodo utilizado para la comunicación entre nodos del mismo clúster.
   - **IP de almacenamiento**: La dirección IP de almacenamiento (SIP) asignada al nodo utilizado para la detección de redes iSCSI y todo el tráfico de red de datos.
   - **ID de VLAN de administración**: ID virtual para la red de área local de administración.
   - **Storage VLAN ID**: El ID virtual de la red de área local de almacenamiento.
   - **Versión**: La versión del software que se ejecuta en cada nodo.
   - **Puerto de replicación**: El puerto utilizado en los nodos para la replicación remota.
   - **Etiqueta de servicio**: El número de etiqueta de servicio exclusivo asignado al nodo.

Ver detalles de los puertos Fibre Channel

Es posible ver detalles de los puertos Fibre Channel, como el estado, el nombre y la dirección de puerto, desde la página puertos FC.

Permite ver información sobre los puertos Fibre Channel que están conectados al clúster.

Pasos

1. Haga clic en **Cluster** > **puertos FC**.
2. Para filtrar información en esta página, haga clic en **filtro**.
3. Consulte los detalles:

- **ID de nodo**: El nodo que aloja la sesión de la conexión.
- **Nombre de nodo**: Nombre de nodo generado por el sistema.
- **Slot**: Número de ranura donde se encuentra el puerto Fibre Channel.
- **Puerto HBA**: Puerto físico en el adaptador de bus de host (HBA) Fibre Channel.
- **WWNN**: El nombre de nodo mundial.
- **WWPN**: El nombre de puerto de destino para todo el mundo.
- **WWN del conmutador**: Nombre mundial del conmutador Fibre Channel.
- **Estado del puerto**: Estado actual del puerto.
- **NPort ID**: El identificador de puerto del nodo en la estructura Fibre Channel.
- **Velocidad**: La velocidad negociada del canal de fibra. Los valores posibles son los siguientes:
  - 4 Gbps
  - 8 Gbps
  - 16 Gbps

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Gestionar redes virtuales

Las redes virtuales del almacenamiento de SolidFire permiten que el tráfico entre varios clientes en redes lógicas independientes se conecten a un clúster. Las conexiones al clúster se separan en la pila de redes mediante el etiquetado de VLAN.

Obtenga más información

- Añadir una red virtual
- Habilite el enrutamiento y el reenvío virtuales
- Editar una red virtual
- Edite las VLAN de VRF
- Eliminar una red virtual

Añadir una red virtual

Es posible añadir una red virtual nueva a la configuración de un clúster para habilitar una conexión de entorno multi-tenant con un clúster donde se ejecuta el software Element.

Lo que necesitará

- Identifique el bloque de direcciones IP que se asignarán a las redes virtuales en los nodos del clúster.
- Identifique una dirección IP de red de almacenamiento (SVIP) que se usará como extremo para todo el tráfico de almacenamiento de NetApp Element.

Debe tener en cuenta los siguientes criterios para esta configuración:

- Las VLAN que no están habilitadas para VRF requieren que haya iniciadores en la misma subred que la SVIP.
- Las VLAN que están habilitadas para VRF no requieren que haya iniciadores en la misma subred que la SVIP y el que enrutamiento esté admitido.
- La SVIP predeterminada no requiere que haya iniciadores en la misma subred que la SVIP y el que enrutamiento esté admitido.

Cuando se añade una red virtual, se crea una interfaz para cada nodo y cada una requiere una dirección IP de red virtual. La cantidad de direcciones IP especificada cuando se crea una red virtual nueva debe ser igual o mayor que la cantidad de nodos del clúster. Las direcciones de red virtuales se aprovisionan de forma masiva y se asignan automáticamente a los nodos individuales. No es necesario asignar manualmente direcciones de red virtual a los nodos del clúster.

Pasos

1. Haga clic en **clúster** > **Red**.
2. Haga clic en **Crear VLAN**.
3. En el cuadro de diálogo **Crear una nueva VLAN**, introduzca valores en los siguientes campos:
   - **Nombre de VLAN**
   - **Etiqueta VLAN**
   - **SVIP**
   - **Netmask**
   - (Opcional) **Descripción**
4. Introduzca la dirección **IP inicial** para el rango de direcciones IP en **IP Address Blocks**.
5. Introduzca el **Tamaño** del intervalo IP como el número de direcciones IP que se incluirán en el bloque.
6. Haga clic en **Agregar un bloque** para agregar un bloque no continuo de direcciones IP para esta VLAN.
7. Haga clic en **Crear VLAN**.

Ver detalles de redes virtuales

Pasos

1. Haga clic en **clúster** > **Red**.
2. Revise los detalles.
   - **ID**: ID exclusivo de la red VLAN, asignada por el sistema.
   - **Nombre**: Nombre exclusivo asignado por el usuario para la red VLAN.
   - **Etiqueta VLAN**: Etiqueta VLAN asignada cuando se creó la red virtual.
   - **SVIP**: Dirección IP virtual de almacenamiento asignada a la red virtual.
   - **Netmask**: Máscara de red para esta red virtual.
   - **Gateway**: Dirección IP única de una puerta de enlace de red virtual. VRF debe estar habilitado.
   - **VRF Enabled**: Indica si el enrutamiento y reenvío virtuales está activado o no.
   - **IP utilizadas**: El rango de direcciones IP de red virtual que se utiliza para la red virtual.

Habilite el enrutamiento y el reenvío virtuales

Puede habilitar el enrutamiento y el reenvío virtuales (VRF), que permite que varias instancias de una tabla de enrutamiento existan en un enrutador y funcionen simultáneamente. Dicha funcionalidad solo está disponible para redes de almacenamiento.

Solo puede habilitar VRF en el momento de crear una VLAN. Si desea volver a un estado sin VRF, debe eliminar y volver a crear la VLAN.

1. Haga clic en **clúster** > **Red**.
2. Para habilitar VRF en una VLAN nueva, seleccione **Crear VLAN**.
   a. Introduzca la información relevante para la nueva VRF/VLAN. Consulte Añadir una red virtual.
   b. Active la casilla de verificación **Activar VRF**.
   c. **Opcional**: Introduzca una puerta de enlace.
3. Haga clic en **Crear VLAN**.

Obtenga más información

Añadir una red virtual

Editar una red virtual

Es posible cambiar los atributos de VLAN, como el nombre de la VLAN, la máscara de red y el tamaño de los bloques de dirección IP. La etiqueta de VLAN y la SVIP no se pueden modificar para una VLAN. El atributo de la puerta de enlace no es un parámetro válido para una VLAN sin VRF.

Si existe alguna sesión de iSCSI, replicación remota u otras sesiones de red, se podría producir un error en la modificación.

Al administrar el tamaño de los rangos de direcciones IP de VLAN, debe tener en cuenta las siguientes limitaciones:

- Solo es posible eliminar direcciones IP del rango de direcciones IP iniciales asignado en el momento en que se creó la VLAN.
- Puede eliminar un bloque de direcciones IP que se agregó después del rango de direcciones IP inicial, pero no puede cambiar el tamaño de un bloque IP eliminando las direcciones IP.
- Cuando intenta quitar direcciones IP, ya sea del rango de direcciones IP inicial o de un bloque IP, que están utilizando los nodos en el clúster, la operación puede generar un error.
- No se pueden reasignar direcciones IP específicas en uso a otros nodos del clúster.

Puede agregar un bloque de direcciones IP mediante el siguiente procedimiento:

1. Seleccione **Cluster** > **Red**.
2. Seleccione el icono Actions de la VLAN que quiera editar.
3. Seleccione **Editar**.
4. En el cuadro de diálogo **Editar VLAN**, introduzca los nuevos atributos para la VLAN.

5. Seleccione **Agregar un bloque** para agregar un bloque no continuo de direcciones IP para la red virtual.
6. Seleccione **Guardar cambios**.

Enlace a artículos de la base de conocimientos de solución de problemas

Enlace a los artículos de la base de conocimientos para obtener ayuda sobre la solución de problemas relacionados con la gestión de los intervalos de direcciones IP de VLAN.

- "Duplique la advertencia de IP después de añadir un nodo de almacenamiento en VLAN en el clúster de Element"
- "Cómo determinar a qué IP de VLAN están en uso y a qué nodos están asignados esas IP en Element"

Edite las VLAN de VRF

Puede cambiar los atributos VLAN del VRF, como el nombre de la VLAN, la máscara de red, la puerta de enlace y los bloques de dirección IP.

1. Haga clic en **clúster** > **Red**.
2. Haga clic en el icono Actions de la VLAN que quiera editar.
3. Haga clic en **Editar**.
4. Introduzca los nuevos atributos para la VLAN del VRF en el cuadro de diálogo **Editar VLAN**.
5. Haga clic en **Guardar cambios**.

Eliminar una red virtual

Puede eliminar un objeto de red virtual. Debe añadir los bloques de dirección a otra red virtual antes de eliminar una red virtual.

1. Haga clic en **clúster** > **Red**.
2. Haga clic en el icono Actions de la VLAN que desea eliminar.
3. Haga clic en **Eliminar**.
4. Confirme el mensaje.

Obtenga más información

Editar una red virtual

Cree un clúster que admita unidades FIPS

La seguridad cada vez resulta más importante para la puesta en marcha de soluciones en muchos entornos de cliente. Los estándares de procesamiento de información federal (FIPS) son estándares de interoperabilidad y seguridad informática. El cifrado certificado FIPS 140-2 para datos en reposo es un componente de la solución de seguridad general.

- "Evite combinar nodos para unidades FIPS"
- "Habilite el cifrado en reposo"
- "Identifique si los nodos están listos para la función de unidades FIPS"
- "Habilite la función de unidades FIPS"

- "Compruebe el estado de la unidad FIPS"
- "Solucione problemas de la función de unidad FIPS"

Evite combinar nodos para unidades FIPS

Para prepararse para habilitar la función de unidades FIPS, debe evitar combinar nodos donde algunos sean compatibles con unidades FIPS y otros no lo sean.

Un clúster se considera compatible con unidades FIPS según las siguientes condiciones:

- Todas las unidades están certificadas como unidades FIPS.
- Todos los nodos son nodos de unidades FIPS.
- El cifrado en reposo (EAR) está habilitado.
- Se habilitó la función de unidades FIPS. Todas las unidades y los nodos deben ser compatibles con FIPS, y el cifrado en reposo debe habilitarse para habilitar la función de unidad FIPS.

Habilite el cifrado en reposo

Puede habilitar y deshabilitar el cifrado en todo el clúster en reposo. Esta función no está habilitada de forma predeterminada. Para admitir las unidades FIPS, debe habilitar el cifrado en reposo.

1. En la interfaz de usuario del software NetApp Element, haga clic en **clúster** > **Configuración**.
2. Haga clic en **Activar cifrado en reposo**.

Obtenga más información

- Habilite y deshabilite el cifrado de un clúster
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Identifique si los nodos están listos para la función de unidades FIPS

Debe comprobar si todos los nodos del clúster de almacenamiento están listos para admitir unidades FIPS mediante el método API GetFipsReport del software NetApp Element.

El informe resultante muestra uno de los siguientes Estados:

- None: El nodo no es compatible con la función de unidades FIPS.
- Parcial: El nodo es compatible con FIPS, pero no todas las unidades son unidades FIPS.
- Ready: El nodo es compatible con FIPS y todas las unidades son unidades FIPS o no existen unidades.

Pasos

1. Con la API de Element, compruebe si los nodos y las unidades del clúster de almacenamiento pueden ver las unidades FIPS introduciendo:

   ```
   GetFipsReport
   ```

2. Revise los resultados y consulte los nodos que no muestran el estado de Ready.
3. En el caso de los nodos que no muestren el estado Listo, compruebe si la unidad es compatible con la función de las unidades FIPS:
   - Utilice la API de Element, introduzca: `GetHardwareList`
   - Observe el valor de **DriveEncryptionCapabilityType**. Si es "fips", el hardware puede admitir la función de unidades FIPS.

     Consulte los detalles acerca de `GetFipsReport` o. `ListDriveHardware` en la "Referencia de la API de Element".
4. Si la unidad no puede admitir la función unidades FIPS, reemplace el hardware con hardware FIPS (nodo o unidades).

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Habilite la función de unidades FIPS

Es posible habilitar la función unidades FIPS mediante el software NetApp Element `EnableFeature` Método API.

El cifrado en reposo debe estar habilitado en el clúster, y todos los nodos y unidades deben ser compatibles con FIPS, tal y como se indica cuando GetFipsReport muestra el estado Ready para todos los nodos.

Paso

1. Mediante la API de Element, habilite FIPS en todas las unidades, introduciendo:

   ```
   EnableFeature params: FipsDrives
   ```

Obtenga más información

- "Gestione el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Compruebe el estado de la unidad FIPS

Puede comprobar si la función de las unidades FIPS está habilitada en el clúster mediante el software NetApp Element `GetFeatureStatus` Método API, que muestra si el estado de las unidades FIPS habilitadas es TRUE o FALSE.

1. Con la API de Element, compruebe la función de las unidades FIPS en el clúster introduciendo:

   ```
   GetFeatureStatus
   ```

2. Revise los resultados del `GetFeatureStatus` Llamada a API. Si el valor de unidades FIPS habilitadas es True, se habilita la función de unidades FIPS.

```
{"enabled": true,
"feature": "FipsDrives"
}
```

Obtenga más información

- "Gestione el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Solucione problemas de la función de unidad FIPS

Con la interfaz de usuario del software NetApp Element, es posible ver alertas sobre errores o errores del clúster en el sistema relacionados con la función de unidades FIPS.

1. Con la interfaz de usuario de Element, seleccione **Informes** > **Alertas**.
2. Busque fallos del clúster, entre los que se incluyen:
   - Las unidades FIPS no coinciden
   - FIPS no cumple las normativas
3. Para obtener sugerencias de resolución, consulte la información sobre el código de avería del clúster.

Obtenga más información

- códigos de error de clúster
- "Gestione el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Habilite FIPS 140-2 para HTTPS en el clúster

Puede utilizar el método API EnableFeature para habilitar el modo operativo FIPS 140-2 para las comunicaciones HTTPS.

Con el software NetApp Element, puede optar por habilitar el modo operativo estándar de procesamiento de información federal (FIPS) 140-2 en el clúster. Al habilitar este modo, se activa el módulo de seguridad criptográfica de NetApp (NCSM) y se utiliza el cifrado certificado FIPS 140-2 de nivel 1 para toda la comunicación mediante HTTPS a la interfaz de usuario y la API de NetApp Element.

> Después de habilitar el modo FIPS 140-2-2, no puede deshabilitarse. Cuando se habilita FIPS 140-2-Mode, cada nodo del clúster se reinicia y ejecuta una prueba automática, lo que garantiza que NCSM se habilite correctamente y funcione en el modo certificado FIPS 140-2-2. Esto provoca una interrupción de las conexiones de gestión y almacenamiento en el clúster. Debe planificar con cuidado y activar este modo únicamente si su entorno necesita el mecanismo de cifrado que ofrece.

Para obtener más información, consulte la información sobre la API de Element.

A continuación se muestra un ejemplo de la solicitud de API para habilitar FIPS:

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "fips"
    },
    "id": 1
}
```

Una vez habilitado este modo operativo, todas las comunicaciones HTTPS utilizan los cifrados aprobados FIPS 140-2.

Obtenga más información

- Cifrados SSL
- "Gestione el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Cifrados SSL

Los cifrados SSL son algoritmos de cifrado que utilizan los hosts para establecer una comunicación segura. Hay cifrados estándar que el software Element admite y no estándar cuando esté habilitado el modo FIPS 140-2-2.

Las siguientes listas proporcionan los cifrados estándar de capa de socket seguro (SSL) que admite el software Element y los cifrados SSL que se admiten cuando el modo FIPS 140-2 está habilitado:

- **FIPS 140-2 desactivado**

  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 habilitado**

  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.

Obtenga más información

Habilite FIPS 140-2 para HTTPS en el clúster

Comience con la gestión de claves externas

La gestión de claves externas (EKM) ofrece gestión de claves de autenticación seguras (AK) en combinación con un servidor de claves externo (EKS) fuera de clúster. El AKS se utiliza para bloquear y desbloquear unidades de cifrado automático (SED) cuando "cifrado en reposo" está habilitado en el clúster. El EKS proporciona una generación y almacenamiento seguros del AKS. El clúster utiliza el protocolo de interoperabilidad de gestión de claves (KMIP, en inglés "Key Management Interoperability Protocol"), un protocolo estándar definido de OASIS para comunicarse con el EKS.

- "Configurar la administración externa"
- "Vuelva a obtener el cifrado de software en la clave maestra de REST"
- "Recuperación de claves de autenticación no válidas o inaccesibles"
- "Comandos de API de gestión de claves externas"

Obtenga más información

- "CreateCluster API que se puede usar para habilitar el cifrado de software en reposo"
- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Configure la gestión de claves externas

Puede seguir estos pasos y usar los métodos API de Element que aparecen para configurar la función de gestión de claves externa.

Lo que necesitará

- Si va a configurar la gestión de claves externas en combinación con el cifrado de software en reposo, debe habilitar el cifrado de software en reposo con el "CreateCluster" método en un nuevo clúster que no contiene volúmenes.

Pasos

1. Establecer una relación de confianza con el servidor de claves externo (EKS).
   a. Cree un par de claves público/privado para el clúster de Element que se utilice para establecer una relación de confianza con el servidor de claves llamando al siguiente método de API: "CreatePublicPrivateKeyPair"
   b. Obtenga la solicitud de firma de certificado (CSR) que la entidad de certificación debe firmar. La CSR permite que el servidor de claves verifique que el clúster de Element que tendrá acceso a las claves se

autentique como clúster de Element. Llame al siguiente método API: "GetClientCertificateSignRequest"

c. Utilice la autoridad EKS/Certificate para firmar la CSR recuperada. Consulte la documentación de terceros para obtener más información.

2. Cree un servidor y un proveedor en el clúster para comunicarse con el EKS. Un proveedor de claves define dónde se debe obtener una clave y un servidor define los atributos específicos del EKS con los que se comunicará.

a. Cree un proveedor de claves en el que residirán los detalles del servidor de claves llamando al siguiente método de API: "CreateKeyProviderKmip"

b. Cree un servidor de claves que proporcione el certificado firmado y el certificado de clave pública de la entidad emisora de certificados llamando a los siguientes métodos API: "CreateKeyServerKmip" "TestKeyServerKmip"

Si la prueba falla, verifique la configuración y la conectividad del servidor. A continuación, repita la prueba.

c. Para agregar el servidor de claves al contenedor de proveedor de claves, llame a los siguientes métodos API:"AddKeyServerToProviderKmip" "TestKeyProviderKmip"

Si la prueba falla, verifique la configuración y la conectividad del servidor. A continuación, repita la prueba.

3. Realice una de las siguientes acciones como siguiente paso para el cifrado en reposo:

a. (Para el cifrado de hardware en reposo) Habilitar "cifrado de hardware en reposo" Mediante la identificación del proveedor de claves que contiene el servidor de claves utilizado para almacenar las claves, llame al "EnableEncryptionAtest" Método API.

> Debe habilitar el cifrado en reposo a través del "API". Si se habilita el cifrado en reposo con el botón existente de interfaz de usuario de Element, la función volverá al uso de claves generadas internamente.

b. (Para el cifrado de software en reposo) en orden de "cifrado de software en reposo" Para utilizar el proveedor de claves recién creado, pase el ID de proveedor de claves al "RekeySoftwareEncryptionAtRestMasterKey" Método API.

Obtenga más información

- "Habilite y deshabilite el cifrado de un clúster"
- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Vuelva a obtener el cifrado de software en la clave maestra de REST

Es posible usar la API de Element para volver a introducir una clave existente. Este proceso crea una nueva clave maestra de reemplazo para el servidor de gestión de claves externo. Las claves maestras siempre se sustituyen por claves maestras nuevas y nunca se duplican ni se sobrescriben.

Es posible que deba volver a introducir la clave como parte de uno de los siguientes procedimientos:

- Cree una nueva clave como parte de un cambio de la gestión de claves interna a la gestión de claves externas.
- Cree una nueva clave como reacción o como protección ante un evento relacionado con la seguridad.

> Este proceso es asíncrono y devuelve una respuesta antes de que se complete la operación de reclave. Puede utilizar el "GetAsyncResult" método para sondear el sistema para ver cuándo se ha completado el proceso.

Lo que necesitará

- Habilitó el cifrado de software en reposo mediante el "CreateCluster" Método en un nuevo clúster que no contiene volúmenes y no tiene I/O. Utilice el enlace:../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] para confirmar que el estado es `enabled` antes de continuar.
- Ya tienes "estableció una relación de confianza" Entre el clúster de SolidFire y un servidor de claves externo (EKS). Ejecute el "TestKeyProviderKmip" método para verificar que se ha establecido una conexión con el proveedor de claves.

Pasos

1. Ejecute el "ListKeyProvidersKmip" Y copie el ID del proveedor de claves (`keyProviderID`).
2. Ejecute el "RekeySoftwareEncryptionAtRestMasterKey" con la `keyManagementType` parámetro como `external` y.. `keyProviderID` Como el número de ID del proveedor de claves del paso anterior:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

3. Copie el `asyncHandle` valor de `RekeySoftwareEncryptionAtRestMasterKey` respuesta del comando.
4. Ejecute el "GetAsyncResult" con el `asyncHandle` valor del paso anterior para confirmar el cambio en la configuración. Desde la respuesta del comando, debe ver que la configuración de la clave maestra anterior se ha actualizado con información de clave nueva. Copie el nuevo ID del proveedor de claves para usarlo en un paso posterior.

```
{
   "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. Ejecute el `GetSoftwareEncryptionatRestInfo` comando para confirmar la información de la nueva clave, incluida la `keyProviderID`, se han actualizado.

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

Obtenga más información

- "Gestione el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Recuperación de claves de autenticación no válidas o inaccesibles

Ocasionalmente, puede producirse un error que requiere la intervención del usuario. En caso de error, se generará un error del clúster (denominado código de avería del clúster). Los dos casos más probables se describen aquí.

El clúster no puede desbloquear las unidades debido a un fallo en el clúster KmipServerFault.

Esto puede suceder cuando el clúster se inicia por primera vez y no se puede acceder al servidor de claves o la clave requerida no está disponible.

1. Siga los pasos de recuperación indicados en los códigos de fallo del clúster (si los hubiera).

Se puede configurar un error slicServiceUnhealthy porque las unidades de metadatos se han marcado como un error y se han colocado en el estado "Available".

Pasos para borrar:

1. Vuelva a añadir las unidades.
2. Después de 3 a 4 minutos, verificar que el `sliceServiceUnhealthy` se borró el error.

Consulte "códigos de error de clúster" si quiere más información.

Comandos de API de gestión de claves externas

Lista de todas las API disponibles para administrar y configurar EKM.

Se utiliza para establecer una relación de confianza entre el clúster y los servidores externos propiedad del cliente:

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

Se utiliza para definir los detalles específicos de los servidores externos propiedad del cliente:

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

Se utiliza para crear y mantener proveedores de claves que gestionan servidores de claves externos:

- CreateKeyProviderKmip

- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

Para obtener información sobre los métodos de API, consulte "Información de referencia de API".

Gestione volúmenes y volúmenes virtuales

Es posible gestionar los datos en un clúster que ejecuta el software Element desde la pestaña Management de la interfaz de usuario de Element. Las funciones de gestión de clúster disponibles incluyen la creación y la gestión de volúmenes de datos, grupos de acceso de volúmenes, iniciadores y políticas de calidad de servicio (QoS).

- "Trabaje con volúmenes"
- "Trabaje con volúmenes virtuales"
- "Trabajar con iniciadores y grupos de acceso de volúmenes"

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Trabaje con volúmenes

El sistema SolidFire aprovisiona el almacenamiento mediante volúmenes. Los volúmenes son dispositivos de bloque a los que los clientes iSCSI o Fibre Channel acceden a través de la red. En la página Volumes de la pestaña Management, puede crear, modificar, clonar y eliminar volúmenes en un nodo. También puede ver estadísticas sobre el ancho de banda de los volúmenes y el uso de I/O.

Obtenga más información

- "Gestione políticas de calidad de servicio"
- "Cree un volumen"
- "Ver detalles de rendimiento de cada volumen"
- "Editar los volúmenes activos"
- "Eliminar un volumen"
- "Restaurar un volumen eliminado"
- "Purgar un volumen"
- "Clonar un volumen"

- "Asigne LUN a volúmenes Fibre Channel"
- "Aplique una política de calidad de servicio en los volúmenes"
- "Quite la asociación de políticas de calidad de servicio de un volumen"

Gestione políticas de calidad de servicio

Una política de calidad de servicio (QoS) permite crear y guardar un ajuste de calidad de servicio estandarizado que se puede aplicar a muchos volúmenes. Las políticas de calidad de servicio se pueden crear, editar y eliminar desde la página QoS Policies de la pestaña Management.

> Si utiliza políticas de calidad de servicio, no use la calidad de servicio personalizada en un volumen. La calidad de servicio personalizada anulará y ajustará los valores de las políticas de calidad de servicio de los volúmenes.

"Vídeo de NetApp: Políticas de calidad de servicio de SolidFire"

Consulte "Rendimiento y calidad del servicio".

- Cree una política de calidad de servicio
- Edite una política de calidad de servicio
- Elimine una política de calidad de servicio

Cree una política de calidad de servicio

Puede crear políticas de calidad de servicio y aplicarlas cuando se creen los volúmenes.

1. Seleccione **Administración** > **políticas QoS**.
2. Haga clic en **Crear directiva QoS**.
3. Introduzca el **Nombre de la directiva**.
4. Introduzca los valores**Min IOPS**, **Max IOPS** y **Burst IOPS**.
5. Haga clic en **Crear directiva QoS**.

Edite una política de calidad de servicio

Una política de calidad de servicio existente se puede cambiar, o bien se pueden editar los valores asociados con esta. Los cambios que se aplican en una política de calidad de servicio afectan a todos los volúmenes asociados con la política.

1. Seleccione **Administración** > **políticas QoS**.
2. Haga clic en el icono Actions de la política de calidad de servicio que quiera editar.
3. En el menú que se abre, seleccione**Edit**.
4. En el cuadro de diálogo **Editar directiva de QoS**, modifique las siguientes propiedades según sea necesario:
   - Nombre de la directiva
   - IOPS mín
   - Tasa máx. De IOPS

◦ IOPS de ráfaga

5. Haga clic en **Guardar cambios**.

Elimine una política de calidad de servicio

Puede eliminar una política de calidad de servicio si ya no es necesaria. Cuando se elimina una política de calidad de servicio, todos los volúmenes asociados con la política se conservan en la configuración de QoS, pero se desasocian de una política.

> Si desea desasociar en lugar de ello un volumen de una política de calidad de servicio, puede cambiar la configuración de calidad de servicio de ese volumen a personalizado.

1. Seleccione **Administración** > **políticas QoS**.
2. Haga clic en el icono Actions de la política de calidad de servicio que quiera eliminar.
3. En el menú que se abre, seleccione **Eliminar**.
4. Confirme la acción.

Obtenga más información

- "Quite la asociación de políticas de calidad de servicio de un volumen"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Gestione los volúmenes

El sistema SolidFire aprovisiona el almacenamiento mediante volúmenes. Los volúmenes son dispositivos de bloque a los que los clientes iSCSI o Fibre Channel acceden a través de la red.

En la página Volumes de la pestaña Management, puede crear, modificar, clonar y eliminar volúmenes en un nodo.

Cree un volumen

Es posible crear un volumen y asociarlo con una cuenta determinada. Cada volumen debe estar asociado con una cuenta. Gracias a esta asociación, la cuenta podrá acceder al volumen a través de iniciadores iSCSI con las credenciales de CHAP.

Puede especificar la configuración de calidad de servicio de un volumen mientras lo crea.

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en **Crear volumen**.
3. En el cuadro de diálogo **Crear un nuevo volumen**, introduzca **Nombre de volumen**.
4. Introduzca el tamaño total del volumen.

> El tamaño de volumen predeterminado se selecciona en GB. Los volúmenes se pueden crear con tamaños en GB o GIB:

◦ 1 GB = 1 000 000 000 bytes

- 1 GIB = 1 073 741 824 bytes

5. Seleccione **Tamaño de bloque** para el volumen.
6. Haga clic en la lista desplegable **cuenta** y seleccione la cuenta que debe tener acceso al volumen.

   Si no existe ninguna cuenta, haga clic en el enlace **Crear cuenta**, escriba un nuevo nombre de cuenta y haga clic en **Crear**. La cuenta se creará y se asociará con el volumen nuevo.

   Si hay más de 50 cuentas, no aparecerá la lista. Comience a escribir y la función de autocompletar mostrará los posibles valores que puede elegir.

7. Para establecer la **calidad del servicio**, realice una de las siguientes acciones:
   a. En **Directiva**, puede seleccionar una directiva QoS existente, si está disponible.
   b. En **Configuración personalizada**, establezca valores mínimos, máximos y de ráfaga personalizados para IOPS o utilice los valores de QoS predeterminados.

      Los volúmenes que tengan un valor de IOPS máximo o de ráfaga superior a 20 20,000 IOPS podrían requerir una profundidad de cola alta o varias sesiones para alcanzar este nivel de IOPS en un único volumen.

8. Haga clic en **Crear volumen**.

Ver los detalles del volumen

1. Seleccione **Gestión** > **volúmenes**.
2. Revise los detalles.
   - **ID**: El ID generado por el sistema para el volumen.
   - **Nombre**: El nombre otorgado al volumen cuando fue creado.
   - **Cuenta**: El nombre de la cuenta asignada al volumen.
   - **Grupos de acceso**: El nombre del grupo o los grupos de acceso de volúmenes a los que pertenece el volumen.
   - **Acceso**: Tipo de acceso asignado al volumen cuando se creó. Los posibles valores son los siguientes:
     - Read/Write: Se aceptan todas las lecturas y las escrituras.
     - Read Only: Se permite toda la actividad de lectura, pero no la de escritura.
     - Locked: Solo se permite el acceso de administrador.
     - ReplicationTarget: Se designa como un volumen de destino en una pareja de volúmenes replicada.
   - **Utilizado**: El porcentaje de espacio utilizado en el volumen.
   - **Tamaño**: El tamaño total (en GB) del volumen.
   - **Instantáneas**: El número de instantáneas creadas para el volumen.
   - **Política de QoS**: Nombre y enlace a la política de QoS definida por el usuario.
   - **Min IOPS**: El número mínimo de IOPS garantizado para el volumen.
   - **Max IOPS**: El número máximo de IOPS permitido para el volumen.
   - **Burst IOPS**: El número máximo de IOPS permitido durante un breve período de tiempo para el volumen. El valor predeterminado es de 15 15,000.
   - **Atributos**: Atributos que se han asignado al volumen como par clave/valor mediante un método API.

- **512e**: Indica si 512e está habilitado en un volumen. Los posibles valores son los siguientes:
  - Sí
  - No
- **Creado el**: Fecha y hora en que se creó el volumen.

Ver los detalles de cada volumen

Es posible ver estadísticas de rendimiento de cada volumen.

1. Seleccione **Informes** > **rendimiento de volumen**.
2. En la lista de volúmenes, haga clic en el icono Actions de un volumen.
3. Haga clic en **Ver detalles**.

   Aparecerá una bandeja en la parte inferior de la página con información general sobre el volumen.
4. Para ver información más detallada sobre el volumen, haga clic en **Ver más detalles**.

   El sistema muestra información detallada y gráficos de rendimiento del volumen.

Editar los volúmenes activos

Es posible modificar atributos de volúmenes, como los valores de calidad de servicio, el tamaño de los volúmenes y la unidad de medida en la que se calculan los valores de bytes. También se puede modificar el acceso de la cuenta para el uso de la replicación o para restringir el acceso al volumen.

Puede cambiar el tamaño de un volumen cuando haya espacio suficiente en el clúster en las siguientes condiciones:

- Condiciones de funcionamiento normales.
- Se informa de los errores de los volúmenes.
- El volumen se clona.
- El volumen se vuelve a sincronizar.

Pasos

1. Seleccione **Gestión** > **volúmenes**.
2. En la ventana **activo**, haga clic en el icono acciones del volumen que desea editar.
3. Haga clic en **Editar**.
4. **Opcional:** cambie el tamaño total del volumen.
   - Puede aumentar el tamaño del volumen, pero no reducirlo. En cada operación de ajuste de tamaño, solo se puede ajustar el tamaño de un volumen. Las operaciones de recopilación de datos basura y las actualizaciones de software no interrumpen la operación de cambio de tamaño.
   - Si desea ajustar el tamaño del volumen para la replicación, primero debe aumentar el tamaño del volumen asignado como el destino de replicación. Posteriormente, puede cambiar el tamaño del volumen de origen. El tamaño del volumen de destino puede ser mayor o igual que el del volumen de origen, pero no menor.

     El tamaño de volumen predeterminado se selecciona en GB. Los volúmenes se pueden crear con tamaños en GB o GIB:

- 1 GB = 1 000 000 000 bytes
- 1 GIB = 1 073 741 824 bytes

5. **Opcional:** Seleccione un nivel de acceso de cuenta diferente de uno de los siguientes:
   - Solo lectura
   - Lectura/Escritura
   - Bloqueado
   - Destino de replicación
6. **Opcional:** Seleccione la cuenta que debería tener acceso al volumen.

   Si la cuenta no existe, haga clic en el enlace **Crear cuenta**, escriba un nuevo nombre de cuenta y haga clic en **Crear**. La cuenta se creará y se asociará con el volumen.

   Si hay más de 50 cuentas, no aparecerá la lista. Comience a escribir y la función de autocompletar mostrará los posibles valores que puede elegir.

7. **Opcional:** para cambiar la selección en **calidad de servicio**, realice una de las siguientes acciones:
   a. En **Directiva**, puede seleccionar una directiva QoS existente, si está disponible.
   b. En **Configuración personalizada**, establezca valores mínimos, máximos y de ráfaga personalizados para IOPS o utilice los valores de QoS predeterminados.

   Si utiliza políticas de calidad de servicio en un volumen, puede establecer la calidad de servicio personalizada para quitar la asociación de la política de calidad de servicio con el volumen. La calidad de servicio personalizada anulará y ajustará los valores de las políticas de calidad de servicio de los volúmenes.

   Cuando cambie los valores de IOPS, debe incrementar sus diez o cien. Los valores de entrada deben ser números enteros válidos.

   Configure los volúmenes con un valor de ráfaga muy alto. De este modo, el sistema podrá procesar grandes cargas de trabajo secuenciales en bloque ocasionales con mayor rapidez, a la vez que se limitan las IOPS sostenidas de un volumen.

8. Haga clic en **Guardar cambios**.

Eliminar un volumen

Es posible eliminar uno o varios volúmenes de un clúster de almacenamiento de Element.

El sistema no purga de manera inmediata un volumen eliminado, sino que este sigue disponible durante aproximadamente ocho horas. Si un volumen se restaura antes de que el sistema lo purgue, el volumen volverá a conectarse y las conexiones iSCSI se restaurarán.

Si se elimina el volumen que se utilizó para crear una snapshot, sus snapshots asociadas pasan a estar inactivas. Cuando se purgan los volúmenes de origen eliminados, también se eliminan del sistema las snapshots inactivas asociadas.

Los volúmenes persistentes asociados con servicios de gestión se crean y se asignan a una nueva cuenta durante la instalación o la actualización. Si utiliza volúmenes persistentes, no modifique o elimine los volúmenes o su cuenta asociada.

Pasos

1. Seleccione **Gestión** > **volúmenes**.
2. Para eliminar un solo volumen, realice los siguientes pasos:
   a. Haga clic en el icono Actions del volumen que desea eliminar.
   b. En el menú que se abre, haga clic en **Eliminar**.
   c. Confirme la acción.

   El sistema mueve el volumen al área **borrada** de la página **Volumes**.
3. Para eliminar varios volúmenes, realice los siguientes pasos:
   a. En la lista de volúmenes, active la casilla junto a los volúmenes que quiera eliminar.
   b. Haga clic en **acciones masivas**.
   c. En el menú que se abre, haga clic en **Eliminar**.
   d. Confirme la acción.

   El sistema mueve los volúmenes al área **Deleted** de la página **Volumes**.

Restaurar un volumen eliminado

Un volumen se puede restaurar en el sistema si se eliminó, pero aún no se purgó. El sistema purga un volumen de manera automática aproximadamente ocho horas después de que fue eliminado. Si el sistema purgó el volumen, no podrá restaurarlo.

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en la ficha **eliminado** para ver la lista de volúmenes eliminados.
3. Haga clic en el icono Actions del volumen que desea restaurar.
4. En el menú que se abre, haga clic en **Restaurar**.
5. Confirme la acción.

   El volumen se coloca en la lista **volúmenes activos** y se restauran las conexiones iSCSI con el volumen.

Purgar un volumen

Cuando se purga un volumen, este se quita de forma permanente del sistema y Se pierden todos los datos del volumen.

El sistema purga de manera automática un volumen eliminado ocho horas después de su eliminación. Sin embargo, si desea purgar un volumen antes de la hora programada, puede hacerlo.

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en el botón **eliminado**.
3. Ejecute los pasos para purgar un único volumen o varios volúmenes.

Opción	Pasos
Purgar un único volumen	a. Haga clic en el icono Actions del volumen que desea purgar. b. Haga clic en **Purgar**. c. Confirme la acción.
Purgar varios volúmenes	a. Seleccione los volúmenes que desea purgar. b. Haga clic en **acciones masivas**. c. En el menú que se abre, seleccione **Purge**. d. Confirme la acción.

Clonar un volumen

Un clon se puede crear de un solo volumen o de varios volúmenes para hacer una copia de los datos en un momento específico. Cuando se clona un volumen, el sistema crea una copia de Snapshot del volumen y, a continuación, crea una copia de los datos que se indican en la copia de Snapshot. Este es un proceso asíncrono, y la cantidad de tiempo que requiere el proceso depende del tamaño del volumen que se clona y de la carga del clúster actual.

El clúster admite hasta dos solicitudes de clones en ejecución por volumen a la vez y hasta ocho operaciones de clones de volúmenes activos a la vez. Las solicitudes que superen este límite se pondrán en cola para procesarlas más adelante.

Los sistemas operativos difieren en la forma en que tratan los volúmenes clonados. VMware ESXi tratará un volumen clonado como una copia de volumen o un volumen Snapshot. El volumen será un dispositivo disponible para usar para crear un nuevo almacén de datos. Para obtener más información sobre el montaje de volúmenes de clones y el tratamiento de LUN de copias Snapshot, consulte la documentación de VMware en "Montar una copia de almacén de datos VMFS" y.. "Gestión de almacenes de datos VMFS duplicados".

Antes de truncar un volumen clonado mediante el clonado en un tamaño más pequeño, asegúrese de preparar las particiones de manera que se adapten al volumen inferior.

Pasos

1. Seleccione **Gestión** > **volúmenes**.
2. Para clonar un solo volumen, realice los siguientes pasos:
   a. En la lista de volúmenes de la página **activo**, haga clic en el icono acciones del volumen que desea clonar.
   b. En el menú que se abre, haga clic en **Clonar**.
   c. En la ventana **Clone Volume**, introduzca un nombre de volumen para el volumen recién clonado.
   d. Seleccione un tamaño y una medida para el volumen utilizando el cuadro de número **Tamaño de volumen** y la lista.

      El tamaño de volumen predeterminado se selecciona en GB. Los volúmenes se pueden crear con tamaños en GB o GIB:

- 1 GB = 1 000 000 000 bytes
- 1 GIB = 1 073 741 824 bytes

e. Seleccione el tipo de acceso para el volumen que se acaba de clonar.

f. Seleccione una cuenta para asociarla con el volumen recién clonado en la lista **cuenta**.

> Puede crear una cuenta durante este paso si hace clic en el enlace **Crear cuenta**, escribe un nombre de cuenta y hace clic en **Crear**. El sistema agrega automáticamente la cuenta a la lista **cuenta** después de crearla.

3. Para clonar varios volúmenes, realice los siguientes pasos:

a. En la lista de volúmenes de la página **Active**, marque la casilla junto a los volúmenes que desee clonar.

b. Haga clic en **acciones masivas**.

c. En el menú que se abre, seleccione **Clonar**.

d. En el cuadro de diálogo **Clonar varios volúmenes**, introduzca un prefijo para los volúmenes clonados en el campo **prefijo de nombre de volumen nuevo**.

e. Seleccione una cuenta para asociarla con los volúmenes clonados en la lista **cuenta**.

f. Seleccione el tipo de acceso de los volúmenes clonados.

4. Haga clic en **Iniciar clonación**.

> Al aumentar el tamaño del volumen de un clon, se genera un volumen nuevo con espacio libre adicional al final del volumen. Según cómo use el volumen, podría necesitar ampliar las particiones o crear otras nuevas en el espacio libre para utilizarlo.

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Asigne LUN a volúmenes Fibre Channel

Puede cambiar la asignación de LUN para un volumen Fibre Channel en un grupo de acceso de volúmenes. También puede hacer asignaciones de LUN de volúmenes de Fibre Channel cuando se crea un grupo de acceso de volúmenes.

La asignación de nuevos LUN de Fibre Channel es una función avanzada y podría tener consecuencias desconocidas en el host de conexión. Por ejemplo, el ID del nuevo LUN podría no detectarse automáticamente en el host y este podría requerir un nuevo análisis para detectar el nuevo ID de LUN.

1. Seleccione **Administración** > **grupos de acceso**.
2. Haga clic en el icono Actions del grupo de acceso que quiera editar.
3. En el menú que se abre, seleccione**Edit**.
4. En **asignar ID de LUN** en el cuadro de diálogo **Editar grupo de acceso de volumen**, haga clic en la flecha de la lista **asignaciones de LUN**.
5. Para cada volumen de la lista a la que desea asignar un LUN, introduzca un nuevo valor en el campo **LUN**

correspondiente.

6. Haga clic en **Guardar cambios**.

Aplique una política de calidad de servicio en los volúmenes

Puede aplicar de forma masiva una política de calidad de servicio existente a uno o varios volúmenes.

Debe existir la política de calidad de servicio que desea aplicar de forma masiva.

1. Seleccione **Gestión** > **volúmenes**.
2. En la lista de volúmenes, active la casilla junto a los volúmenes a los que quiera aplicar la política de calidad de servicio.
3. Haga clic en **acciones masivas**.
4. En el menú que aparece, haga clic en **aplicar directiva QoS**.
5. Seleccione la política de calidad de servicio de la lista desplegable.
6. Haga clic en **aplicar**.

Obtenga más información

Políticas de calidad de servicio

Quite la asociación de políticas de calidad de servicio de un volumen

Si desea quitar la asociación de una política de calidad de servicio de un volumen, seleccione una configuración de calidad de servicio personalizada.

El volumen que desea modificar debe estar asociado a una política de calidad de servicio.

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en el icono Actions de un volumen que contiene una política de calidad de servicio que desea modificar.
3. Haga clic en **Editar**.
4. En el menú que aparece en **calidad de servicio**, haga clic en **Configuración personalizada**.
5. Modifique **Min IOPS**, **Max IOPS** y **Burst IOPS**, o mantenga la configuración predeterminada.
6. Haga clic en **Guardar cambios**.

Obtenga más información

Elimine una política de calidad de servicio

Trabaje con volúmenes virtuales

Es posible ver información y realizar tareas en relación con los volúmenes virtuales y sus contenedores de almacenamiento, extremos de protocolo, vinculaciones y hosts asociados mediante la interfaz de usuario de Element.

El sistema de almacenamiento del software NetApp Element se envía con la función Virtual Volumes (VVol)

deshabilitada. Debe realizar una tarea puntual que realice la habilitación manual de la funcionalidad VVol de vSphere a través de la interfaz de usuario de Element.

Después de habilitar la funcionalidad VVol, aparecerá una pestaña VVols en la interfaz de usuario de que ofrece opciones de gestión limitada y supervisión relacionadas con VVol. Además, un componente de software del almacenamiento que se conoce como "proveedor VASA" actúa como un servicio de reconocimiento de almacenamiento de vSphere. La mayoría de los comandos de VVol, como la creación, el clonado y la edición de VVol, se inician en un host de vCenter Server o ESXi y se traducen en el proveedor VASA de API de Element para el sistema de almacenamiento del software Element. Los comandos para crear, eliminar y gestionar contenedores de almacenamiento y eliminar volúmenes virtuales se pueden iniciar mediante la interfaz de usuario de Element.

La mayoría de las configuraciones que se necesitan para usar la funcionalidad Virtual Volumes con los sistemas de almacenamiento del software Element se establecen en vSphere. Consulte la guía de configuración de Virtual Volumes de VMware vSphere para el almacenamiento SolidFire_ para registrar el proveedor VASA en vCenter, crear y gestionar almacenes de datos de VVol, y gestionar el almacenamiento en función de políticas.

No se deben registrar más de un proveedor de VASA de NetApp Element en una sola instancia de vCenter. Cuando se añade un segundo proveedor de VASA NetApp Element, esto hace que no se pueda acceder a todos los almacenes de datos DE VVOL.

La compatibilidad CON VASA para varias vCenter está disponible como revisión de actualización si ya se registró un proveedor de VASA en el para vCenter. Para instalar, descargue el archivo VASA39 .tar.gz de "Descargas de software de NetApp" el sitio y siga las instrucciones en el manifiesto. El proveedor VASA de NetApp Element utiliza un certificado de NetApp. Con este parche, vCenter utiliza el certificado sin modificar para admitir varias instancias de vCenter para que usen VASA y VVol. No modifique el certificado. VASA no admite los certificados SSL personalizados.

Obtenga más información

- Habilite Virtual Volumes
- Ver los detalles de los volúmenes virtuales
- Eliminar un volumen virtual
- Cree un contenedor de almacenamiento
- Editar un contenedor de almacenamiento
- Eliminar un contenedor de almacenamiento
- Extremos de protocolo
- Vinculaciones
- Detalles del host

Habilite Virtual Volumes

Debe habilitar manualmente la funcionalidad vSphere Virtual Volumes (VVol) de a través del software NetApp Element. El sistema de software Element viene con la funcionalidad VVol deshabilitada de forma predeterminada y no se habilita automáticamente como parte de una nueva instalación o actualización. Habilitar la función VVol es una tarea de configuración que solo debe hacer una vez.

Lo que necesitará

- El clúster debe ejecutar Element 9.0 o una versión posterior.
- El clúster de debe estar conectado a un entorno ESXi 6.0 o posterior que sea compatible con VVol.
- Si se utiliza Element 11.3 o una versión posterior, el clúster debe estar conectado a un entorno de ESXi 6.0 Update 3 o posterior.

> Al habilitar la funcionalidad vSphere Virtual Volumes, la configuración del software Element se modifica irreversiblemente. Solo debe habilitar la funcionalidad VVol si el clúster está conectado a un entorno de VMware ESXi compatible con VVol. Puede deshabilitar la función VVol y restaurar la configuración predeterminada solo si devuelve el clúster a la imagen de fábrica, lo que elimina todos los datos del sistema.

Pasos

1. Seleccione **Clusters** > **Ajustes**.
2. Busque la configuración específica del clúster para Virtual Volumes.
3. Haga clic en **Activar volúmenes virtuales**.
4. Haga clic en **Sí** para confirmar el cambio de configuración de Virtual Volumes.

   La pestaña **VVols** aparece en la interfaz de usuario de Element.

   > Cuando se habilita la funcionalidad VVol, el clúster de SolidFire inicia el proveedor VASA, abre el puerto 8444 para el tráfico VASA y crea extremos de protocolo que vCenter y todos los hosts ESXi puedan detectar.

5. Copie la URL del proveedor VASA de la configuración de Virtual Volumes (VVols) en **Clusters** > **Settings**. Esta URL se usará para registrar el proveedor VASA en vCenter.
6. Cree un contenedor de almacenamiento en **VVols** > **contenedores de almacenamiento**.

   > Debe crear al menos un contenedor de almacenamiento para que se puedan aprovisionar las máquinas virtuales en un almacén de datos de VVol.

7. Seleccione **VVols** > **Protocol Endpoints**.
8. Compruebe que se ha creado un extremo de protocolo para cada nodo del clúster.

   > Se requieren tareas adicionales de configuración en vSphere. Consulte la guía de configuración de Virtual Volumes de VMware vSphere para el almacenamiento SolidFire_ para registrar el proveedor VASA en vCenter, crear y gestionar almacenes de datos de VVol, y gestionar el almacenamiento en función de políticas.

Obtenga más información

"Guía de configuración de VMware vSphere Virtual Volumes para SolidFire Storage"

Ver los detalles de los volúmenes virtuales

En la interfaz de usuario de Element, se puede revisar la información relacionada con los volúmenes virtuales activos del clúster. También se puede ver la actividad de rendimiento de cada volumen virtual, como la entrada, la salida, el rendimiento y la latencia,

profundidad de cola e información de volumen.

Lo que necesitará

- Debe haber habilitado la funcionalidad VVol en la interfaz de usuario de Element para el clúster.
- Debe haber creado un contenedor de almacenamiento asociado.
- Debe haber configurado el clúster de vSphere para usar la funcionalidad VVol del software Element.
- Debe haber creado al menos una máquina virtual en vSphere.

Pasos

1. Haga clic en **VVols** > **Virtual Volumes**.

   Se muestra la información de todos los volúmenes virtuales activos.

2. Haga clic en el icono **acciones** del volumen virtual que desee revisar.
3. En el menú que se abre, seleccione **Ver detalles**.

Detalles

La página Virtual Volumes de la pestaña VVols proporciona información sobre cada volumen virtual activo en el clúster, como el ID de volumen, el ID de snapshot, el ID de volumen virtual primario y el ID de volumen virtual.

- **ID de volumen**: El ID del volumen subyacente.
- **ID de instantánea**: El ID de la instantánea de volumen subyacente. El valor es 0 si el volumen virtual no representa una snapshot de SolidFire.
- **Id. De volumen virtual principal**: El ID de volumen virtual del volumen virtual principal. Si el ID solo está formado por ceros, indica que el volumen virtual es independiente y no tiene ningún enlace a un volumen principal.
- **Virtual Volume ID**: El UUID del volumen virtual.
- **Nombre**: Nombre asignado al volumen virtual.
- **Contenedor de almacenamiento**: El contenedor de almacenamiento que posee el volumen virtual.
- **Tipo de SO invitado**: Sistema operativo asociado al volumen virtual.
- **Tipo de volumen virtual**: Tipo de volumen virtual: Config, datos, memoria, intercambio u otro.
- **Access**: Los permisos de lectura y escritura asignados al volumen virtual.
- **Tamaño**: El tamaño del volumen virtual en GB o GIB.
- **Instantáneas**: El número de instantáneas asociadas. Haga clic en el número para vincular a detalles de instantánea.
- **Min IOPS**: El valor mínimo de QoS de IOPS del volumen virtual.
- **Max IOPS**: El valor máximo de QoS para IOPS del volumen virtual.
- **Burst IOPS**: El valor máximo de QoS de ráfaga del volumen virtual.
- **VMW_VMID**: VMware define la información de los campos que van precedidos por "VMW_".
- **Crear tiempo**: La hora en que se completó la tarea de creación de volumen virtual.

Detalles de cada volumen virtual

La página Virtual Volumes de la pestaña VVols proporciona la siguiente información sobre volúmenes virtuales cuando selecciona un volumen virtual y desea ver sus detalles.

- **VMW_XXX**: VMware define la información de los campos que van precedidos por "VMW_".
- **Id. De volumen virtual principal**: El ID de volumen virtual del volumen virtual principal. Si el ID solo está formado por ceros, indica que el volumen virtual es independiente y no tiene ningún enlace a un volumen principal.
- **Virtual Volume ID**: El UUID del volumen virtual.
- **Tipo de volumen virtual**: Tipo de volumen virtual: Config, datos, memoria, intercambio u otro.
- **ID de volumen**: El ID del volumen subyacente.
- **Access**: Los permisos de lectura y escritura asignados al volumen virtual.
- **Nombre de cuenta**: Nombre de la cuenta que contiene el volumen.
- **Grupos de acceso**: Grupos de acceso de volúmenes asociados.
- **Tamaño total del volumen**: Capacidad total aprovisionada en bytes.
- * Bloques no cero*: Número total de bloques de 4 KiB con datos después de haber completado la última operación de recopilación de basura.
- * Cero bloques*: Número total de bloques de 4 KiB sin datos después de haber completado la última ronda de recolección de basura.
- **Instantáneas**: El número de instantáneas asociadas. Haga clic en el número para vincular a detalles de instantánea.
- **Min IOPS**: El valor mínimo de QoS de IOPS del volumen virtual.
- **Max IOPS**: El valor máximo de QoS para IOPS del volumen virtual.
- **Burst IOPS**: El valor máximo de QoS de ráfaga del volumen virtual.
- **Activar 512**: Debido a que los volúmenes virtuales siempre utilizan emulación de tamaño de bloque de 512 bytes, el valor es siempre yes.
- **Volúmenes emparejados**: Indica si un volumen está emparejado.
- **Crear tiempo**: La hora en que se completó la tarea de creación de volumen virtual.
- **Tamaño de los bloques**: Tamaño de los bloques en el volumen.
- **Escrituras no alineadas**: Para volúmenes 512e, el número de operaciones de escritura que no estaban en un ámbito de sector 4k. Si el número de escrituras no alineadas es grande, puede indicar que la alineación de las particiones no es la adecuada.
- **Lecturas no alineadas**: Para los volúmenes 512e, el número de operaciones de lectura que no estaban en un ámbito del sector 4k. Si el número de lecturas no alineadas es grande, puede indicar que la alineación de las particiones no es la adecuada.
- **SsiEUIDeviceID**: Identificador único global de dispositivo SCSI para el volumen en formato de 16 bytes basado en EUI-64.
- **SscsiNAADeviceID**: Identificador de dispositivo SCSI exclusivo global para el volumen en el formato extendido registrado de NAA según IEEE.
- **Atributos**: Lista de pares nombre-valor en formato de objeto JSON.

Eliminar un volumen virtual

Si bien los volúmenes virtuales se deben eliminar siempre en el nivel de gestión de VMware, la funcionalidad que le permite eliminar volúmenes virtuales se habilita en la interfaz de usuario de Element. Solo debe eliminar un volumen virtual en la interfaz de usuario de Element cuando sea absolutamente necesario, como cuando vSphere no logra limpiar los volúmenes virtuales en el almacenamiento de SolidFire.

1. Seleccione **VVols** > **Virtual Volumes**.
2. Haga clic en el icono Actions del volumen virtual que desee eliminar.
3. En el menú que se abre, seleccione **Eliminar**.

> Debe eliminar un volumen virtual en el nivel de gestión de VMware para garantizar que el volumen virtual esté correctamente desvinculado antes de su eliminación. Solo debe eliminar un volumen virtual en la interfaz de usuario de Element cuando sea absolutamente necesario, como cuando vSphere no logra limpiar los volúmenes virtuales en el almacenamiento de SolidFire. Si elimina un volumen virtual en la interfaz de usuario de Element, el volumen se depurará inmediatamente.

4. Confirme la acción.
5. Actualice la lista de volúmenes virtuales para confirmar que el volumen virtual se ha eliminado.
6. **Opcional**: Seleccione **Informe** > **Registro de sucesos** para confirmar que la purga se ha realizado correctamente.

Gestione los contenedores de almacenamiento

Un contenedor de almacenamiento es una representación de almacén de datos de vSphere creada en un clúster donde se ejecuta el software Element.

Los contenedores de almacenamiento se crean y están ligados a cuentas de NetApp Element. Un contenedor de almacenamiento que se crea en el almacenamiento Element se muestra como un almacén de datos de vSphere en vCenter y ESXi. Los contenedores de almacenamiento no asignan espacio en el almacenamiento de Element. Simplemente se utilizan para asociar volúmenes virtuales de forma lógica.

Se permite un máximo de cuatro contenedores de almacenamiento por clúster. Se requiere un mínimo de un contenedor de almacenamiento para habilitar la funcionalidad de VVol.

Cree un contenedor de almacenamiento

Los contenedores de almacenamiento se pueden crear en la interfaz de usuario de Element y se pueden detectar en vCenter. Es necesario crear al menos un contenedor de almacenamiento para comenzar a aprovisionar máquinas virtuales respaldadas por VVol.

Antes de comenzar, habilite la funcionalidad de VVol en la interfaz de usuario de Element para el clúster.

Pasos

1. Seleccione **VVols** > **contenedores de almacenamiento**.
2. Haga clic en el botón **Crear contenedores de almacenamiento**.
3. Introduzca la información del contenedor de almacenamiento en el cuadro de diálogo **Crear un contenedor de almacenamiento nuevo**:

a. Escriba un nombre para el contenedor de almacenamiento.

b. Configure el iniciador y los secretos de destino para CHAP.

> Deje los campos CHAP Settings vacíos para que los secretos se generen automáticamente.

c. Haga clic en el botón **Crear contenedor de almacenamiento**.

4. Compruebe que el nuevo contenedor de almacenamiento aparece en la lista de la subpestaña **contenedores de almacenamiento**.

> Dado que el ID de cuenta de NetApp Element se crea automáticamente y se asigna al contenedor de almacenamiento, no es necesario crear una cuenta de forma manual.

Ver los detalles del contenedor de almacenamiento

En la página Storage Containers de la pestaña VVols, puede ver información relativa a todos los contenedores de almacenamiento activos del clúster.

- **ID de cuenta**: El ID de la cuenta NetApp Element asociada con el contenedor de almacenamiento.
- **Nombre**: El nombre del contenedor de almacenamiento.
- **Estado**: El estado del contenedor de almacenamiento. Los posibles valores son los siguientes:
  - Active: El contenedor de almacenamiento está en uso.
  - Locked: El contenedor de almacenamiento está bloqueado.
- **Tipo PE**: Tipo de extremo de protocolo (SCSI es el único protocolo disponible para el software Element).
- **ID del contenedor de almacenamiento**: El UUID del contenedor de almacenamiento del volumen virtual.
- **Active Virtual Volumes**: El número de volúmenes virtuales activos asociados con el contenedor de almacenamiento.

Ver los detalles de cada contenedor de almacenamiento

Si desea ver la información de un contenedor de almacenamiento específico, selecciónelo en la página Storage Containers de la pestaña VVols.

- **ID de cuenta**: El ID de la cuenta NetApp Element asociada con el contenedor de almacenamiento.
- **Nombre**: El nombre del contenedor de almacenamiento.
- **Estado**: El estado del contenedor de almacenamiento. Los posibles valores son los siguientes:
  - Active: El contenedor de almacenamiento está en uso.
  - Locked: El contenedor de almacenamiento está bloqueado.
- **Secreto CHAP del iniciador**: El secreto CHAP único para el iniciador.
- **Secreto objetivo CHAP**: El secreto CHAP único para el destino.
- **ID del contenedor de almacenamiento**: El UUID del contenedor de almacenamiento del volumen virtual.
- **Tipo de extremo de protocolo**: Indica el tipo de extremo de protocolo (SCSI es el único protocolo disponible).

Editar un contenedor de almacenamiento

La autenticación CHAP del contenedor de almacenamiento se puede modificar en la interfaz de usuario de Element.

1. Seleccione **VVols** > **contenedores de almacenamiento**.
2. Haga clic en el icono **acciones** del contenedor de almacenamiento que desee editar.
3. En el menú que se abre, seleccione **Editar**.
4. En CHAP Settings, edite las credenciales de Initiator Secret y Target Secret que se han usado para la autenticación.

   Si no se modifican las credenciales en CHAP Settings, seguirán siendo las mismas. Si deja vacíos los campos de las credenciales, el sistema generará automáticamente secretos nuevos.

5. Haga clic en **Guardar cambios**.

Eliminar un contenedor de almacenamiento

Los contenedores de almacenamiento se pueden eliminar de la interfaz de usuario de Element.

Lo que necesitará

Asegúrese de que todas las máquinas virtuales se hayan eliminado del almacén de datos de VVol.

Pasos

1. Seleccione **VVols** > **contenedores de almacenamiento**.
2. Haga clic en el icono **acciones** del contenedor de almacenamiento que desea eliminar.
3. En el menú que se abre, seleccione **Eliminar**.
4. Confirme la acción.
5. Actualice la lista de contenedores de almacenamiento en la subpestaña **contenedores de almacenamiento** para confirmar que se ha eliminado el contenedor de almacenamiento.

Extremos de protocolo

Los extremos de protocolo son puntos de acceso que utiliza un host para abordar el almacenamiento de un clúster que ejecuta el software NetApp Element. Los usuarios no pueden eliminar ni modificar los extremos de protocolo. Tampoco se pueden asociar con una cuenta ni se pueden añadir a un grupo de acceso de volúmenes.

Un clúster que ejecuta el software Element crea automáticamente un extremo de protocolo por nodo de almacenamiento en el clúster. Por ejemplo, un clúster de almacenamiento de seis nodos tiene seis extremos de protocolo que se asignan a cada host ESXi. Los extremos de protocolo se gestionan dinámicamente con el software Element y se crean, mueven o eliminan según sea necesario sin intervención. Los extremos de protocolo son el objetivo para las rutas múltiples y actúan como proxy I/o para las LUN subsidiarias. Cada extremo de protocolo consume una dirección SCSI disponible, al igual que un destino iSCSI estándar. Los extremos de protocolo aparecen como un dispositivo de almacenamiento de bloque único (512 bytes) en el cliente vSphere, pero este dispositivo de almacenamiento no está disponible para formatearse o usarse como almacenamiento.

ISCSI es el único protocolo compatible. No se admite el protocolo Fibre Channel.

Detalles de los extremos de protocolo

La página Protocol Endpoints en la pestaña VVols proporciona información sobre extremos de protocolo.

- **ID de proveedor primario**

  El ID del proveedor de extremo de protocolo principal.

- **ID de proveedor secundario**

  El ID del proveedor de extremo de protocolo secundario.

- **ID de extremo de protocolo**

  El UUID del extremo de protocolo.

- **Estado del extremo de protocolo**

  El estado del extremo de protocolo. Los valores posibles son los siguientes:

  - Active: El extremo de protocolo está en uso.
  - Start: El extremo de protocolo se está iniciando.
  - Failover: El extremo de protocolo se conmutó al nodo de respaldo.
  - Reserved: El extremo de protocolo está reservado.

- **Tipo de proveedor**

  El tipo de proveedor del extremo de protocolo. Los valores posibles son los siguientes:

  - Primario
  - Secundario

- **SCSI NAA DEVICE ID**

  El identificador exclusivo de dispositivo SCSI para el extremo de protocolo a nivel global en el formato extendido registrado de NAA según la norma IEEE.

Vinculaciones

Para realizar operaciones de I/o con un volumen virtual, el volumen virtual se debe vincular primero a un host ESXi.

El clúster de SolidFire elige un extremo de protocolo adecuado, crea una vinculación que asocia el host ESXi y el volumen virtual con el extremo del protocolo, y devuelve la vinculación al host ESXi. Una vez enlazados, el host ESXi puede llevar a cabo operaciones de I/o con el volumen virtual vinculado.

Detalles de vinculaciones

La página Bindings de la pestaña VVols proporciona información relacionada con la vinculación de cada volumen virtual.

Se muestra la siguiente información:

- **ID de host**

  El UUID del host ESXi que aloja los volúmenes virtuales y es conocido para el clúster.

- **ID de extremo de protocolo**

  Los ID de extremo de protocolo que corresponden a cada nodo del clúster de SolidFire.

- **Protocol Endpoint in Band ID**

  El ID de dispositivo SCSI de NAA según el extremo de protocolo.

- **Tipo de extremo de protocolo**

  El tipo de extremo de protocolo.

- **ID de enlace de VVol**

  El UUID de vinculación del volumen virtual.

- **ID de VVol**

  El identificador único universal (UUID) del volumen virtual.

- **ID secundario de VVol**

  El ID secundario del volumen virtual que es un ID de LUN de segundo nivel para SCSI.

Detalles del host

La página hosts de la pestaña VVols proporciona información sobre los hosts VMware ESXi que alojan los volúmenes virtuales.

Se muestra la siguiente información:

- **ID de host**

  El UUID del host ESXi que aloja los volúmenes virtuales y es conocido para el clúster.

- **Dirección de host**

  La dirección IP o el nombre DNS del host ESXi.

- **Enlaces**

  Los ID de vinculación de todos los volúmenes virtuales que están vinculados por el host ESXi.

- **ID de clúster ESX**

  El ID del clúster host de vSphere o GUID de vCenter.

- **IQN del iniciador**

  Los IQN de iniciador para el host de volúmenes virtuales.

- **ID de extremo de protocolo de SolidFire**

  Los extremos del protocolo que el host ESXi puede ver en ese momento.

Trabajar con iniciadores y grupos de acceso de volúmenes

Es posible usar iniciadores iSCSI o iniciadores de Fibre Channel para acceder a los volúmenes definidos dentro de los grupos de acceso de volúmenes.

Los grupos de acceso se pueden crear asignando IQN de iniciadores de iSCSI o WWPN de Fibre Channel en una colección de volúmenes. Cada IQN que se añade a un grupo de acceso puede acceder a cada volumen del grupo sin necesidad de contar con autenticación CHAP.

Existen dos tipos de métodos de autenticación CHAP:

- Autenticación CHAP en el nivel de la cuenta: Se puede asignar la autenticación CHAP para la cuenta.
- Autenticación CHAP a nivel de iniciador: Puede asignar secretos y destino CHAP únicos para iniciadores específicos sin estar enlazados a una única cuenta en. Esta autenticación CHAP a nivel de iniciador sustituye las credenciales de nivel de cuenta.

De manera opcional, con CHAP por iniciador, puede aplicar la autorización de iniciador y la autenticación CHAP por iniciador. Estas opciones se pueden definir por iniciador y un grupo de acceso puede contener una combinación de iniciadores con diferentes opciones.

Cada WWPN que se añade a un grupo de acceso habilita el acceso a la red de Fibre Channel a los volúmenes del grupo de acceso.

Los grupos de acceso de volúmenes presentan los siguientes límites:

- Se permiten hasta 64 IQN o WWPN en un grupo de acceso.
- Un grupo de acceso puede estar formado por un máximo de 2000 volúmenes.
- Un IQN o un WWPN solo pueden pertenecer a un grupo de acceso.
- Un volumen puede pertenecer a hasta cuatro grupos de acceso.

Obtenga más información

- Cree un grupo de acceso de volúmenes
- Añada volúmenes a un grupo de acceso
- Quite volúmenes de un grupo de acceso
- Cree un iniciador
- Edite un iniciador
- Añada un único iniciador a un grupo de acceso de volúmenes
- Añada varios iniciadores a un grupo de acceso de volúmenes
- Quite los iniciadores de un grupo de acceso
- Eliminar un grupo de acceso
- Eliminar un iniciador

Cree un grupo de acceso de volúmenes

Los grupos de acceso de volúmenes se pueden crear asignando iniciadores a una colección de volúmenes para garantizar el acceso seguro. A continuación, podrá otorgar acceso a los volúmenes del grupo con un secreto de iniciador CHAP de cuenta y un secreto de destino.

Si utiliza CHAP basado en iniciador, puede añadir credenciales de CHAP para un único iniciador en un grupo de acceso de volúmenes, lo que proporciona más seguridad. Esto permite aplicar esta opción a los grupos de acceso de volúmenes que ya existen.

Pasos

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en **Crear grupo de acceso**.
3. Escriba un nombre para el grupo de acceso de volúmenes en el campo **Nombre**.
4. Añada un iniciador al grupo de acceso de volúmenes de una de las siguientes maneras:

Opción	Descripción
Se añade un iniciador de Fibre Channel	a. En Add Initiators, seleccione un iniciador de Fibre Channel existente en la lista Unbound Fibre Channel Initiators. b. Haga clic en **Agregar iniciador FC**. Puede crear un iniciador durante este paso si hace clic en el enlace **Crear iniciador**, escribe un nombre de iniciador y hace clic en **Crear**. El sistema añade automáticamente el iniciador a la lista Initiators después de crearlo. A continuación, se ofrece un ejemplo de formato: `5f:47:ac:c0:5c:74:d4:02`

Opción	Descripción
Adición de un iniciador de iSCSI	En Add Initiators, seleccione un iniciador de existente en la lista Initiators. **Nota:** puede crear un iniciador durante este paso si hace clic en el enlace **Crear iniciador**, introduce un nombre de iniciador y haz clic en **Crear**. El sistema añade automáticamente el iniciador a la lista Initiators después de crearlo. A continuación, se ofrece un ejemplo de formato: `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b` Puede encontrar el IQN del iniciador para cada volumen seleccionando **Ver detalles** en el menú acciones del volumen en la lista **Gestión** > **volúmenes** > **activo**. Al modificar un iniciador, puede cambiar el atributo requiredCHAP a True, lo que permite configurar el secreto de iniciador de destino. Para obtener más información, consulte la información de API acerca del método API ModifyInitiator. "Gestione el almacenamiento con la API de Element"

5. **Opcional:** Agregue más iniciadores según sea necesario.
6. En Agregar volúmenes, seleccione un volumen de la lista **volúmenes**.

   El volumen aparece en la lista **volúmenes adjuntos**.
7. **Opcional:** Agregue más volúmenes según sea necesario.
8. Haga clic en **Crear grupo de acceso**.

Obtenga más información

Añada volúmenes a un grupo de acceso

Ver detalles de cada grupo de acceso

Es posible ver los detalles de un grupo de acceso individual, como iniciadores y volúmenes conectados, en formato gráfico.

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en el icono Actions de un grupo de acceso.
3. Haga clic en **Ver detalles**.

Detalles del grupo de acceso de volúmenes

En la página Access Groups de la pestaña Management, se proporciona información sobre los grupos de acceso de volúmenes.

Se muestra la siguiente información:

- **ID**: El ID generado por el sistema para el grupo de acceso.
- **Nombre**: El nombre otorgado al grupo de acceso cuando se creó.
- **Volúmenes activos**: Número de volúmenes activos en el grupo de acceso.
- **Compresión**: La puntuación de eficiencia de compresión del grupo de acceso.
- **Deduplicación**: La puntuación de eficiencia de deduplicación del grupo de acceso.
- **Thin Provisioning**: Puntuación de eficiencia de thin provisioning para el grupo de acceso.
- **Eficiencia general**: La puntuación de eficiencia general del grupo de acceso.
- **Initiators**: El número de iniciadores conectados al grupo de acceso.

Añada volúmenes a un grupo de acceso

Es posible añadir volúmenes a un grupo de acceso de volúmenes. Cada volumen puede pertenecer a más de un grupo de acceso de volúmenes. Puede ver los grupos a los que pertenece cada volumen en la página **volúmenes activos**.

También puede usar este procedimiento para añadir volúmenes a un grupo de acceso de volúmenes de Fibre Channel.

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en el icono Actions del grupo de acceso al que desea añadir volúmenes.
3. Haga clic en el botón **Editar**.
4. En Agregar volúmenes, seleccione un volumen de la lista **volúmenes**.

   Puede añadir más volúmenes repitiendo este paso.

5. Haga clic en **Guardar cambios**.

Quite volúmenes de un grupo de acceso

Cuando se quita un volumen de un grupo de acceso, el grupo ya no puede acceder a dicho volumen.

Si se modifica la configuración de CHAP en una cuenta o se quitan los iniciadores o los volúmenes de un grupo de acceso, se podría interrumpir el acceso de los iniciadores a los volúmenes de forma inesperada. Para asegurarse de que no se interrumpirá el acceso a los volúmenes de forma inesperada, siempre debe cerrar las sesiones iSCSI afectadas por alguno de los cambios en la cuenta o en el grupo de acceso. Asimismo, compruebe que los iniciadores pueden volver a conectarse con los volúmenes una vez que se hayan realizado los cambios en la configuración del iniciador y la configuración del clúster.

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en el icono Actions del grupo de acceso del que desea quitar volúmenes.
3. Haga clic en **Editar**.
4. En Agregar volúmenes en el cuadro de diálogo **Editar grupo de acceso de volumen**, haga clic en la flecha de la lista **volúmenes adjuntos**.
5. Seleccione el volumen que desea eliminar de la lista y haga clic en el icono **x** para eliminar el volumen de

la lista.

Puede eliminar más volúmenes repitiendo este paso.

6. Haga clic en **Guardar cambios**.

Cree un iniciador

Es posible crear iniciadores iSCSI o Fibre Channel y, opcionalmente, asignarles alias.

También puede asignar atributos CHAP basados en iniciadores mediante una llamada API. Para añadir un nombre de cuenta CHAP y credenciales por iniciador, debe usar `CreateInitiator` Llamada API para eliminar y añadir acceso y atributos CHAP. El acceso del iniciador se puede restringir a una o varias VLAN especificando uno o varios virtualNetworkID a través del `CreateInitiators` y.. `ModifyInitiators` Llamadas API. Si no se especifica ninguna red virtual, el iniciador puede acceder a todas las redes.

Para obtener más detalles, consulte la información de referencia de API."Gestione el almacenamiento con la API de Element"

Pasos

1. Haga clic en **Administración** > **iniciadores**.
2. Haga clic en **Crear iniciador**.
3. Siga los pasos para crear un solo iniciador o varios iniciadores:

Opción	Pasos
Cree un solo iniciador	a. Haga clic en **Crear un único iniciador**. b. Introduzca el IQN o el WWPN del iniciador en el campo **IQN/WWPN**. c. Introduzca un nombre descriptivo para el iniciador en el campo **Alias**. d. Haga clic en **Crear iniciador**.
Cree varios iniciadores	a. Haga clic en **Bulk Create Initiators**. b. Introduzca una lista de varios IQN o WWPN en el cuadro de texto. c. Haga clic en **Add Initiators**. d. Elija un iniciador de la lista resultante y haga clic en el icono Agregar correspondiente en la columna **Alias** para añadir un alias para el iniciador. e. Haga clic en la Marca de verificación para confirmar el nuevo alias. f. Haga clic en **Crear iniciadores**.

Edite un iniciador

Es posible cambiar el alias de un iniciador existente o añadir un alias si aún no hay ninguno.

Para añadir un nombre de cuenta CHAP y credenciales por iniciador, debe usar `ModifyInitiator` Llamada API para eliminar y añadir acceso y atributos CHAP.

Consulte "Gestione el almacenamiento con la API de Element".

Pasos

1. Haga clic en **Administración** > **iniciadores**.
2. Haga clic en el icono Actions del iniciador que quiera editar.
3. Haga clic en **Editar**.
4. Introduzca un nuevo alias para el iniciador en el campo **Alias**.
5. Haga clic en **Guardar cambios**.

Añada un único iniciador a un grupo de acceso de volúmenes

Es posible añadir un iniciador a un grupo de acceso de volúmenes existente.

Cuando se añade un iniciador a un grupo de acceso de volúmenes, el iniciador tiene acceso a todos los volúmenes en ese grupo de acceso de volúmenes.

Para buscar el iniciador de cada volumen, haga clic en el icono Actions y seleccione **View Details** para el volumen en la lista de volúmenes activos.

Si utiliza CHAP basado en iniciador, puede añadir credenciales de CHAP para un único iniciador en un grupo de acceso de volúmenes, lo que proporciona más seguridad. Esto permite aplicar esta opción a los grupos de acceso de volúmenes que ya existen.

Pasos

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en el icono **acciones** del grupo de acceso que desea editar.
3. Haga clic en **Editar**.
4. Para añadir un iniciador de Fibre Channel al grupo de acceso de volúmenes, realice los pasos siguientes:

   a. En Add Initiators, seleccione un iniciador de Fibre Channel existente en la lista **Unbound Fibre Channel Initiators**.

   b. Haga clic en **Agregar iniciador FC**.

   Puede crear un iniciador durante este paso si hace clic en el enlace **Crear iniciador**, escribe un nombre de iniciador y hace clic en **Crear**. El sistema agrega automáticamente el iniciador a la lista **Initiators** después de crearlo.

   A continuación, se ofrece un ejemplo de formato:

```
5f:47:ac:c0:5c:74:d4:02
```

5. Para añadir un iniciador iSCSI al grupo de acceso de volúmenes, en Add Initiators, seleccione un iniciador existente en la lista **Initiators**.

   Puede crear un iniciador durante este paso si hace clic en el enlace **Crear iniciador**, escribe un nombre de iniciador y hace clic en **Crear**. El sistema agrega automáticamente el iniciador a la lista **Initiators** después de crearlo.

El formato aceptado de un IQN de iniciador es el siguiente: iqn.aaaa-mm, en el cual a y m son dígitos, seguidos de texto que solo puede contener dígitos, caracteres alfabéticos en minúscula, un punto (.), dos puntos (:) o un guion (-).

A continuación, se ofrece un ejemplo de formato:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

Puede encontrar el IQN del iniciador para cada volumen desde la página **Management** > **Volumes** Active Volumes haciendo clic en el icono Actions y, a continuación, seleccionando **View Details** para el volumen.

6. Haga clic en **Guardar cambios**.

Añada varios iniciadores a un grupo de acceso de volúmenes

Es posible añadir varios iniciadores a un grupo de acceso de volúmenes existente para permitir el acceso a volúmenes en el grupo de acceso de volúmenes con o sin necesidad de contar con autenticación CHAP.

Cuando se añaden un iniciador a un grupo de acceso de volúmenes, los iniciadores tienen acceso a todos los volúmenes en ese grupo de acceso de volúmenes.

Para buscar el iniciador de cada volumen, haga clic en el icono Actions y, a continuación, en **View Details** para el volumen en la lista de volúmenes activos.

Es posible añadir varios iniciadores a un grupo de acceso de volúmenes existente para habilitar el acceso a volúmenes y asignar credenciales CHAP únicas para cada iniciador de ese grupo de acceso de volúmenes. Esto permite aplicar esta opción a los grupos de acceso de volúmenes que ya existen.

Puede asignar atributos CHAP basados en iniciadores mediante una llamada API. Para añadir un nombre de cuenta CHAP y credenciales por iniciador, debe utilizar la llamada API ModifyInitiator para quitar y agregar acceso y atributos de CHAP.

Para obtener más información, consulte "Gestione el almacenamiento con la API de Element".

Pasos

1. Haga clic en **Administración** > **iniciadores**.
2. Seleccione los iniciadores que desea añadir a un grupo de acceso.
3. Haga clic en el botón **acciones masivas**.
4. Haga clic en **Agregar a grupo de acceso de volumen**.
5. En el cuadro de diálogo Add to Volume Access Group, seleccione un grupo de acceso en la lista **Volume Access Group**.
6. Haga clic en **Agregar**.

Quite los iniciadores de un grupo de acceso

Cuando se quita un iniciador de un grupo de acceso, este ya no puede acceder a los

volúmenes de ese grupo de acceso de volúmenes. El acceso normal de cuenta al volumen no se interrumpe.

Si se modifica la configuración de CHAP en una cuenta o se quitan los iniciadores o los volúmenes de un grupo de acceso, se podría interrumpir el acceso de los iniciadores a los volúmenes de forma inesperada. Para asegurarse de que no se interrumpirá el acceso a los volúmenes de forma inesperada, siempre debe cerrar las sesiones iSCSI afectadas por alguno de los cambios en la cuenta o en el grupo de acceso. Asimismo, compruebe que los iniciadores pueden volver a conectarse con los volúmenes una vez que se hayan realizado los cambios en la configuración del iniciador y la configuración del clúster.

Pasos

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en el icono **acciones** del grupo de acceso que desea quitar.
3. En el menú que se abre, seleccione **Editar**.
4. En Add Initiators en el cuadro de diálogo **Edit Volume Access Group**, haga clic en la flecha de la lista **Initiators**.
5. Seleccione el icono de x para cada iniciador que desea quitar del grupo de acceso.
6. Haga clic en **Guardar cambios**.

Eliminar un grupo de acceso

Puede eliminar un grupo de acceso cuando ya no sea necesario. No hace falta que elimine los ID de iniciador ni los ID de volumen del grupo de acceso de volúmenes antes de eliminar el grupo. Una vez que se elimine el grupo de acceso, se interrumpirá el acceso del grupo al volumen.

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en el icono **acciones** del grupo de acceso que desea eliminar.
3. En el menú que se abre, haga clic en **Eliminar**.
4. Para eliminar también los iniciadores asociados con este grupo de acceso, active la casilla de verificación **Eliminar iniciadores de este grupo de acceso** .
5. Confirme la acción.

Eliminar un iniciador

Es posible eliminar un iniciador cuando ya no se necesita. Cuando se elimina un iniciador, el sistema la quita de los grupos de acceso de volúmenes asociados. Las conexiones que usan el iniciador siguen siendo válidas hasta que se restablece la conexión.

Pasos

1. Haga clic en **Administración** > **iniciadores**.
2. Siga los pasos para eliminar un solo iniciador o varios iniciadores:

Opción	Pasos
Elimine un solo iniciador	a. Haga clic en el icono **acciones** del iniciador que desea eliminar. b. Haga clic en **Eliminar**. c. Confirme la acción.
Elimine varios iniciadores	a. Seleccione las casillas junto a los iniciadores que desea eliminar. b. Haga clic en el botón **acciones masivas**. c. En el menú que se abre, seleccione **Eliminar**. d. Confirme la acción.

Proteja sus datos

El software NetApp Element permite proteger los datos de diversos modos con funcionalidades como copias de Snapshot de volúmenes o grupos de volúmenes individuales, replicación entre clústeres y volúmenes que se ejecutan en Element y replicación en sistemas ONTAP.

- **Instantáneas**

  La protección de datos con Snapshot replica los datos modificados en momentos específicos a un clúster remoto. Solo se replican las copias de Snapshot que se crean en el clúster de origen. No se producen las escrituras activas del volumen de origen.

  Use copias Snapshot de volumen para la protección de datos

- **Replicación remota entre clústeres y volúmenes que se ejecutan en Element**

  Es posible replicar datos de volúmenes de forma síncrona o asíncrona desde un clúster de una pareja de clústeres, tanto en ejecución en Element para los escenarios de conmutación por error y conmutación tras recuperación.

  Llevar a cabo la replicación remota entre los clústeres que ejecutan el software NetApp Element

- **Replicación entre clústeres de Element y ONTAP mediante tecnología SnapMirror**

  Con la tecnología SnapMirror de NetApp, puede replicar copias de Snapshot que se hayan realizado utilizando Element en ONTAP con fines de recuperación ante desastres. En una relación de SnapMirror, Element es un extremo y ONTAP es el otro.

  Use la replicación de SnapMirror entre clústeres de Element y ONTAP

- **Copia de seguridad y restauración de volúmenes desde almacenes de objetos SolidFire, S3 o Swift**

  Es posible realizar backups y restaurar volúmenes en otro almacenamiento de SolidFire, así como en almacenes de objetos secundarios que sean compatibles con OpenStack Swift o Amazon S3.

  Realizar backups y restaurar volúmenes en almacenes de objetos SolidFire, S3 o Swift

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Use copias Snapshot de volumen para la protección de datos

Una copia de Snapshot de volumen es una copia de un momento específico de un volumen. Puede realizar una copia de Snapshot de un volumen y usarla más adelante si se tiene que revertir un volumen al estado que tenía en el momento de creación de la copia de Snapshot.

Las copias Snapshot son similares a los clones de volúmenes. No obstante, las copias de Snapshot son réplicas de los metadatos del volumen, por lo que no es posible montarlas ni escribir en ellas. Además, para crear una copia de Snapshot de volumen, solo se requiere una pequeña cantidad de espacio y recursos del sistema, lo cual es más rápido crear una copia de Snapshot que clonar.

Es posible realizar una copia de Snapshot de un volumen individual o un conjunto de volúmenes.

Opcionalmente, replique las snapshots en un clúster de remoto y utilícelos como copia de backup del volumen. Gracias a ello, es posible revertir un volumen a un momento específico mediante la copia de Snapshot replicada. Como alternativa, es posible crear un clon de un volumen a partir de una copia de Snapshot replicada.

Obtenga más información

- Use copias de Snapshot de volumen individuales para la protección de datos
- El uso de copias de Snapshot de grupo para la tarea de protección de datos
- Programar una copia de Snapshot

Use copias de Snapshot de volumen individuales para la protección de datos

Una copia de Snapshot de volumen es una copia de un momento específico de un volumen. Se puede usar un volumen individual en lugar de un grupo de volúmenes para la copia de Snapshot.

Obtenga más información

- Cree una copia de Snapshot de volumen
- Editar la retención de snapshot
- Eliminar una copia de Snapshot
- Clonar un volumen a partir de una copia de Snapshot
- Revertir un volumen a una copia de Snapshot
- Realizar backups de una copia de Snapshot de volumen en un almacén de objetos Amazon S3
- Realizar backups de una copia de Snapshot de volumen en un almacén de objetos OpenStack Swift
- Realizar backups de una copia de Snapshot de volumen en un clúster de SolidFire

Cree una copia de Snapshot de volumen

Se puede crear una copia de Snapshot de un volumen activo para conservar la imagen del volumen en un momento determinado. Es posible crear hasta 32 copias de Snapshot de un solo volumen.

1. Haga clic en **Administración** > **volúmenes**.
2. Haga clic en el icono **acciones** del volumen que desea utilizar para la instantánea.
3. En el menú que se abre, seleccione **Snapshot**.
4. En el cuadro de diálogo **Crear instantánea del volumen**, introduzca el nuevo nombre de instantánea.
5. **Opcional:** Active la casilla de verificación **incluir instantánea en la replicación cuando se empareja** para asegurarse de que la instantánea se captura en la replicación cuando el volumen principal está emparejado.
6. Para configurar la retención de la copia de Snapshot, seleccione una de las siguientes opciones:
   - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.
   - Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para elegir un período de tiempo durante el cual el sistema retendrá la instantánea.
7. Para crear una sola snapshot de forma inmediata, realice los siguientes pasos:
   a. Haga clic en **tomar instantánea ahora**.
   b. Haga clic en **Crear Snapshot**.
8. Para programar que la copia de Snapshot se ejecute en el futuro, realice los siguientes pasos:
   a. Haga clic en **Crear programación Snapshot**.
   b. Introduzca un **Nuevo nombre de programa**.
   c. Seleccione un **Tipo de programación** de la lista.
   d. **Opcional:** Active la casilla de verificación **Programación periódica** para repetir periódicamente la instantánea programada.
   e. Haga clic en **Crear programación**.

Obtenga más información

Programar una copia de Snapshot

Editar la retención de snapshot

Puede cambiar el período de retención de una snapshot y determinar si el sistema elimina las snapshots y cuándo. El período de retención que se especifica comienza cuando se introduce el nuevo intervalo. Cuando se establece un período de retención, se puede seleccionar un período que comience en ese mismo momento (la retención no se calcula a partir del momento de creación de la copia de Snapshot). Los intervalos se pueden especificar en minutos, horas y días.

Pasos

1. Haga clic en **Protección de datos** > **instantáneas**.
2. Haga clic en el icono **acciones** de la instantánea que desea editar.

3. En el menú que se abre, haga clic en **Editar**.
4. **Opcional:** Active la casilla de verificación **incluir instantánea en la replicación cuando se empareje** para asegurarse de que la instantánea se capture en la replicación cuando el volumen primario se empareje.
5. **Opcional:** Seleccione una opción de retención para la instantánea:
   - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.
   - Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para seleccionar un período de tiempo durante el cual el sistema retendrá la instantánea.
6. Haga clic en **Guardar cambios**.

Eliminar una copia de Snapshot

Es posible eliminar una copia de Snapshot de volumen de un clúster de almacenamiento donde se ejecuta el software Element. Cuando se elimina una copia de Snapshot, el sistema la quita de forma inmediata.

Es posible eliminar del clúster de origen copias de Snapshot que se están replicando. Si una snapshot se está sincronizando en el clúster de destino cuando se la elimina, se completa la replicación sincrónica y la snapshot se elimina del clúster de origen. La copia de Snapshot no se elimina del clúster de destino.

También es posible eliminar del clúster de destino las copias de Snapshot que se hayan replicado en el destino. La copia de Snapshot eliminada se guarda en una lista de copias de Snapshot eliminadas en el destino hasta que el sistema detecta que se ha eliminado la copia de Snapshot en el clúster de origen. Cuando el destino detecta que se ha eliminado la copia de Snapshot de origen, el destino detiene la replicación de la copia de Snapshot.

Cuando se elimina una snapshot del clúster de origen, la snapshot del clúster de destino no se ve afectada (lo contrario también aplica).

1. Haga clic en **Protección de datos** > **instantáneas**.
2. Haga clic en el icono **acciones** de la instantánea que desea eliminar.
3. En el menú que se abre, seleccione **Eliminar**.
4. Confirme la acción.

Clonar un volumen a partir de una copia de Snapshot

Es posible crear un nuevo volumen a partir de una copia de Snapshot de un volumen. En ese caso, el sistema utiliza la información de la copia de Snapshot para clonar un volumen nuevo con los datos que contenía el volumen en el momento en el que se creó la copia de Snapshot. En este proceso se almacena información sobre otras copias de Snapshot del volumen en el volumen que se acaba de crear.

1. Haga clic en **Protección de datos** > **instantáneas**.
2. Haga clic en el icono **acciones** de la instantánea que desee utilizar para la clonación de volumen.
3. En el menú que se abre, haga clic en **Clone Volume from Snapshot**.
4. Introduzca un **Nombre de volumen** en el cuadro de diálogo **Clonar volumen desde Snapshot**.
5. Seleccione una **Tamaño total** y unidades de tamaño para el nuevo volumen.

6. Seleccione un tipo **Access** para el volumen.
7. Seleccione una **cuenta** de la lista para asociarla con el nuevo volumen.
8. Haga clic en **Iniciar clonación**.

Revertir un volumen a una copia de Snapshot

Siempre que lo desee, es posible revertir un volumen a una snapshot anterior. De este modo se revierten los cambios que se hayan hecho al volumen desde el momento de la creación de la snapshot.

Pasos

1. Haga clic en **Protección de datos** > **instantáneas**.
2. Haga clic en el icono **acciones** de la instantánea que desee utilizar para la reversión de volumen.
3. En el menú que se abre, seleccione **revertir volumen a instantánea**.
4. **Opcional:** para guardar el estado actual del volumen antes de retroceder a la instantánea:
   a. En el cuadro de diálogo **revertir a instantánea**, seleccione **Guardar estado actual del volumen como instantánea**.
   b. Escriba un nombre para la snapshot nueva.
5. Haga clic en **revertir Snapshot**.

Realice un backup de una copia de Snapshot de volumen

La función integrada de backup se puede usar para realizar un backup de una copia de Snapshot de volumen. Es posible realizar backups de snapshots de un clúster de SolidFire en un almacén de objetos externo o en otro clúster de SolidFire. Cuando se crea un backup de una copia de Snapshot en un almacén de objetos externo, debe haber una conexión con el almacén de objetos que permita realizar operaciones de lectura y escritura.

- "Realice backups de una copia de Snapshot de volumen en un almacén de objetos Amazon S3"
- "Realice backups de una copia de Snapshot de volumen en un almacén de objetos OpenStack Swift"
- "Realice backups de una copia de Snapshot de volumen en un clúster de SolidFire"

Realice backups de una copia de Snapshot de volumen en un almacén de objetos Amazon S3

Es posible realizar backups de snapshots de SolidFire en almacenes de objetos externos que sean compatibles con Amazon S3.

1. Haga clic en**Protección de datos** > **Snapshots**.
2. Haga clic en el icono **acciones** de la instantánea de la que desea realizar la copia de seguridad.
3. En el menú que se abre, haga clic en **copia de seguridad en**.
4. En el cuadro de diálogo **copia de seguridad integrada** en **copia de seguridad a**, seleccione **S3**.
5. Seleccione una opción en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.

- **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.

6. Introduzca un nombre de host para acceder al almacén de objetos en el campo **Hostname**.
7. Introduzca un ID de clave de acceso para la cuenta en el campo **ID de clave de acceso**.
8. Introduzca la clave de acceso secreta de la cuenta en el campo **clave de acceso secreta**.
9. Introduzca el bloque S3 en el que desea almacenar la copia de seguridad en el campo **S3 Bucket**.
10. **Opcional**: Introduzca una etiqueta de nombre para adjuntarla al prefijo en el campo **etiqueta de nombre**.
11. Haga clic en **Iniciar lectura**.

Realice backups de una copia de Snapshot de volumen en un almacén de objetos OpenStack Swift

Es posible realizar backups de snapshots de SolidFire en almacenes de objetos secundarios que sean compatibles con OpenStack Swift.

1. Haga clic en **Protección de datos** > **instantáneas**.
2. Haga clic en el icono **acciones** de la instantánea de la que desea realizar la copia de seguridad.
3. En el menú que se abre, haga clic en **copia de seguridad en**.
4. En el cuadro de diálogo **Backup integrado**, en **Backup to**, seleccione **Swift**.
5. Seleccione una opción en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
6. Introduzca una **URL** para acceder al almacén de objetos.
7. Introduzca un **Nombre de usuario** para la cuenta.
8. Introduzca **clave de autenticación** para la cuenta.
9. Introduzca el **contenedor** en el que desea almacenar la copia de seguridad.
10. **Opcional**: Introduzca una **etiqueta de nombre**.
11. Haga clic en **Iniciar lectura**.

Realice backups de una copia de Snapshot de volumen en un clúster de SolidFire

Puede realizar backups de snapshots de volumen que residen en un clúster de SolidFire en un clúster de SolidFire remoto.

Debe confirmar que los clústeres de origen y destino están emparejados.

Cuando se crea un backup o se restaura de un clúster a otro, el sistema genera una clave que se debe usar como autenticación entre los clústeres. Con esta clave de escritura masiva de volúmenes, el clúster de origen puede autenticarse con el clúster de destino, lo que permite ofrecer un nivel de seguridad cuando se escribe en el volumen de destino. Como parte del proceso de backup o restauración, debe generar una clave de escritura masiva de volúmenes desde el volumen de destino antes de iniciar la operación.

1. En el clúster de destino, haga clic en **Administración** > **volúmenes**.
2. Haga clic en el icono **acciones** del volumen de destino.
3. En el menú que se abre, haga clic en **Restaurar de**.
4. En el cuadro de diálogo **Restauración integrada**, en **Restaurar de**, seleccione **SolidFire**.

5. Seleccione un formato de datos en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
6. Haga clic en **generar clave**.
7. Copie la clave del cuadro **Bulk Volume Write Key** en el portapapeles.
8. En el clúster de origen, haga clic en **Protección de datos** > **instantáneas**.
9. Haga clic en el icono Actions de la snapshot que quiera usar para el backup.
10. En el menú que se abre, haga clic en **copia de seguridad en**.
11. En el cuadro de diálogo**copia de seguridad integrada**, en **copia de seguridad en**, seleccione **SolidFire**.
12. Seleccione el mismo formato de datos que haya seleccionado anteriormente en el campo **Formato de datos**.
13. Introduzca la dirección IP virtual de administración del clúster del volumen de destino en el campo **Remote Cluster MVIP**.
14. Introduzca el nombre de usuario del clúster remoto en el campo **Nombre de usuario del clúster remoto**.
15. Introduzca la contraseña del clúster remoto en el campo **Remote Cluster Password**.
16. En el campo **Bulk Volume Write Key**, pegue la clave que ha generado en el clúster de destino anteriormente.
17. Haga clic en **Iniciar lectura**.

El uso de copias de Snapshot de grupo para la tarea de protección de datos

Se puede crear una copia de Snapshot de grupo de un conjunto relacionado de volúmenes para conservar una copia de un momento específico de los metadatos de cada volumen. La snapshot de grupo se puede usar más adelante como un backup o una reversión para restaurar el estado del grupo de volúmenes en un estado anterior.

Obtenga más información

- Crear una copia de Snapshot de grupo
- Editar copias de Snapshot de grupo
- Editar los miembros de la copia de Snapshot de grupo
- Eliminar una copia de Snapshot de grupo
- Revertir volúmenes a una copia de Snapshot de grupo
- Clone varios volúmenes
- Clone varios volúmenes a partir de una copia de Snapshot de grupo

Detalles de la copia de Snapshot de grupo

En la página Group Snapshots de la pestaña Data Protection, se proporciona información sobre las snapshots de grupo.

- **ID**

  El ID que genera el sistema para la copia de Snapshot de grupo.

- **UUID**

  El ID único de la copia de Snapshot de grupo.

- **Nombre**

  El nombre definido por el usuario para la snapshot de grupo.

- **Crear tiempo**

  La hora en la que se ha creado la snapshot de grupo.

- **Estado**

  El estado actual de la copia de Snapshot de grupo. Los posibles valores son los siguientes:

  - Preparing: La copia de Snapshot se está preparando para poder usarla y aún no se puede escribir en ella.
  - Done: Esta snapshot se ha terminado de preparar y se puede usar.
  - Active: La snapshot es la rama activa.

- **# volúmenes**

  El número de volúmenes en el grupo.

- **Mantener hasta**

  La fecha y la hora en las que se eliminó la copia de Snapshot.

- **Replicación remota**

  Indica si la snapshot se habilita para la replicación en un clúster de SolidFire remoto. Los posibles valores son los siguientes:

  - Enabled: La snapshot está habilitada para la replicación remota.
  - Disabled: La snapshot no está habilitada para la replicación remota.

Crear una copia de Snapshot de grupo

Puede crear una snapshot de un grupo de volúmenes, así como planificar snapshots de grupo para automatizarlas. Una copia de Snapshot de grupo puede realizar copias de forma constante de hasta 32 volúmenes a la vez.

Pasos

1. Haga clic en **Administración** > **volúmenes**.
2. Use las casillas para seleccionar varios volúmenes de un grupo de volúmenes.
3. Haga clic en **acciones masivas**.
4. Haga clic en **instantánea de grupo**.
5. Introduzca un nombre de snapshot de grupo nuevo en el cuadro de diálogo Create Group Snapshot of Volumes.
6. **Opcional:** Active la casilla de verificación **incluir cada miembro de instantánea de grupo en**

replicación cuando se empareja para asegurarse de que cada instantánea se captura en la replicación cuando el volumen principal está emparejado.

7. Seleccione una opción de retención para la copia de Snapshot de grupo:
   - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.
   - Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para elegir un período de tiempo durante el cual el sistema retendrá la instantánea.
8. Para crear una sola snapshot de forma inmediata, realice los siguientes pasos:
   a. Haga clic en **tomar instantánea de grupo ahora**.
   b. Haga clic en **Crear instantánea de grupo**.
9. Para programar que la copia de Snapshot se ejecute en el futuro, realice los siguientes pasos:
   a. Haga clic en **Crear programación Snapshot de grupo**.
   b. Introduzca un **Nuevo nombre de programa**.
   c. Seleccione un **Tipo de programación** de la lista.
   d. **Opcional:** Active la casilla de verificación **Programación periódica** para repetir periódicamente la instantánea programada.
   e. Haga clic en **Crear programación**.

Editar copias de Snapshot de grupo

La configuración de la replicación y la retención se puede editar para las snapshots de grupos existentes.

1. Haga clic en **Protección de datos** > **instantáneas de grupo**.
2. Haga clic en el icono Actions de la snapshot de grupo que quiera editar.
3. En el menú que se abre, seleccione **Editar**.
4. **Opcional:** para cambiar la configuración de replicación de la instantánea de grupo:
   a. Haga clic en **Editar** junto a **replicación actual**.
   b. Active la casilla de verificación **incluir cada miembro de Snapshot de grupo en replicación cuando se empareja** para asegurarse de que cada instantánea se capture en la replicación cuando el volumen primario esté emparejado.
5. **Opcional:** para cambiar la configuración de retención de la instantánea de grupo, seleccione una de las siguientes opciones:
   a. Haga clic en **Editar** junto a **retención actual**.
   b. Seleccione una opción de retención para la copia de Snapshot de grupo:
      - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.
      - Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para elegir un período de tiempo durante el cual el sistema retendrá la instantánea.
6. Haga clic en **Guardar cambios**.

Eliminar una copia de Snapshot de grupo

Es posible eliminar una copia de Snapshot de grupo del sistema. Cuando se elimina la copia de Snapshot de grupo, se puede elegir si se eliminarán todas las copias de

Snapshot asociadas al grupo o si se retendrán como copias de Snapshot individuales.

Si elimina un volumen o una copia de Snapshot que forma parte de una copia de Snapshot de grupo, no se puede revertir a la copia de Snapshot de grupo. Sin embargo, se puede revertir a cada volumen de forma individual.

1. Haga clic en **Protección de datos** > **instantáneas de grupo**.
2. Haga clic en el icono Actions de la snapshot que quiera eliminar.
3. En el menú que se abre, haga clic en **Eliminar**.
4. Seleccione una de las siguientes opciones en el cuadro de diálogo de confirmación:
   - Haga clic en **Eliminar instantánea de grupo Y todos los miembros de instantánea de grupo** para eliminar la instantánea de grupo y todas las instantáneas de miembro.
   - Haga clic en **retener miembros de instantánea de grupo como instantáneas individuales** para eliminar la instantánea de grupo pero conservar todas las instantáneas de miembro.
5. Confirme la acción.

Revertir volúmenes a una copia de Snapshot de grupo

Siempre que lo desee, puede revertir un grupo de volúmenes a una snapshot de grupo.

Cuando se restaura un grupo de volúmenes, todos los volúmenes del grupo se restauran con el estado que tenían en el momento en que se creó la snapshot de grupo. La reversión también restaura el tamaño registrado en la snapshot original de los volúmenes. Si el sistema ha purgado un volumen, todas las copias de Snapshot de dicho volumen se eliminan durante la purga. Por ello, el sistema no restaura ninguna de las copias de Snapshot de volumen eliminadas.

1. Haga clic en **Protección de datos** > **instantáneas de grupo**.
2. Haga clic en el icono Actions de la snapshot de grupo que desee usar para revertir el volumen.
3. En el menú que se abre, seleccione **revertir volúmenes a Group Snapshot**.
4. **Opcional**: Para guardar el estado actual de los volúmenes antes de revertir a la instantánea:
   a. En el cuadro de diálogo **revertir a instantánea**, seleccione **Guardar volúmenes' Estado actual como una instantánea de grupo**.
   b. Escriba un nombre para la snapshot nueva.
5. Haga clic en **revertir Snapshot de grupo**.

Editar miembros de la copia de Snapshot de grupo

La configuración de retención se puede editar para los miembros de una copia de Snapshot de grupo existente.

1. Haga clic en **Protección de datos** > **instantáneas**.
2. Haga clic en la ficha **Miembros**.
3. Haga clic en el icono Actions del miembro de la snapshot de grupo que desea editar.
4. En el menú que se abre, seleccione **Editar**.
5. Para cambiar la configuración de replicación de la snapshot, seleccione una de las siguientes opciones:
   - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.

- Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para elegir un período de tiempo durante el cual el sistema retendrá la instantánea.

6. Haga clic en **Guardar cambios**.

Clone varios volúmenes

Es posible crear varios clones de volúmenes en una única operación para crear una copia de los datos de un momento específico en un grupo de volúmenes.

Cuando se clona un volumen, el sistema crea una copia Snapshot del volumen y, a continuación, crea un nuevo volumen a partir de los datos de la copia. Es posible montar el nuevo clon de volumen y escribir en él. El clonado de varios volúmenes es un proceso asíncrono cuya duración puede variar en función del tamaño y el número de volúmenes que se van a clonar.

El tamaño del volumen y la carga del clúster actual influirán en el tiempo que se necesite para completar una operación de clonado.

Pasos

1. Haga clic en **Administración** > **volúmenes**.
2. Haga clic en la ficha **activo**.
3. Use las casillas para seleccionar varios volúmenes con el fin de crear un grupo de volúmenes.
4. Haga clic en **acciones masivas**.
5. Haga clic en **Clonar** en el menú que aparece.
6. Introduzca un * prefijo de nombre de nuevo volumen* en el cuadro de diálogo **Clonar varios volúmenes**.

   El prefijo se aplica a todos los volúmenes del grupo.

7. **Opcional:** Seleccione otra cuenta a la que pertenecerá el clon.

   Si no selecciona ninguna cuenta, el sistema asignará los nuevos volúmenes a la cuenta de volumen actual.

8. **Opcional:** Seleccione un método de acceso diferente para los volúmenes del clon.

   Si no selecciona ninguno, el sistema usará el acceso de volumen actual.

9. Haga clic en **Iniciar clonación**.

Clonar varios volúmenes a partir de una copia de Snapshot de grupo

Es posible clonar un grupo de volúmenes desde una copia de Snapshot de grupo específica. Esta operación requiere la existencia de una snapshot de grupo de los volúmenes, puesto que la snapshot de grupo sirve como base para crear los volúmenes. Después de crear los volúmenes, es posible usarlos como cualquier otro volumen del sistema.

El tamaño del volumen y la carga del clúster actual influirán en el tiempo que se necesite para completar una operación de clonado.

1. Haga clic en **Protección de datos** > **instantáneas de grupo**.

2. Haga clic en el icono Actions de la snapshot de grupo que desee usar para los clones de volúmenes.
3. En el menú que se abre, seleccione **Clonar volúmenes desde Group Snapshot**.
4. Introduzca un * prefijo de nombre de nuevo volumen* en el cuadro de diálogo **Clonar volúmenes desde Snapshot de grupo**.

   El prefijo se aplica a todos los volúmenes que se creen a partir de la copia de Snapshot de grupo.

5. **Opcional:** Seleccione otra cuenta a la que pertenecerá el clon.

   Si no selecciona ninguna cuenta, el sistema asignará los nuevos volúmenes a la cuenta de volumen actual.

6. **Opcional:** Seleccione un método de acceso diferente para los volúmenes del clon.

   Si no selecciona ninguno, el sistema usará el acceso de volumen actual.

7. Haga clic en **Iniciar clonación**.

Programar una copia de Snapshot

Se pueden proteger datos en un volumen o un grupo de volúmenes mediante la programación de copias de Snapshot de volumen para que se produzcan en intervalos concretos. Se pueden programar las copias de Snapshot de un solo volumen o las copias de Snapshot de grupo para que se ejecuten automáticamente.

Cuando se configura una programación de Snapshot, se puede elegir entre intervalos de tiempo basados en los días de la semana o los días del mes. También es posible especificar los días, las horas y los minutos antes de que se produzca la siguiente copia de Snapshot. Las snapshots resultantes se pueden almacenar en un sistema de almacenamiento de remoto si el volumen se está replicando.

Obtenga más información

- Crear una programación de Snapshot
- Editar una programación de Snapshot
- Eliminar una programación de Snapshot
- Copiar una programación de Snapshot

Detalles de la programación de Snapshot

En la página Data Protection > Schedules, puede ver la siguiente información en la lista de programaciones de snapshots.

- **ID**

  El ID que genera el sistema para la copia de Snapshot.

- **Tipo**

  El tipo de programación. Actualmente, Snapshot es el único tipo admitido.

- **Nombre**

El nombre que se le dio a la programación cuando se creó. Los nombres de las programaciones de snapshots pueden tener hasta 223 caracteres y contener a-z, 9 y guion (-).

- **Frecuencia**

  La frecuencia con la que se ejecuta la programación. La frecuencia se puede establecer en horas y minutos, semanas o meses.

- **Recurrente**

  Indicación de si el programa se ejecutará sólo una vez o a intervalos regulares.

- **Pausado manualmente**

  Indica si la programación se pausó manualmente o no.

- **ID de volumen**

  El ID del volumen que usará la programación cuando se ejecute.

- **Última ejecución**

  La última vez que se ejecutó la programación.

- **Estado de la última ejecución**

  El resultado de la última ejecución de la programación. Los posibles valores son los siguientes:

  ◦ Correcto
  ◦ Fallo

Crear una programación de Snapshot

Se puede programar la ejecución automática de una copia de Snapshot de un volumen o de varios volúmenes en intervalos concretos.

Cuando se configura una programación de Snapshot, se puede elegir entre intervalos de tiempo basados en los días de la semana o los días del mes. Igualmente, se puede crear una programación recurrente y especificar los días, las horas y los minutos antes de que se ejecute la siguiente snapshot.

Si se programa la ejecución de una copia de Snapshot en un período que no sea divisible entre 5 minutos, la copia de Snapshot se ejecutará en el siguiente período que lo sea 5. Por ejemplo, si se programa la ejecución de una copia de Snapshot a las 12:42:00 UTC, se realizará a las 12:45:00 UTC. No se podrá programar la ejecución de una copia de Snapshot en intervalos inferiores a 5 minutos.

Pasos

1. Haga clic en **Protección de datos** > **programas**.
2. Haga clic en **Crear programación**.
3. En el campo **ID de volumen CSV**, introduzca un ID de volumen único o una lista separada por comas con los ID de volumen que desea incluir en la operación de instantánea.
4. Introduzca un nombre de programación nuevo.
5. Seleccione un tipo de programación y establezca la programación entre las opciones proporcionadas.

6. **Opcional:** Seleccione **Recurring Schedule** para repetir la programación de la instantánea de forma indefinida.
7. **Opcional:** Escriba un nombre para la nueva instantánea en el campo **Nuevo nombre de instantánea**.

   Si se deja el campo vacío, el sistema usará como nombre la hora y la fecha de la creación de la copia de Snapshot.

8. **Opcional:** Active la casilla de verificación **incluir instantáneas en replicación cuando se empareja** para asegurarse de que las instantáneas se capturan en la replicación cuando el volumen principal está emparejado.
9. Para configurar la retención de la snapshot, seleccione una de las siguientes opciones:
   - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.
   - Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para elegir un período de tiempo durante el cual el sistema retendrá la instantánea.
10. Haga clic en **Crear programación**.

Editar una programación de Snapshot

Puede modificar las programaciones de Snapshot que ya tenga. Después de modificarlas, la próxima vez que se ejecute la programación, se utilizarán los atributos actualizados. Las copias de Snapshot que se crean con la programación original siguen en el sistema de almacenamiento.

Pasos

1. Haga clic en **Protección de datos** > **programas**.
2. Haga clic en el icono **acciones** de la programación que desea cambiar.
3. En el menú que se abre, haga clic en **Editar**.
4. En el campo **ID de volumen CSV**, modifique el ID de volumen único o la lista separada por comas de los ID de volumen actualmente incluidos en la operación de instantánea.
5. Para pausar o reanudar la programación, seleccione una de las siguientes opciones:
   - Para pausar una programación activa, seleccione **Sí** en la lista **Pausa manual**.
   - Para reanudar una programación pausada, seleccione **no** en la lista **Pausa Manual**.
6. Introduzca otro nombre para la programación en el campo **Nombre de programación nuevo** si lo desea.
7. Para cambiar la programación para que se ejecute en distintos días de la semana o del mes, seleccione **Tipo de programación** y cambie la programación de las opciones proporcionadas.
8. **Opcional:** Seleccione **Recurring Schedule** para repetir la programación de la instantánea de forma indefinida.
9. **Opcional:** Introduzca o modifique el nombre de la nueva instantánea en el campo **Nuevo nombre de instantánea**.

   Si se deja el campo vacío, el sistema usará como nombre la hora y la fecha de la creación de la copia de Snapshot.

10. **Opcional:** Active la casilla de verificación **incluir instantáneas en replicación cuando se empareja** para asegurarse de que las instantáneas se capturan en la replicación cuando el volumen principal está emparejado.

11. Para cambiar la configuración de retención, seleccione una de las siguientes opciones:
    - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.
    - Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para seleccionar un período de tiempo durante el cual el sistema retendrá la instantánea.
12. Haga clic en **Guardar cambios**.

Copiar una programación de Snapshot

Puede copiar una programación y mantener sus atributos actuales.

1. Haga clic en **Protección de datos** > **programas**.
2. Haga clic en el icono Actions de la programación que quiera copiar.
3. En el menú que se abre, haga clic en **hacer una copia**.

   Aparece el cuadro de diálogo **Crear programación**, con los atributos actuales de la programación.

4. **Opcional:** Introduzca un nombre y atributos actualizados para la nueva programación.
5. Haga clic en **Crear programación**.

Eliminar una programación de Snapshot

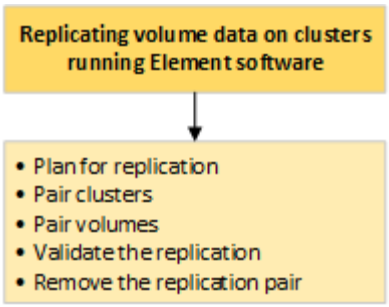
Es posible eliminar programaciones de Snapshot. Después de eliminar una programación, no se ejecutan las siguientes copias de Snapshot programadas. Las copias de Snapshot creadas con la programación permanecen en el sistema de almacenamiento.

1. Haga clic en **Protección de datos** > **programas**.
2. Haga clic en el icono **acciones** de la programación que desea eliminar.
3. En el menú que se abre, haga clic en **Eliminar**.
4. Confirme la acción.

Llevar a cabo la replicación remota entre los clústeres que ejecutan el software NetApp Element

Para los clústeres que ejecutan el software Element, la replicación en tiempo real permite la creación rápida de copias remotas de datos de volumen. Un clúster de almacenamiento se puede emparejar con hasta otros cuatro clústeres de almacenamiento. Es posible replicar datos de volúmenes de forma síncrona o asíncrona desde un clúster de una pareja de clústeres para escenarios de conmutación por error y conmutación tras recuperación.

El proceso de replicación incluye los siguientes pasos:



- "Planifique el emparejamiento de clústeres y volúmenes para la replicación en tiempo real"
- "Emparejar clústeres para la replicación"
- "Emparejar volúmenes"
- "Validar la replicación de volúmenes"
- "Eliminar una relación de volumen después de la replicación"
- "Gestionar relaciones de volumen"

Planifique el emparejamiento de clústeres y volúmenes para la replicación en tiempo real

La replicación remota en tiempo real requiere emparejar dos clústeres de almacenamiento que ejecutan el software Element, emparejar volúmenes en cada clúster y validar la replicación. Una vez que se completa la replicación, se debe eliminar la relación de volumen.

Lo que necesitará

- Debe tener privilegios de administrador del clúster en uno de los clústeres que se está emparejando, o en ambos.
- Todas las direcciones IP de nodos en las redes de gestión y almacenamiento para los clústeres emparejados se deben enrutar entre sí.
- La MTU de todos los nodos emparejados debe ser la misma y debe ser compatible entre clústeres de un extremo a otro.
- Ambos clústeres de almacenamiento deben tener nombres de clúster únicos, MVIP, SVIP y todas las direcciones IP de los nodos.
- La diferencia entre las versiones del software Element en los clústeres no debe ser superior a la versión principal. Si la diferencia es superior, se debe actualizar uno de los clústeres para ejecutar la replicación de datos.

> NetApp no ha autorizado los dispositivos aceleradores WAN para usarlos al replicar datos. Estos dispositivos pueden interferir con la compresión y la deduplicación si se implementan entre dos clústeres que están replicando datos. Asegúrese de autorizar por completo los efectos de cualquier dispositivo acelerador WAN antes de implementarlo en un entorno de producción.

Obtenga más información

- Emparejar clústeres para la replicación

- Emparejar volúmenes
- Asigne un origen y un destino de replicación a los volúmenes emparejados

Emparejar clústeres para la replicación

Debe emparejar dos clústeres como primer paso para utilizar la funcionalidad de replicación en tiempo real. Después de emparejar y conectar dos clústeres, es posible configurar volúmenes activos en un clúster para que se repliquen continuamente en un segundo clúster; esto proporciona protección de datos continua (CDP).

Lo que necesitará

- Debe tener privilegios de administrador del clúster en uno de los clústeres que se está emparejando, o en ambos.
- Todos los MIPs y SIPs de nodos están enrutados entre sí.
- Debe haber menos de 2000 ms de latencia de ida y vuelta entre clústeres.
- Ambos clústeres de almacenamiento deben tener nombres de clúster únicos, MVIP, SVIP y todas las direcciones IP de los nodos.
- La diferencia entre las versiones del software Element en los clústeres no debe ser superior a la versión principal. Si la diferencia es superior, se debe actualizar uno de los clústeres para ejecutar la replicación de datos.

> El emparejamiento de clústeres requiere una conectividad completa entre los nodos en la red de gestión. La replicación requiere conectividad entre los nodos individuales en la red de clústeres de almacenamiento.

Un clúster se puede emparejar con hasta otros cuatro clústeres para replicar volúmenes. De igual manera, los clústeres que pertenecen a un grupo de clústeres se pueden emparejar entre sí.

Obtenga más información

Requisitos de puerto de red

Emparejar clústeres con la MVIP o una clave de emparejamiento

Es posible emparejar un clúster de origen y de destino mediante la dirección MVIP de un clúster de destino si ambos clústeres ofrece acceso de administrador de clúster. Si solo un clúster en una pareja de clústeres ofrece acceso de administrador del clúster, se puede usar una clave de emparejamiento en el clúster de destino para completar el emparejamiento de clústeres.

1. Seleccione uno de los siguientes métodos para emparejar clústeres:
   - Emparejar clústeres con la MVIP: Utilice este método si ambos clústeres tienen acceso de administrador del clúster. Este método utiliza la dirección MVIP del clúster remoto para emparejar dos clústeres.
   - Emparejar clústeres con una clave de emparejamiento: Utilice este método si solo uno de los clústeres ofrece acceso de administrador del clúster. Este método genera una clave de emparejamiento que se puede usar en el clúster de destino para completar el emparejamiento de clústeres.

Obtenga más información

- Emparejar clústeres con la MVIP
- Emparejar clústeres con una clave de emparejamiento

Emparejar clústeres con la MVIP

Es posible emparejar dos clústeres para la replicación en tiempo real mediante la dirección MVIP de un clúster para establecer una conexión con el otro clúster. Para usar este método, debe tener acceso de administrador de clúster en ambos clústeres. La contraseña y el nombre de usuario del administrador de clúster se usan para autenticar el acceso a los clústeres antes de que estos se puedan emparejar.

1. En el clúster local, seleccione **Data Protection** > **Cluster Pairs**.
2. Haga clic en **Pair Cluster**.
3. Haga clic en **Iniciar emparejamiento** y haga clic en **Sí** para indicar que tiene acceso al clúster remoto.
4. Introduzca la dirección de MVIP del clúster remoto.
5. Haga clic en **emparejamiento completo en clúster remoto**.

   En la ventana **autenticación requerida**, introduzca el nombre de usuario y la contraseña del administrador del clúster remoto.

6. En el clúster remoto, seleccione **Protección de datos** > **pares de clústeres**.
7. Haga clic en **Pair Cluster**.
8. Haga clic en **Complete Pairing**.
9. Haga clic en el botón **Complete Pairing**.

Obtenga más información

- Emparejar clústeres con una clave de emparejamiento
- "Emparejar clústeres con la MVIP (vídeo)"

Emparejar clústeres con una clave de emparejamiento

Si tiene acceso de administrador del clúster a un clúster local, pero no al clúster remoto, puede emparejar los clústeres mediante una clave de emparejamiento. Una clave de emparejamiento se genera en un clúster local y se envía de forma segura a un administrador de clúster en un sitio remoto a fin de establecer una conexión y completar el emparejamiento de clústeres para la replicación en tiempo real.

1. En el clúster local, seleccione **Data Protection** > **Cluster Pairs**.
2. Haga clic en **Pair Cluster**.
3. Haga clic en **Iniciar emparejamiento** y haga clic en **no** para indicar que no tiene acceso al clúster remoto.
4. Haga clic en **generar clave**.

Esta acción genera una clave de texto para el emparejamiento y crea una pareja de clústeres sin configurar en el clúster local. Si no completa el procedimiento, deberá eliminar manualmente la pareja de clústeres.

5. Copie la clave de emparejamiento del clúster en el portapapeles.
6. Ponga la clave de emparejamiento a disposición del administrador de clúster en el sitio del clúster remoto.

La clave de emparejamiento de clústeres contiene una versión de la dirección MVIP, el nombre de usuario, la contraseña y la información de la base de datos para permitir las conexiones de volúmenes para la replicación remota. Esta clave se debe tratar de una forma segura y no se debe almacenar de manera que se pueda acceder de forma accidental o insegura al nombre de usuario o a la contraseña.

No modifique ningún carácter de la clave de emparejamiento. La clave pierde su validez si se modifica.

7. En el clúster remoto, seleccione **Protección de datos** > **pares de clústeres**.
8. Haga clic en **Pair Cluster**.
9. Haga clic en **Complete Pairing** e introduzca la clave de emparejamiento en el campo **Pairing Key** (pegue es el método recomendado).
10. Haga clic en **Complete Pairing**.

Obtenga más información

- Emparejar clústeres con la MVIP
- "Emparejamiento de clústeres con una clave de emparejamiento de clúster (vídeo)"

Valide la conexión de la pareja de clústeres

Una vez que se ha completado el emparejamiento de clústeres, es posible que desee verificar la conexión de la pareja de clústeres para garantizar que la replicación se haya realizado correctamente.

1. En el clúster local, seleccione **Data Protection** > **Cluster Pairs**.
2. En la ventana **Cluster Pairs**, compruebe que el par de clústeres esté conectado.
3. **Opcional:** vuelva al clúster local y a la ventana **Cluster Pairs** y compruebe que el par de clústeres esté conectado.

Emparejar volúmenes

Después de establecer una conexión entre los clústeres de una pareja de clústeres, es posible emparejar un volumen de un clúster con un volumen en el otro clúster de la pareja. Cuando se establece una relación de emparejamiento de volúmenes, es necesario identificar qué volumen es el destino de replicación.

Es posible emparejar dos volúmenes para replicación en tiempo real si están almacenados en clústeres de almacenamiento diferentes en una pareja de clústeres conectados. Después de emparejar dos clústeres, es posible configurar volúmenes activos en un clúster para que se repliquen continuamente en un segundo

clúster; esto proporciona protección de datos continua (CDP). También es posible asignar cada volumen como origen o destino de la replicación.

Los emparejamientos de volúmenes se realizan siempre de uno a uno. Una vez que un volumen forma parte de un emparejamiento con un volumen de otro clúster, no se puede volver a emparejar con otro volumen.

Lo que necesitará

- Estableció una conexión entre los clústeres de una pareja de clústeres.
- Tiene privilegios de administrador del clúster en uno de los clústeres que se está emparejando, o en ambos.

Pasos

1. Cree un volumen objetivo con acceso de lectura o escritura
2. Emparejar volúmenes con un ID de volumen o una clave de emparejamiento
3. Asigne un origen y un destino de replicación a los volúmenes emparejados

Cree un volumen objetivo con acceso de lectura o escritura

El proceso de replicación implica dos extremos: El volumen de origen y el de destino. Cuando se crea el volumen objetivo, el volumen se establece automáticamente en el modo de lectura/escritura para aceptar los datos durante la replicación.

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en **Crear volumen**.
3. En el cuadro de diálogo Create a New Volume, introduzca el nombre del volumen en Volume Name.
4. Introduzca el tamaño total del volumen, seleccione un tamaño de bloque para el volumen y seleccione la cuenta que debe tener acceso al volumen.
5. Haga clic en **Crear volumen**.
6. En la ventana Active, haga clic en el icono Actions del volumen.
7. Haga clic en **Editar**.
8. Cambie el nivel de acceso de cuenta a destino de replicación.
9. Haga clic en **Guardar cambios**.

Emparejar volúmenes con un ID de volumen o una clave de emparejamiento

El proceso de emparejamiento implica el emparejamiento de dos volúmenes mediante un ID de volumen o una clave de emparejamiento.

1. Emparejar volúmenes seleccionando uno de los siguientes métodos:
   - Usar un ID de volumen: Utilice este método si tiene acceso de administrador de clúster a los dos clústeres donde planea emparejar volúmenes. Este método utiliza el ID de volumen del volumen en el clúster remoto para iniciar una conexión.
   - Usar una clave de emparejamiento: Utilice este método si solo tiene acceso de administrador del clúster al clúster de origen. Este método genera una clave de emparejamiento que se puede usar en el clúster remoto para completar el emparejamiento de volúmenes.

La clave de emparejamiento de volúmenes contiene una versión cifrada de la información de los volúmenes y puede contener información confidencial. Únicamente comparta esta clave de forma segura.

Obtenga más información

- Emparejar volúmenes con un ID de volumen
- Emparejar volúmenes con una clave de emparejamiento

Emparejar volúmenes con un ID de volumen

Es posible emparejar un volumen con otro volumen en un clúster remoto si tiene credenciales de administrador de clústeres para el clúster remoto.

Lo que necesitará

- Confirme que los clústeres que contienen los volúmenes están emparejados.
- Cree un nuevo volumen en el clúster remoto.

Puede asignar un origen y un destino de replicación después del proceso de emparejamiento. Un origen u objetivo de replicación pueden ser un volumen de una pareja de volúmenes. Debe crear un volumen de destino que no contenga datos y que tenga las mismas características que el volumen de origen, como el tamaño, la configuración de tamaño de bloque para los volúmenes (512e o 4k) y la configuración de calidad de servicio. Si asigna un volumen existente como objetivo de replicación, los datos de ese volumen se sobrescriben. El tamaño del volumen de destino puede ser mayor o igual que el del volumen de origen, pero no menor.

- Determine el ID del volumen de destino.

Pasos

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en el icono **acciones** del volumen que desea emparejar.
3. Haga clic en **par**.
4. En el cuadro de diálogo **volumen de par**, seleccione **Iniciar emparejamiento**.
5. Seleccione **i do** para indicar que tiene acceso al clúster remoto.
6. Seleccione un **modo de replicación** de la lista:
   - **Tiempo real (asíncrono)**: Las escrituras se reconocen en el cliente después de que se aplican en el clúster de origen.
   - **Real-Time (Synchronous)**: Las escrituras se reconocen en el cliente después de que se aplican tanto en los clústeres de origen como de destino.
   - **Sólo instantáneas**: Sólo se replican las instantáneas creadas en el clúster de origen. No se replican las escrituras activas del volumen de origen.
7. Seleccione un clúster remoto de la lista Remote Cluster.
8. Seleccione un ID de volumen remoto.
9. Haga clic en **Iniciar emparejamiento**.

El sistema abre una pestaña del navegador web que se conecta a la interfaz de usuario de Element del clúster remoto. Es posible que se le pida iniciar sesión en el clúster remoto con las credenciales de administrador de clúster.

10. En la interfaz de usuario de Element del clúster remoto, seleccione **Complete Pairing**.
11. Confirme los detalles en **Confirmar emparejamiento de volúmenes**.
12. Haga clic en **Complete Pairing**.

    Después de confirmar el emparejamiento, los dos clústeres comienzan el proceso de conexión de los volúmenes para el emparejamiento. Durante el proceso de emparejamiento, puede ver mensajes en la columna **Estado del volumen** de la ventana **pares de volúmenes**. Se muestra la pareja de volúmenes `PausedMisconfigured` hasta que se asignan el origen y el destino de la pareja de volúmenes.

    Después de completar correctamente el emparejamiento, debe actualizar la tabla Volumes para eliminar la opción **Pair** de la lista **Actions** del volumen emparejado. Si no actualiza la tabla, la opción **par** permanece disponible para su selección. Si vuelve a seleccionar la opción **par**, se abre una nueva pestaña y, dado que el volumen ya está emparejado, el sistema informa un `StartVolumePairing Failed: xVolumeAlreadyPaired` Mensaje de error en la ventana **Pair Volume** de la página UI de Element.

Obtenga más información

- Mensajes sobre el emparejamiento de volúmenes
- Advertencias sobre el emparejamiento de volúmenes
- Asigne un origen y un destino de replicación a los volúmenes emparejados

Emparejar volúmenes con una clave de emparejamiento

Si no tiene credenciales de administrador del clúster para un clúster remoto, puede emparejar un volumen con otro volumen en un clúster remoto mediante una clave de emparejamiento.

Lo que necesitará

- Confirme que los clústeres que contienen los volúmenes están emparejados.
- Compruebe que haya un volumen en el clúster remoto que utilice para el emparejamiento.

> Puede asignar un origen y un destino de replicación después del proceso de emparejamiento. Un origen u objetivo de replicación pueden ser un volumen de una pareja de volúmenes. Debe crear un volumen de destino que no contenga datos y que tenga las mismas características que el volumen de origen, como el tamaño, la configuración de tamaño de bloque para los volúmenes (512e o 4k) y la configuración de calidad de servicio. Si asigna un volumen existente como objetivo de replicación, los datos de ese volumen se sobrescriben. El tamaño del volumen de destino puede ser mayor o igual que el del volumen de origen, pero no menor.

Pasos

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en el icono **acciones** del volumen que desea emparejar.
3. Haga clic en **par**.

4. En el cuadro de diálogo **volumen de par**, seleccione **Iniciar emparejamiento**.
5. Seleccione **no** para indicar que no tiene acceso al clúster remoto.
6. Seleccione un **modo de replicación** de la lista:
   - **Tiempo real (asíncrono)**: Las escrituras se reconocen en el cliente después de que se aplican en el clúster de origen.
   - **Real-Time (Synchronous)**: Las escrituras se reconocen en el cliente después de que se aplican tanto en los clústeres de origen como de destino.
   - **Sólo instantáneas**: Sólo se replican las instantáneas creadas en el clúster de origen. No se replican las escrituras activas del volumen de origen.
7. Haga clic en **generar clave**.

   Esta acción genera una clave de texto para el emparejamiento y crea una pareja de volúmenes sin configurar en el clúster local. Si no completa el procedimiento, deberá eliminar manualmente la pareja de volúmenes.

8. Copie la clave de emparejamiento en el portapapeles de su equipo.
9. Ponga la clave de emparejamiento a disposición del administrador del clúster en el sitio del clúster remoto.

   La clave de emparejamiento se debe tratar de una forma segura y no se debe utilizar de manera que se pueda acceder de forma accidental o insegura a ella.

   No modifique ningún carácter de la clave de emparejamiento. La clave pierde su validez si se modifica.

10. En la interfaz de usuario de elemento de clúster remoto, seleccione **Administración** > **volúmenes**.
11. Haga clic en el icono Actions del volumen que quiere emparejar.
12. Haga clic en **par**.
13. En el cuadro de diálogo **volumen de par**, seleccione **emparejamiento completo**.
14. Pegue la clave de emparejamiento del otro clúster en el cuadro **clave de emparejamiento**.
15. Haga clic en **Complete Pairing**.

    Después de confirmar el emparejamiento, los dos clústeres comienzan el proceso de conexión de los volúmenes para el emparejamiento. Durante el proceso de emparejamiento, puede ver mensajes en la columna **Estado del volumen** de la ventana **pares de volúmenes**. Se muestra la pareja de volúmenes `PausedMisconfigured` hasta que se asignan el origen y el destino de la pareja de volúmenes.

    Después de completar correctamente el emparejamiento, debe actualizar la tabla Volumes para eliminar la opción **Pair** de la lista **Actions** del volumen emparejado. Si no actualiza la tabla, la opción **par** permanece disponible para su selección. Si vuelve a seleccionar la opción **par**, se abre una nueva pestaña y, dado que el volumen ya está emparejado, el sistema informa un `StartVolumePairing Failed: xVolumeAlreadyPaired` Mensaje de error en la ventana **Pair Volume** de la página UI de Element.

Obtenga más información

- Mensajes sobre el emparejamiento de volúmenes
- Advertencias sobre el emparejamiento de volúmenes

- Asigne un origen y un destino de replicación a los volúmenes emparejados

Asigne un origen y un destino de replicación a los volúmenes emparejados

Después de emparejar los volúmenes, debe asignar un volumen de origen y su volumen de destino de replicación. Un origen u objetivo de replicación pueden ser un volumen de una pareja de volúmenes. Este procedimiento también se puede usar para redirigir los datos enviados a un volumen de origen hacia un volumen de destino remoto en caso de que no esté disponible el volumen de origen.

Lo que necesitará

Debe tener acceso a los clústeres que contienen los volúmenes de origen y de destino.

Pasos

1. Prepare el volumen de origen:
   a. En el clúster que contiene el volumen que desea asignar como origen, seleccione **Administración** > **volúmenes**.
   b. Haga clic en el icono **acciones** del volumen que desea asignar como origen y haga clic en **Editar**.
   c. En la lista desplegable **Access**, seleccione **Read/Write**.

   > Si va a revertir la asignación de origen y objetivo, esta acción hará que la pareja de volúmenes muestre el siguiente mensaje hasta que se asigne un nuevo objetivo de replicación: `PausedMisconfigured`

   Cambiar el acceso pone en pausa la replicación de volumen y provoca el cese de la transmisión de datos. Asegúrese de haber coordinado estos cambios en ambos sitios.

   a. Haga clic en **Guardar cambios**.
2. Prepare el volumen objetivo:
   a. Desde el clúster que contiene el volumen que desea asignar como destino, seleccione **Gestión** > **volúmenes**.
   b. Haga clic en el icono Actions del volumen que desea asignar como destino y haga clic en **Editar**.
   c. En la lista desplegable **Access**, seleccione **destino de replicación**.

   > Si asigna un volumen existente como objetivo de replicación, los datos de ese volumen se sobrescriben. Debe usar un nuevo volumen de destino que no contiene datos y que tenga las mismas características que el volumen de origen, como el tamaño, la configuración 512e y la configuración de calidad de servicio. El tamaño del volumen de destino puede ser mayor o igual que el del volumen de origen, pero no menor.

   d. Haga clic en **Guardar cambios**.

Obtenga más información

- Emparejar volúmenes con un ID de volumen
- Emparejar volúmenes con una clave de emparejamiento

Validar la replicación de volúmenes

Una vez que se replica un volumen, los volúmenes de origen y objetivo deben estar activos. Cuando en un estado activo, los volúmenes se emparejan, los datos se envían del volumen de origen al de destino y los datos están sincronizados.

1. En ambos clústeres, seleccione **Protección de datos** > **pares de volúmenes**.
2. Compruebe que el estado del volumen sea Active.

Obtenga más información

Advertencias sobre el emparejamiento de volúmenes

Eliminar una relación de volumen después de la replicación

Una vez que se completa la replicación y ya no se necesita la relación de pareja de volúmenes, es posible eliminar la relación de volumen.

1. Seleccione **Protección de datos** > **pares de volúmenes**.
2. Haga clic en el icono **acciones** del par de volúmenes que desee eliminar.
3. Haga clic en **Eliminar**.
4. Confirme el mensaje.

Gestionar relaciones de volumen

Es posible gestionar las relaciones de volúmenes de muchas maneras, como pausar la replicación, revertir el emparejamiento de volúmenes, cambiar el modo de replicación, eliminar una pareja de volúmenes o eliminar una pareja de clústeres.

Obtenga más información

- Detenga la replicación
- Cambie el modo de replicación
- Eliminar parejas de volúmenes

Detenga la replicación

Puede pausar manualmente la replicación si necesita detener el procesamiento de I/o durante un breve periodo de tiempo. Puede que desee pausar la replicación si hay un aumento en el procesamiento de I/o y desea reducir la carga de procesamiento.

1. Seleccione **Protección de datos** > **pares de volúmenes**.
2. Haga clic en el icono Actions de la pareja de volúmenes.
3. Haga clic en **Editar**.
4. En el panel **Editar par de volúmenes**, detenga manualmente el proceso de replicación.

Cuando se pausa o se reanuda manualmente una replicación de volumen, se detiene o se reanuda la transmisión de datos. Asegúrese de haber coordinado estos cambios en ambos sitios.

5. Haga clic en **Guardar cambios**.

Cambie el modo de replicación

Es posible editar las propiedades de una pareja de volúmenes para cambiar el modo de replicación de la relación de pareja de volúmenes.

1. Seleccione **Protección de datos** > **pares de volúmenes**.
2. Haga clic en el icono Actions de la pareja de volúmenes.
3. Haga clic en **Editar**.
4. En el panel **Editar par de volúmenes**, seleccione un nuevo modo de replicación:
   - **Tiempo real (asíncrono)**: Las escrituras se reconocen en el cliente después de que se aplican en el clúster de origen.
   - **Real-Time (Synchronous)**: Las escrituras se reconocen en el cliente después de que se aplican tanto en los clústeres de origen como de destino.
   - **Sólo instantáneas**: Sólo se replican las instantáneas creadas en el clúster de origen. No se replican las escrituras activas del volumen de origen. **Atención:** al cambiar el modo de replicación, se cambia el modo inmediatamente. Asegúrese de haber coordinado estos cambios en ambos sitios.
5. Haga clic en **Guardar cambios**.

Eliminar parejas de volúmenes

Es posible eliminar una pareja de volúmenes si se desea quitar una asociación de pareja entre dos volúmenes.

1. Seleccione **Protección de datos** > **pares de volúmenes**.
2. Haga clic en el icono Actions de la pareja de volúmenes que desea eliminar.
3. Haga clic en **Eliminar**.
4. Confirme el mensaje.

Elimine una pareja de clústeres

Es posible eliminar una pareja de clústeres desde la interfaz de usuario de Element de cualquiera de los clústeres que componen la pareja.

1. Haga clic en **Protección de datos** > **pares de clústeres**.
2. Haga clic en el icono Actions de una pareja de clústeres.
3. En el menú que se abre, haga clic en **Eliminar**.
4. Confirme la acción.
5. Repita los pasos desde el segundo clúster de la pareja de clústeres.

Detalles de parejas de clústeres

La página Cluster Pairs de la pestaña Data Protection proporciona información sobre los clústeres que se hayan emparejado o que estén en proceso de emparejarse. El sistema muestra mensajes de emparejamiento y progreso en la columna Status.

- **ID**

  Un ID generado por el sistema que se otorga a cada pareja de clústeres.

- **Nombre de clúster remoto**

  El nombre del otro clúster de la pareja.

- **MVIP remoto**

  La dirección IP virtual de gestión del otro clúster en la pareja.

- **Estado**

  El estado de replicación del clúster remoto

- **Replicación de volúmenes**

  La cantidad de volúmenes que contiene el clúster emparejados para la replicación.

- **UUID**

  Un ID único que se otorga a cada clúster en la pareja.

Detalles de parejas de volúmenes

La página Volume Pairs de la pestaña Data Protection proporciona información sobre los volúmenes que se hayan emparejado o que estén en proceso de emparejarse. El sistema muestra los mensajes de emparejamiento y progreso en la columna Volume Status.

- **ID**

  El ID que genera el sistema para el volumen.

- **Nombre**

  El nombre que se le dio al volumen cuando se creó. Los nombres de volumen pueden tener hasta 223 caracteres y contener a-z, 9 y guion (-).

- **Cuenta**

  El nombre de la cuenta asignada al volumen.

- **Estado del volumen**

  El estado de replicación del volumen

- **Estado de instantánea**

  El estado del volumen de snapshot.

- **Modo**

  El método de replicación de escritura del cliente. Los valores posibles son los siguientes:

  - Asincrónica
  - Solo Snapshot
  - Sincr

- **Dirección**

  La dirección de los datos del volumen:

  - Icono de volumen de origen ( ) indica que los datos se escriben en un objetivo fuera del clúster.
  - Icono de volumen de destino ( ) indica que los datos se escriben en el volumen local desde un origen externo.

- **Retraso asíncrono**

  El tiempo transcurrido desde que el volumen se sincronizó por última vez con el clúster remoto. Si el volumen no se empareja, el valor es nulo.

- **Cluster remoto**

  El nombre del clúster remoto en el que reside el volumen.

- **ID de volumen remoto**

  El ID de volumen del volumen en el clúster remoto.

- **Nombre del volumen remoto**

  El nombre que se le dio al volumen remoto cuando se creó.

Mensajes sobre el emparejamiento de volúmenes

Es posible ver mensajes de emparejamiento de volúmenes durante el proceso inicial de emparejamiento desde la página Volume Pairs de la pestaña Data Protection. Estos mensajes pueden aparecer tanto en los extremos de origen como de destino de la pareja en la vista de lista Replicating Volumes.

- **PausedDisconnected**

  Se agotó el tiempo de ejecución de la replicación de origen o los RPC de sincronización. Se perdió la conexión con el clúster remoto. Compruebe las conexiones de red con el clúster.

- **ResumingConnected**

  La sincronización de replicación remota está activa. Se inicia el proceso de sincronización y se esperan los datos.

- **ResumingRRSync**

  Se hace una copia sencilla de Helix de los metadatos del volumen en el clúster emparejado.

- **ResumingLocalSync**

  Se hace una copia doble de Helix de los metadatos del volumen en el clúster emparejado.

- **ReumingDataTransfer**

  Se reanudó la transferencia de datos.

- **Activo**

  Los volúmenes están emparejados y los datos se envían del volumen de origen al de destino; los datos están sincronizados.

- **Inactivo**

  No se produce ninguna actividad de replicación.

Advertencias sobre el emparejamiento de volúmenes

Lapágina Volume Pairs en la pestaña Data Protection proporciona estos mensajes después de emparejar volúmenes. Estos mensajes pueden aparecer tanto en los extremos de origen como de destino de la pareja (a menos que se indique lo contrario) en la vista de lista Replicating Volumes.

- **PausedaClusterFull**

  Dado que el clúster de destino está lleno, la replicación de origen y la transferencia de datos masivos no pueden continuar. El mensaje aparece solamente en el extremo de origen de la pareja.

- **PausedExceedededededMaxSnapshotCount**

  El volumen de destino ya cuenta con el número máximo de copias de Snapshot y no puede replicar copias de Snapshot adicionales.

- **PausedManual**

  El volumen local se pausó manualmente. La pausa se debe cancelar antes de que se reanude la replicación.

- **PausedManualRemote**

  El volumen remoto se pausó manualmente. Se requiere intervención manual para cancelar la pausa del volumen remoto antes de que se reanude la replicación.

- **PausedMisconfigured**

  Se esperan un origen y un destino activos. Se requiere intervención manual para reanudar la replicación.

- **PausedQoS**

La calidad de servicio de destino no pudo sostener el I/o de entrada. La replicación se reanuda automáticamente. El mensaje aparece solamente en el extremo de origen de la pareja.

- **PausedSlowLink**

  Se detectó un enlace lento y se detuvo la replicación. La replicación se reanuda automáticamente. El mensaje aparece solamente en el extremo de origen de la pareja.

- **PausedVolumeSizediscordancia**

  El volumen de destino no tiene el mismo tamaño que el volumen de origen.

- **PausedXCopy**

  Se envía un comando SCSI XCOPY a un volumen de origen. El comando debe completarse antes de que la replicación se pueda reanudar. El mensaje aparece solamente en el extremo de origen de la pareja.

- **StoppedMisconfigured**

  Se detectó un error de configuración permanente. El volumen remoto se purgó o se desemparejó. No se puede realizar ninguna acción correctiva y se debe establecer un nuevo emparejamiento.

Use la replicación de SnapMirror entre clústeres de Element y ONTAP

Las relaciones de SnapMirror se pueden crear en la pestaña Data Protection de la interfaz de usuario de NetApp Element. La funcionalidad de SnapMirror debe estar habilitada para poder verla en la interfaz de usuario de.

IPv6 no es compatible con la replicación de SnapMirror entre el software NetApp Element y los clústeres de ONTAP.

"Vídeo de NetApp: SnapMirror para software NetApp HCI y Element"

Los sistemas que ejecutan el software NetApp Element admiten la funcionalidad SnapMirror para copiar y restaurar copias Snapshot con sistemas ONTAP de NetApp. El principal motivo para usar esta tecnología es la recuperación ante desastres de NetApp HCI a ONTAP. Los extremos incluyen ONTAP, ONTAP Select y Cloud Volumes ONTAP. Consulte TR-4641 Protección de datos de NetApp HCI.

"Informe técnico de NetApp 4641: Protección de datos de NetApp HCI"

Obtenga más información

- "Crear una estructura de datos con NetApp HCI, ONTAP e infraestructura convergente"
- "Replicación entre software de NetApp Element y ONTAP"

Información general de SnapMirror

Los sistemas que ejecutan el software NetApp Element admiten la funcionalidad SnapMirror para copiar y restaurar copias Snapshot con los sistemas ONTAP de NetApp.

Los sistemas que ejecutan Element pueden comunicarse directamente con SnapMirror en los sistemas ONTAP 9.3 o posteriores. La API de NetApp Element proporciona métodos para habilitar la funcionalidad de SnapMirror en clústeres, volúmenes y snapshots. Además, la interfaz de usuario de Element incluye toda la

funcionalidad necesaria para gestionar las relaciones de SnapMirror entre el software Element y los sistemas ONTAP.

Es posible replicar volúmenes originados de ONTAP en volúmenes de Element en casos de uso específicos con funcionalidad limitada. Para obtener más información, consulte la documentación de ONTAP.

Obtenga más información

"Replicación entre software de Element y ONTAP"

Habilite SnapMirror en el clúster

Debe habilitar manualmente la funcionalidad de SnapMirror en el nivel del clúster a través de la interfaz de usuario de NetApp Element. El sistema viene con la funcionalidad de SnapMirror deshabilitada de forma predeterminada y no se habilita automáticamente como parte de una nueva instalación o actualización. Habilitar la función SnapMirror es una tarea de configuración que solo debe hacer una vez.

SnapMirror solo se puede habilitar en clústeres que ejecutan el software Element que se usa junto con volúmenes de un sistema ONTAP de NetApp. Solo debe habilitar la funcionalidad SnapMirror si el clúster está conectado para usarlo con volúmenes de ONTAP de NetApp.

Lo que necesitará

El clúster de almacenamiento debe ejecutar el software NetApp Element.

Pasos

1. Haga clic en **Clusters** > **Configuración**.
2. Busque la configuración específica del clúster para SnapMirror.
3. Haga clic en **Activar SnapMirror**.

> Al habilitar la funcionalidad SnapMirror, se modifica la configuración del software Element de forma permanente. Puede deshabilitar la función SnapMirror y restaurar la configuración predeterminada solo si devuelve el clúster a la imagen de fábrica.

4. Haga clic en **Sí** para confirmar el cambio de configuración de SnapMirror.

Habilite SnapMirror en el volumen

Debe habilitar SnapMirror en el volumen en la interfaz de usuario de Element. Esto permite la replicación de datos en volúmenes de ONTAP especificados. Se trata de un permiso del administrador del clúster donde se ejecuta el software NetApp Element para que SnapMirror controle un volumen.

Lo que necesitará

- Debe habilitar SnapMirror en la interfaz de usuario de Element para el clúster.
- Existe un extremo de SnapMirror disponible.
- El volumen debe ser el tamaño de bloque 512e.
- El volumen no participa en la replicación remota.

- El tipo de acceso de volumen no es destino de replicación.

> También puede establecer esta propiedad al crear o clonar un volumen.

Pasos

1. Haga clic en **Administración** > **volúmenes**.
2. Haga clic en el icono **acciones** del volumen para el que desea activar SnapMirror.
3. En el menú que se abre, seleccione **Editar**.
4. En el cuadro de diálogo **Editar volumen**, active la casilla de verificación **Activar SnapMirror**.
5. Haga clic en **Guardar cambios**.

Cree un extremo de SnapMirror

Debe crear un extremo de SnapMirror en la interfaz de usuario de NetApp Element para poder crear una relación.

Un extremo de SnapMirror es un clúster de ONTAP que funciona como destino de replicación para un clúster que ejecuta el software Element. Antes de crear una relación de SnapMirror, primero se debe crear un extremo de SnapMirror.

Es posible crear y gestionar hasta cuatro extremos de SnapMirror en un clúster de almacenamiento que ejecuta el software Element.

> Si originalmente se creó un extremo existente mediante la API y no se guardaron las credenciales, puede ver el extremo en la interfaz de usuario de Element y verificar su existencia, pero no se puede gestionar mediante la interfaz de usuario de Element. Este extremo solo puede gestionarse mediante la API de Element.

Para obtener más información sobre los métodos API, consulte "Gestione el almacenamiento con la API de Element".

Lo que necesitará

- Debe haber habilitado SnapMirror en la interfaz de usuario de Element para el clúster de almacenamiento.
- Conoce las credenciales de ONTAP para el extremo.

Pasos

1. Haga clic en **Protección de datos** > **terminales de SnapMirror**.
2. Haga clic en **Crear extremo**.
3. En el cuadro de diálogo **Crear un nuevo extremo**, introduzca la dirección IP de administración del clúster del sistema ONTAP.
4. Introduzca las credenciales de administrador de ONTAP asociadas con el extremo.
5. Consulte información adicional:
   - LIF: Enumera las interfaces lógicas de interconexión de clústeres de ONTAP que se utilizan para comunicarse con Element.
   - Status: Muestra el estado actual del extremo de SnapMirror. Los valores posibles son: Conectado, desconectado y no administrado.
6. Haga clic en **Crear extremo**.

Crear una relación de SnapMirror

Debe crear una relación de SnapMirror en la interfaz de usuario de NetApp Element.

> Cuando aún no se habilita un volumen para SnapMirror y seleccione para crear una relación desde la interfaz de usuario de Element, se habilita automáticamente SnapMirror en ese volumen.

Lo que necesitará

Está habilitado SnapMirror en el volumen.

Pasos

1. Haga clic en **Administración** > **volúmenes**.
2. Haga clic en el icono **acciones** del volumen que va a formar parte de la relación.
3. Haga clic en **Crear una relación de SnapMirror**.
4. En el cuadro de diálogo **Crear una relación de SnapMirror**, seleccione un extremo de la lista **Endpoint**.
5. Seleccione si la relación se creará con un volumen de ONTAP nuevo o con un volumen de ONTAP existente.
6. Para crear un nuevo volumen ONTAP en la interfaz de usuario de Element, haga clic en **Crear nuevo volumen**.
   a. Seleccione **Storage Virtual Machine** para esta relación.
   b. Seleccione **aggregate** en la lista desplegable.
   c. En el campo **sufijo de nombre de volumen**, introduzca un sufijo.

      > El sistema detecta el nombre del volumen de origen y lo copia en el campo **Nombre de volumen**. El sufijo que introduzca anexa el nombre.

   d. Haga clic en **Crear volumen de destino**.
7. Para utilizar un volumen de ONTAP existente, haga clic en **utilizar volumen existente**.
   a. Seleccione **Storage Virtual Machine** para esta relación.
   b. Seleccione el volumen que será el destino de esta nueva relación.
8. En la sección **Detalles de la relación**, seleccione una directiva. Si la directiva seleccionada tiene reglas de mantenimiento, la tabla Reglas muestra las reglas y las etiquetas asociadas.
9. **Opcional**: Selecciona un horario.

   Esto determina la frecuencia con la que la relación crea copias.
10. **Opcional**: En el campo **limitar ancho de banda a**, introduzca la cantidad máxima de ancho de banda que pueden consumir las transferencias de datos asociadas con esta relación.
11. Consulte información adicional:
    - **Estado**: Estado actual de la relación del volumen de destino. Los valores posibles son:
      - Inicializado: El volumen de destino no se ha inicializado.
      - snapmirror: El volumen de destino se ha inicializado y está listo para recibir actualizaciones de SnapMirror.

        - Roto-off: El volumen de destino es de lectura/escritura y existen snapshots.
    - **Estado**: Estado actual de la relación. Los valores posibles son ralentí, transferencia, comprobación, desactivación, inactivo, puesta en cola, preparación, finalización, anulación y ruptura.
    - **Tiempo de retardo**: La cantidad de tiempo en segundos que el sistema de destino está retrasado con respecto al sistema de origen. El tiempo de desfase no debe superar el intervalo de programación de transferencia.
    - **Límite de ancho de banda**: La cantidad máxima de ancho de banda que pueden consumir las transferencias de datos asociadas a esta relación.
    - **Última transferencia**: Marca de hora de la última instantánea transferida. Haga clic para obtener más información.
    - **Nombre de la política**: Nombre de la política de SnapMirror de ONTAP para la relación.
    - **Tipo de directiva**: Tipo de política de SnapMirror de ONTAP seleccionada para la relación. Los valores posibles son:
        - async_mirror
        - mirror_vault
    - **Nombre del programa**: Nombre del programa preexistente del sistema ONTAP seleccionado para esta relación.
12. Para no inicializar en este momento, asegúrese de que la casilla de verificación **inicializar** no está activada.

    La inicialización puede requerir mucho tiempo. Tal vez desee ejecutarlo durante las horas de menor actividad. La inicialización realiza una transferencia básica; realiza una copia Snapshot del volumen de origen y, a continuación, transfiere esa copia y todos los bloques de datos a los que hace referencia al volumen de destino. Puede inicializar manualmente o utilizar una programación para iniciar el proceso de inicialización (y las actualizaciones posteriores) según la programación.

13. Haga clic en **Crear relación**.
14. Haga clic en **Protección de datos** > **Relaciones de SnapMirror** para ver esta nueva relación de SnapMirror.

Acciones de relaciones con SnapMirror

Puede configurar una relación desde la página SnapMirror Relationships de la pestaña Data Protection. Las opciones del icono acciones se describen aquí.

- **Edición**: Edita la directiva utilizada o la programación de la relación.
- **Eliminar**: Elimina la relación de SnapMirror. Esta función no elimina el volumen de destino.
- **Inicializar**: Realiza la primera transferencia inicial de datos de línea de base para establecer una nueva relación.
- **Actualizar**: Realiza una actualización bajo demanda de la relación, replicando los datos nuevos y las copias Snapshot incluidas desde la última actualización al destino.
- **Quiesce**: Previene cualquier actualización adicional para una relación.
- **Reanudar**: Reanuda una relación que se detiene.
- **Break**: Hace que el volumen de destino sea de lectura y escritura y detiene todas las transferencias actuales y futuras. Determine que los clientes no utilizan el volumen de origen original, ya que la operación

de resincronización inversa hace que el volumen de origen original sea de solo lectura.

- **Resync**: Restablece una relación rota en la misma dirección antes de que se produjera la ruptura.
- **Resync inversa**: Automatiza los pasos necesarios para crear e inicializar una nueva relación en la dirección opuesta. Esto sólo se puede hacer si la relación existente se encuentra en un estado roto. Esta operación no eliminará la relación actual. El volumen de origen original se revierte a la copia Snapshot común más reciente y se vuelve a sincronizar con el destino. Se perderán todos los cambios realizados en el volumen de origen original desde la última actualización correcta de SnapMirror. Los cambios realizados o los nuevos datos escritos en el volumen de destino actual se devuelven al volumen de origen original.
- **Anular**: Cancela una transferencia actual en curso. Si se emite una actualización de SnapMirror para una relación abortada, la relación continúa con la última transferencia desde el último punto de comprobación de reinicio que se creó antes de que se produjera la anulación.

Etiquetas de SnapMirror

Una etiqueta de SnapMirror sirve como marcador para la transferencia de una copia de Snapshot específica según las reglas de retención de la relación.

Si se aplica una etiqueta a una copia de Snapshot, esta se Marca como destino de la replicación de SnapMirror. El rol de la relación es aplicar las reglas sobre la transferencia de datos seleccionando la snapshot con la etiqueta correspondiente, copiándola al volumen de destino y garantizando que se conserva el número correcto de copias. Se refiere a la política para determinar el recuento de retenciones y el período de retención. La directiva puede tener un número cualquiera de reglas y cada regla tiene una etiqueta única. Esta etiqueta actúa como enlace entre la snapshot y la regla de retención.

Es la etiqueta de SnapMirror que indica qué regla se aplica a la snapshot, la snapshot de grupo o la programación seleccionada.

Añada etiquetas de SnapMirror a snapshots

Las etiquetas de SnapMirror especifican la política de retención de snapshots en el extremo de SnapMirror. Se pueden añadir etiquetas a las copias de Snapshot y las copias de Snapshot de grupo.

Puede ver las etiquetas disponibles en un cuadro de diálogo existente de relación de SnapMirror o en el Administrador del sistema ONTAP de NetApp.

> Cuando se añade una etiqueta a una copia de Snapshot de grupo, se sobrescriben todas las etiquetas existentes a copias de Snapshot individuales.

Lo que necesitará

- Se habilita SnapMirror en el clúster.
- La etiqueta que desea añadir ya existe en ONTAP.

Pasos

1. Haga clic en **Protección de datos** > **Snapshots** o **instantánea de grupo**.
2. Haga clic en el icono **acciones** de la instantánea o la instantánea de grupo a la que desea agregar una etiqueta de SnapMirror.
3. En el cuadro de diálogo **Editar instantánea**, introduzca texto en el campo **etiqueta de SnapMirror**. La etiqueta debe coincidir con una etiqueta de regla de la política aplicada a la relación de SnapMirror.

4. Haga clic en **Guardar cambios**.

Añadir etiquetas de SnapMirror a las programaciones de Snapshot

Puede añadir etiquetas de SnapMirror a programaciones de Snapshot para garantizar que se aplique una política de SnapMirror. Puede ver las etiquetas disponibles en un cuadro de diálogo existente de relación de SnapMirror o en ONTAP System Manager de NetApp.

Lo que necesitará

- Se debe habilitar SnapMirror en el nivel de clúster.
- La etiqueta que desea añadir ya existe en ONTAP.

Pasos

1. Haga clic en **Protección de datos** > **programas**.
2. Añada una etiqueta de SnapMirror a una programación de una de las siguientes maneras:

Opción	Pasos
Crear una nueva programación	a. Seleccione **Crear programación**. b. Introduzca todos los demás detalles relevantes. c. Seleccione **Crear programación**.
Modificación de la programación existente	a. Haga clic en el icono **acciones** de la programación a la que desea agregar una etiqueta y seleccione **Editar**. b. En el cuadro de diálogo que aparece, introduzca texto en el campo **etiqueta de SnapMirror**. c. Seleccione **Guardar cambios**.

Obtenga más información

Crear una programación de Snapshot

Recuperación ante desastres mediante SnapMirror

En caso de producirse un problema con un volumen o un clúster que ejecuta el software NetApp Element, utilice la funcionalidad SnapMirror para dividir la relación y la conmutación por error al volumen de destino.

Si el clúster original ha fallado completamente o no existe, póngase en contacto con el soporte de NetApp para obtener ayuda.

Ejecute una conmutación al nodo de respaldo desde un clúster de Element

Puede realizar una conmutación al nodo de respaldo desde el clúster de Element para hacer que el volumen de destino sea de lectura/escritura y accesible para los hosts en el lado de destino. Antes de realizar una conmutación al nodo de respaldo del clúster de

Element, debe interrumpir la relación de SnapMirror.

Use la interfaz de usuario de NetApp Element para realizar la conmutación al respaldo. Si la interfaz de usuario de Element no está disponible, también es posible usar ONTAP System Manager o la CLI de ONTAP para ejecutar el comando break Relationship.

Lo que necesitará

- Existe una relación de SnapMirror y tiene al menos una snapshot válida en el volumen de destino.
- Necesita una conmutación al nodo de respaldo en el volumen de destino debido a una interrupción del servicio no planificada o un evento planificado en el sitio principal.

Pasos

1. En la interfaz de usuario de Element, haga clic en **Protección de datos** > **Relaciones de SnapMirror**.
2. Busque la relación con el volumen de origen que desea conmutar al nodo de respaldo.
3. Haga clic en el icono **acciones**.
4. Haga clic en **descanso**.
5. Confirme la acción.

   El volumen del clúster de destino ahora tiene acceso de lectura/escritura y se puede montar en los hosts de la aplicación para reanudar las cargas de trabajo de producción. Toda la replicación de SnapMirror se detiene como resultado de esta acción. La relación muestra un estado de ruptura.

Realice una conmutación tras recuperación al elemento

Cuando se mitigó el problema en el lado primario, se debe volver a sincronizar el volumen de origen original y conmutar al software NetApp Element. Los pasos que realice varían en función de si todavía existe el volumen de origen original o si necesita realizar la conmutación tras recuperación en un volumen recién creado.

Obtenga más información

- Realice una conmutación tras recuperación cuando el volumen de origen siga existiendo
- Realice una conmutación tras recuperación cuando el volumen de origen ya no exista
- Escenarios de conmutación tras recuperación de SnapMirror

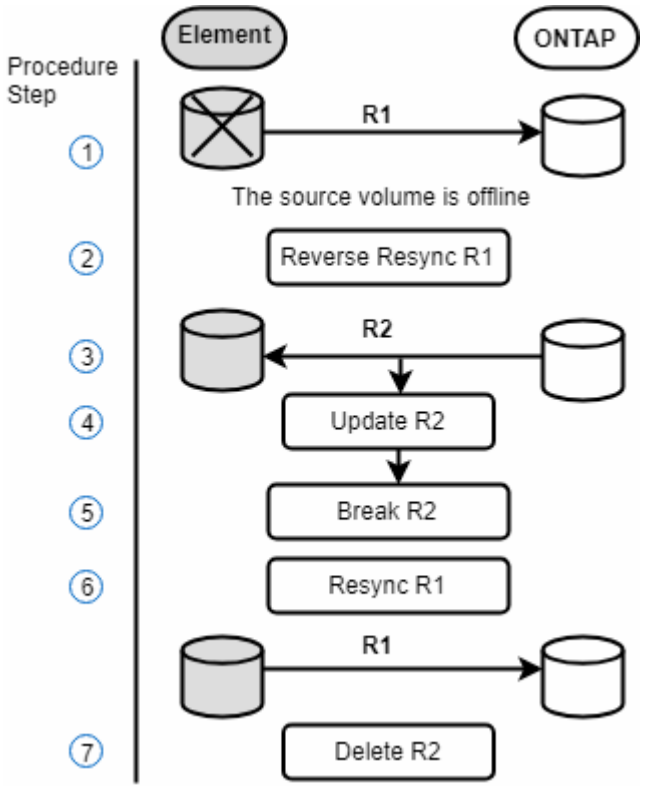
Escenarios de conmutación tras recuperación de SnapMirror

La funcionalidad de recuperación ante desastres de SnapMirror se ilustra en dos escenarios de conmutación tras recuperación. Se asume que la relación original ha sido fallida (rota).

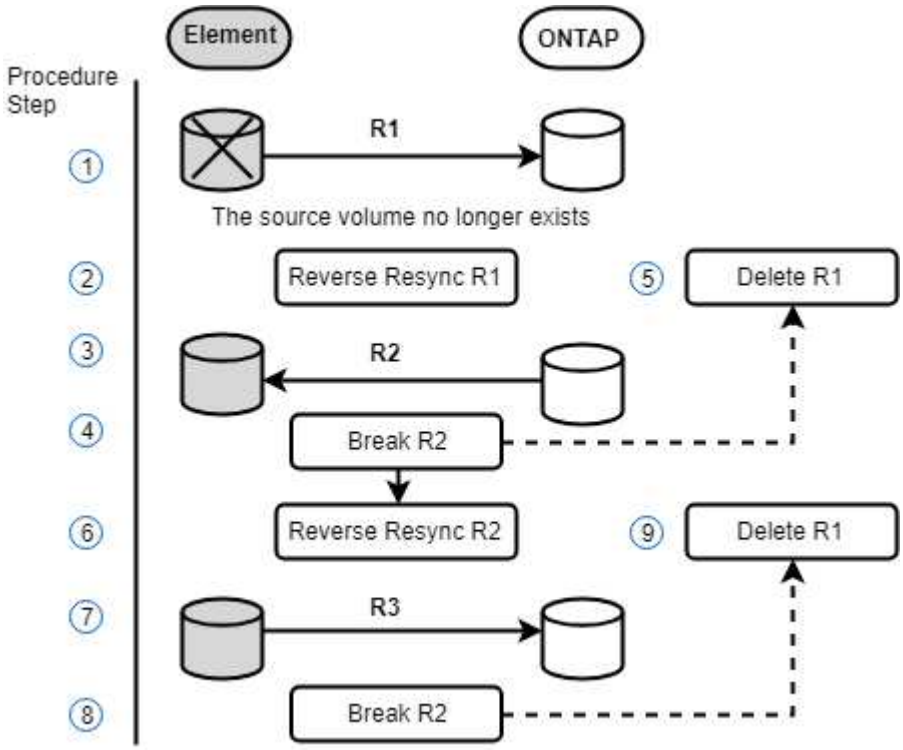
Los pasos de los procedimientos correspondientes se añaden como referencia.

En los ejemplos que se muestran aquí, R1 = la relación original en la que el clúster que ejecuta el software NetApp Element es el volumen de origen original (elemento) y ONTAP es el volumen de destino original (ONTAP). R2 y R3 representan las relaciones inversas creadas a través de la operación de resincronización inversa.

La siguiente imagen muestra el escenario de conmutación por recuperación cuando el volumen de origen sigue existiendo:



La siguiente imagen muestra el escenario de conmutación por recuperación cuando el volumen de origen ya no existe:



Obtenga más información

- Realice una conmutación tras recuperación cuando el volumen de origen siga existiendo
- Realice una conmutación tras recuperación cuando el volumen de origen ya no exista

Realice una conmutación tras recuperación cuando el volumen de origen siga existiendo

Es posible resincronizar el volumen de origen original y conmutar por error con la interfaz de usuario de NetApp Element. Este procedimiento se aplica a situaciones en las que aún existe el volumen de origen original.

1. En la interfaz de usuario de Element, busque la relación que rompió para realizar la conmutación al respaldo.
2. Haga clic en el icono acciones y haga clic en **Reverse Resync**.
3. Confirme la acción.

> La operación de resincronización inversa crea una nueva relación en la que se invierten los roles de los volúmenes de origen y de destino originales (esto provoca dos relaciones a medida que persiste la relación original). Los datos nuevos del volumen de destino original se transfieren al volumen de origen original como parte de la operación de resincronización inversa. Puede seguir accediendo al volumen activo y escribiendo datos en el lado de destino, pero deberá desconectar todos los hosts del volumen de origen y realizar una actualización de SnapMirror antes de volver a redirigir al volumen primario original.

4. Haga clic en el icono acciones de la relación inversa que acaba de crear y haga clic en **Actualizar**.

   Ahora que ha completado la resincronización inversa y aseguró que no hay sesiones activas conectadas al volumen en el lado de destino y que los datos más recientes se encuentran en el volumen primario original, es posible realizar los siguientes pasos para completar la conmutación tras recuperación y reactivar el volumen primario original:

5. Haga clic en el icono Actions de la relación inversa y haga clic en **Break**.
6. Haga clic en el icono Actions de la relación original y haga clic en **Resync**.

> El volumen primario original ahora se puede montar para reanudar las cargas de trabajo de producción en el volumen primario original. La replicación original de SnapMirror se reanuda a partir de la normativa y el programa que se ha configurado para la relación.

7. Después de confirmar que el estado original de la relación es "sinreflejado", haga clic en el icono acciones de la relación inversa y haga clic en **Eliminar**.

Obtenga más información

Escenarios de conmutación tras recuperación de SnapMirror

Realice una conmutación tras recuperación cuando el volumen de origen ya no exista

Es posible resincronizar el volumen de origen original y conmutar por error con la interfaz de usuario de NetApp Element. Esta sección se aplica a situaciones en las que se ha perdido el volumen de origen original, pero el clúster original sigue intacto. Para obtener

instrucciones sobre cómo restaurar en un clúster nuevo, consulte la documentación en el sitio de soporte de NetApp.

Lo que necesitará

- Tiene una relación de replicación despareja entre los volúmenes de Element y ONTAP.
- El volumen de Element se pierde de forma irreversiblemente.
- El nombre del volumen original se muestra como NO ENCONTRADO.

Pasos

1. En la interfaz de usuario de Element, busque la relación que rompió para realizar la conmutación al respaldo.

   Mejor práctica: anote la política de SnapMirror y los detalles del horario de la relación original de compensación. Esta información será necesaria al recrear la relación.

2. Haga clic en el icono **acciones** y haga clic en **Reverse Resync**.
3. Confirme la acción.

   La operación de resincronización inversa crea una nueva relación en la que se revierten los roles del volumen de origen y del volumen de destino (esto provoca dos relaciones a medida que persiste la relación original). Como el volumen original ya no existe, el sistema crea un nuevo volumen de Element con el mismo nombre de volumen y tamaño de volumen que el volumen de origen original. Al nuevo volumen se le asigna una política de calidad de servicio predeterminada denominada recuperación sm y se asocia a una cuenta predeterminada denominada recuperación sm. Deberá editar manualmente la cuenta y la política de calidad de servicio de todos los volúmenes creados por SnapMirror para reemplazar los volúmenes de origen originales destruidos.

   Los datos de la copia snapshot más reciente se transfieren al nuevo volumen como parte de la operación de resincronización inversa. Puede seguir accediendo al volumen activo y escribiendo datos en el lado de destino, pero deberá desconectar todos los hosts del volumen activo y realizar una actualización de SnapMirror antes de restablecer la relación primaria original en un paso posterior. Una vez finalizada la resincronización inversa y asegúrese de que no haya sesiones activas conectadas al volumen en el lado de destino y que los últimos datos estén en el volumen primario original, siga estos pasos para completar la conmutación por recuperación y reactivar el volumen primario original:

4. Haga clic en el icono **acciones** de la relación inversa que se creó durante la operación Reverse Resync y haga clic en **Break**.
5. Haga clic en el icono **acciones** de la relación original, en la que el volumen de origen no existe, y haga clic en **Eliminar**.
6. Haga clic en el icono **acciones** de la relación inversa, que rompió en el paso 4, y haga clic en **Resync inversa**.
7. De este modo, se revierte el origen y el destino y se establece una relación con el mismo origen y el mismo destino de volumen que la relación original.
8. Haga clic en el icono **acciones** y en **Editar** para actualizar esta relación con la directiva QoS original y la configuración de programación de la que tomó nota.
9. Ahora es seguro eliminar la relación inversa que usted reynced en el paso 6.

Obtenga más información

Escenarios de conmutación tras recuperación de SnapMirror

Realice una transferencia o una migración puntual de ONTAP a Element

Generalmente, cuando se usa SnapMirror para la recuperación ante desastres de un clúster de almacenamiento de SolidFire que ejecuta el software NetApp Element al software ONTAP, Element es el origen y ONTAP el destino. Sin embargo, en algunos casos, el sistema de almacenamiento ONTAP puede actuar como el origen y elemento como el destino.

- Existen dos situaciones hipotéticas:
  - No existe ninguna relación anterior de recuperación ante desastres. Siga todos los pasos de este procedimiento.
  - Existe una relación anterior de recuperación ante desastres, pero no entre los volúmenes que se utilizan para esta mitigación. En este caso, siga sólo los pasos 3 y 4 que se indican a continuación.

Lo que necesitará

- ONTAP debe haber accesible el nodo de destino de Element.
- El volumen de Element debe estar habilitado para la replicación de SnapMirror.

Debe especificar la ruta de destino del elemento en el formato hotip:/lun/<id_number>, donde lun es la cadena real '"lun"' e id_number es el ID del volumen del elemento.

Pasos

1. Con ONTAP, cree la relación con el clúster de Element:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume
-destination-path hostip:/lun/name -type XDP -schedule schedule -policy
    policy
```

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy MirrorLatest
```

2. Compruebe que la relación de SnapMirror se ha creado mediante el comando ONTAP snapmirror show.

   Consulte la información sobre la creación de una relación de replicación en la documentación de ONTAP y, para obtener una sintaxis de comando completa, consulte la página man de ONTAP.

3. Con el `ElementCreateVolume` API, cree el volumen objetivo y establezca el modo de acceso del volumen de destino en SnapMirror:

   Cree un volumen de Element mediante la API de Element

```
{
   "method": "CreateVolume",
   "params": {
        "name": "SMTargetVolumeTest2",
        "accountID": 1,
        "totalSize": 100000000000,
        "enable512e": true,
        "attributes": {},
        "qosPolicyID": 1,
        "enableSnapMirrorReplication": true,
        "access": "snapMirrorTarget"
    },
    "id": 1
}
```

4. Inicialice la relación de replicación mediante la ONTAP `snapmirror initialize` comando:

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

Realice backups y restaure volúmenes

Es posible realizar backups y restaurar volúmenes en otro almacenamiento de SolidFire, así como en almacenes de objetos secundarios que sean compatibles con OpenStack Swift o Amazon S3.

Cuando se restauran volúmenes desde OpenStack Swift o Amazon S3, se necesita información de manifiesto desde el proceso de backup original. Si desea restaurar un volumen de del cual se había realizado un backup en un sistema de almacenamiento de SolidFire, no será necesaria ninguna información de manifiesto.

Obtenga más información

- Realice backups de un volumen en un almacén de objetos Amazon S3
- Realice backups de un volumen en un almacén de objetos OpenStack Swift
- Realice backups de un volumen en un clúster de almacenamiento de SolidFire
- Restaure un volumen a partir de un backup en un almacén de objetos Amazon S3
- Restaure un volumen a partir de un backup en un almacén de objetos OpenStack Swift
- Restaure un volumen a partir de un backup en un clúster de almacenamiento de SolidFire

Realice backups de un volumen en un almacén de objetos Amazon S3

Es posible realizar backups de volúmenes de en almacenes de objetos externos que sean compatibles con Amazon S3.

1. Haga clic en **Administración** > **volúmenes**.
2. Haga clic en el icono Actions del volumen del que desea realizar un backup.
3. En el menú que se abre, haga clic en **copia de seguridad en**.
4. En el cuadro de diálogo **copia de seguridad integrada** en **copia de seguridad a**, seleccione **S3**.
5. Seleccione una opción en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
6. Introduzca un nombre de host para acceder al almacén de objetos en el campo **Hostname**.
7. Introduzca un ID de clave de acceso para la cuenta en el campo **ID de clave de acceso**.
8. Introduzca la clave de acceso secreta de la cuenta en el campo **clave de acceso secreta**.
9. Introduzca el bloque S3 en el que desea almacenar la copia de seguridad en el campo **S3 Bucket**.
10. Introduzca una etiqueta de nombre para adjuntarla al prefijo en el campo **etiqueta de nombre**.
11. Haga clic en **Iniciar lectura**.

Realice backups de un volumen en un almacén de objetos OpenStack Swift

Es posible realizar backups de volúmenes de en almacenes de objetos externos que sean compatibles con OpenStack Swift.

1. Haga clic en **Administración** > **volúmenes**.
2. Haga clic en el icono Actions del volumen del que desea realizar un backup.
3. En el menú que se abre, haga clic en **copia de seguridad en**.
4. En el cuadro de diálogo **copia de seguridad integrada** en **copia de seguridad a**, seleccione **Swift**.
5. Seleccione un formato de datos en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
6. Introduzca una dirección URL para acceder al almacén de objetos en el campo **URL**.
7. Introduzca un nombre de usuario para la cuenta en el campo **Nombre de usuario**.
8. Introduzca la clave de autenticación de la cuenta en el campo **clave de autenticación**.
9. Introduzca el contenedor en el que desea almacenar la copia de seguridad en el campo **Container**.
10. **Opcional**: Introduzca una etiqueta de nombre para adjuntarla al prefijo en el campo **nametag**.
11. Haga clic en **Iniciar lectura**.

Realice backups de un volumen en un clúster de almacenamiento de SolidFire

Es posible realizar backups de volúmenes que residen en un clúster de en un clúster remoto de para los clústeres de almacenamiento que ejecutan el software Element.

Debe confirmar que los clústeres de origen y destino están emparejados.

Consulte "Emparejar clústeres para la replicación".

Cuando se crea un backup o se restaura de un clúster a otro, el sistema genera una clave que se debe usar

como autenticación entre los clústeres. Con esta clave de escritura masiva de volúmenes, el clúster de origen puede autenticarse con el clúster de destino, lo que permite ofrecer un nivel de seguridad cuando se escribe en el volumen de destino. Como parte del proceso de backup o restauración, debe generar una clave de escritura masiva de volúmenes desde el volumen de destino antes de iniciar la operación.

1. En el clúster de destino, **Administración** > **volúmenes**.
2. Haga clic en el icono Actions del volumen de destino.
3. En el menú que se abre, haga clic en **Restaurar de**.
4. En el cuadro de diálogo **Restauración integrada**, en **Restaurar de**, seleccione **SolidFire**.
5. Seleccione una opción en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
6. Haga clic en **generar clave**.
7. Copie la clave del cuadro **Bulk Volume Write Key** en el portapapeles.
8. En el clúster de origen, vaya a **Administración** > **volúmenes**.
9. Haga clic en el icono Actions del volumen del que desea realizar un backup.
10. En el menú que se abre, haga clic en **copia de seguridad en**.
11. En el cuadro de diálogo **copia de seguridad integrada**, en **copia de seguridad a**, seleccione **SolidFire**.
12. Seleccione la misma opción que seleccionó anteriormente en el campo **Formato de datos**.
13. Introduzca la dirección IP virtual de administración del clúster del volumen de destino en el campo **Remote Cluster MVIP**.
14. Introduzca el nombre de usuario del clúster remoto en el campo **Nombre de usuario del clúster remoto**.
15. Introduzca la contraseña del clúster remoto en el campo **Remote Cluster Password**.
16. En el campo **Bulk Volume Write Key**, pegue la clave que ha generado en el clúster de destino anteriormente.
17. Haga clic en **Iniciar lectura**.

Restaure un volumen a partir de un backup en un almacén de objetos Amazon S3

Es posible restaurar un volumen a partir de un backup en un almacén de objetos Amazon S3.

1. Haga clic en **Informes** > **Registro de sucesos**.
2. Busque el evento de backup que creó el backup que debe restaurar.
3. En la columna **Detalles** del evento, haga clic en **Mostrar detalles**.
4. Copie la información de manifiesto en el portapapeles.
5. Haga clic en **Administración** > **volúmenes**.
6. Haga clic en el icono Actions del volumen que desea restaurar.
7. En el menú que se abre, haga clic en **Restaurar de**.
8. En el cuadro de diálogo **Restauración integrada** en **Restaurar de**, seleccione **S3**.
9. Seleccione la opción que coincide con la copia de seguridad en **Formato de datos**:

- **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
- **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.

10. Introduzca un nombre de host para acceder al almacén de objetos en el campo **Hostname**.
11. Introduzca un ID de clave de acceso para la cuenta en el campo **ID de clave de acceso**.
12. Introduzca la clave de acceso secreta de la cuenta en el campo **clave de acceso secreta**.
13. Introduzca el bloque S3 en el que desea almacenar la copia de seguridad en el campo **S3 Bucket**.
14. Pegue la información del manifiesto en el campo **manifiesto**.
15. Haga clic en **Iniciar escritura**.

Restaure un volumen a partir de un backup en un almacén de objetos OpenStack Swift

Es posible restaurar un volumen a partir de un backup en un almacén de objetos OpenStack Swift.

1. Haga clic en **Informes** > **Registro de sucesos**.
2. Busque el evento de backup que creó el backup que debe restaurar.
3. En la columna **Detalles** del evento, haga clic en **Mostrar detalles**.
4. Copie la información de manifiesto en el portapapeles.
5. Haga clic en **Administración** > **volúmenes**.
6. Haga clic en el icono Actions del volumen que desea restaurar.
7. En el menú que se abre, haga clic en **Restaurar de**.
8. En el cuadro de diálogo **Integrated Restore**, en **Restore from**, seleccione **Swift**.
9. Seleccione la opción que coincide con la copia de seguridad en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
10. Introduzca una dirección URL para acceder al almacén de objetos en el campo **URL**.
11. Introduzca un nombre de usuario para la cuenta en el campo **Nombre de usuario**.
12. Introduzca la clave de autenticación de la cuenta en el campo **clave de autenticación**.
13. Introduzca el nombre del contenedor en el que se almacena la copia de seguridad en el campo **Container**.
14. Pegue la información del manifiesto en el campo **manifiesto**.
15. Haga clic en **Iniciar escritura**.

Restaure un volumen a partir de un backup en un clúster de almacenamiento de SolidFire

Es posible restaurar un volumen a partir de un backup en un clúster de almacenamiento de SolidFire.

Cuando se crea un backup o se restaura de un clúster a otro, el sistema genera una clave que se debe usar como autenticación entre los clústeres. Con esta clave de escritura masiva de volúmenes, el clúster de origen puede autenticarse con el clúster de destino, lo que permite ofrecer un nivel de seguridad cuando se escribe en el volumen de destino. Como parte del proceso de backup o restauración, debe generar una clave de escritura masiva de volúmenes desde el volumen de destino antes de iniciar la operación.

1. En el clúster de destino, haga clic en **Administración** > **volúmenes**.
2. Haga clic en el icono Actions del volumen que desea restaurar.
3. En el menú que se abre, haga clic en **Restaurar de**.
4. En el cuadro de diálogo **Restauración integrada**, en **Restaurar de**, seleccione **SolidFire**.
5. Seleccione la opción que coincide con la copia de seguridad en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
6. Haga clic en **generar clave**.
7. Copie la información de **Bulk Volume Write Key** en el portapapeles.
8. En el clúster de origen, haga clic en **Administración** > **volúmenes**.
9. Haga clic en el icono Actions del volumen que quiera usar para la restauración.
10. En el menú que se abre, haga clic en **copia de seguridad en**.
11. En el cuadro de diálogo **copia de seguridad integrada**, seleccione **SolidFire** en **copia de seguridad**.
12. Seleccione la opción que coincide con la copia de seguridad en **Formato de datos**.
13. Introduzca la dirección IP virtual de administración del clúster del volumen de destino en el campo **Remote Cluster MVIP**.
14. Introduzca el nombre de usuario del clúster remoto en el campo **Nombre de usuario del clúster remoto**.
15. Introduzca la contraseña del clúster remoto en el campo **Remote Cluster Password**.
16. Pegue la clave del portapapeles en el campo **Bulk Volume Write Key**.
17. Haga clic en **Iniciar lectura**.

Solucionar los problemas del sistema

Debe supervisar el sistema para realizar diagnósticos y obtener información acerca de las tendencias y los Estados de rendimiento de varios operaciones del sistema. Puede que deba sustituir nodos o SSD por motivos de mantenimiento.

- "Ver información acerca de los eventos del sistema"
- "Ver el estado de las tareas en ejecución"
- "Ver las alertas del sistema"
- "Ver la actividad de rendimiento del nodo"
- "Ver el rendimiento del volumen"
- "Ver sesiones iSCSI"
- "Consulte las sesiones Fibre Channel"
- "Solucione problemas de unidades"
- "Solucione los problemas de los nodos"
- "Trabaje con utilidades por nodo para los nodos de almacenamiento"
- "Trabaje con el nodo de gestión"
- "Comprender los niveles de llenado de clústeres"

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Ver información acerca de los eventos del sistema

Es posible ver información sobre varios eventos detectados en el sistema. El sistema actualiza los mensajes de evento cada 30 segundos. El registro de eventos muestra eventos clave para el clúster.

1. En la interfaz de usuario de Element, seleccione **Reporting** > **Event Log**.

   Para cada evento, verá la siguiente información:

Elemento	Descripción
ID	ID exclusivo asociado con cada evento.
Tipo de evento	Tipo de evento que se está registrando; por ejemplo, eventos de API o eventos de clon.
Mensaje	Mensaje asociado con el evento.
Detalles	Información que ayuda a identificar por qué ocurre el evento.
ID de servicio	El servicio que notificó el evento (si corresponde).
Nodo	El nodo que notificó el evento (si corresponde).
ID de unidad	La unidad que notificó el evento (si corresponde).
Hora del evento	La hora en la que ocurrió el evento.

Obtenga más información

Tipos de evento

Tipos de evento

El sistema informa de varios tipos de eventos, cada uno de los cuales es una operación que completó el sistema. Los eventos son rutinarios y normales, o bien eventos que requieren la atención del administrador. La columna Event Types en la página Event Log indica en qué parte del sistema se ha producido el evento.

El sistema no registra comandos de API de solo lectura en el registro de eventos.

En la siguiente lista, se describen los tipos de eventos que aparecen en el registro de eventos:

- **ApiEvent**

  Eventos que inicia un usuario a través de una API o una interfaz de usuario web que modifican la configuración.

- **BinAssignmentEvent**

  Eventos relacionados con la asignación de ubicaciones de datos. En esencia, las ubicaciones son contenedores que incluyen datos que se asignan en el clúster.

- **BinSyncEvent**

  Eventos del sistema relacionados con una reasignación de los datos entre los servicios de bloques.

- **BsCheckEvent**

  Eventos del sistema relacionados con las comprobaciones de servicios de bloques.

- **BsKillEvent**

  Eventos del sistema relacionados con las terminaciones de servicios de bloques.

- **BulkOpEvent**

  Eventos relacionados con operaciones realizadas en un volumen completo, como un backup, una restauración, una copia de Snapshot o un clon.

- **ClonEvent**

  Eventos relacionados con el clonado de volúmenes.

- **ClusterMasterEvent**

  Eventos que aparecen tras la inicialización del clúster o tras los cambios de configuración en el clúster, como la adición o la eliminación de nodos.

- **CsumEvent**

  Eventos relacionados con sumas de comprobación de datos no válidas en el disco.

- **DataEvent**

  Eventos relacionados con la lectura y la escritura de datos.

- **DbEvent**

  Eventos relacionados con la base de datos global que mantienen los nodos del conjunto en el clúster.

- **DriveEvent**

  Eventos relacionados con las operaciones de unidades.

- **EncryptionAtRestEvent**

Eventos relacionados con el proceso de cifrado en un clúster.

- **EnsembleEvent**

  Eventos relacionados con el aumento o la reducción del número de nodos en un conjunto.

- **FiberChannelEvent**

  Eventos relacionados con la configuración de los nodos y las conexiones con ellos.

- **GcEvent**

  Eventos relacionados con los procesos que se ejecutan cada 60 minutos para reclamar almacenamiento en las unidades de bloques. Este proceso también se conoce como recolección de basura.

- **IeEvent**

  Error interno del sistema.

- **InstallEvent**

  Eventos de instalación automática del software. El software se instala automáticamente en un nodo pendiente.

- **ISCSIEvent**

  Eventos relacionados con los problemas de iSCSI en el sistema.

- **LimitEvent**

  Eventos relacionados con el número de volúmenes o volúmenes virtuales en una cuenta o en el clúster que se acercan al máximo permitido.

- **MantenimientoModeEvent**

  Eventos relacionados con el modo de mantenimiento de los nodos, como deshabilitar el nodo.

- **NetworkEvent**

  Eventos relacionados con el estado de las redes virtuales.

- **PlatformHardwarwareEvent**

  Eventos relacionados con los problemas detectados en los dispositivos de hardware.

- **RemoteClusterEvent**

  Eventos relacionados con el emparejamiento de clústeres remotos.

- **PlaneerEvent**

  Eventos relacionados con las copias de Snapshot programadas.

- **ServiceEvent**

  Eventos relacionados con el estado de servicio del sistema.

- **SliceEvent**

  Eventos relacionados con el servidor de segmentos, como la eliminación de un volumen o una unidad de metadatos.

  Existen tres tipos de eventos de reasignación de segmentos, que incluyen información acerca del servicio al que se asigna un volumen:

  - voltear: cambiar el servicio primario a un nuevo servicio primario

    ```
    sliceID oldPrimaryServiceID->newPrimaryServiceID
    ```

  - mover: cambiar el servicio secundario a un nuevo servicio secundario

    ```
    sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
    ```

  - eliminar: eliminar un volumen de un conjunto de servicios

    ```
    sliceID {oldSecondaryServiceID(s)}
    ```

- **SnmpTrapEvent**

  Eventos relacionados con capturas SNMP.

- **StatEvent**

  Eventos relacionados con las estadísticas del sistema.

- **TsEvent**

  Eventos relacionados con el servicio de transporte del sistema.

- **Inesperado Exception**

  Eventos relacionados con las excepciones del sistema inesperadas.

- **UreEvent**

  Eventos relacionados con errores de lectura irrecuperables que se producen durante la lectura desde el dispositivo de almacenamiento.

- **VasaProviderEvent**

  Eventos relacionados con un proveedor de VASA (API de vSphere para el reconocimiento del almacenamiento).

Ver el estado de las tareas en ejecución

Puede ver el progreso y el estado de finalización de las tareas en ejecución de la interfaz

de usuario web que notifican los métodos API ListSyncJobs y ListBulkVolumeJobs. Puede acceder a la página Running Tasks desde la pestaña Reporting de la interfaz de usuario de Element.

En el caso de que haya un gran número de tareas, el sistema puede ponerlas en cola y ejecutarlas en lotes. En la página Running Tasks se muestran los servicios que se están sincronizando en ese momento. Cuando una tarea se completa, se reemplaza por la siguiente tarea de sincronización en la cola. Las tareas de sincronización pueden seguir apareciendo en la página Running Tasks hasta que no haya más tareas pendientes.

Los datos de las sincronizaciones de replicación de los volúmenes que se están replicando se pueden ver en la página Running Tasks del clúster que contiene el volumen de destino.

Ver las alertas del sistema

Puede ver las alertas para obtener información sobre errores del clúster en el sistema. Las alertas pueden tratarse de información, advertencias o errores, y son un buen indicador del funcionamiento del clúster. La mayoría de errores se resuelven automáticamente por sí mismos.

Puede usar el método API ListClusterFaults para automatizar la supervisión de alertas. De este modo podrá recibir notificaciones sobre todas las alertas que se produzcan.

1. En la interfaz de usuario de Element, seleccione **Reporting** > **Alerts**.

   El sistema actualiza las alertas de la página cada 30 segundos.

   Para cada evento, verá la siguiente información:

Elemento	Descripción
ID	ID único asociado con una alerta de clúster.
Gravedad	El grado de importancia de la alerta. Los posibles valores son los siguientes: • Warning: Un problema menor que podría requerir su atención pronto. Las actualizaciones del sistema todavía están permitidas. • Error: Un error que puede provocar la degradación del rendimiento o la pérdida de alta disponibilidad (ha). En general, los errores no deben afectar el servicio de otro modo. • Critical: Un error grave que afecta el servicio. El sistema no es capaz de atender las solicitudes de I/o de la API o el cliente. El funcionamiento en este estado podría provocar la pérdida potencial de datos. • BestPractice: No se utiliza una práctica recomendada de configuración del sistema.

Tipo	El componente al que afecta el fallo. Puede ser nodo, unidad, clúster, servicio o volumen.
Nodo	ID de nodo para el nodo al que hace referencia este error. Se incluye para los errores de nodo y de unidad; de lo contrario se establece como - (guion).
ID de unidad	ID de unidad para la unidad a la que hace referencia este error. Se incluye para los errores drive; de lo contrario se establece como - (guion).
Código de error	Código descriptivo que indica cuál es la causa del error.
Detalles	Una descripción del error con detalles adicionales.
Fecha	La fecha y la hora en la que se registró el error.

2. Haga clic en **Mostrar detalles** para ver una alerta individual y ver información sobre la alerta.
3. Para ver los detalles de todas las alertas de la página, haga clic en la columna Details.

   Una vez que el sistema resuelve una alerta, toda la información sobre la alerta, incluida la fecha en la que se solucionó, se traslada al área Resolved.

Obtenga más información

- códigos de error de clúster
- "Gestione el almacenamiento con la API de Element"

códigos de error de clúster

El sistema informa de un error o un estado que puede ser de su interés al generar un código de error, que se incluye en la página Alerts. Estos códigos ayudan a determinar en qué componente del sistema se generó la alerta y por qué se generó.

En la siguiente lista se describen los distintos tipos de códigos:

- **AutenticaciónServiceFault**

  El servicio de autenticación en uno o más nodos del clúster no funciona según lo esperado.

  Comuníquese con el soporte de NetApp para obtener ayuda.

- **Disponible VirtualNetworkIPAddressLow**

  El número de direcciones de red virtual en el bloque de direcciones IP es bajo.

  Para resolver esta falla, añada más direcciones IP al bloque de direcciones de red virtual.

- **BlockBlockClusterFull**

  No hay suficiente espacio libre de almacenamiento basado en bloques para admitir la pérdida de un solo nodo. Consulte el método API GetClusterFullThreshold para obtener detalles sobre los niveles de ocupación de los clústeres. Esta falla del clúster indica una de las siguientes condiciones:

  - Stage3Low (Advertencia): Se superó el umbral definido por el usuario. Ajuste la configuración del clúster lleno o añada más nodos.
  - Stage4Critical (error): No hay espacio suficiente para recuperar el sistema de un fallo de 1 nodo. No se permite la creación de volúmenes, snapshots y clones.
  - Stage5CompletelyConsumed (crítico)1; no se permiten escrituras ni nuevas conexiones iSCSI. Se mantendrán las conexiones iSCSI actuales. Las escrituras fallarán hasta que se añada más capacidad al clúster. Para resolver esta falla, purgue o elimine volúmenes o añada otro nodo de almacenamiento al clúster de almacenamiento.

- * BlocksDegraded*

  Los datos de bloques ya no se replican por completo debido a un fallo.

Gravedad	Descripción
Advertencia	Solo se puede acceder a dos copias completas de datos en bloques.
Error	Solo se puede acceder a una única copia completa de los datos en bloque.
Crítico	No se puede acceder a ninguna copia completa de los datos en bloque.

  Nota: el estado de aviso sólo puede ocurrir en un sistema de Triple Helix.

  Para resolver esta falla, restaure los nodos sin conexión o los servicios de bloques, o póngase en contacto con el soporte de NetApp para obtener ayuda.

- **BlockServiceTooFull**

  Un servicio de bloques está utilizando demasiado espacio.

  Para resolver esta falla, añada más capacidad aprovisionada.

- **BlockServiceUnhealthy**

  Se detectó que un servicio de bloques está en mal estado:

  - Gravedad = Advertencia: No se realiza ninguna acción. Este período de advertencia caducará en cTimeUntilBSIsKilledMSec=330000 milisegundos.
  - Gravedad = error: El sistema decomisiona automáticamente los datos y vuelve a replicar los datos en otras unidades en buen estado.
  - Severidad = crítico: Hay servicios de bloque con errores en varios nodos mayores o iguales al número de replicación (2 para Double Helix). Los datos no están disponibles y la sincronización de bandejas no finalizará. Compruebe si existen problemas de conectividad de red y errores de hardware. Si se han

producido errores en componentes de hardware específicos, habrá otros errores. El fallo se borrará cuando se pueda acceder al servicio de bloqueo o cuando se haya retirado el servicio.

- **RelojSkewExceedsFaultThreshold**

  El desfase de tiempo entre el maestro de clústeres y el nodo que presenta un token supera el umbral recomendado. El clúster de almacenamiento no puede corregir el desfase de hora entre los nodos automáticamente.

  Para resolver esta falla, use los servidores NTP internos a la red en lugar de los que vienen predeterminados en la instalación. Si usa un servidor NTP interno, comuníquese con el soporte de NetApp para obtener ayuda.

- **ClusterCannotSync**

  Hay una condición de falta de espacio y los datos en las unidades de almacenamiento en bloque desconectadas no pueden sincronizarse con las unidades que siguen activas.

  Para resolver esta falla, añada más almacenamiento.

- **ClusterFull**

  No hay más espacio de almacenamiento libre en el clúster de almacenamiento.

  Para resolver esta falla, añada más almacenamiento.

- **ClusterIOPSAreOverProvisioned**

  Hay un sobreaprovisionamiento de IOPS en el clúster. La suma de todas las IOPS de calidad de servicio mínima es mayor que el número de IOPS que se espera del clúster. No puede mantenerse una calidad de servicio mínima para todos los volúmenes en simultáneo.

  Para resolver este problema, reduzca la configuración mínima de IOPS de calidad de servicio para los volúmenes.

- **DisableDriveSecurityFailed**

  El clúster no se configura para habilitar la seguridad de la unidad (cifrado en reposo), pero al menos una unidad tiene la seguridad de la unidad habilitada, lo cual significa que se deshabilita la seguridad de la unidad en esas unidades. Este fallo se registra con la gravedad "'Advertencia'".

  Para resolver esta falla, compruebe los detalles de la falla por el motivo por el que no se pudo deshabilitar la seguridad de la unidad. Los posibles motivos son:

  - No se pudo adquirir la clave de cifrado, investigue el problema de acceso a la clave o al servidor de claves externo.
  - Se produjo un error en la operación de desactivación de la unidad, determine si es posible que se haya adquirido una clave incorrecta. Si ninguno de estos son el motivo del fallo, es posible que sea necesario sustituir la unidad.

  Es posible intentar recuperar una unidad que no deshabilita la seguridad correctamente incluso cuando se proporciona la clave de autenticación correcta. Para realizar esta operación, quite las unidades del sistema moverlas a Available, ejecute un borrado seguro en la unidad y vuelva a moverlas a Active.

- **DesconecttedClusterPair**

Una pareja de clústeres está desconectada o configurada incorrectamente. Compruebe la conectividad de red entre los clústeres.

- **DisconnectedRemoteNode**

  Un nodo remoto está desconectado o configurado incorrectamente. Compruebe la conectividad de red entre los nodos.

- **DesconectadoSnapMirrorEndpoint**

  Un extremo de SnapMirror remoto está desconectado o configurado incorrectamente. Compruebe la conectividad de red entre el clúster y el SnapMirrorEndpoint remoto.

- **Disponible**

  Hay una o más unidades disponibles en el clúster. En general, todos los clústeres deben tener todas las unidades añadidas, y ninguna debe estar en estado disponible. Si esta falla aparece de forma inesperada, comuníquese con el soporte de NetApp.

  Para resolver esta falla, añada las unidades disponibles al clúster de almacenamiento.

- **DriveFailed**

  El clúster devuelve esta falla cuando una o más unidades han fallado, lo cual indica una de las siguientes condiciones:

  - El administrador de unidades no puede acceder a la unidad.
  - El servicio de segmentos o bloques se ha producido un error demasiadas veces, probablemente debido a fallos de lectura o escritura de la unidad y no se puede reiniciar.
  - Falta la unidad.
  - No se puede acceder al servicio maestro del nodo (todas las unidades del nodo se consideran ausentes o con errores).
  - La unidad está bloqueada y no puede adquirirse la clave de autenticación de la unidad.
  - La unidad se bloqueó y la operación de desbloqueo falla. Para resolver este problema:
  - Compruebe la conectividad de red del nodo.
  - Sustituya la unidad.
  - Asegúrese de que la clave de autenticación esté disponible.

- **HealthdriveFault**

  Se produjo un error en la comprobación DEL estado INTELIGENTE de una unidad y, como resultado, se reducen las funciones de la unidad. Existe un nivel de gravedad crítico para esta falla:

  - Unidad con serie: <serial number> en ranura: <node slot> <drive slot> no superó la comprobación de estado general INTELIGENTE. Para resolver esta falla, reemplace la unidad.

- **DriveWeFault**

  La vida útil restante de una unidad cayó por debajo del umbral permitido, pero la unidad sigue funcionando.existen dos niveles de gravedad posibles para este fallo: Crucial y Advertencia:

  - Unidad con serie: <serial number> en ranura: <node slot> <drive slot> tiene niveles de desgaste críticos.

- Unidad con serie: <serial number> en ranura: <node slot> <drive slot> tiene bajas reservas de desgaste. Para resolver esta falla, reemplace la unidad cuanto antes.

- **DuplicateClusterMasterCandidates**

  Se detectó más de un candidato maestro de clúster de almacenamiento. Comuníquese con el soporte de NetApp para obtener ayuda.

- **EnableDriveSecurityFailed**

  El clúster se configura para requerir seguridad de unidades (cifrado en reposo), pero la seguridad de unidades no se pudo habilitar en al menos una unidad. Este fallo se registra con la gravedad "'Advertencia'".

  Para resolver esta falla, compruebe los detalles de la falla por el motivo por el que no se pudo habilitar la seguridad de la unidad. Los posibles motivos son:

  - No se pudo adquirir la clave de cifrado, investigue el problema de acceso a la clave o al servidor de claves externo.
  - Se produjo un error en la operación de habilitación en la unidad, para determinar si podría haberse adquirido una clave incorrecta. Si ninguno de estos son el motivo del fallo, es posible que sea necesario sustituir la unidad.

  Es posible intentar recuperar una unidad que no habilita la seguridad correctamente incluso cuando se proporciona la clave de autenticación correcta. Para realizar esta operación, quite las unidades del sistema moverlas a Available, ejecute un borrado seguro en la unidad y vuelva a moverlas a Active.

- * Ensembergraded*

  Se perdió la alimentación de energía o la conectividad de red en uno o varios de los nodos del conjunto.

  Para resolver esta falla, restaure la alimentación o la conectividad de red.

- **excepción**

  Una falla que no es de rutina. Estas fallas no se borran automáticamente de la cola de fallas. Comuníquese con el soporte de NetApp para obtener ayuda.

- **FailedSpaceTooFull**

  Un servicio de bloques no responde a las solicitudes de escritura de datos. Esto provoca que el servicio de segmentos se quede sin espacio para almacenar escrituras fallidas.

  Para resolver esto, restaure la funcionalidad de servicios de bloques de modo que las escrituras puedan continuar normalmente y que el espacio con fallas se vacíe en el servicio de segmentos.

- **FanSensor**

  Un sensor de ventilador presenta una falla o está ausente.

  Para resolver esta falla, reemplace cualquier hardware con errores.

- **FiberChannelAccessDegraded**

  Un nodo Fibre Channel no responde a otros nodos en el clúster de almacenamiento a través de su dirección IP de almacenamiento durante un período. En este estado, se considera que el nodo no

responde y se genera una falla en el clúster. Compruebe la conectividad de red.

- **FiberChannelAccessUnavailable**

  Ninguno de los nodos Fibre Channel responde. Se muestran los ID de los nodos. Compruebe la conectividad de red.

- **FiberChannelActiveIxL**

  El número de Nexus IXL se acerca al límite admitido de 8000 sesiones activas por nodo Fibre Channel.

  - El límite de mejores prácticas es de 5500.
  - El límite de advertencia es 7500.
  - El límite máximo (no forzado) es 8192. Para resolver esta falla, reduzca el número de Nexus IXL por debajo del límite de mejores prácticas de 5500.

- **FiberChannelConfig**

  Esta falla del clúster indica una de las siguientes condiciones:

  - Hay un puerto de Fibre Channel no esperado en una ranura PCI.
  - Hay un modelo de adaptador de bus de host de Fibre Channel no esperado.
  - Hay un problema con el firmware de un adaptador de bus de host de Fibre Channel.
  - Un puerto de Fibre Channel no está en línea.
  - Hay un problema persistente en la configuración de traspaso de Fibre Channel. Comuníquese con el soporte de NetApp para obtener ayuda.

- **FiberChannelIOPS**

  El número total de IOPS está cerca del límite de IOPS para los nodos Fibre Channel del clúster. Los límites son:

  - FC0025: Límite de 450 000 IOPS con un tamaño de bloque de 4 KB por nodo Fibre Channel.
  - FCN001: Límite de 625K OPS a un tamaño de bloque de 4K por nodo Fibre Channel. Para resolver esta falla, equilibre la carga en todos los nodos Fibre Channel disponibles.

- **FiberChannelStaticIxL**

  El número de Nexus IXL se acerca al límite admitido de 16000 sesiones estáticas por nodo Fibre Channel.

  - El límite de mejores prácticas es de 11000.
  - El límite de advertencia es 15000.
  - El límite máximo (obligatorio) es 16384. Para resolver esta falla, reduzca el número de Nexus IXL por debajo del límite de mejores prácticas de 11000.

- **FileSystemCapacidadLow**

  No hay espacio suficiente en uno de los sistemas de archivos.

  Para resolver esta falla, añada más capacidad al sistema de archivos.

- **FipsDrivesdiscordancia**

  Se insertó de forma física una unidad que no es FIPS en un nodo de almacenamiento compatible con

FIPS o se insertó de forma física una unidad FIPS en un nodo de almacenamiento que no es FIPS. Se genera un solo error por nodo y se enumera todas las unidades afectadas.

Para resolver esta falla, quite o sustituya la unidad o las unidades con discrepancias.

- **FipsDrivesOutOfCompliance**

  El sistema detectó que se deshabilitó el cifrado en reposo después de habilitar la función FIPS Drives. Esta falla también se genera cuando la función de unidades FIPS está habilitada y hay un nodo o una unidad no FIPS en el clúster de almacenamiento.

  Para resolver esta falla, habilite el cifrado en reposo o elimine el hardware que no es FIPS del clúster de almacenamiento.

- **FipsSelfTestFailure**

  El subsistema FIPS detectó un fallo durante la autoprueba.

  Comuníquese con el soporte de NetApp para obtener ayuda.

- **HardwareConfigdiscordancia**

  Esta falla del clúster indica una de las siguientes condiciones:

  - La configuración no coincide con la definición del nodo.
  - El tamaño de unidad para este tipo de nodo es incorrecto.
  - Se detectó una unidad no compatible. Un posible motivo es que la versión de elemento instalada no reconoce esta unidad. Recomienda actualizar el software Element en este nodo.
  - Hay un error de coincidencia en el firmware de la unidad.
  - El estado de capacidad de cifrado de la unidad no coincide con el nodo. Comuníquese con el soporte de NetApp para obtener ayuda.

- **IdPCertificateExpiración**

  El certificado SSL del proveedor de servicios del clúster para su uso con un proveedor de identidades (IDP) de terceros está a punto de expirar o ya ha caducado. Este fallo utiliza las siguientes gravedades en función de la urgencia:

Gravedad	Descripción
Advertencia	El certificado caduca dentro de los 30 días.
Error	El certificado caduca dentro de los 7 días.
Crítico	El certificado caduca en un plazo de 3 días o ya ha caducado.

  Para resolver esta falla, actualice el certificado SSL antes de que caduque. Utilice el método API UpdateIdpConfiguration con `refreshCertificateExpirationTime=true` Para proporcionar el certificado SSL actualizado.

- **InconstentBondModes**

Los modos de enlace en el dispositivo de VLAN no están presentes. Esta falla muestra el modo de enlace esperado y el modo de enlace actualmente en uso.

- **InconstentInterfaceConfiguration**

  La configuración de la interfaz es inconsistente.

  Para resolver esta falla, asegúrese de que las interfaces de nodos en el clúster de almacenamiento estén configuradas de manera consistente.

- * InconstentMtus*

  Esta falla del clúster indica una de las siguientes condiciones:

  - Bond1G mismatch: Se detectaron varias MTU inconsistentes en interfaces Bond1G.
  - Bond10G mismatch: Se detectaron varias MTU inconsistentes en interfaces Bond10G. Esta falla muestra los nodos en cuestión junto con el valor de MTU asociado.

- **InconstentRoutingRules**

  Las reglas de enrutamiento de esta interfaz son inconsistentes.

- * InconstentSubnetMasks*

  La máscara de red en el dispositivo de VLAN no coincide con la máscara de red registrada internamente para la VLAN. Esta falla muestra la máscara de red esperada y la máscara de red actualmente en uso.

- * IncorrectBondPortCount*

  El número de puertos de enlace es incorrecto.

- **InvalidConfigdFiberChannelNodeCount**

  Una de las dos conexiones de nodos Fibre Channel esperadas está degradada. Esta falla aparece cuando se conecta un solo nodo Fibre Channel.

  Para resolver esta falla, compruebe la conectividad de red y el cableado de red del clúster y compruebe los servicios con errores. Si no hay problemas de red o servicio, comuníquese con el soporte de NetApp para obtener el reemplazo de un nodo Fibre Channel.

- **IrqBalanceFailed**

  Se produjo una excepción al intentar balancear las interrupciones.

  Comuníquese con el soporte de NetApp para obtener ayuda.

- **KmipCertificateFault**
  - El certificado de la entidad de certificación raíz (CA) está cerca de su vencimiento.

    Para resolver este fallo, adquiera un nuevo certificado de la CA raíz con una fecha de caducidad de al menos 30 días y utilice ModifyKeyServerKmip para proporcionar el certificado de CA raíz actualizado.

  - El certificado de cliente está a punto de expirar.

    Para resolver esta falla, cree una nueva CSR con GetClientCertificateSigningRequest, asegúrese de

que la nueva fecha de caducidad se agota al menos 30 días y utilice ModifyKeyServerKmip para reemplazar el certificado de cliente KMIP que caduca con el nuevo certificado.

- El certificado de la entidad de certificación raíz (CA) ha caducado.

  Para resolver este fallo, adquiera un nuevo certificado de la CA raíz con una fecha de caducidad de al menos 30 días y utilice ModifyKeyServerKmip para proporcionar el certificado de CA raíz actualizado.

- El certificado de cliente ha caducado.

  Para resolver esta falla, cree una nueva CSR con GetClientCertificateSigningRequest, asegúrese de que la nueva fecha de caducidad se agota al menos 30 días y utilice ModifyKeyServerKmip para reemplazar el certificado de cliente KMIP caducado con el nuevo certificado.

- Error de certificado de entidad de certificación raíz (CA).

  Para resolver esta falla, compruebe que se proporcionó el certificado correcto y, si fuera necesario, vuelva a adquirir el certificado de la CA raíz. Utilice ModifyKeyServerKmip para instalar el certificado de cliente KMIP correcto.

- Error del certificado de cliente.

  Para resolver esta falla, compruebe que esté instalado el certificado de cliente KMIP correcto. La CA raíz del certificado de cliente debe instalarse en el EKS. Utilice ModifyKeyServerKmip para instalar el certificado de cliente KMIP correcto.

- **KmipServerFault**
  - Error de conexión

    Para resolver esta falla, compruebe que el servidor de claves externo esté vivo y sea posible acceder a él a través de la red. Utilice TestKeyServerKimp y TestKeyProviderKmip para probar su conexión.

  - Error de autenticación

    Para resolver esta falla, compruebe que se estén utilizando los certificados de cliente KMIP y de CA raíz correctos, y que coincidan las claves privadas y el certificado de cliente KMIP.

  - Error del servidor

    Para resolver esta falla, compruebe los detalles del error. Es posible que sea necesario solucionar los problemas en el servidor de claves externo según el error que se devuelve.

- **MemoryEccThreshold**

  Se ha detectado un gran número de errores ECC corregibles o no corregibles. Este fallo utiliza las siguientes gravedades en función de la urgencia:

Evento	Gravedad	Descripción
Un único módulo DIMM cErrorCount llega a cDimmcorrectableErrWarnThreshold.	Advertencia	Errores corregibles de memoria ECC por encima del umbral en DIMM: <Processor> <DIMM Slot>

Un único DIMM cErrorCount permanece por encima de cDimmcorrectableErrWarnThreshold hasta que el temporizador ciErrorFaultTimer caduca para el DIMM.	Error	Errores corregibles de memoria ECC por encima del umbral en DIMM: <Processor> <DIMM>
Un controlador de memoria informa cErrorCount encima de cMemCtlrcorrectableErrWarnThreshold y se especifica cMemCtlrcorrectableErrWarnDuration.	Advertencia	Errores corregibles de memoria ECC por encima del umbral en el controlador de memoria: <Processor> <Memory Controller>
Un controlador de memoria informa cErrorCount sobre cMemCtlrcorrectableErrWarnThreshold hasta que cErrorFaultTimer caduca para el controlador de memoria.	Error	Errores corregibles de memoria ECC por encima del umbral en DIMM: <Processor> <DIMM>
Un módulo DIMM único informa de un uErrorCount por encima de cero, pero inferior a cDimmUncorrectTaberreErrFaultThreshold.	Advertencia	Errores de memoria ECC no corregibles detectados en el módulo DIMM: <Processor> <DIMM Slot>
Un módulo DIMM único informa de un uErrorCount de al menos cmimUncorrecttableErrFaultThreshold.	Error	Errores de memoria ECC no corregibles detectados en el módulo DIMM: <Processor> <DIMM Slot>
Un controlador de memoria informa de un uErrorCount por encima de cero, pero menor que cMemctlenseUncorrecttableErrFaultThreshold.	Advertencia	Errores de memoria ECC no corregibles detectados en el controlador de memoria: <Processor> <Memory Controller>
Un controlador de memoria informa de un uErrorCount de al menos cMemctlrUncorrecttableErrFaultThreshold.	Error	Errores de memoria ECC no corregibles detectados en el controlador de memoria: <Processor> <Memory Controller>

Para resolver esta falla, comuníquese con el soporte de NetApp para obtener ayuda.

- **MemyUsageThreshold**

  El uso de memoria está por encima de lo normal. Este fallo utiliza las siguientes gravedades en función de la urgencia:

Consulte el encabezado **Detalles** del error para obtener información más detallada sobre el tipo de fallo.

Gravedad	Descripción
Advertencia	La memoria del sistema es baja.
Error	La memoria del sistema es muy baja.
Crítico	La memoria del sistema se ha consumido por completo.

Para resolver esta falla, comuníquese con el soporte de NetApp para obtener ayuda.

- **MetadataClusterFull**

  No hay suficiente espacio libre de almacenamiento de metadatos para admitir la pérdida de un solo nodo. Consulte el método API GetClusterFullThreshold para obtener detalles sobre los niveles de ocupación de los clústeres. Esta falla del clúster indica una de las siguientes condiciones:

  - Stage3Low (Advertencia): Se superó el umbral definido por el usuario. Ajuste la configuración del clúster lleno o añada más nodos.
  - Stage4Critical (error): No hay espacio suficiente para recuperar el sistema de un fallo de 1 nodo. No se permite la creación de volúmenes, snapshots y clones.
  - Stage5CompletelyConsumed (crítico)1; no se permiten escrituras ni nuevas conexiones iSCSI. Se mantendrán las conexiones iSCSI actuales. Las escrituras fallarán hasta que se añada más capacidad al clúster. Purgue o elimine datos o añada más nodos. Para resolver esta falla, purgue o elimine volúmenes o añada otro nodo de almacenamiento al clúster de almacenamiento.
- **MtuCheckFailure**

  Un dispositivo de red no tiene configurado el tamaño de MTU correcto.

  Para resolver esta falla, asegúrese de que todas las interfaces de red y puertos del switch tengan configuradas tramas gigantes (MTU de hasta 9000 bytes de tamaño).
- **NetworkConfig**

  Esta falla del clúster indica una de las siguientes condiciones:

  - No hay una interfaz esperada.
  - Hay una interfaz duplicada.
  - Una interfaz configurada está inactiva.
  - Se requiere reiniciar la red. Comuníquese con el soporte de NetApp para obtener ayuda.
- **NoAvailableVirtualNetworkIPAddresses**

  No hay direcciones de red virtual disponibles en el bloque de direcciones IP.

  - VirtualNetworkID # TAG(#) no tiene direcciones IP de almacenamiento disponibles. No es posible agregar nodos adicionales al clúster. Para resolver esta falla, añada más direcciones IP al bloque de direcciones de red virtual.

- **NodeHardwarFault (falla de interfaz de red <name> o el cable está desconectado)**

  Una interfaz de red está desconectada o el cable está desenchufado.

  Para resolver esta falla, compruebe la conectividad de red de los nodos.

- **NodeHardwarfault (el estado de capacidad de cifrado de la unidad coincide con el estado de capacidad de cifrado del nodo para la unidad en la ranura <node slot> <drive slot>)**

  Una unidad no coincide con las funcionalidades de cifrado del nodo de almacenamiento en el que se instala.

- **NodeHardwareFault (error de tamaño de unidad <drive type> <actual size> para la unidad en la ranura <node slot> <drive slot> para este tipo de nodo - <expected size> esperado)**

  Un nodo de almacenamiento contiene una unidad que tiene un tamaño incorrecto para este nodo.

- **NodeHardwareFault (unidad no compatible detectada en la ranura <node slot> <drive slot>; las estadísticas de la unidad y la información de estado no estarán disponibles)**

  Un nodo de almacenamiento contiene una unidad que no es compatible.

- **NodeHardwareFault (la unidad de la ranura <node slot> <drive slot> debe utilizar la versión de firmware <expected version>, pero utiliza la versión no compatible <actual version>)**

  Un nodo de almacenamiento contiene una unidad que ejecuta una versión de firmware no compatible.

- * NodeMaintenanceMode*

  Se ha colocado un nodo en modo de mantenimiento. Este fallo utiliza las siguientes gravedades en función de la urgencia:

Gravedad	Descripción
Advertencia	Indica que el nodo aún está en modo de mantenimiento.
Error	Indica que el modo de mantenimiento no se ha desactivado, lo más probable es que se deba a stabys activos o con errores.

  Para resolver esta falla, deshabilite el modo de mantenimiento una vez que finalice el mantenimiento. Si el fallo del nivel de error persiste, comuníquese con el soporte de NetApp para obtener ayuda.

- **NodeOffline**

  El software Element no puede comunicarse con el nodo especificado. Compruebe la conectividad de red.

- **NotUsingLACPBondMode**

  El modo de enlace LACP no está configurado.

  Para resolver esta falla, use el enlace LACP cuando se implementan nodos de almacenamiento; es posible que los clientes experimenten problemas de rendimiento si LACP no está habilitado y configurado

correctamente.

- **NtpServerUnalcanzable**

  El clúster de almacenamiento no puede comunicarse con los servidores NTP especificados.

  Para resolver esta falla, compruebe la configuración del servidor NTP, de la red y del firewall.

- **NtpTimeNotInSync**

  La diferencia entre el tiempo del clúster de almacenamiento y el tiempo del servidor NTP es demasiado amplia. El clúster de almacenamiento no puede corregir esta diferencia automáticamente.

  Para resolver esta falla, use los servidores NTP internos a la red en lugar de los que vienen predeterminados en la instalación. Si usa los servidores NTP internos y el problema persiste, comuníquese con el soporte de NetApp para obtener ayuda.

- **NvramDeviceStatus**

  Un dispositivo NVRAM presenta un error, está fallando o ya falló. Este fallo tiene las siguientes gravedades:

Gravedad	Descripción
Advertencia	El hardware ha detectado una advertencia. Esta condición puede ser transitoria, como una advertencia de temperatura. • NvmLifetimeerror • NvmLifetimeStatus • EnergySourceLifetimeStatus • EnergySourceTemperatureStatus • WarningThresholdExceeded
Error	El hardware ha detectado un error o estado crítico. El maestro de clústeres intenta quitar la unidad de segmentos de la operación (esto genera un evento de eliminación de la unidad). Si no hay servicios de segmentos secundarios disponibles, no se eliminará la unidad. Errores devueltos además de los errores de nivel de advertencia: • El punto de montaje del dispositivo NVRAM no existe. • La partición del dispositivo NVRAM no existe. • Existe una partición del dispositivo NVRAM, pero no está montada.

Crítico	El hardware ha detectado un error o estado crítico. El maestro de clústeres intenta quitar la unidad de segmentos de la operación (esto genera un evento de eliminación de la unidad). Si no hay servicios de segmentos secundarios disponibles, no se eliminará la unidad. • Persistente perdido • ArmStatusSaveNArmed • CsaveStatuserror

Sustituya cualquier hardware con fallos en el nodo. Si esto no se resuelve el problema, comuníquese con el soporte de NetApp para obtener ayuda.

- **PowerSupplyError**

  Esta falla del clúster indica una de las siguientes condiciones:

  - No hay un suministro de alimentación.
  - Se produjo un error de suministro de alimentación.
  - La entrada de un suministro de alimentación es nula o está fuera de rango. Para resolver esta falla, compruebe que se suministra alimentación redundante a todos los nodos. Comuníquese con el soporte de NetApp para obtener ayuda.

- **AprovisionadoSpaceTooFull**

  La capacidad general aprovisionada del clúster está demasiado llena.

  Para resolver esta falla, añada más espacio aprovisionado, o elimine y purgue los volúmenes.

- **RemoteRepAsyncDelayExceeded**

  Se superó la demora de replicación asíncrona configurada. Compruebe la conectividad de red entre clústeres.

- **RemoteRepClusterFull**

  Los volúmenes pusieron en pausa la replicación remota porque el clúster de almacenamiento de destino está demasiado lleno.

  Para resolver esta falla, libere un poco de espacio en el clúster de almacenamiento de destino.

- **RemoteRepSnapshotClusterFull**

  Los volúmenes pusieron en pausa la replicación remota de copias de Snapshot porque el clúster de almacenamiento de destino está demasiado lleno.

  Para resolver esta falla, libere un poco de espacio en el clúster de almacenamiento de destino.

- **RemoteRepSnapshotsExceedLimit**

  Los volúmenes pusieron en pausa la replicación remota de copias de Snapshot porque el volumen del clúster de almacenamiento de destino superó su límite de copias de Snapshot.

Para resolver esta falla, aumente el límite de snapshots en el clúster de almacenamiento de destino.

- * Error de Acción de Ugenera*

  Ocurrió un error en la ejecución de una o más actividades programadas.

  La falla se borra si la actividad programada se vuelve a ejecutar, esta vez, correctamente, si la actividad programada se elimina o si la actividad se pone en pausa y luego se reanuda.

- **SensorReadingFailed**

  La autoprueba de la controladora de gestión de placa base (BMC) produjo un error o un sensor no pudo comunicarse con la BMC.

  Comuníquese con el soporte de NetApp para obtener ayuda.

- **ServiceNotRunning**

  Un servicio requerido no está en ejecución.

  Comuníquese con el soporte de NetApp para obtener ayuda.

- **SliceServiceTooFull**

  Un servicio de segmentos tiene asignada muy poca capacidad aprovisionada.

  Para resolver esta falla, añada más capacidad aprovisionada.

- **SliceServiceUnhealthy**

  El sistema detectó que un servicio de segmentos está en estado incorrecto y lo decomisiona automáticamente.

  - Gravedad = Advertencia: No se realiza ninguna acción. Este período de aviso caducará en 6 minutos.
  - Gravedad = error: El sistema decomisiona automáticamente los datos y vuelve a replicar los datos en otras unidades en buen estado. Compruebe si existen problemas de conectividad de red y errores de hardware. Si se han producido errores en componentes de hardware específicos, habrá otros errores. El fallo se borrará cuando se pueda acceder al servicio de cortes o cuando se haya retirado el servicio.

- **SshEnabled**

  El servicio SSH está habilitado en uno o más nodos del clúster de almacenamiento.

  Para resolver esta falla, deshabilite el servicio SSH en los nodos correspondientes o comuníquese con el soporte de NetApp para obtener ayuda.

- **SslCertificateExpiración**

  El certificado SSL asociado con este nodo está cerca de su vencimiento o ha caducado. Este fallo utiliza las siguientes gravedades en función de la urgencia:

Gravedad	Descripción
Advertencia	El certificado caduca dentro de los 30 días.

Error	El certificado caduca dentro de los 7 días.
Crítico	El certificado caduca en un plazo de 3 días o ya ha caducado.

Para resolver esta falla, reemplace el certificado SSL por uno nuevo. Si es necesario, comuníquese con el soporte de NetApp para obtener ayuda.

- **StrandedCapacity**

  Un solo nodo representa más de la mitad de la capacidad de un clúster de almacenamiento.

  Para mantener la redundancia de datos, el sistema reduce la capacidad del nodo más grande de manera que parte de su capacidad de bloque se quede sin utilizar (no se utiliza).

  Para resolver esta falla, añada más unidades a los nodos de almacenamiento existentes o añada nodos de almacenamiento al clúster.

- **Sensor de temperatura**

  Un sensor de temperatura informa de temperaturas más altas que las normales. Esta falla puede activarse en conjunto con fallas de tipo powerSupplyError o fanSensor.

  Para resolver esta falla, compruebe que el flujo de aire no esté obstruido cerca del clúster de almacenamiento. Si es necesario, comuníquese con el soporte de NetApp para obtener ayuda.

- **actualización**

  Hay una actualización en curso desde hace más de 24 horas.

  Para resolver esta falla, reanude la actualización o comuníquese con el soporte de NetApp para obtener ayuda.

- **UnresponveService**

  Un servicio ha dejado de responder.

  Comuníquese con el soporte de NetApp para obtener ayuda.

- **VirtualNetworkConfig**

  Esta falla del clúster indica una de las siguientes condiciones:

  - No hay una interfaz presente.
  - La interfaz tiene un espacio de nombres incorrecto.
  - Hay una máscara de red incorrecta.
  - Hay una dirección IP incorrecta.
  - Una interfaz no está en funcionamiento.
  - Hay una interfaz superflua en un nodo. Comuníquese con el soporte de NetApp para obtener ayuda.

- **VolumesDegraded**

Los volúmenes secundarios aún se están replicando y sincronizando. El mensaje se borra al finalizar la sincronización.

- **VolumesOffline**

  Uno o más volúmenes del clúster de almacenamiento están fuera de línea. El fallo **volumeDegraded** también estará presente.

  Comuníquese con el soporte de NetApp para obtener ayuda.

Ver la actividad de rendimiento del nodo

La actividad de rendimiento de cada nodo se puede ver en formato de gráfico. Esta información proporciona estadísticas en tiempo real para las operaciones de I/o de lectura/escritura por segundo (IOPS) de CPU y en cada unidad del nodo. El gráfico de uso se actualiza cada cinco segundos y el gráfico de estadísticas de unidad se actualiza cada diez segundos.

1. Haga clic en **Cluster** > **Nodes**.
2. Haga clic en **acciones** para el nodo que desea ver.
3. Haga clic en **Ver detalles**.

Puede ver momentos específicos en los gráficos de líneas y barras colocando el cursor sobre la línea o la barra.

Ver el rendimiento del volumen

Puede ver información detallada del rendimiento de todos los volúmenes del clúster. Esta información se puede ordenar por ID de volumen o por cualquier otra de las columnas de rendimiento. También puede usar filtros de la información según determinados criterios.

Puede cambiar la frecuencia con la que el sistema actualiza la información de rendimiento en la página haciendo clic en la lista **Actualizar cada** y eligiendo un valor diferente. El intervalo de actualización predeterminado es de 10 segundos si el clúster tiene menos de 1000 volúmenes; de lo contrario, el valor predeterminado es de 60 segundos. Si elige Never, se deshabilita la actualización automática de página.

Puede volver a activar la actualización automática haciendo clic en **Activar la actualización automática**.

1. En la interfaz de usuario de Element, seleccione **Reporting** > **Volume Performance**.
2. En la lista de volúmenes, haga clic en el icono Actions de un volumen.
3. Haga clic en **Ver detalles**.

   Aparecerá una bandeja en la parte inferior de la página con información general sobre el volumen.

4. Para ver información más detallada sobre el volumen, haga clic en **Ver más detalles**.

   El sistema muestra información detallada y gráficos de rendimiento del volumen.

Obtenga más información

Detalles de rendimiento de volumen

Detalles de rendimiento de volumen

Las estadísticas de rendimiento de los volúmenes se pueden ver en la página Volume Performance de la pestaña Reporting en la interfaz de usuario de Element.

La lista siguiente describe los detalles que tienen a su disposición:

- **ID**

  El ID que genera el sistema para el volumen.

- **Nombre**

  El nombre que se le dio al volumen cuando se creó.

- **Cuenta**

  El nombre de la cuenta asignada al volumen.

- **Grupos de acceso**

  El nombre del grupo o los grupos de acceso de volúmenes a los que pertenece el volumen.

- **Utilización de volumen**

  Un valor de porcentaje que describe la cantidad del volumen que está usando el cliente.

  Los posibles valores son los siguientes:

  - 0 = el cliente no usa el volumen
  - 100 = el cliente usa el máximo
  - >100 = el cliente está utilizando la ráfaga

- **IOPS total**

  El número total de IOPS (lectura y escritura) que se está ejecutando en el volumen.

- **Leer IOPS**

  El número total de IOPS de lectura que se está ejecutando en el volumen.

- **Escribir IOPS**

  El número total de IOPS de escritura que se está ejecutando en el volumen.

- **Rendimiento total**

  La cantidad total de rendimiento (lectura y escritura) que se está ejecutando en el volumen.

- **Rendimiento de lectura**

La cantidad total de rendimiento de lectura que se está ejecutando en el volumen.

- **Grabación**

  La cantidad total de rendimiento de escritura que se está ejecutando en el volumen.

- **Latencia total**

  El tiempo medio, en microsegundos, para completar operaciones de lectura y escritura en un volumen.

- **Latencia de lectura**

  El tiempo medio, en microsegundos, para completar operaciones de lectura del volumen en los últimos 500 milisegundos.

- **Latencia de escritura**

  El tiempo medio, en microsegundos, para completar operaciones de escritura a un volumen en los últimos 500 milisegundos.

- **Profundidad de cola**

  Número de operaciones de lectura y escritura pendientes en el volumen.

- **Tamaño medio de E/S**

  Tamaño promedio en bytes de I/o reciente en el volumen en los últimos 500 milisegundos.

Ver sesiones iSCSI

Es posible ver las sesiones iSCSI que están conectadas al clúster. Puede filtrar la información para que incluya solo las sesiones que desea.

1. En la interfaz de usuario de Element, seleccione **Reporting** > **iSCSI Sessions**.
2. Para ver los campos de criterios de filtro, haga clic en **filtro**.

Obtenga más información

Detalles de la sesión iSCSI

Detalles de la sesión iSCSI

Es posible ver información sobre las sesiones iSCSI que están conectadas al clúster.

En la lista siguiente se describe la información que se puede encontrar acerca de las sesiones iSCSI:

- **Nodo**

  El nodo que aloja la partición de metadatos principal del volumen.

- **Cuenta**

  El nombre de la cuenta a la que pertenece el volumen. Si el valor está vacío, se muestra un guion (-).

- **Volumen**

  El nombre del volumen identificado en el nodo.

- **ID de volumen**

  El ID del volumen asociado con el IQN de destino.

- **ID de iniciador**

  Un ID que genera el sistema para el iniciador.

- **Alias del iniciador**

  Un nombre opcional para el iniciador que facilite encontrar el iniciador cuando la lista es larga.

- **IP de Initator**

  La dirección IP del extremo que inicia la sesión.

- **IQN del iniciador**

  El IQN del extremo que inicia la sesión.

- **IP de destino**

  La dirección IP del nodo donde se aloja el volumen.

- **IQN objetivo**

  El IQN del volumen.

- **Creado el**

  La fecha en la que se estableció la sesión.

Consulte las sesiones Fibre Channel

Es posible ver las sesiones Fibre Channel (FC) que están conectadas al clúster. Puede filtrar la información para que incluya únicamente las conexiones que desea que aparezcan en la ventana.

1. En la interfaz de usuario de Element, seleccione **Reporting** > **FC Sessions**.
2. Para ver los campos de criterios de filtro, haga clic en **filtro**.

Obtenga más información

Detalles de la sesión Fibre Channel

Detalles de la sesión Fibre Channel

Se proporciona información sobre las sesiones activas de Fibre Channel (FC) que están conectadas al clúster.

En la lista siguiente se describe la información que puede encontrar acerca de las sesiones FC conectadas al clúster:

- **ID de nodo**

  El nodo que aloja la sesión de la conexión.

- **Nombre de nodo**

  El nombre del nodo que genera el sistema.

- **ID de iniciador**

  Un ID que genera el sistema para el iniciador.

- **WWPN del iniciador**

  El nombre de puerto que se inicia a nivel mundial.

- **Alias del iniciador**

  Un nombre opcional para el iniciador que facilite encontrar el iniciador cuando la lista es larga.

- **WWPN de destino**

  El nombre de puerto objetivo a nivel mundial.

- **Grupo de acceso por volumen**

  El nombre del grupo de acceso de volúmenes al que pertenece la sesión.

- **ID de grupo de acceso de volumen**

  El ID que genera el sistema para el grupo de acceso.

Solucione problemas de unidades

Una unidad de estado sólido (SSD) con fallos se puede sustituir con una unidad de reemplazo. Las unidades SSD de los nodos de almacenamiento SolidFire se pueden intercambiar en caliente. Si sospecha que una unidad SSD puede tener errores, póngase en contacto con el soporte de NetApp para verificar el error y le guiaremos por el procedimiento de resolución de problemas adecuado. El soporte de NetApp también trabaja con usted para obtener una unidad de reemplazo de acuerdo con su acuerdo de nivel de servicio.

Cómo se puede cambiar en este caso esto significa que es posible quitar una unidad con error de un nodo activo y reemplazarla por una nueva unidad SSD de NetApp. No se recomienda quitar unidades sin errores en un clúster activo.

Debe mantener las piezas de repuesto que sugiere el soporte de NetApp para poder sustituir inmediatamente la unidad si falla.

Para realizar pruebas, si simula un error en una unidad al extraer una unidad de un nodo, debe esperar 30 segundos para poder insertar la unidad de nuevo en la ranura.

Si una unidad falla, Double Helix redistribuye los datos de la unidad por los nodos que permanecen en el clúster. Varios fallos de unidad en el mismo nodo no suponen un problema, ya que el software Element protege frente a dos copias de datos que residen en el mismo nodo. Una unidad con errores produce los siguientes eventos:

- Los datos se migran fuera de la unidad.
- La capacidad general del clúster se reduce según la capacidad de la unidad.
- La protección de datos Double Helix garantiza que haya dos copias válidas de los datos.

Los sistemas de almacenamiento de SolidFire no permiten que se elimine una unidad si esto provoca que haya una cantidad insuficiente de almacenamiento para migrar los datos.

Si quiere más información

- Quite las unidades con errores del clúster
- Solución de problemas básica de unidades MDSS
- Quite las unidades MDSS
- "Reemplazar unidades para nodos de almacenamiento SolidFire"
- "Reemplazar unidades para nodos de almacenamiento serie H600S"
- "Información de hardware H410S y H610S"
- "Información sobre hardware de SF-Series"

Quite las unidades con errores del clúster

El sistema SolidFire pone una unidad en estado de error cuando el sistema de autodiagnóstico de la unidad indica al nodo que se ha producido un error o cuando la comunicación con la unidad se detiene durante cinco minutos y medio o más. El sistema muestra una lista de las unidades con errores. Debe quitar una unidad con error de la lista de unidades con errores en el software NetApp Element.

Las unidades de la lista **Alertas** aparecen como **blockServiceUnhealthy** cuando un nodo está desconectado. Cuando se reinicia el nodo, si el nodo y sus unidades vuelven a estar en línea en un plazo de cinco minutos y medio, las unidades se actualizan automáticamente y siguen mostrándose como unidades activas en el clúster.

1. En la interfaz de usuario de Element, seleccione **Cluster** > **Drives**.
2. Haga clic en **error** para ver la lista de unidades con errores.
3. Anote el número de ranura de la unidad con error.

   Esta información se necesita para localizar la unidad con error en el chasis.

4. Quite las unidades con errores mediante uno de los siguientes métodos:

Opción	Pasos

Para quitar unidades individuales	a. Haga clic en **acciones** para la unidad que desea quitar. b. Haga clic en **Quitar**.
Para quitar varias unidades	a. Seleccione todas las unidades que desee quitar y haga clic en **acciones masivas**. b. Haga clic en **Quitar**.

Solución de problemas básica de unidades MDSS

Puede recuperar las unidades de metadatos (o de segmentos) si se vuelven a añadir al clúster en el caso de que se produzca un error en una o en ambas unidades de metadatos. Puede llevar a cabo la operación de recuperación en la interfaz de usuario de NetApp Element si la función MDSS ya está habilitada en el nodo.

Si se produce un error en una de las unidades de metadatos de un nodo o en las dos, el servicio de segmentos se cerrará y se realizarán backups de los datos de ambas unidades en distintas unidades del nodo.

En los siguientes escenarios se describen posibles escenarios de fallos y se ofrecen recomendaciones básicas para corregir el problema:

Error en la unidad de segmentos del sistema

- En este caso, la ranura 2 se verifica y vuelve a un estado available.
- La unidad de segmentos del sistema se debe volver a rellenar antes de que el servicio de segmentos vuelva a conectarse.
- Debe sustituir la unidad de segmentos del sistema cuando esta esté disponible, añada la unidad y la unidad de la ranura 2 a la vez.

> No es posible añadir la unidad de la ranura 2 por sí misma como una unidad de metadatos. Debe volver a añadir al nodo ambas unidades a la vez.

Error en la ranura 2

- En este escenario, la unidad de segmentos del sistema se verifica y vuelve a un estado available.
- Debe reemplazar la ranura 2 con una unidad de repuesto y, cuando la ranura 2 esté disponible, añada la unidad de segmentos del sistema y la unidad de la ranura 2 al mismo tiempo.

Se produce un error en la unidad de segmentos del sistema y en la ranura 2

- Debe reemplazar la unidad de segmentos del sistema y la ranura 2 con una unidad de repuesto. Cuando las dos unidades estén disponibles, añada la unidad de segmentos del sistema y la unidad de la ranura 2 al mismo tiempo.

Orden de las operaciones

- Reemplace la unidad de hardware en la que se haya producido el error con una unidad de repuesto (reemplace ambas unidades en caso de que las dos tengan errores).

- Vuelva a añadir las unidades al clúster cuando se hayan rellenado de nuevo y estén en el estado available.

Verificar operaciones

- Verifique que las unidades de la ranura 0 (o internas) y la ranura 2 se hayan identificado como unidades de metadatos en la lista de unidades activas.
- Compruebe que el equilibrado de todos los segmentos se ha completado (no hay más mensajes del tipo moving slices en el registro de eventos durante al menos 30 minutos).

Si quiere más información

Añada unidades MDSS

Añada unidades MDSS

Es posible añadir una segunda unidad de metadatos en un nodo de SolidFire de si se convierte la unidad de bloques de la ranura 2 en una unidad de segmentos. Para ello, debe habilitar la función del servicio de segmentos de varias unidades (MDSS). Para habilitar esta función, debe ponerse en contacto con el soporte de NetApp.

Para que una unidad de segmentos tenga el estado available, puede que deba reemplazar una unidad con errores por una unidad nueva o de repuesto. Debe añadir la unidad de segmentos del sistema al mismo tiempo que añade la unidad para la ranura 2. Si intenta añadir solo la unidad de segmentos de la ranura 2 o añadirla antes de la unidad de segmentos del sistema, el sistema mostrará un error.

1. Haga clic en **Cluster** > **Drives**.
2. Haga clic en **disponible** para ver la lista de unidades disponibles.
3. Seleccione las unidades de segmentos que desea añadir.
4. Haga clic en **acciones masivas**.
5. Haga clic en **Agregar**.
6. Confirme en la ficha **Active Drives** que las unidades se han añadido.

Quite las unidades MDSS

Es posible quitar las unidades del servicio de segmentos de varias unidades (MDSS). Este procedimiento solo se aplica si el nodo tiene varias unidades de segmentos.

> Si se produce un error en la unidad de segmentos del sistema y en la unidad de ranura 2, el sistema cerrará los servicios de segmentos y quitará las unidades. Si no se produce ningún error y quita las unidades, tendrá que quitar ambas unidades a la vez.

1. Haga clic en **Cluster** > **Drives**.
2. En la ficha unidades **disponibles** , haga clic en la casilla de verificación correspondiente a las unidades de segmentos que se van a eliminar.
3. Haga clic en **acciones masivas**.
4. Haga clic en **Quitar**.
5. Confirme la acción.

Solucione los problemas de los nodos

Los nodos se pueden quitar de un clúster cuando requieren mantenimiento o se deben sustituir. Debe usar la API o la interfaz de usuario de NetApp Element para quitar los nodos antes de desconectarlos.

A continuación, se ofrece una descripción general del procedimiento para quitar nodos de almacenamiento:

- Compruebe que haya suficiente capacidad en el clúster para crear una copia de los datos en el nodo.
- Quite las unidades del clúster mediante la interfaz de usuario o el método API RemoveDrives.

  Esto provoca que el sistema migre los datos desde las unidades del nodo a otras unidades en el clúster. El tiempo que se tarda en realizar este proceso depende de la cantidad de datos que haya que migrar.

- Quite el nodo del clúster.

Tenga en cuenta las siguientes consideraciones antes de apagar o encender un nodo:

- La desconexión de nodos y clústeres implica riesgos si no se realiza correctamente.

  La desconexión de un nodo se debe hacer bajo la supervisión del soporte de NetApp.

- Si un nodo ha estado desconectado más de 5.5 minutos en alguna condición de apagado, la protección de datos de Double Helix comienza la tarea de escritura de bloques replicados sencillos en otro nodo para replicar los datos. En este caso, póngase en contacto con el soporte de NetApp para obtener ayuda con el análisis del nodo con errores.
- Para reiniciar o desconectar correctamente un nodo, puede usar el comando de API Shutdown.
- Si un nodo está sin actividad o desconectado, debe ponerse en contacto con el soporte de NetApp antes de volver a conectarlo.
- Una vez que el nodo se ha conectado de nuevo, debe volver a añadir las unidades al clúster, en función de la cantidad de tiempo que ha estado fuera de servicio.

Si quiere más información

"Reemplazar un chasis SolidFire con fallos"

"Reemplazar un nodo serie H600S con fallos"

Apague un clúster

Realice el siguiente procedimiento para desconectar un clúster completo.

Pasos

1. (Opcional) comuníquese con el soporte de NetApp para obtener ayuda en la realización de los pasos preliminares.
2. Verifique que todas las operaciones de I/o se hayan detenido.
3. Desconecte todas las sesiones de iSCSI:
   a. Acceda a la dirección IP virtual de gestión (MVIP) en el clúster para abrir la interfaz de usuario de Element.
   b. Revise los nodos que aparecen en la lista Nodes.

c. Ejecute el método API Shutdown especificando la opción halt en cada ID de nodo del clúster.

Cuando reinicia el clúster, debe seguir algunos pasos para verificar que todos los nodos entran en línea:

1. Compruebe que todas las gravedad crítica y. `volumesOffline` se resolvieron errores del clúster.
2. Espere de 10 a 15 minutos para que el clúster se asiente.
3. Empiece a poner los hosts a acceder a los datos.

Si desea permitir más tiempo al encender los nodos y verificar que su estado sea después del mantenimiento, póngase en contacto con el soporte técnico para obtener ayuda con la demora de la sincronización de datos para evitar la sincronización innecesaria de bandejas.

Obtenga más información

"Cómo apagar y encender correctamente un clúster de almacenamiento SolidFire/HCI de NetApp"

Trabaje con utilidades por nodo para los nodos de almacenamiento

Puede usar las utilidades por nodo para solucionar problemas de red si las herramientas de supervisión estándar de la interfaz de usuario del software NetApp Element no proporcionan suficiente información para la solución de problemas. Las utilidades por nodo proporcionan información y herramientas específicas que pueden ayudarle a solucionar problemas de red entre los nodos o con el nodo de gestión.

Obtenga más información

- Acceda a la configuración por nodo con la interfaz de usuario por nodo
- Los detalles de la configuración de red de la interfaz de usuario por nodo
- Detalles de la configuración de clúster de la interfaz de usuario por nodo
- Ejecute las pruebas del sistema usando la interfaz de usuario por nodo
- Ejecute las utilidades del sistema con la interfaz de usuario por nodo

Acceda a la configuración por nodo con la interfaz de usuario por nodo

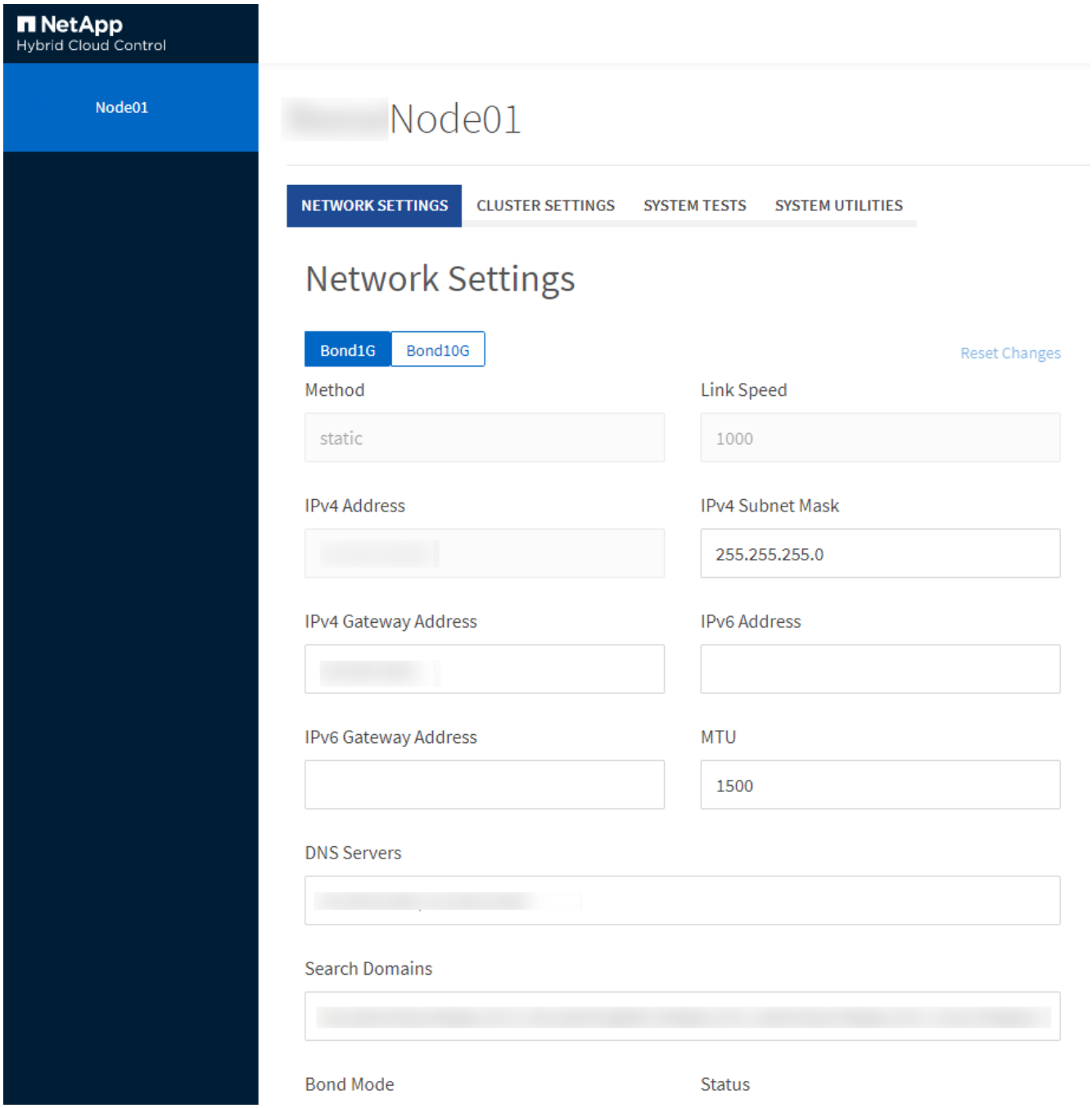
Tras introducir la IP y la autenticación del nodo de gestión, puede acceder a los ajustes de red, los ajustes del clúster y las pruebas y las utilidades del sistema en la interfaz de usuario por nodo de gestión.

Si desea modificar la configuración de un nodo en un estado Active que forme parte de un clúster, debe iniciar sesión como usuario de administrador de clúster.

Debe configurar o modificar un nodo por vez. Debe asegurarse de que la configuración de red especificada tenga el efecto deseado y que la red sea estable y se ejecute correctamente antes de hacer modificaciones en otro nodo.

1. Abra la interfaz de usuario por nodo mediante uno de los siguientes métodos:

- Introduzca la dirección IP de administración seguida de :442 en una ventana del navegador e inicie sesión con un nombre de usuario y una contraseña de administrador.
- En la interfaz de usuario de Element, seleccione **Cluster** > **Nodes** y haga clic en el enlace de la dirección IP de administración correspondiente al nodo que desea configurar o modificar. En la ventana del navegador que se abre, puede editar la configuración del nodo.



Los detalles de la configuración de red de la interfaz de usuario por nodo

Es posible cambiar la configuración de red del nodo de almacenamiento para dar al nodo un nuevo conjunto de atributos de red.

Puede ver la configuración de red para un nodo de almacenamiento en la página **Configuración de red** cuando inicia sesión en el nodo (https://<node IP>:442/hcc/node/network-settings). Puede seleccionar las opciones **Bond1G** (administración) o **Bond10G** (almacenamiento). En la lista siguiente se describe la

configuración que se puede modificar cuando el estado de un nodo de almacenamiento es Available, Pending o Active:

- **Método**

  El método que se utiliza para configurar la interfaz. Métodos posibles:

  - Loopback: Se utiliza para definir la interfaz de bucle invertido de IPv4.
  - Manual: Se utiliza para definir interfaces para las que no se realiza ninguna configuración de forma predeterminada.
  - dhcp: Se utiliza para obtener una dirección IP a través de DHCP.
  - Static: Se utiliza para definir interfaces Ethernet con direcciones IPv4 asignadas de forma estática.

- **Velocidad de enlace**

  La velocidad negociada por la NIC virtual.

- **Dirección IPv4**

  La dirección IPv4 de la red eth0.

- **Máscara de subred IPv4**

  Las subdivisiones de dirección de la red IPv4.

- **Dirección de puerta de enlace IPv4**

  La dirección de red del enrutador para enviar paquetes fuera de la red local.

- **Dirección IPv6**

  La dirección IPv6 de la red eth0.

- **Dirección de puerta de enlace IPv6**

  La dirección de red del enrutador para enviar paquetes fuera de la red local.

- **MTU**

  Tamaño de paquete más grande que un protocolo de red puede transmitir. Debe ser mayor o igual que 1500. Si se añade un segundo NIC de almacenamiento, el valor debería ser 9000.

- **Servidores DNS**

  La interfaz de red que se utiliza para la comunicación del clúster.

- **Buscar dominios**

  La búsqueda de direcciones MAC adicionales que hay disponibles en el sistema.

- **Modo Bond**

  Puede ser uno de los siguientes modos:

  - ActivePassive (predeterminado)

- ALB
- LACP

- **Estado**

  Los posibles valores son los siguientes:

  - UpAndRunning
  - Abajo
  - Arriba

- **Etiqueta de red virtual**

  La etiqueta asignada cuando se creó la red virtual.

- **Rutas**

  Las rutas estáticas para especificar hosts o redes a través de la interfaz asociada que se ha configurado para que usen las rutas.

Detalles de la configuración de clúster de la interfaz de usuario por nodo

Puede verificar la configuración del clúster para un nodo de almacenamiento después de la configuración del clúster y modificar el nombre de host del nodo.

En la siguiente lista se describe la configuración del clúster para un nodo de almacenamiento que se indica en la página **Configuración de clúster** de la interfaz de usuario por nodo (https://<node IP>:442/hcc/node/cluster-settings).

- **Rol**

  El rol que tiene el nodo en el clúster. Los posibles valores son los siguientes:

  - Storage: Nodo de almacenamiento o Fibre Channel.
  - Management: Se trata de un nodo de gestión.

- **Nombre de host**

  El nombre del nodo.

- **Cluster**

  El nombre del clúster.

- **Composición de grupo**

  El estado del nodo. Los posibles valores son los siguientes:

  - Available: El nodo no tienen ningún nombre de clúster asociado y aún no forma parte de un clúster.
  - Pending: Se ha configurado el nodo y se puede añadir a un clúster designado. No es necesario autenticarse para acceder al nodo.
  - PendingActive: El sistema está instalando el software compatible en el nodo. Cuando finalice, el nodo se moverá al estado Active.

- Active: El nodo participa en un clúster. Es necesario autenticarse para modificar el nodo.

- **Versión**

  La versión del software Element que se ejecuta en el nodo.

- **Ensemble**

  Los nodos que forman parte del conjunto de base de datos.

- **ID de nodo**

  El ID asignado cuando se añade un nodo al clúster.

- **Interfaz de clúster**

  La interfaz de red que se utiliza para la comunicación del clúster.

- **Interfaz de administración**

  La interfaz de red de gestión. De forma predeterminada es Bond1G, pero también puede usar Bond10G.

- **Interfaz de almacenamiento**

  La interfaz de red de almacenamiento que usa Bond10G.

- **Capacidad de cifrado**

  Indica si el nodo admite el cifrado de unidad o no.

Ejecute las pruebas del sistema usando la interfaz de usuario por nodo

Es posible probar los cambios en los ajustes de red después de confirmar los cambios en la configuración de red. Es posible ejecutar las pruebas para garantizar que el nodo de almacenamiento sea estable y que se pueda conectar sin ningún problema.

Inició sesión en la interfaz de usuario por nodo del nodo de almacenamiento.

1. Haga clic en **pruebas del sistema**.
2. Haga clic en **Ejecutar prueba** junto a la prueba que desea ejecutar o seleccione **Ejecutar todas las pruebas**.

   La ejecución de todas las operaciones de prueba puede llevar bastante tiempo y solo se debe realizar según lo indique el soporte de NetApp.

   - **Comprobar Ensemble** conectado

     Prueba y verifica la conectividad con un conjunto de bases de datos. De forma predeterminada, la prueba utiliza el conjunto para el clúster con el que está asociado el nodo. Como alternativa, puede proporcionar un conjunto diferente para probar la conectividad.

   - **Test Connect Mvip**

     Hace ping en la dirección IP virtual de gestión especificada (MVIP) y, a continuación, ejecuta una

llamada API sencilla a la MVIP para verificar la conectividad. De manera predeterminada, la prueba utiliza la MVIP para el clúster con el que está asociado el nodo.

- **Test Connect SVIP**

  Hace ping en la dirección IP virtual de almacenamiento especificada (SVIP) mediante los paquetes del protocolo de mensajes de control de Internet (ICMP) que coinciden con el tamaño de unidad de transmisión máxima (MTU) establecido en el adaptador de red. Se conecta entonces con la SVIP como un iniciador iSCSI. De forma predeterminada, la prueba utiliza la SVIP para el clúster con el que está asociado el nodo.

- **Configuración del hardware de prueba**

  Prueba que todas las configuraciones de hardware sean correctas, valida que las versiones de firmware sean correctas y confirma que todas las unidades estén instaladas y se ejecuten correctamente. Es lo mismo que las pruebas de fábrica.

  Esta prueba consume muchos recursos y solo se debe ejecutar si lo solicita el soporte de NetApp.

- **Probar conectividad local**

  Prueba la conectividad con todos los otros nodos del clúster haciendo ping en la IP de clúster (CIP) en cada nodo. Esta prueba solo se mostrará en un nodo si el nodo forma parte de un clúster activo.

- **Probar grupo de localización**

  Valida que el nodo pueda localizar el clúster especificado en la configuración del clúster.

- **Probar configuración de red**

  Verifica que la configuración de red que se ha establecido coincide con la configuración de red que se está usando en el sistema. Esta prueba no se realiza con la intención de detectar errores en el hardware cuando un nodo participa de forma activa en un clúster.

- **Probar ping**

  Hace ping en una lista de hosts determinada o, si no se especifica ninguna, crea de forma dinámica una lista de todos los nodos registrados en el clúster y hace ping en cada uno de ellos para establecer una conectividad sencilla.

- **Probar la conectividad remota**

  Prueba la conectividad con todos los nodos de clústeres emparejados de forma remota haciendo ping en la IP de clúster (CIP) en cada nodo. Esta prueba solo se mostrará en un nodo si el nodo forma parte de un clúster activo.

Ejecute las utilidades del sistema con la interfaz de usuario por nodo

Se puede usar la interfaz de usuario por nodo para el nodo de almacenamiento a fin de crear o eliminar paquetes de soporte, restablecer la configuración de las unidades y reiniciar los servicios de red o de clúster.

Inició sesión en la interfaz de usuario por nodo del nodo de almacenamiento.

1. Haga clic en **Utilidades del sistema**.
2. Haga clic en el botón de la utilidad del sistema que desea ejecutar.
   - **Alimentación de control**

     Reinicia, apaga o enciende el nodo.

     > Esta operación provoca la pérdida temporal de conectividad de red.

     Especifique los siguientes parámetros:

     - Acción: Las opciones incluyen reinicio y parada (apagado).
     - Retraso en el reactivación: En cualquier momento adicional antes de que el nodo vuelva a estar online.
   - **Recopilar registros de nodos**

     Crea un paquete de soporte en el directorio /tmp/bundles del nodo.

     Especifique los siguientes parámetros:

     - Bundle Name: Nombre único para cada paquete de soporte creado. Si no se proporciona ningún nombre, "supportBundle" y el nombre de nodo se utilizan como nombre de archivo.
     - Extra args: Este parámetro se alimenta con el script sf_make_support_bundle. Este parámetro solo se debe usar si lo solicita el soporte de NetApp.
     - Timeout Sec: Especifique el número de segundos que se deben esperar para cada respuesta ping individual.
   - **Borrar registros de nodos**

     Elimina todos los paquetes de soporte actuales del nodo que se crearon con **Crear paquete de soporte de clúster** o el método API CreateSupportBundle.
   - **Restablecer las unidades**

     Inicializa las unidades y quita todos los datos que residen en ese momento en la unidad. Es posible reutilizar la unidad en un nodo existente o en un nodo actualizado.

     Especifique el siguiente parámetro:

     - Unidades: Lista de nombres de dispositivos (no driveID) que se van a restablecer.
   - **Restablecer configuración de red**

     Ayuda a resolver problemas de configuración de red para un nodo individual y restablece la configuración de red de un nodo individual a la configuración predeterminada de fábrica.
   - **Restablecer nodo**

     Restablece un nodo a la configuración de fábrica. Todos los datos se quitan, pero la configuración de red del nodo se conserva durante esta operación. Los nodos solo se pueden restablecer si no se han asignado a un clúster y en estado disponible.

Cuando utiliza esta opción, se eliminan del nodo todos los datos, paquetes (actualizaciones de software), configuraciones y archivos de registro.

- **Reinicie Networking**

  Reinicia todos los servicios de red de un nodo.

  Esta operación puede provocar la pérdida temporal de conectividad de red.

- **Reinicie Servicios**

  Reinicia los servicios del software Element en un nodo.

  Esta operación puede provocar una interrupción temporal del servicio de los nodos. Debe realizar esta operación solo cuando lo indique el soporte de NetApp.

  Especifique los siguientes parámetros:

  - Servicio: Nombre del servicio que se va a reiniciar.
  - Acción: Acción a realizar en el servicio. Las opciones incluyen inicio, parada y reinicio.

Trabaje con el nodo de gestión

Es posible usar el nodo de gestión (mNode) para actualizar los servicios del sistema, gestionar los activos y la configuración del clúster, ejecutar pruebas y utilidades del sistema, configurar Active IQ para la supervisión del sistema y habilitar el acceso al soporte de NetApp para la solución de problemas.

Como práctica recomendada, solo asocie un nodo de gestión a una instancia de VMware vCenter y evite definir los mismos recursos de almacenamiento y computación o instancias de vCenter en varios nodos de gestión.

Consulte "documentación del nodo de gestión" si quiere más información.

Comprender los niveles de llenado de clústeres

El clúster que ejecuta el software Element genera errores de clúster para advertir al administrador de almacenamiento cuándo se está quedando sin capacidad el clúster. Hay tres niveles de ocupación del clúster, cada uno de los cuales se muestra en la interfaz de usuario de NetApp Element: Warning, error y Critical.

El sistema usa el código de error BlockClusterFull para informar sobre el nivel de ocupación del almacenamiento en bloque de clúster. Puede ver los niveles de gravedad de ocupación del clúster en la pestaña Alerts de la interfaz de usuario de Element.

La siguiente lista incluye información sobre los niveles de gravedad de BlockClusterFull:

- **Advertencia**

  Se trata de una advertencia que puede configurar el cliente y que aparece cuando la capacidad de

bloques del clúster se acerca al nivel de gravedad de error. De forma predeterminada, este nivel se establece en el tres % por debajo del nivel de error y se puede ajustar a través de la interfaz de usuario y la API de Element. Debe añadir más capacidad o liberar capacidad Lo antes posible..

- **Error**

  Cuando el clúster presenta este estado, si se pierde un nodo, no habrá suficiente capacidad en el clúster para reconstruir la protección de datos de Double Helix. La creación de los volúmenes, los clones y las snapshots se bloquea cuando el clúster está en este estado. No es un estado seguro y no se recomienda para ningún clúster. Debe añadir más capacidad o liberar capacidad de inmediato.

- **Crítico**

  Este error crítico se ha producido porque se ha consumido el 100 % del clúster. Se trata de un estado de solo lectura y no se puede realizar ninguna conexión iSCSI nueva con el clúster. Cuando se alcanza este estado, debe liberar capacidad o añadir más de inmediato.

El sistema utiliza el código de error MetadataClusterFull para informar sobre la ocupación del almacenamiento de metadatos del clúster. Puede ver la ocupación del almacenamiento de metadatos del clúster en la sección Cluster Capacity en la página Overview de la pestaña Reporting en la interfaz de usuario de Element.

En la siguiente lista, se incluye información acerca de los niveles de gravedad de MetadataClusterFull:

- **Advertencia**

  Se trata de una advertencia que puede configurar el cliente y que aparece cuando la capacidad de datos de metadatos del clúster se acerca al nivel de gravedad de error. De forma predeterminada, este nivel se establece en el tres por ciento por debajo del nivel de error y se puede ajustar a través de la API de Element. Debe añadir más capacidad o liberar capacidad Lo antes posible..

- **Error**

  Cuando el clúster presenta este estado, si se pierde un nodo, no habrá suficiente capacidad en el clúster para reconstruir la protección de datos de Double Helix. La creación de los volúmenes, los clones y las snapshots se bloquea cuando el clúster está en este estado. No es un estado seguro y no se recomienda para ningún clúster. Debe añadir más capacidad o liberar capacidad de inmediato.

- **Crítico**

  Este error crítico se ha producido porque se ha consumido el 100 % del clúster. Se trata de un estado de solo lectura y no se puede realizar ninguna conexión iSCSI nueva con el clúster. Cuando se alcanza este estado, debe liberar capacidad o añadir más de inmediato.

Lo siguiente se aplica a los umbrales de clúster de dos nodos:

- El error de ocupación de metadatos está un 20% por debajo de crítico.
- El error de ocupación de los bloques es 1 unidad de bloque (incluida la capacidad desaprovechada) que se encuentra por debajo de la crucial. Esto significa que vale de dos unidades de bloque la capacidad por debajo de la crítica.

Gestione y supervise el almacenamiento con Hybrid Cloud Control de NetApp

Con el almacenamiento all-flash SolidFire de NetApp, puede gestionar y supervisar activos de almacenamiento y configurar componentes en su sistema de almacenamiento con el control de cloud híbrido de NetApp.

- "Añadir y gestionar clústeres de almacenamiento"
- "Configure el acceso completo a la interfaz de usuario web de Nombre de dominio"
- "Crear y administrar cuentas de usuario"
- "Cree y gestione volúmenes"
- "Permite crear y gestionar grupos de acceso de volúmenes"
- "Cree y gestione iniciadores"
- "Cree y gestione políticas de calidad de servicio de volúmenes"
- "Supervise su sistema SolidFire con el control del cloud híbrido de NetApp"

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Añada y gestione clústeres de almacenamiento utilizando Hybrid Cloud Control de NetApp

Puede añadir clústeres de almacenamiento al inventario de activos del nodo de gestión para poder gestionarlos mediante el control del cloud híbrido (HCC) de NetApp. El primer clúster de almacenamiento añadido durante la configuración del sistema es el valor predeterminado "clúster de almacenamiento fiable", Pero se pueden añadir agrupaciones adicionales con la interfaz de usuario de HCC.

Después de añadir un clúster de almacenamiento, es posible supervisar el rendimiento del clúster, cambiar las credenciales del clúster de almacenamiento del activo gestionado o quitar un clúster de almacenamiento del inventario de activos del nodo de gestión si ya no se necesita gestionar mediante HCC.

Lo que necesitará

- **Permisos de administrador de clúster**: Tiene permisos como administrador en "clúster de almacenamiento fiable". El clúster de autoridad es el primer clúster que se ha agregado al inventario de nodos de gestión durante la configuración del sistema.
- **Software Element**: La versión del clúster de almacenamiento ejecuta el software NetApp Element 11.3 o posterior.
- **Nodo de gestión**: Ha implementado un nodo de gestión que ejecuta la versión 11.3 o posterior.
- **Servicios de administración**: Ha actualizado su paquete de servicios de administración a la versión 2.17 o posterior.

Opciones

- Añada un clúster de almacenamiento
- Confirmar el estado del clúster de almacenamiento
- Editar credenciales del clúster de almacenamiento
- Quite un clúster de almacenamiento de
- Habilite y deshabilite el modo de mantenimiento

Añada un clúster de almacenamiento

Puede añadir un clúster de almacenamiento al inventario de activos del nodo de gestión con Hybrid Cloud Control de NetApp. Esto permite gestionar y supervisar el clúster con la interfaz de usuario de HCC.

Pasos

1. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador autorizadas del clúster de almacenamiento.
2. En el panel de control, seleccione el menú de opciones de la parte superior derecha y seleccione **Configurar**.
3. En el panel **clústeres de almacenamiento**, seleccione **Detalles del clúster de almacenamiento**.
4. Seleccione **Agregar clúster de almacenamiento**.
5. Introduzca la siguiente información:
   - Dirección IP virtual de gestión del clúster de almacenamiento

     Solo se pueden añadir clústeres de almacenamiento remotos que actualmente no están gestionados por un nodo de gestión.

   - Nombre de usuario y contraseña del clúster de almacenamiento
6. Seleccione **Agregar**.

   Después de añadir el clúster de almacenamiento, el inventario de clústeres puede tardar hasta 2 minutos en actualizarse y mostrar los nuevos adición. Es posible que deba actualizar la página en el explorador para ver los cambios.

Confirmar el estado del clúster de almacenamiento

Puede supervisar el estado de conexión de activos de clústeres de almacenamiento mediante la interfaz de usuario de control de cloud híbrido de NetApp.

Pasos

1. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador autorizadas del clúster de almacenamiento.
2. En el panel de control, seleccione el menú de opciones de la parte superior derecha y seleccione **Configurar**.
3. Revise el estado de los clústeres de almacenamiento de en el inventario.
4. En el panel **clústeres de almacenamiento**, seleccione **Detalles del clúster de almacenamiento** para obtener más información.

Editar credenciales del clúster de almacenamiento

Puede editar el nombre de usuario y la contraseña del administrador del clúster de almacenamiento mediante la interfaz de usuario de NetApp Hybrid Cloud Control.

Pasos

1. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador autorizadas del clúster de almacenamiento.
2. En el panel de control, seleccione el menú de opciones de la parte superior derecha y seleccione **Configurar**.
3. En el panel **clústeres de almacenamiento**, seleccione **Detalles del clúster de almacenamiento**.
4. Seleccione el menú **acciones** para el clúster y seleccione **Editar credenciales de clúster**.
5. Actualice el nombre de usuario y la contraseña del clúster de almacenamiento.
6. Seleccione **Guardar**.

Quite un clúster de almacenamiento de

Al quitar un clúster de almacenamiento de NetApp Hybrid Cloud Control, se quita el clúster del inventario del nodo de gestión. Una vez que se quita un clúster de almacenamiento, el clúster ya no puede gestionarse mediante HCC y solo es posible acceder a él; para ello, solo debe navegar directamente a su dirección IP de gestión.

No se puede quitar el clúster autorizado del inventario. Para determinar el clúster autorizado, vaya a **Administración de usuarios > usuarios**. El clúster autorizado se muestra junto al encabezado **usuarios**.

Pasos

1. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador autorizadas del clúster de almacenamiento.
2. En el panel de control, seleccione el menú de opciones de la parte superior derecha y seleccione **Configurar**.
3. En el panel **clústeres de almacenamiento**, seleccione **Detalles del clúster de almacenamiento**.
4. Seleccione el menú **acciones** del clúster y seleccione **Quitar clúster de almacenamiento**.

   Si selecciona **Sí** a continuación, se eliminará el clúster de la instalación.

5. Seleccione **Sí**.

Habilite y deshabilite el modo de mantenimiento

Si necesita desconectar un nodo de almacenamiento para realizar tareas de mantenimiento, como actualizaciones de software o reparaciones de host, puede minimizar el impacto de I/o del resto del clúster de almacenamiento habilitación el modo de mantenimiento para ese nodo. Cuando usted desactivar del modo de mantenimiento, el nodo se supervisa para garantizar que se cumplen ciertos criterios antes de que el nodo pueda pasar del modo de mantenimiento.

Lo que necesitará

- **Software Element**: La versión del clúster de almacenamiento ejecuta el software NetApp Element 12.2 o posterior.

- **Nodo de gestión**: Ha implementado un nodo de gestión que ejecuta la versión 12.2 o posterior.
- **Servicios de administración**: Ha actualizado su paquete de servicios de administración a la versión 2.19 o posterior.
- Tiene acceso para iniciar sesión en el nivel de administrador.

Habilitar el modo de mantenimiento

Puede utilizar el siguiente procedimiento para habilitar el modo de mantenimiento para un nodo de clúster de almacenamiento.

Solo un nodo puede estar en modo de mantenimiento a la vez.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

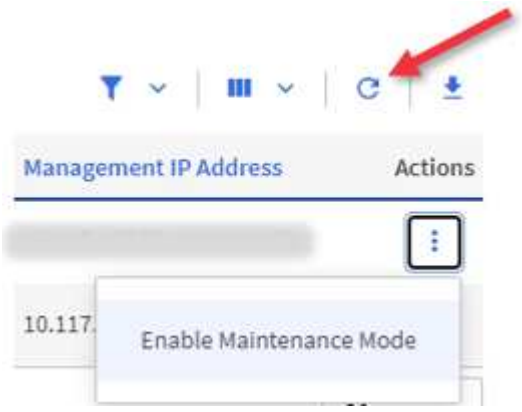
```
https://[management node IP address]
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento all-flash SolidFire.

Las opciones de las funciones del modo de mantenimiento se deshabilitan en el nivel de solo lectura.

3. En el cuadro azul de navegación izquierdo, seleccione la instalación all-flash de SolidFire.
4. En el panel de navegación izquierdo, seleccione **Nodes**.
5. Para ver la información del inventario de almacenamiento, seleccione **almacenamiento**.
6. Habilite el modo de mantenimiento en un nodo de almacenamiento:

La tabla nodos de almacenamiento se actualiza automáticamente cada dos minutos para las acciones iniciadas por el usuario no. Antes de una acción, para asegurarse de tener el estado más actualizado, puede actualizar la tabla nodos con el icono de actualización ubicado en el lado superior derecho de la tabla nodos.



a. En **acciones**, seleccione **Activar modo de mantenimiento**.

Mientras **modo de mantenimiento** está activado, las acciones del modo de mantenimiento no están

disponibles para el nodo seleccionado y para todos los demás nodos del mismo clúster.

Una vez completada **activación del modo de mantenimiento**, la columna **Estado del nodo** muestra un icono de llave y el texto "**modo de mantenimiento**" para el nodo que está en modo de mantenimiento.

desactive el modo de mantenimiento

Una vez que un nodo se ha colocado correctamente en modo de mantenimiento, la acción **Desactivar modo de mantenimiento** está disponible para este nodo. Las acciones en los otros nodos no están disponibles hasta que el modo de mantenimiento se deshabilita correctamente en el nodo que experimenta mantenimiento.

Pasos

1. Para el nodo en modo de mantenimiento, en **acciones**, seleccione **Desactivar modo de mantenimiento**.

   Mientras **el modo de mantenimiento** está desactivado, las acciones del modo de mantenimiento no están disponibles para el nodo seleccionado y para todos los demás nodos del mismo clúster.

   Después de que se completa **desactivación del modo de mantenimiento**, la columna **Estado del nodo** muestra **activo**.

   > Cuando un nodo se encuentra en modo de mantenimiento, no acepta datos nuevos. Como resultado, puede tardar más tiempo en deshabilitar el modo de mantenimiento, porque el nodo debe sincronizar sus datos de nuevo para poder salir del modo de mantenimiento. Cuanto más tiempo gaste en el modo de mantenimiento, más tiempo será necesario para deshabilitar el modo de mantenimiento.

Solucionar problemas

Si se producen errores cuando se habilita o se deshabilita el modo de mantenimiento, se muestra un error de banner en la parte superior de la tabla Nodes. Para obtener más información sobre el error, puede seleccionar el enlace **Mostrar detalles** que se proporciona en el banner para mostrar cuáles son las devoluciones de la API.

Obtenga más información

- "Crear y gestionar activos de clúster de almacenamiento"
- "Documentación de SolidFire y el software Element"

Cree y gestione cuentas de usuario con NetApp Hybrid Cloud Control

En los sistemas de almacenamiento basados en Element, se pueden crear usuarios de clúster autorizados para permitir el acceso de inicio de sesión a Hybrid Cloud Control de NetApp en función de los permisos que desee para los usuarios "Administrator" o "Read-only". Además de los usuarios del clúster, también hay cuentas de volúmenes que permiten que los clientes se conecten a volúmenes en un nodo de almacenamiento.

Gestione los siguientes tipos de cuentas:

- Administrar cuentas de clúster autorizadas
- Permite gestionar cuentas de volumen

Habilite LDAP

Para utilizar LDAP en cualquier cuenta de usuario, primero debe habilitar LDAP.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En el panel de control, seleccione en la parte superior derecha del icono Opciones y seleccione **Gestión de usuarios**.
3. En la página Users (usuarios), seleccione **Configure LDAP** (Configurar LDAP*).
4. Defina su configuración de LDAP.
5. Seleccione el tipo de autenticación Search and Bind o Direct Bind.
6. Antes de guardar los cambios, seleccione **probar el registro LDAP** en la parte superior de la página, introduzca el nombre de usuario y la contraseña de un usuario que sepa que existe y seleccione **Prueba**.
7. Seleccione **Guardar**.

Administrar cuentas de clúster autorizadas

"Cuentas de usuario autoritativas" Se gestionan desde la opción de gestión de usuarios del menú superior derecho del control del cloud híbrido de NetApp. Estos tipos de cuentas permiten la autenticación en cualquier activo de almacenamiento asociado con una instancia de NetApp Hybrid Cloud Control de nodos y clústeres. Con esta cuenta, puede gestionar volúmenes, cuentas, grupos de acceso y mucho más en todos los clústeres.

Cree una cuenta de clúster autorizada

Puede crear una cuenta con Hybrid Cloud Control de NetApp.

Esta cuenta puede usarse para iniciar sesión en el control de cloud híbrido, la interfaz de usuario por nodo del clúster y el clúster de almacenamiento en el software NetApp Element.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En el panel de control, seleccione en la parte superior derecha del icono Opciones y seleccione **Gestión de usuarios**.
3. Seleccione **Crear usuario**.
4. Seleccione el tipo de autenticación del clúster o LDAP.
5. Realice una de las siguientes acciones:
   - Si seleccionó LDAP, introduzca el DN.

     Para usar LDAP, primero se debe habilitar LDAP o LDAPS. Consulte Habilite LDAP.

   - Si seleccionó Cluster como Auth Type, introduzca un nombre y una contraseña para la nueva cuenta.
6. Seleccione permisos de administrador o de solo lectura.

Para ver los permisos del software NetApp Element, seleccione **Mostrar permisos heredados**. Si selecciona un subconjunto de estos permisos, a la cuenta se le asignan permisos de sólo lectura. Si selecciona todos los permisos heredados, la cuenta tiene permisos de administrador asignados.

Para asegurarse de que todos los hijos de un grupo heredan permisos, cree un grupo de administración de organización DN en el servidor LDAP. Todas las cuentas secundarias de ese grupo heredarán dichos permisos.

7. Marque la casilla que indica que "he leído y acepto el contrato de licencia para usuario final de NetApp".
8. Seleccione **Crear usuario**.

Edite una cuenta de clúster autorizada

Puede cambiar los permisos o la contraseña de una cuenta de usuario mediante NetApp Hybrid Cloud Control.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En el panel de control, seleccione en el icono de la parte superior derecha y seleccione **Gestión de usuarios**.
3. Si lo desea, puede filtrar la lista de cuentas de usuario seleccionando **Cluster**, **LDAP** o **IDP**.

   Si configuró usuarios en el clúster de almacenamiento con LDAP, esas cuentas muestran un tipo de usuario "LDAP". Si configuró usuarios en el clúster de almacenamiento con IDP, esas cuentas muestran un tipo de usuario "IDP".

4. En la columna **acciones** de la tabla, expanda el menú de la cuenta y seleccione **Editar**.
5. Realice los cambios necesarios.
6. Seleccione **Guardar**.
7. Cierre la sesión en Hybrid Cloud Control de NetApp.

Es posible que la interfaz de usuario de control de cloud híbrido de NetApp demore hasta 2 minutos en actualizar el inventario. Para actualizar manualmente el inventario, acceda al servicio de inventario de la interfaz de usuario de LA API DE REST `https://[management node IP]/inventory/1/` y correr `GET /installations /{id}` para el clúster.

8. Inicie sesión en NetApp Hybrid Cloud Control.

Elimine una cuenta de usuario autorizada

Puede eliminar una o varias cuentas cuando ya no sea necesaria. Es posible eliminar una cuenta de usuario de LDAP.

No puede eliminar la cuenta de usuario de administrador principal para el clúster autorizado.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En el panel de control, seleccione en el icono de la parte superior derecha y seleccione **Gestión de usuarios**.
3. En la columna **acciones** de la tabla Users (usuarios), expanda el menú de la cuenta y seleccione **Delete** (Eliminar).
4. Confirme la eliminación seleccionando **Sí**.

Permite gestionar cuentas de volumen

"Cuentas de volumen" Se gestionan en la tabla volúmenes de control del cloud híbrido de NetApp. Estas cuentas solo son específicas del clúster de almacenamiento en el que se crearon. Estos tipos de cuentas permiten establecer permisos en los volúmenes de la red, pero no afectan fuera de dichos volúmenes.

Una cuenta de volumen contiene la autenticación CHAP que se necesita para acceder a los volúmenes que tiene asignados.

Cree una cuenta de volumen

Cree una cuenta específica para este volumen.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En el panel de control, seleccione **almacenamiento** > **volúmenes**.
3. Seleccione la ficha **Cuentas**.
4. Seleccione el botón **Crear cuenta**.
5. Escriba un nombre para la cuenta nueva.
6. En la sección CHAP Settings, introduzca la siguiente información:
   - Initiator Secret para la autenticación CHAP de la sesión de nodo
   - Target Secret para la autenticación CHAP de la sesión de nodo

   Para generar automáticamente cualquiera de las contraseñas, deje los campos de credenciales vacíos.
7. Seleccione **Crear cuenta**.

Editar una cuenta de volumen

Puede cambiar la información de CHAP y cambiar si una cuenta está activa o bloqueada.

Si se elimina o se bloquea una cuenta asociada con el nodo de gestión, se produce un nodo de gestión inaccesible.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.

2. En el panel de control, seleccione **almacenamiento** > **volúmenes**.
3. Seleccione la ficha **Cuentas**.
4. En la columna **acciones** de la tabla, expanda el menú de la cuenta y seleccione **Editar**.
5. Realice los cambios necesarios.
6. Confirme los cambios seleccionando **Sí**.

Eliminar una cuenta de volumen

Elimine una cuenta que ya no necesite.

Antes de eliminar una cuenta de volumen, elimine y purgue todos los volúmenes asociados con la cuenta en primer lugar.

> Si se elimina o se bloquea una cuenta asociada con el nodo de gestión, se produce un nodo de gestión inaccesible.

> Los volúmenes persistentes asociados con servicios de gestión se asignan a una cuenta nueva durante la instalación o la actualización. Si utiliza volúmenes persistentes, no modifique o elimine los volúmenes o su cuenta asociada. Si elimina estas cuentas, podría dejar el nodo de gestión en estado inutilizable.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En el panel de control, seleccione **almacenamiento** > **volúmenes**.
3. Seleccione la ficha **Cuentas**.
4. En la columna **acciones** de la tabla, expanda el menú de la cuenta y seleccione **Eliminar**.
5. Confirme la eliminación seleccionando **Sí**.

Obtenga más información

- "Más información acerca de las cuentas"
- "Trabaje con cuentas que utilicen CHAP"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Cree y gestione volúmenes mediante Hybrid Cloud Control de NetApp

Es posible crear un volumen y asociarlo con una cuenta determinada. Al asociar un volumen con una cuenta, la cuenta podrá acceder al volumen a través de iniciadores iSCSI y las credenciales de CHAP.

Puede especificar la configuración de calidad de servicio de un volumen mientras lo crea.

Puede gestionar volúmenes en NetApp Hybrid Cloud Control de las siguientes formas:

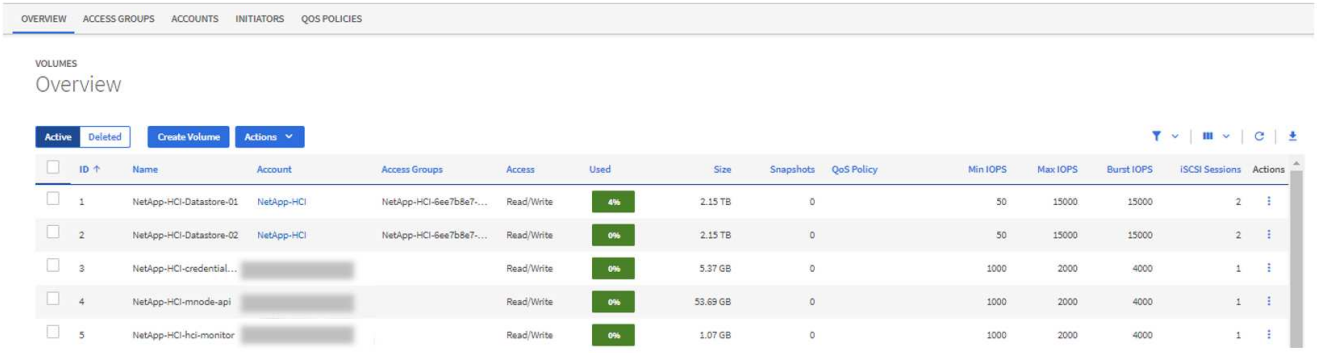
- Cree un volumen
- Aplique una política de calidad de servicio en un volumen
- Editar un volumen
- Clonar volúmenes
- Añada volúmenes a un grupo de acceso de volúmenes
- Eliminar un volumen
- Restaurar un volumen eliminado
- Purgar un volumen eliminado

Cree un volumen

Puede crear un volumen de almacenamiento con NetApp Hybrid Cloud Control.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione la ficha **volúmenes** > **Descripción general**.



4. Seleccione **Crear volumen**.
5. Escriba un nombre para el volumen nuevo.
6. Introduzca el tamaño total del volumen.

> El tamaño de volumen predeterminado se selecciona en GB. Los volúmenes se pueden crear con tamaños en GB o GIB: 1 GB = 1 000 000 000 bytes 1 GIB = 1 073 741 824 bytes

7. Seleccione un tamaño de bloque para el volumen.
8. En la lista **cuenta**, seleccione la cuenta que debe tener acceso al volumen.

   Si no existe una cuenta, seleccione **Crear cuenta nueva**, introduzca un nuevo nombre de cuenta y seleccione **Crear cuenta**. La cuenta se crea y se asocia con el nuevo volumen en la lista **cuenta**.

> Si hay más de 50 cuentas, no aparecerá la lista. Comience a escribir y la función de autocompletar mostrará los valores que puede elegir.

9. Para configurar Quality of Service del volumen, realice una de las siguientes acciones:

- En **Configuración de calidad de servicio**, establezca valores mínimos, máximos y de ráfaga personalizados para IOPS o utilice los valores de QoS predeterminados.
- Seleccione una política de QoS existente activando la opción **asignar directiva de calidad de servicio** y eligiendo una política de QoS existente en la lista resultante.
- Cree y asigne una nueva directiva QoS activando la opción **asignar directiva de calidad de servicio** y seleccionando **Crear nueva directiva QoS**. En la ventana que se abre, escriba un nombre para la política de calidad de servicio y, a continuación, escriba los valores de calidad de servicio. Cuando termine, seleccione **Crear política de calidad de servicio**.

Los volúmenes que tengan un valor de IOPS máximo o de ráfaga superior a 20 20,000 IOPS podrían requerir una profundidad de cola alta o varias sesiones para alcanzar este nivel de IOPS en un único volumen.

10. Seleccione **Crear volumen**.

Aplique una política de calidad de servicio en un volumen

Puede aplicar una política de calidad de servicio a los volúmenes de almacenamiento existentes mediante Cloud Control de NetApp. Si en cambio, debe establecer valores de calidad de servicio personalizados para un volumen, puede hacerlo Editar un volumen. Para crear una nueva política de calidad de servicio, consulte "Cree y gestione políticas de calidad de servicio de volúmenes".

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes** > **Descripción general**.
4. Seleccione uno o varios volúmenes para asociarlos con una política de calidad de servicio.
5. Seleccione la lista desplegable **acciones** en la parte superior de la tabla Volumes y seleccione **aplicar política de QoS**.
6. En la ventana resultante, seleccione una directiva QoS de la lista y seleccione **aplicar directiva QoS**.

Si utiliza políticas de calidad de servicio en un volumen, puede establecer la calidad de servicio personalizada para quitar la asociación de la política de calidad de servicio con el volumen. Los valores de calidad de servicio personalizados anulan los valores de política de calidad de servicio de los volúmenes.

Editar un volumen

Con Hybrid Cloud Control de NetApp, es posible editar atributos de volúmenes como los valores de calidad de servicio, el tamaño de los volúmenes y la unidad de medida mediante la cual se calculan los valores de bytes. También se puede modificar el acceso de la cuenta para el uso de la replicación o para restringir el acceso al volumen.

Acerca de esta tarea

Puede cambiar el tamaño de un volumen cuando haya espacio suficiente en el clúster en las siguientes condiciones:

- Condiciones de funcionamiento normales.

- Se informa de los errores de los volúmenes.
- El volumen se clona.
- El volumen se vuelve a sincronizar.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes** > **Descripción general**.
4. En la columna **acciones** de la tabla Volumes, expanda el menú para el volumen y seleccione **Editar**.
5. Realice los cambios necesarios:

   a. Cambie el tamaño total del volumen.

   Puede aumentar el tamaño del volumen, pero no reducirlo. En cada operación de ajuste de tamaño, solo se puede ajustar el tamaño de un volumen. Las operaciones de recopilación de datos basura y las actualizaciones de software no interrumpen la operación de cambio de tamaño.

   Si desea ajustar el tamaño del volumen para la replicación, primero aumente el tamaño del volumen asignado como el destino de replicación. Posteriormente, puede cambiar el tamaño del volumen de origen. El tamaño del volumen de destino puede ser mayor o igual que el del volumen de origen, pero no menor.

   El tamaño de volumen predeterminado se selecciona en GB. Los volúmenes se pueden crear con tamaños en GB o GIB: 1 GB = 1 000 000 000 bytes 1 GIB = 1 073 741 824 bytes

   b. Seleccione un nivel de acceso de cuenta diferente:
      - Solo lectura
      - Lectura/Escritura
      - Bloqueado
      - Destino de replicación

   c. Seleccione la cuenta que debería tener acceso al volumen.

      Comience a escribir y la función de autocompletar mostrará los posibles valores que puede elegir.

      Si no existe ninguna cuenta, seleccione **Crear nueva cuenta**, introduzca un nuevo nombre de cuenta y seleccione **Crear**. La cuenta se creará y se asociará con el volumen existente.

   d. Cambie la calidad de servicio llevando a cabo una de las siguientes acciones:
      i. Seleccione una política existente.
      ii. En Custom Settings, establezca los valores mínimos, máximos y de ráfaga para IOPS, o bien utilice los valores predeterminados.

Si utiliza políticas de calidad de servicio en un volumen, puede establecer la calidad de servicio personalizada para quitar la asociación de la política de calidad de servicio con el volumen. La calidad de servicio personalizada anulará los valores de las políticas de calidad de servicio de los volúmenes.

Cuando cambie los valores de IOPS, debe incrementar sus diez o cien. Los valores de entrada deben ser números enteros válidos. Configure los volúmenes con un valor de ráfaga muy alto. De este modo, el sistema podrá procesar grandes cargas de trabajo secuenciales en bloque ocasionales con mayor rapidez, a la vez que se limitan las IOPS sostenidas de un volumen.

6. Seleccione **Guardar**.

Clonar volúmenes

Es posible crear un clon de un solo volumen de almacenamiento o clonar un grupo de volúmenes para hacer una copia de los datos en un momento específico. Cuando se clona un volumen, el sistema crea una copia de Snapshot del volumen y, a continuación, crea una copia de los datos que se indican en la copia de Snapshot.

Antes de empezar

- Debe haber al menos un clúster añadido y en ejecución.
- Se creó al menos un volumen.
- Se creó una cuenta de usuario.
- El espacio sin aprovisionar disponible debe ser igual o mayor que el tamaño del volumen.

Acerca de esta tarea

El clúster admite hasta dos solicitudes de clones en ejecución por volumen a la vez y hasta 8 operaciones de clones de volúmenes activos a la vez. Las solicitudes que superen este límite se pondrán en cola para procesarlas más adelante.

El clonado de volúmenes es un proceso asíncrono, y la cantidad de tiempo que requiere el proceso depende del tamaño del volumen que se clona y de la carga del clúster actual.

Los volúmenes clonados no heredan pertenencia al grupo de acceso de volúmenes en el volumen de origen.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione la ficha **volúmenes** > **Descripción general**.
4. Seleccione cada volumen que desea clonar.
5. Seleccione la lista desplegable **acciones** en la parte superior de la tabla Volumes y seleccione **Clonar**.
6. En la ventana que se abre, realice lo siguiente:

    a. Introduzca un prefijo de nombre de volumen (lo cual es opcional).

    b. Seleccione el tipo de acceso en la lista **Access**.

c. Elija una cuenta para asociar con el nuevo clon de volumen (de forma predeterminada, se selecciona **Copiar desde volumen**, que utilizará la misma cuenta que el volumen original).

d. Si no existe una cuenta, seleccione **Crear cuenta nueva**, introduzca un nuevo nombre de cuenta y seleccione **Crear cuenta**. La cuenta se creará y se asociará con el volumen.

Utilice prácticas recomendadas de nomenclatura descriptiva. Esto es especialmente importante si se utilizan varios clústeres o instancias de vCenter Server en el entorno.

Al aumentar el tamaño del volumen de un clon, se genera un volumen nuevo con espacio libre adicional al final del volumen. Según cómo use el volumen, podría necesitar ampliar las particiones o crear otras nuevas en el espacio libre para utilizarlo.

a. Seleccione **Clonar volúmenes**.

El tiempo para completar una operación de clonación se ve afectado por el tamaño del volumen y la carga actual del clúster. Actualice la página si el volumen clonado no aparece en la lista de volúmenes.

Añada volúmenes a un grupo de acceso de volúmenes

Es posible añadir un volumen único o un grupo de volúmenes a un grupo de acceso de volúmenes.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes** > **Descripción general**.
4. Seleccione uno o varios volúmenes para asociarlos con un grupo de acceso de volúmenes.
5. Seleccione la lista desplegable **acciones** en la parte superior de la tabla Volumes y seleccione **Agregar a grupo de acceso**.
6. En la ventana que aparece, seleccione un grupo de acceso de volúmenes de la lista **Grupo de acceso de volúmenes**.
7. Seleccione **Añadir volumen**.

Eliminar un volumen

Es posible eliminar uno o varios volúmenes de un clúster de almacenamiento de Element.

Acerca de esta tarea

El sistema no purga de manera inmediata volúmenes eliminados; estos siguen disponibles durante aproximadamente ocho horas. Después de ocho horas, se purgan y ya no están disponibles. Si un volumen se restaura antes de que el sistema lo purgue, el volumen volverá a conectarse y las conexiones iSCSI se restaurarán.

Si se elimina el volumen que se utilizó para crear una snapshot, sus snapshots asociadas pasan a estar inactivas. Cuando se purgan los volúmenes de origen eliminados, también se eliminan del sistema las snapshots inactivas asociadas.

Los volúmenes persistentes asociados con servicios de gestión se crean y se asignan a una nueva cuenta durante la instalación o la actualización. Si utiliza volúmenes persistentes, no modifique o elimine los volúmenes o su cuenta asociada. Si elimina estos volúmenes, podría dejar el nodo de gestión inutilizable.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes** > **Descripción general**.
4. Seleccione uno o varios volúmenes para eliminarlos.
5. Seleccione la lista desplegable **acciones** en la parte superior de la tabla Volumes y seleccione **Eliminar**.
6. En la ventana resultante, confirme la acción seleccionando **Sí**.

Restaurar un volumen eliminado

Después de eliminar un volumen de almacenamiento, es posible restaurarlo si lo hace antes de ocho horas después de la eliminación.

El sistema no purga de manera inmediata volúmenes eliminados; estos siguen disponibles durante aproximadamente ocho horas. Después de ocho horas, se purgan y ya no están disponibles. Si un volumen se restaura antes de que el sistema lo purgue, el volumen volverá a conectarse y las conexiones iSCSI se restaurarán.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes** > **Descripción general**.
4. Seleccione **eliminado**.
5. En la columna **acciones** de la tabla Volumes, expanda el menú para el volumen y seleccione **Restaurar**.
6. Confirme el proceso seleccionando **Sí**.

Purgar un volumen eliminado

Una vez que se eliminan los volúmenes de almacenamiento, siguen disponibles durante ocho horas aproximadamente. Después de ocho horas, se purgan automáticamente y ya no están disponibles. Si no desea esperar las ocho horas, puede eliminarse

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes** > **Descripción general**.
4. Seleccione **eliminado**.
5. Seleccione uno o varios volúmenes para purgar.

6. Debe realizar una de las siguientes acciones:
   - Si ha seleccionado varios volúmenes, seleccione el filtro rápido **Purge** en la parte superior de la tabla.
   - Si seleccionó un único volumen, en la columna **acciones** de la tabla Volumes, expanda el menú para el volumen y seleccione **Purgar**.
7. En la columna **acciones** de la tabla de volúmenes, expanda el menú para el volumen y seleccione **Purgar**.
8. Confirme el proceso seleccionando **Sí**.

Obtenga más información

- "Más información acerca de los volúmenes"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Permite crear y gestionar grupos de acceso de volúmenes

Se pueden crear nuevos grupos de acceso de volúmenes, realizar cambios en el nombre, los iniciadores asociados o los volúmenes asociados de los grupos de acceso, o eliminar los grupos de acceso de volúmenes existentes mediante NetApp Hybrid Cloud Control.

Lo que necesitará

- Tiene credenciales de administrador para este sistema de almacenamiento all-flash SolidFire.
- Ha actualizado sus servicios de administración a al menos la versión 2.15.28. La gestión del almacenamiento de control de cloud híbrido de NetApp no está disponible en versiones anteriores del paquete de servicio.
- Asegúrese de tener un esquema de nomenclatura lógico para los grupos de acceso de volúmenes.

Añadir un grupo de acceso de volúmenes

Es posible añadir un grupo de acceso de volúmenes a un clúster de almacenamiento mediante NetApp Hybrid Cloud Control.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la ficha **grupos de acceso**.
5. Seleccione el botón **Crear grupo de acceso**.
6. En el cuadro de diálogo que se abre, escriba un nombre para el nuevo grupo de acceso de volúmenes.
7. (Opcional) en la sección **Initiators**, seleccione uno o más iniciadores para asociarlos con el nuevo grupo de acceso de volúmenes.

Si asocia un iniciador con el grupo de acceso de volúmenes, ese iniciador puede acceder a cada volumen del grupo sin necesidad de autenticación.

8. (Opcional) en la sección **Volumes**, seleccione uno o varios volúmenes para incluirlos en este grupo de acceso de volúmenes.
9. Seleccione **Crear grupo de acceso**.

Edite un grupo de acceso de volúmenes

Puede editar las propiedades de un grupo de acceso de volúmenes existente mediante NetApp Hybrid Cloud Control. Es posible realizar cambios en el nombre, los iniciadores asociados o los volúmenes asociados de un grupo de acceso.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la ficha **grupos de acceso**.
5. En la columna **acciones** de la tabla de grupos de acceso, expanda el menú de opciones para el grupo de acceso que necesita editar.
6. En el menú de opciones, seleccione **Editar**.
7. Realice los cambios necesarios en el nombre, los iniciadores asociados o los volúmenes asociados.
8. Confirme los cambios seleccionando **Guardar**.
9. En la tabla **grupos de acceso**, compruebe que el grupo de acceso refleja los cambios.

Elimine un grupo de acceso de volúmenes

Es posible quitar un grupo de acceso de volúmenes mediante NetApp Hybrid Cloud Control y, al mismo tiempo, quitar los iniciadores asociados con este grupo de acceso del sistema.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la ficha **grupos de acceso**.
5. En la columna **acciones** de la tabla de grupos de acceso, expanda el menú de opciones para el grupo de acceso que necesita eliminar.
6. En el menú de opciones, seleccione **Eliminar**.
7. Si no desea eliminar los iniciadores asociados con el grupo de acceso, anule la selección de la casilla de verificación **Eliminar iniciadores de este grupo de acceso**.
8. Confirme la operación de eliminación seleccionando **Sí**.

Obtenga más información

- "Obtenga información acerca de los grupos de acceso de volúmenes"
- "Añada un iniciador de a un grupo de acceso de volúmenes"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Cree y gestione iniciadores

Puede utilizar "iniciadores" Para el acceso basado en CHAP en lugar de basado en la cuenta a los volúmenes. Los iniciadores se pueden crear y eliminar, y es posible asignarles alias descriptivos para simplificar la administración y el acceso de los volúmenes. Cuando se añade un iniciador a un grupo de acceso de volúmenes, ese iniciador permite el acceso a todos los volúmenes del grupo.

Lo que necesitará

- Tiene credenciales de administrador del clúster.
- Ha actualizado sus servicios de administración a al menos la versión 2.17. La gestión del iniciador de control de cloud híbrido de NetApp no está disponible en versiones anteriores del paquete de servicio.

Opciones

- Cree un iniciador
- Añada iniciadores a un grupo de acceso de volúmenes
- Cambie un alias de iniciador
- Elimine los iniciadores

Cree un iniciador

Es posible crear iniciadores iSCSI o Fibre Channel y, opcionalmente, asignarles alias.

Acerca de esta tarea

El formato aceptado de un IQN de iniciador es `iqn.yyyy-mm` donde y y m son dígitos seguidos de texto que solo puede contener dígitos, caracteres alfabéticos en minúscula, un punto (`.`), dos puntos (`:`) o guión (`-`). A continuación, se ofrece un ejemplo de formato:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

El formato aceptado de WWPN de un iniciador Fibre Channel es `:Aa:bB:CC:dd:11:22:33:44` o. `AabBCCdd11223344`. A continuación, se ofrece un ejemplo de formato:

```
5f:47:ac:c0:5c:74:d4:02
```

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.

3. Seleccione **volúmenes**.
4. Seleccione la pestaña **Initiators**.
5. Seleccione el botón **Crear iniciadores**.

Opción	Pasos
Cree uno o varios iniciadores	a. Introduzca el IQN o el WWPN del iniciador en el campo **IQN/WWPN**. b. Introduzca un nombre descriptivo para el iniciador en el campo **Alias**. c. (Opcional) Seleccione **Agregar iniciador** para abrir nuevos campos de iniciador o utilice la opción creación masiva en su lugar. d. Seleccione **Crear iniciadores**.
Cree iniciadores masivos	a. Seleccione **adición masiva de IQN/WWPN**. b. Introduzca una lista de varios IQN o WWPN en el cuadro de texto. Cada IQN o WWPN debe estar separado por comas o espacios en su propia línea. c. Seleccione **Agregar IQN/WWPN**. d. (Opcional) Añada alias únicos a cada iniciador. e. Quite todos los iniciadores de la lista que puedan existir ya en la instalación. f. Seleccione **Crear iniciadores**.

Añada iniciadores a un grupo de acceso de volúmenes

Es posible añadir un iniciador a un grupo de acceso de volúmenes. Cuando se añade un iniciador a un grupo de acceso de volúmenes, el iniciador permite el acceso a todos los volúmenes en ese grupo de acceso de volúmenes.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la pestaña **Initiators**.
5. Seleccione uno o varios iniciadores que desee añadir.
6. Seleccione **acciones > Agregar a grupo de acceso**.
7. Seleccione el grupo de acceso.
8. Confirme los cambios seleccionando **Agregar iniciador**.

Cambie un alias de iniciador

Es posible cambiar el alias de un iniciador existente o añadir un alias si aún no hay ninguno.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la pestaña **Initiators**.
5. En la columna **acciones**, expanda el menú de opciones del iniciador.
6. Seleccione **Editar**.
7. Realice los cambios necesarios en el alias o agregue un nuevo alias.
8. Seleccione **Guardar**.

Elimine los iniciadores

Puede eliminar uno o varios iniciadores. Cuando se elimina un iniciador, el sistema la quita de los grupos de acceso de volúmenes asociados. Las conexiones que usan el iniciador siguen siendo válidas hasta que se restablece la conexión.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la pestaña **Initiators**.
5. Elimine uno o varios iniciadores:
   a. Seleccione el o los iniciadores que desea eliminar.
   b. Seleccione **acciones > Eliminar**.
   c. Confirme la operación de eliminación y seleccione **Sí**.

Obtenga más información

- "Obtenga más información acerca de los iniciadores"
- "Obtenga información acerca de los grupos de acceso de volúmenes"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Cree y gestione políticas de calidad de servicio de volúmenes

Una política de calidad de servicio (QoS) permite crear y guardar un ajuste de calidad de servicio estandarizado que se puede aplicar a muchos volúmenes. El clúster

seleccionado debe ser Element 10.0 o posterior para usar políticas de calidad de servicio; de lo contrario, las funciones de las políticas de calidad de servicio no estarán disponibles.

Consulte el contenido de los conceptos de almacenamiento all-flash de SolidFire para obtener más información sobre cómo usar "Políticas de calidad de servicio" en lugar de volumen individual "Calidad de servicio".

Con el control del cloud híbrido de NetApp, puede crear y gestionar políticas de calidad de servicio completando las siguientes tareas:

- Cree una política de calidad de servicio
- Aplique una política de calidad de servicio en un volumen
- Cambie la asignación de políticas de calidad de servicio de un volumen
- Edite una política de calidad de servicio
- Elimine una política de calidad de servicio

Cree una política de calidad de servicio

Puede crear políticas de calidad de servicio y aplicarlas a volúmenes que tengan un rendimiento equivalente.

Si utiliza políticas de calidad de servicio, no use la calidad de servicio personalizada en un volumen. La calidad de servicio personalizada anulará y ajustará los valores de las políticas de calidad de servicio de los volúmenes.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el menú para su clúster de almacenamiento.
3. Seleccione **almacenamiento > volúmenes**.
4. Seleccione la ficha **políticas de QoS**.
5. Seleccione **Crear directiva**.
6. Introduzca el **Nombre de la directiva**.

   Utilice prácticas recomendadas de nomenclatura descriptiva. Esto es especialmente importante si se utilizan varios clústeres o instancias de vCenter Server en el entorno.

7. Introduzca los valores mínimos de IOPS, máximo de IOPS y de IOPS de ráfaga.
8. Seleccione **Crear directiva QoS**.

   Se genera un ID del sistema para la política y esta se muestra en la página QoS Policies con sus valores de calidad de servicio asignados.

Aplique una política de calidad de servicio en un volumen

Puede asignar una política de calidad de servicio existente a un volumen con Hybrid Cloud Control de NetApp.

Lo que necesitará

Se ha aplicado la política de calidad de servicio que desea asignar creado.

Acerca de esta tarea

En esta tarea, se describe cómo asignar una política de calidad de servicio a un volumen individual mediante el cambio de configuración. La última versión de Hybrid Cloud Control de NetApp no tiene una opción de asignación masiva para más de un volumen. Hasta que la funcionalidad que se debe asignar de forma masiva se proporcione en una versión futura, se puede usar la interfaz de usuario web de Element o la interfaz de usuario del plugin de vCenter para asignar de forma masiva políticas de calidad de servicio.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el menú para su clúster de almacenamiento.
3. Seleccione **almacenamiento > volúmenes**.
4. Seleccione el menú **acciones** situado junto al volumen que desea modificar.
5. En el menú que se abre, seleccione **Editar**.
6. En el cuadro de diálogo, habilite **asignar directiva QoS** y seleccione la directiva QoS en la lista desplegable para aplicarla al volumen seleccionado.

   La asignación de calidad de servicio anulará los valores de QoS de cada volumen que se hayan aplicado anteriormente.

7. Seleccione **Guardar**.

Cambie la asignación de políticas de calidad de servicio de un volumen

Puede quitar la asignación de una política de calidad de servicio de un volumen, o bien seleccionar otra política de calidad de servicio o personalizar la calidad de servicio.

Lo que necesitará

El volumen que desea modificar es asignado Una política de calidad de servicio.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el menú para su clúster de almacenamiento.
3. Seleccione **almacenamiento > volúmenes**.
4. Seleccione el menú **acciones** situado junto al volumen que desea modificar.
5. En el menú que se abre, seleccione **Editar**.
6. En el cuadro de diálogo, realice una de las siguientes acciones:
   - Desactive **asignar directiva de QoS** y modifique los valores **Min IOPS**, **Max IOPS** y **Burst IOPS** para la QoS de volumen individual.

     Cuando se deshabilitan las políticas de calidad de servicio, el volumen utiliza valores de IOPS de calidad de servicio predeterminados, a menos que se modifiquen de otro modo.

- Seleccione una política de calidad de servicio diferente de la lista desplegable que desee aplicar al volumen seleccionado.

7. Seleccione **Guardar**.

Edite una política de calidad de servicio

Una política de calidad de servicio existente se puede cambiar, o bien se pueden editar los valores asociados con esta. Los cambios en los valores de rendimiento de las políticas de calidad de servicio afectan a la calidad de servicio de todos los volúmenes asociados con la política.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el menú para su clúster de almacenamiento.
3. Seleccione **almacenamiento > volúmenes**.
4. Seleccione la ficha **políticas de QoS**.
5. Seleccione el menú **acciones** situado junto a la directiva QoS que desea modificar.
6. Seleccione **Editar**.
7. En el cuadro de diálogo **Editar directiva de QoS**, cambie una o más de las siguientes opciones:
   - **Nombre**: El nombre definido por el usuario para la directiva QoS.
   - **Min IOPS**: El número mínimo de IOPS garantizado para el volumen. El valor predeterminado es de 15 50.
   - **Max IOPS**: El número máximo de IOPS permitido para el volumen. El valor predeterminado es de 15 15,000.
   - **Burst IOPS**: El número máximo de IOPS permitido durante un breve período de tiempo para el volumen. El valor predeterminado es de 15 15,000.
8. Seleccione **Guardar**.

Puede seleccionar en el enlace de la columna **volúmenes activos** para que una directiva muestre una lista filtrada de los volúmenes asignados a esa directiva.

Elimine una política de calidad de servicio

Puede eliminar una política de calidad de servicio si ya no es necesaria. Cuando se elimina una política de calidad de servicio, todos los volúmenes asignados con la política se conservan los valores de calidad de servicio definidos previamente por la política, pero como calidad de servicio de un volumen individual. Se eliminará cualquier asociación con la política de calidad de servicio eliminada.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el menú para su clúster de almacenamiento.
3. Seleccione **almacenamiento > volúmenes**.
4. Seleccione la ficha **políticas de QoS**.
5. Seleccione el menú **acciones** situado junto a la directiva QoS que desea modificar.

6. Seleccione **Eliminar**.
7. Confirme la acción.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Supervise su sistema SolidFire con el control del cloud híbrido de NetApp

Supervise los recursos de almacenamiento en la consola de control del cloud híbrido

Con la consola de control del cloud híbrido de NetApp, puede ver todos los recursos de almacenamiento de un solo vistazo. Además, puede supervisar la capacidad de almacenamiento y el rendimiento del almacenamiento.

> Cuando inicia una nueva sesión de control del cloud híbrido de NetApp por primera vez, es posible que haya un retraso al cargar la vista de la consola de control del cloud híbrido de NetApp cuando el nodo de gestión gestiona muchos clústeres. El tiempo de carga varía en función del número de clústeres que gestiona el nodo de gestión activamente. Para lanzamientos posteriores, experimentará tiempos de carga más rápidos.

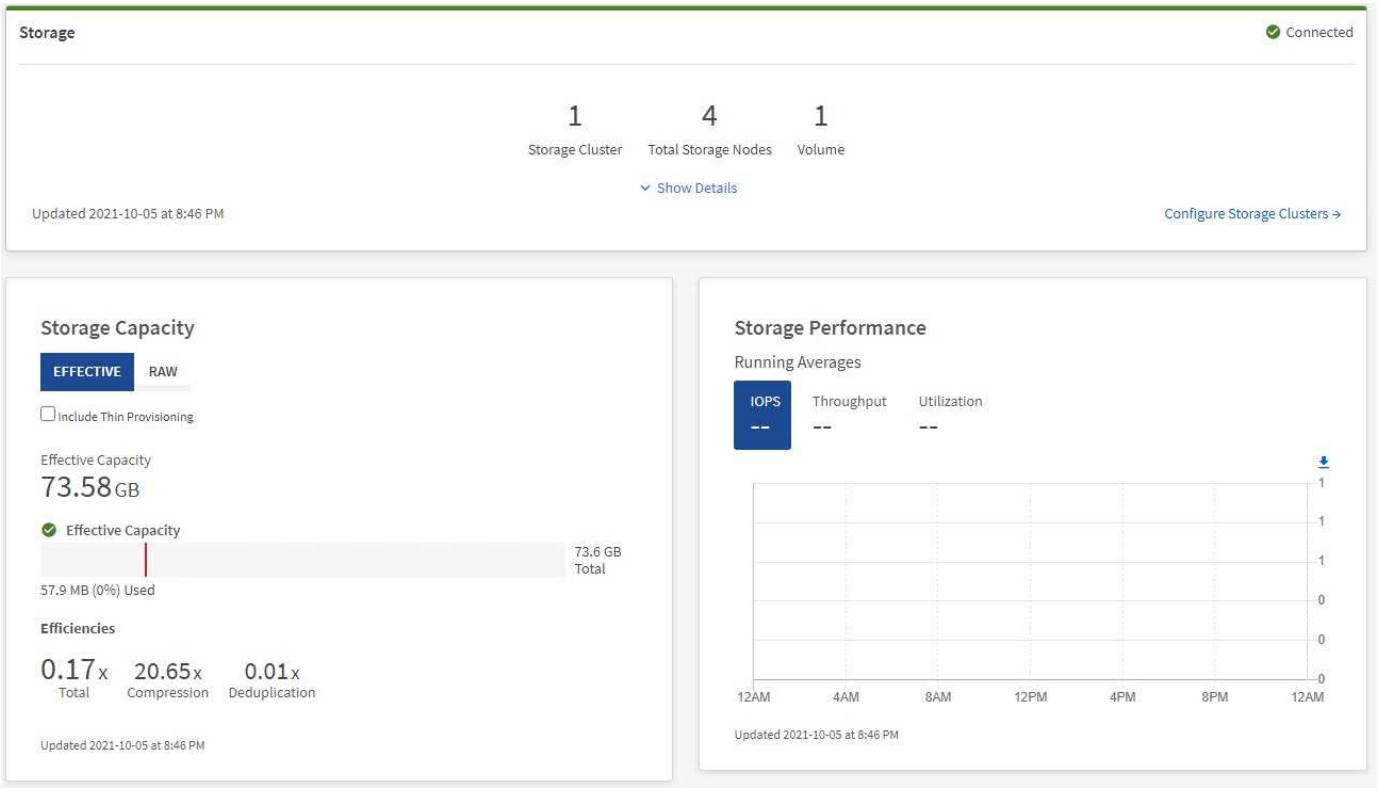
- Acceda a la consola HCC de NetApp
- Supervise los recursos de almacenamiento
- Supervise la capacidad de almacenamiento
- Supervise el rendimiento del almacenamiento

Acceda a la consola HCC de NetApp

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

   ```
   https://[management node IP address]
   ```

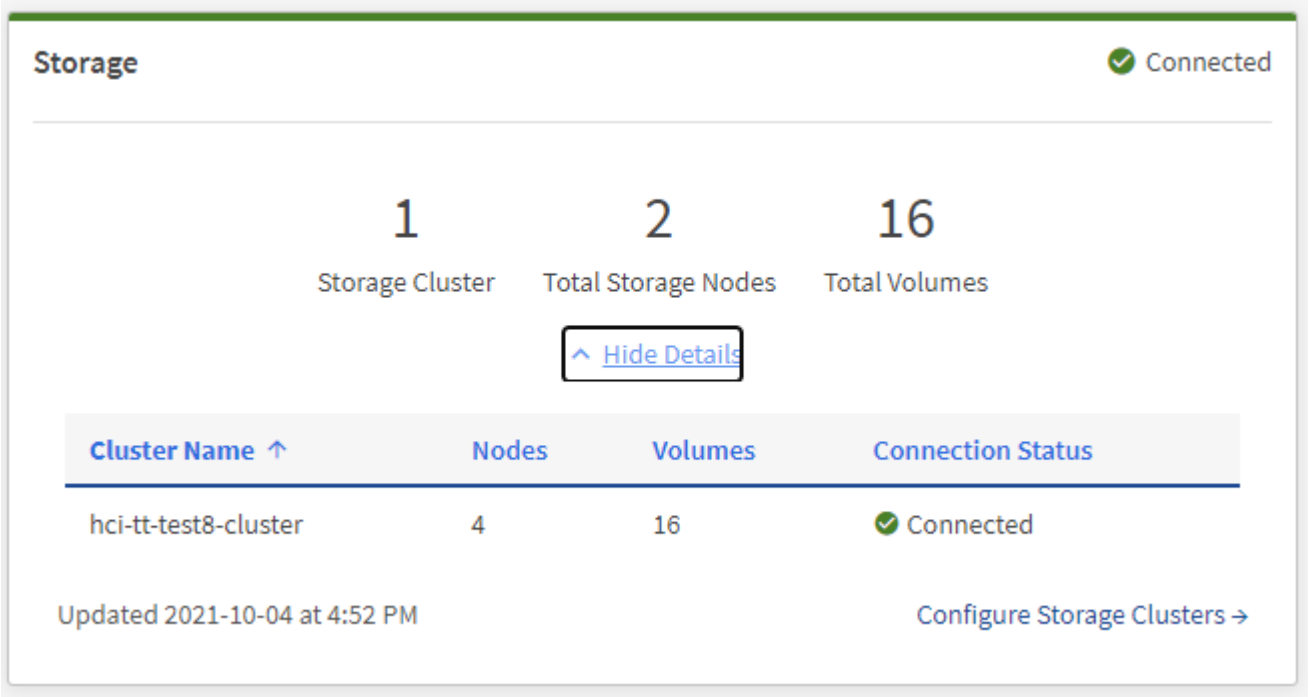
2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento all-flash SolidFire.
3. Consulte la consola de control del cloud híbrido.



Supervise los recursos de almacenamiento

Utilice el panel **almacenamiento** para ver su entorno de almacenamiento total. Es posible supervisar el número de clústeres de almacenamiento, los nodos de almacenamiento y el total de volúmenes.

Para ver los detalles, en el panel almacenamiento, seleccione **Mostrar detalles**.



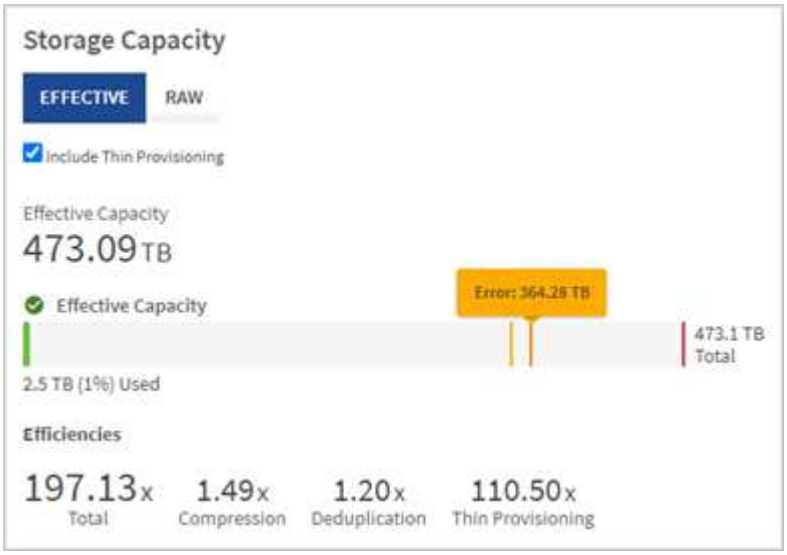
El número total de nodos de almacenamiento no incluye nodos de testigos de clústeres de almacenamiento de dos nodos. Los nodos de testigos se incluyen en el número de nodos de la sección de detalles de ese clúster.

Para ver los datos más recientes del clúster de almacenamiento, use la página Storage Clusters, donde el sondeo se produce con más frecuencia que en la consola.

Supervise la capacidad de almacenamiento

Supervisar la capacidad de almacenamiento del entorno es crucial. Mediante el panel capacidad de almacenamiento, puede determinar sus ganancias en eficiencia de la capacidad del almacenamiento con o sin funciones de compresión, deduplicación y thin provisioning habilitadas.

Puede ver el espacio de almacenamiento físico total disponible en su clúster en la ficha **RAW** e información sobre el almacenamiento aprovisionado en la ficha **EFECTIVO**.



Pasos

1. Seleccione la ficha **RAW** para ver el espacio de almacenamiento físico total utilizado y disponible en el clúster.

   Observe las líneas verticales para determinar si la capacidad que ha utilizado es inferior al total o inferior a los umbrales de advertencia, error o crítico. Pase el ratón por las líneas para ver los detalles.

   Puede establecer el umbral de Advertencia, que por defecto es 3% inferior al umbral de error. Los umbrales error y crítico están predefinidos y no se pueden configurar por diseño. El umbral de error indica que aún hay menos de un nodo de capacidad en el clúster. Para conocer los pasos para establecer el umbral, consulte "Configurar el umbral completo del clúster".

   Para obtener más detalles sobre la API de Element de umbrales de clúster relacionados, consulte "“GetClusterFullThreshold”" En la documentación de la API del software *Element*. Para ver detalles sobre la capacidad de metadatos y bloques, consulte "Niveles de llenado de clústeres" En la documentación del software *Element*.

2. Seleccione la ficha **EFECTIVO** para ver información sobre el almacenamiento total aprovisionado a los

hosts conectados y para ver los índices de eficiencia.

a. Opcionalmente, compruebe **incluir Thin Provisioning** para ver las tasas de eficiencia de Thin Provisioning en el gráfico de barras de capacidad efectiva.

b. **Cuadro de barras de capacidad efectiva**: Observe las líneas verticales para determinar si la capacidad utilizada es inferior o inferior a los umbrales de advertencia, error o crítico. De forma similar a la ficha RAW, puede pasar el ratón por encima de las líneas verticales para ver los detalles.

c. **Eficiencias**: Examine estas calificaciones para determinar el aumento de la eficiencia de la capacidad de almacenamiento con las funciones de compresión, deduplicación y thin provisioning activadas. Por ejemplo, si la compresión se muestra como «1,3x», esto significa que la eficiencia del almacenamiento con compresión habilitada es 1.3 veces más eficiente que sin ella.

> Las eficiencias totales son iguales a (factor de eficiencia maxUsedSpace *) / 2, donde efficiencyfactor = (thinProvisioningfactor * deDuplicationfactor * compressionfactor). Cuando no se selecciona thin provisioning, no se incluye en la eficiencia total.

d. Si la capacidad de almacenamiento efectiva se acerca a un umbral de error o crítico, considere borrar los datos de su sistema.

3. Para un análisis más profundo y un contexto histórico, mire "Detalles de SolidFire Active IQ de NetApp".

Supervise el rendimiento del almacenamiento

Puede ver cuántas IOPS o rendimiento puede obtener de un clúster sin superar el rendimiento útil de ese recurso mediante el panel rendimiento del almacenamiento. El rendimiento del almacenamiento es el punto en el que se obtiene la utilización máxima antes de que la latencia empeore.

El panel rendimiento del almacenamiento le ayuda a identificar si el rendimiento se está alcanzando el punto en el que el rendimiento podría degradarse si las cargas de trabajo aumentan.

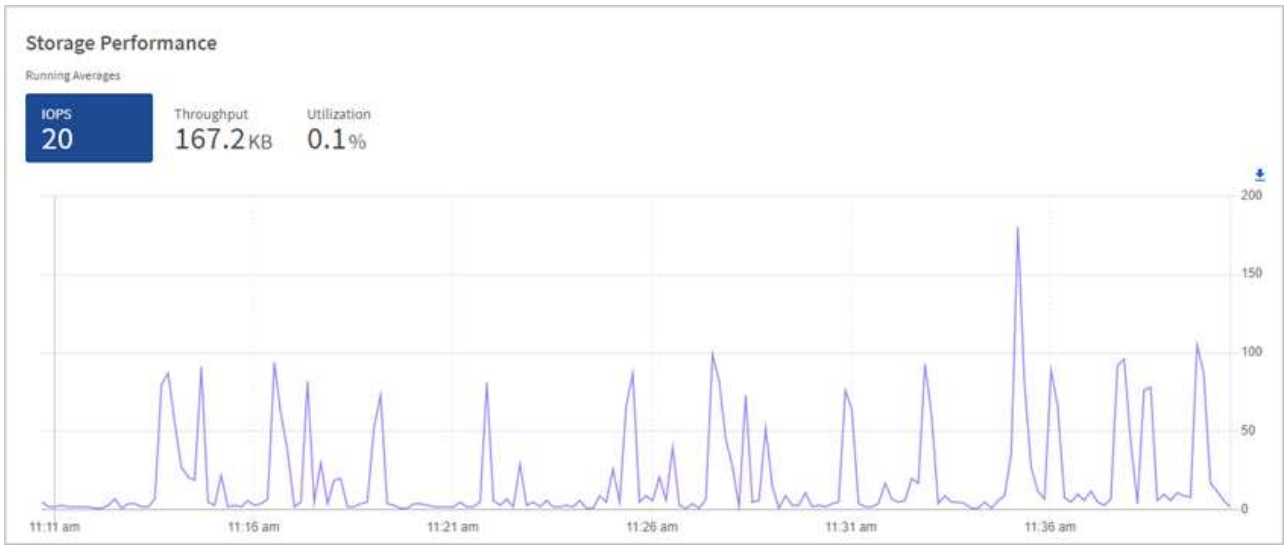
La información de este panel se actualiza cada 10 segundos y muestra un promedio de todos los puntos del gráfico.

Para obtener detalles sobre el método API de Element asociado, consulte "GetClusterStats" Método en la documentación de la API del software *Element*.

Pasos

1. Consulte el panel Storage Performance. Para obtener detalles, pase el ratón sobre los puntos del gráfico.

a. **Pestaña IOPS**: Consulte las operaciones actuales por segundo. Busque tendencias de datos o picos. Por ejemplo, si observa que el número máximo de IOPS es 160 000 y 100 000 de IOPS libres o disponibles, puede considerar la posibilidad de añadir más cargas de trabajo a este clúster. Por otro lado, si observa que solo 140K está disponible, puede considerar la descarga de cargas de trabajo o la ampliación del sistema.



b. **Ficha de rendimiento**: Patrones de monitor o picos de rendimiento. Además, supervise constantemente valores de rendimiento elevados, lo que podría indicar que se está acercando al rendimiento máximo útil del recurso.

c. **Ficha utilización**: Controlar la utilización de IOPS en relación con el total de IOPS disponibles resumido a nivel de clúster.

2. Para obtener más análisis, observe el rendimiento del almacenamiento mediante el complemento de NetApp Element para vCenter Server.

   "Rendimiento que se muestra en el plugin de NetApp Element para vCenter Server".

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Consulte el inventario en la página Nodes

Puede ver los activos de almacenamiento en el sistema y determinar sus direcciones IP, nombres y versiones de software.

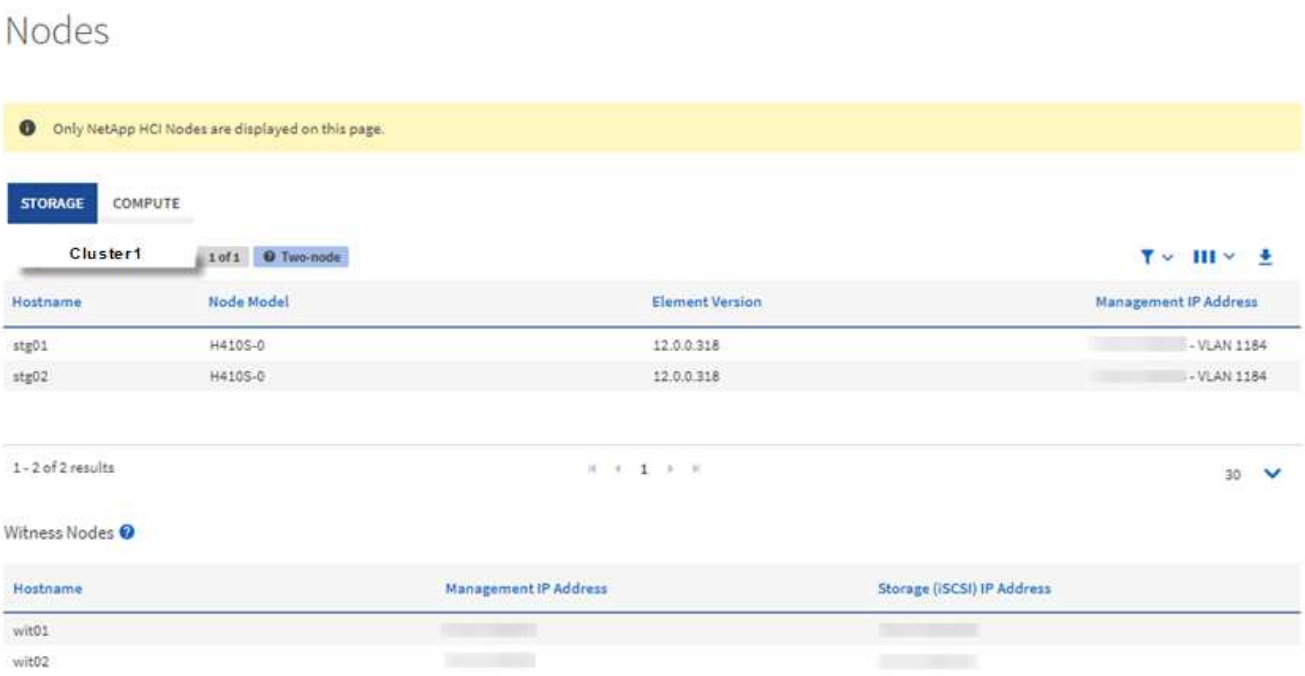
Puede ver información de almacenamiento de los sistemas de varios nodos. Si "dominios de protección personalizados" se asignan, puede ver qué dominios de protección se asignan a nodos específicos.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

   ```
   https://[management node IP address]
   ```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento all-flash SolidFire.
3. En la navegación de la izquierda, seleccione **Nodes**.



Cuando inicia una nueva sesión de control del cloud híbrido de NetApp por primera vez, es posible que haya un retraso en la carga de la página nodos de control del cloud híbrido de NetApp cuando el nodo de gestión gestiona muchos clústeres. El tiempo de carga varía en función del número de clústeres que gestiona el nodo de gestión activamente. Para lanzamientos posteriores, experimentará tiempos de carga más rápidos.

4. En la ficha **almacenamiento** de la página Nodes, revise la siguiente información:
   a. Clústeres de dos nodos: Aparece una etiqueta de “dos nodos” en la ficha almacenamiento y se muestran los nodos de testigos asociados.
   b. Clústeres de tres nodos: Se enumeran los nodos de almacenamiento y los nodos testigo asociados. Los clústeres de tres nodos tienen un nodo testigo puesto en marcha en espera para mantener la alta disponibilidad en caso de fallo del nodo.
   c. Clústeres con cuatro nodos o más: Se muestra información para los clústeres con cuatro o más nodos. Los nodos de testigos no se aplican. Si comenzó con dos o tres nodos de almacenamiento y añadió más nodos, los nodos testigos seguirán apareciendo. De lo contrario, la tabla de nodos de testigos no aparecerá.
   d. La versión del paquete de firmware: A partir de la versión 2.14 de los servicios de gestión, si los clústeres ejecutan Element 12.0 o una versión posterior, es posible ver la versión del paquete de firmware de estos clústeres. Si los nodos de un clúster tienen diferentes versiones de firmware en ellos, puede ver **multiple** en la columna **Versión de paquete de firmware**.
   e. Dominios de protección personalizados: Si en el clúster se usan dominios de protección personalizados, puede ver asignaciones de dominios de protección personalizadas para cada nodo del clúster. Si los dominios de protección personalizados no están habilitados, esta columna no aparece.
5. Puede manipular la información de estas páginas de varias maneras:
   a. Para filtrar la lista de elementos de los resultados, seleccione el icono **filtro** y seleccione los filtros. También puede introducir texto para el filtro.
   b. Para mostrar u ocultar columnas, seleccione el icono **Mostrar/ocultar columnas**.
   c. Para descargar la tabla, seleccione el icono **Descargar**.

Para ver el número de almacenamiento, observe la consola de control del cloud híbrido (HCC) de NetApp. Consulte "Supervise los recursos de almacenamiento con la consola HCC".

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Supervise los volúmenes en el clúster de almacenamiento de

El sistema SolidFire aprovisiona el almacenamiento mediante volúmenes. Los volúmenes son dispositivos de bloque a los que los clientes iSCSI o Fibre Channel acceden a través de la red. Es posible supervisar detalles sobre los grupos de acceso, las cuentas, los iniciadores, la capacidad utilizada, el estado de protección de datos de Snapshot, el número de sesiones iSCSI y la política de calidad de servicio asociada con el volumen.

También se pueden ver detalles sobre los volúmenes activos y eliminados.

Con esta vista, es posible que primero desee supervisar la columna capacidad utilizada.

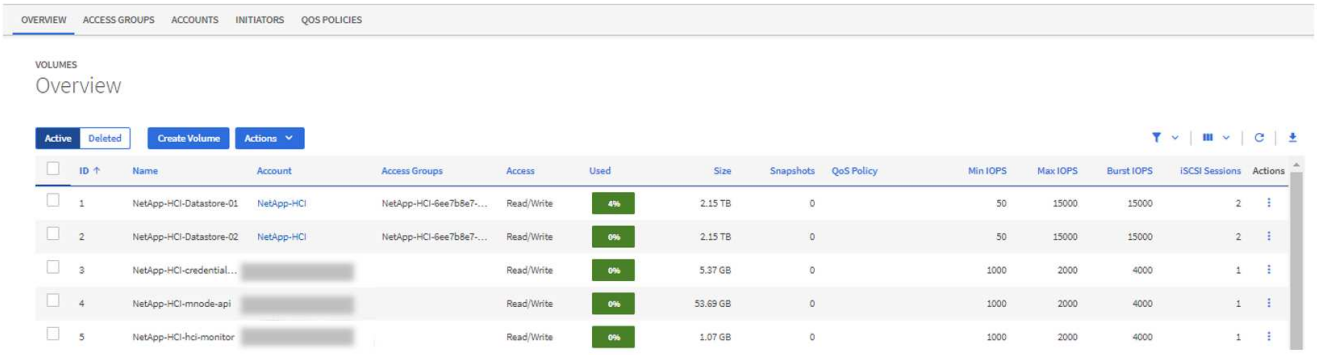
Solo puede acceder a esta información si tiene privilegios administrativos de Hybrid Cloud Control de NetApp.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://[management node IP address]
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento all-flash SolidFire.
3. En el cuadro azul de navegación de la izquierda, seleccione la instalación de almacenamiento all-flash de SolidFire.
4. En la navegación de la izquierda, seleccione el clúster y seleccione **almacenamiento** > **volúmenes**.



5. En la página Volumes, utilice las siguientes opciones:

a. Filtre los resultados seleccionando el icono **filtro**.

b. Oculte o muestre columnas seleccionando el icono **Ocultar/Mostrar**.

c. Actualice los datos seleccionando el icono **Actualizar**.

d. Descargue un archivo CSV seleccionando en el icono **Descargar**.

6. Supervise la columna capacidad utilizada. Si se alcanzan los umbrales Advertencia, error o crítico, el color representa el estado de capacidad utilizada:

a. Advertencia - Amarillo

b. Error: Naranja

c. Crítico: Rojo

7. En la vista Volumes, seleccione las pestañas para ver detalles adicionales sobre los volúmenes:

a. **Grupos de acceso**: Puede ver los grupos de acceso de volúmenes que están asignados de iniciadores a una colección de volúmenes para un acceso seguro.

Consulte la información acerca de "los grupos de acceso de volúmenes".

b. **Cuentas**: Puede ver las cuentas de usuario, que permiten a los clientes conectarse a volúmenes en un nodo. Cuando crea un volumen, este se asigna a una cuenta de usuario específica.

Consulte la información acerca de "Cuentas de usuario del sistema de almacenamiento all-flash SolidFire".

c. **Initiators**: Puede ver el IQN del iniciador iSCSI o los WWPN de Fibre Channel para el volumen. Cada IQN que se añade a un grupo de acceso puede acceder a cada volumen del grupo sin necesidad de contar con autenticación CHAP. Cada WWPN que se añade a un grupo de acceso habilita el acceso a la red de Fibre Channel a los volúmenes del grupo de acceso.

d. **Políticas de QoS**: Puede ver la política de QoS aplicada al volumen. Una política de calidad de servicio aplica ajustes estandarizados para IOPS mínimos, IOPS máximos y IOPS de ráfaga en varios volúmenes.

Consulte la información acerca de "Políticas de rendimiento y calidad de servicio".

Obtenga más información

- "Documentación de SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Recopile registros para solucionar problemas

Si tiene problemas con la instalación de su sistema de almacenamiento all-flash de SolidFire, puede recopilar registros para enviar al soporte de NetApp y ayudarle en el diagnóstico. Es posible usar NetApp Hybrid Cloud Control o la API REST para recoger registros en un sistema Element.

Lo que necesitará

- Asegúrese de que la versión del clúster de almacenamiento ejecute la versión 11.3 o posterior del software NetApp Element.
- Asegúrese de haber implementado un nodo de gestión que ejecuta la versión 11.3 o una versión posterior.

Opciones de recopilación de registros

Seleccione una de las siguientes opciones:

- Utilice el control del cloud híbrido de NetApp para recopilar registros
- Use la API DE REST para recoger registros

Utilice el control del cloud híbrido de NetApp para recopilar registros

Puede acceder al área de recogida de registros desde la consola de Cloud Control híbrido de NetApp.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

   ```
   https://[management node IP address]
   ```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
3. En el panel de control, seleccione el menú de la parte superior derecha.
4. Seleccione **recopilar registros**.

   Si recogió los registros antes, puede descargar el paquete de registros existente o iniciar una nueva recopilación de registros.

5. Seleccione un intervalo de fechas en el menú desplegable **intervalo de fechas** para especificar las fechas que deben incluir los registros.

   Si especifica una fecha de inicio personalizada, puede seleccionar la fecha para comenzar el rango de fechas. Los registros se recogerán a partir de esa fecha hasta la hora actual.

6. En la sección **Log Collection**, seleccione los tipos de archivos de registro que debe incluir el paquete de registro.

   Para los registros de almacenamiento, puede expandir la lista de nodos de almacenamiento y seleccionar nodos individuales para recopilar registros (o todos los nodos de la lista).

7. Seleccione **recopilar registros** para iniciar la recopilación de registros.

   La recogida de registros se ejecuta en segundo plano y la página muestra el progreso.

   > Dependiendo de los registros que recoja, la barra de progreso puede permanecer en un porcentaje determinado durante varios minutos o avanzar muy lentamente en algunos puntos.

8. Seleccione **Descargar registros** para descargar el paquete de registro.

Este paquete de registro está en un formato de archivo .tgz comprimido.

Use la API DE REST para recoger registros

Es posible usar la API DE REST para recoger registros de Element.

Pasos

1. Busque el ID del clúster de almacenamiento:
   a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

      ```
      https://[management node IP]/logs/1/
      ```

   b. Seleccione **autorizar** y complete lo siguiente:
      i. Introduzca el nombre de usuario y la contraseña del clúster.
      ii. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.
      iii. Seleccione **autorizar** para iniciar una sesión.
2. Recopilar registros de Element:
   a. Seleccione **POST /Bundle**.
   b. Seleccione **probar**.
   c. Cambie los valores de los siguientes parámetros en el campo **cuerpo de la solicitud** dependiendo del tipo de registros que necesite recopilar y del intervalo de tiempo:

Parámetro	Tipo	Descripción
`modifiedSince`	Cadena de fecha	Solo incluya los registros modificados después de esta fecha y hora. Por ejemplo, el valor "2020-07-14T20:19:00.000Z" define una fecha de inicio del 14 de julio de 2020 a las 20:19 UTC.
`mnodeLogs`	Booleano	Configure este parámetro en `true` para incluir los registros del nodo de gestión.
`storageCrashDumps`	Booleano	Configure este parámetro en `true` para incluir los registros de depuración de fallos del nodo de almacenamiento.
`storageLogs`	Booleano	Configure este parámetro en `true` para incluir los registros del nodo de almacenamiento.

Parámetro	Tipo	Descripción
`storageNodeIds`	Cabina de UUID	Si `storageLogs` se establece en `true`, Rellene este parámetro con los Id. De nodo del clúster de almacenamiento para limitar la colección de registros a esos nodos de almacenamiento específicos. Utilice la `GET https://[management node IP]/logs/1/bundle/options` Extremo para ver todos los posibles ID de nodo que puede utilizar.

d. Seleccione **Ejecutar** para iniciar la recopilación de registros. La respuesta debe devolver una respuesta similar a la siguiente:

```
{
  "_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. Compruebe el estado de la tarea de recopilación de registros:
   a. Seleccione **GET /Bundle**.
   b. Seleccione **probar**.
   c. Seleccione **Ejecutar** para devolver un estado de la tarea de recopilación.
   d. Desplácese hasta la parte inferior del cuerpo de respuesta.

      Debería ver un `percentComplete` atributo que detalla el progreso de la colección. Si la colección está completa, el `downloadLink` atributo contiene el enlace de descarga completo, incluido el nombre de archivo del paquete de registro.

   e. Copie el nombre del archivo al final del `downloadLink` atributo.
4. Descargue el paquete de registro recopilado:
   a. Seleccione **GET /Bundle/{filename}**.
   b. Seleccione **probar**.
   c. Pegue el nombre de archivo que copió anteriormente en la `filename` campo de texto de parámetros.
   d. Seleccione **Ejecutar**.

      Después de la ejecución, aparece un enlace de descarga en el área del cuerpo de respuesta.

   e. Seleccione **Descargar archivo** y guarde el archivo resultante en el equipo.

Este paquete de registro está en un formato de archivo .tgz comprimido.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Gestione el almacenamiento con la API de Element

Los clústeres de almacenamiento de Element se pueden gestionar mediante la API del software Element.

La API de Element se basa en el protocolo JSON-RPC a través de HTTPS. JSON-RPC es un protocolo RPC sencillo basado en texto que se basa en el formato ligero de intercambio de datos JSON. Las bibliotecas de clientes están disponibles para todos los principales lenguajes de programación.

- Acerca de la API del software Element
- Objetos comunes
- Métodos comunes
- Métodos de API de cuenta
- Métodos API de administrador
- Métodos de API de clúster
- Métodos API de creación de clúster
- Métodos de API de unidad
- Métodos de API de Fibre Channel
- Métodos de API del iniciador
- Métodos de API de LDAP
- Métodos de API de autenticación multifactor
- Métodos API de autenticación de sesión
- Métodos de API de nodo
- Métodos de API de replicación
- Métodos de API de seguridad
- Métodos de API de SnapMirror
- Métodos de la API de configuración del sistema
- Métodos de API de redes múltiples inquilinos
- Métodos de API de volumen
- Métodos API de grupo de acceso de volúmenes
- Métodos de API de Snapshot de volumen
- Métodos de API para volúmenes virtuales
- Control de acceso
- Ejemplos de respuestas

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Centro de documentación de SolidFire y el software Element"

Acerca de la API del software Element

La API de Element se basa en el protocolo JSON-RPC a través de HTTPS. JSON-RPC es un protocolo RPC sencillo basado en texto que se basa en el formato ligero de intercambio de datos JSON. Las bibliotecas de clientes están disponibles para todos los principales lenguajes de programación.

Puede realizar solicitudes de API a través de solicitudes HTTPS POSTERIORES al extremo de la API. El cuerpo de la solicitud POST es un objeto de solicitud JSON-RPC. Actualmente, la API no admite solicitudes por lotes (varios objetos de solicitud en UNA SOLA ENTRADA). Cuando envíe solicitudes de API, debe usar "Application/json-rpc" como el tipo de contenido de la solicitud y asegurarse de que el cuerpo no esté codificado en forma.

> La interfaz de usuario web de Element utiliza los métodos de API que se describen en este documento. Puede supervisar las operaciones de API en la interfaz de usuario habilitando el registro de API; esto permite ver los métodos que se emiten al sistema. Puede activar tanto las solicitudes como las respuestas para ver cómo responde el sistema a los métodos que se emiten.

A menos que se especifique lo contrario, todas las cadenas de fecha de las respuestas API tienen el formato UTC+0.

> Cuando el clúster de almacenamiento tiene una gran carga o envía muchas solicitudes de API consecutivas sin retrasos, puede que un método falle y devuelva el error "xDBVersionmismatch". Si esto ocurre, vuelva a intentar la llamada al método.

- Solicitar miembros de objeto
- Miembros del objeto de respuesta
- Extremos de solicitudes
- Autenticación API
- Métodos asíncronos
- Atributos

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Solicitar miembros de objeto

Cada solicitud de API del software Element tiene las siguientes partes básicas:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
método	Nombre del método que se va a invocar.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
parámetros	Objeto que contiene los parámetros del método que se está invocando. Los parámetros con nombre son necesarios. No se permiten parámetros posicionales (pasados como matriz).	Objeto JSON	{}	No
id	Identificador utilizado para hacer coincidir la solicitud con la respuesta, devuelto en el resultado.	cadena o entero	{}	No

Miembros del objeto de respuesta

Cada cuerpo de respuesta de API del software Element tiene las siguientes partes básicas:

Nombre	Descripción	Tipo
resultado	Objeto devuelto por el método. El sistema devuelve un objeto con miembros con nombre que corresponde al valor de retorno documentado del método. Este miembro no está presente si se ha producido un error.	Objeto JSON
error	El objeto devuelto cuando se produce un error. Este miembro sólo está presente si se ha producido un error.	Objeto
id	Identificador utilizado para hacer coincidir la solicitud con la respuesta, tal y como se indica en la solicitud.	cadena o entero

Nombre	Descripción	Tipo
Parámetros no usedParameters	Mensaje de advertencia de que al menos un parámetro incorrecto se ha pasado al método API y no se ha utilizado.	Objeto

Extremos de solicitudes

Existen tres tipos de extremos de solicitud utilizados en la API (clúster de almacenamiento, creación de clústeres de almacenamiento y por nodo). Siempre debe utilizar el extremo más reciente admitido por la versión del software Element.

Los tres extremos de solicitud de la API se designan de las siguientes formas:

Métodos de API de clúster

El extremo de HTTPS para solicitudes de API para todo el clúster de almacenamiento es `https://<mvip>/json-rpc/<api-version>`, donde:

- `<mvip>` Es la dirección IP virtual de gestión del clúster de almacenamiento.
- `<api-version>` Es la versión de la API que está usando.

Creación de clústeres y métodos API de bootstrap

El extremo de HTTPS para crear un clúster de almacenamiento y acceder a las solicitudes de la API de bootstrap es `https://<nodeIP>/json-rpc/<api-version>`, donde:

- `<nodeIP>` Es la dirección IP del nodo que va a añadir al clúster.
- `<api-version>` Es la versión de la API que está usando.

Métodos API por nodo

El extremo de HTTPS para solicitudes de API de nodo de almacenamiento individuales es `https://<nodeIP>:442/json-rpc/<api-version>`, donde:

- `<nodeIP>` Es la dirección IP de gestión del nodo de almacenamiento; 442 es el puerto en el que se ejecuta el servidor HTTPS.
- `<api-version>` Es la versión de la API que está usando.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Autenticación API

Puede autenticarse con el sistema cuando utilice la API incluyendo un encabezado de autenticación básica HTTP con todas las solicitudes de API. Si omite la información de

autenticación, el sistema rechaza la solicitud sin autenticar con una respuesta HTTP 401. El sistema es compatible con la autenticación básica de HTTP sobre TLS.

Use la cuenta de administrador de clúster para la autenticación API.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Métodos asíncronos

Algunos métodos API son asíncronos, lo que significa que es posible que la operación que realizan no se complete cuando se devuelve el método. Los métodos asíncronos devuelven un identificador al que se puede consultar para ver el estado de la operación. La información de estado de algunas operaciones puede incluir un porcentaje de la finalización.

Al consultar una operación asíncrona, el resultado puede ser uno de los siguientes tipos:

- `DriveAdd`: El sistema está agregando una unidad al clúster.
- `BulkVolume`: El sistema está realizando una operación de copia entre volúmenes, como una copia de seguridad o restauración.
- `Clone`: El sistema está clonando un volumen.
- `DriveRemoval`: El sistema está copiando datos de una unidad como preparación para eliminarla del clúster.
- `RtfiPendingNode`: El sistema está instalando software compatible en un nodo antes de agregarlo al clúster.

Tenga en cuenta los siguientes puntos cuando se utilizan métodos asíncronos o se obtiene el estado de una operación asíncrona en ejecución:

- Los métodos asíncronos se indican en la documentación de cada método.
- Los métodos asincrónicos devuelven un "'establish de la ley'", que es un identificador conocido por el método API de emisión. Puede usar el identificador para sondear el estado o el resultado de la operación asíncrona.
- Puede obtener el resultado de métodos asíncronos individuales con el método GetAsyncResult. Cuando utiliza GetAsyncResult para consultar una operación completada, el sistema devuelve el resultado y purga automáticamente el resultado del sistema. Cuando utiliza GetAsyncResult para consultar una operación incompleta, el sistema devuelve el resultado pero no lo purga.
- Puede obtener el estado y los resultados de todos los métodos asíncronos en ejecución o completados mediante el método ListAsyncResults. En este caso, el sistema no purga los resultados para las operaciones completadas.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Atributos

Muchas de las solicitudes y respuestas de API utilizan objetos, así como tipos simples. Los objetos son una colección de pares clave-valor, donde el valor es un tipo simple o posiblemente otro objeto. Los atributos son pares personalizados nombre-valor que puede establecer el usuario en objetos JSON. Algunos métodos permiten agregar atributos al crear o modificar objetos.

Hay un límite de 1000 bytes en los objetos de atributos codificados.

Miembro del objeto

Este objeto contiene el siguiente miembro:

Nombre	Descripción	Tipo
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON

Ejemplo de solicitud

En el siguiente ejemplo de solicitud se utiliza el método AddClusterAdmin:

```
{
   "method": "AddClusterAdmin",
   "params": {
      "username": "joeadmin",
      "password": "68!5Aru268)$",
      "access": [
         "volume",
         "reporting"
      ],
      "attributes": {
         "name1": "value1",
         "name2": "value2",
         "name3": "value3"
      }
   }
}
```

Objetos comunes

La API del software Element utiliza objetos JSON para representar conceptos de datos organizados. Muchos de estos métodos de API utilizan estos objetos para la entrada y salida de datos. Esta sección documenta estos objetos de uso común; los objetos que sólo se utilizan dentro de un único método se documentan con ese método en lugar de

hacerlo en esta sección.

- cuenta
- AuthSessionInfo
- BulkVolumeJob
- vinculación (volúmenes virtuales)
- Detalles del certificado
- clúster
- ClusterAdmin
- ClusterCapacity
- ClusterConfig
- ClusterInfo
- ClusterPair
- ClusterStats
- ClusterStructure
- unidad
- DriveStats
- error
- evento
- fallo
- Puerto de FiberChannelPort
- FipsErrorNodeReport
- FipsNodeReport
- FipsReport
- GroupSnapshot
- HardwareInfo
- host (volúmenes virtuales)
- IdpConfigInfo
- iniciador
- KeyProviderKmip
- KeyServerKmip
- LdapConfiguration
- LoggingServer
- red (interfaces unidas)
- red (todas las interfaces)
- Red (interfaces Ethernet)
- red (interfaces locales)
- Red (SNMP)

- NetworkInterface
- nodo
- ProtectionDomains de nodo
- Estadísticas de nodos
- OntapVersionInfo
- PendingActiveNode
- PendingNode
- ProtectionDomain
- ProtectionDomainLevel
- ProtectionDomainResiliency
- ProtectionDomainTolerance
- ProtectionSchemeResiliency
- ProtectionSchemeTolerance
- ProtocolEndpoint
- Calidad de servicio
- QoSPolicy
- RemoteClusterSnapshotStatus
- programación
- Sesión (Fibre Channel)
- Sesión (iSCSI)
- SnapMirrorAggregate
- SnapMirrorClusterIdentity
- SnapMirrorEndpoint
- SnapMirrorJobScheduleCronInfo
- SnapMirrorLunInfo
- SnapMirrorNetworkInterface
- SnapMirrorNode
- SnapMirrorPolicy
- SnapMirrorPolicyRule
- SnapMirrorRelationship
- SnapMirrorVolume
- SnapMirrorVolumeInfo
- SnapMirrorVServer
- SnapMirrorVserveragregateInfo
- snapshot
- SnmpTrapRecipient
- Contenedor de almacenamiento

- SyncJob
- tarea (volúmenes virtuales)
- UsumUsuario
- VirtualNetwork
- Volumen virtual
- volumen
- VolumeAccessGroup
- Pareja de volúmenes
- VolumeStats

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

cuenta

El objeto de la cuenta contiene información sobre una cuenta. Este objeto solo incluye información "configurada" sobre la cuenta, no información sobre el tiempo de ejecución ni el uso.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de cuenta	El ID de cuenta único de la cuenta.	entero
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON
EnableChap	Especifica si un iniciador puede utilizar las credenciales de la cuenta CHAP para acceder a volúmenes.	booleano
InitiatorSecret	El secreto CHAP del iniciador.	cadena

Nombre	Descripción	Tipo
estado	El estado actual de la cuenta. Los posibles valores son los siguientes: • Active: Una cuenta activa. • Locked: Una cuenta bloqueada. • Deleted: Una cuenta que se ha eliminado y purgado.	cadena
ID de almacenamiento ContainerID	El ID único del contenedor de almacenamiento de volumen virtual asociado con esta cuenta.	UUID
TargetSecret	El secreto CHAP de destino.	cadena
nombre de usuario	El nombre de usuario de la cuenta.	cadena
volúmenes	Una lista de ID de volumen para los volúmenes que pertenecen a esta cuenta.	matriz en números enteros

Obtenga más información

- AddAccount
- GetAccountByID
- GetAccountByName
- Cuentas de lista

AuthSessionInfo

El objeto authSessionInfo contiene información acerca de una sesión de autenticación.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
AccessGroupList	Lista de los grupos de acceso del usuario.	matriz de cadenas

Nombre	Descripción	Tipo
AuthMethod	El tipo de autorización que tiene el usuario administrador de clúster. Los posibles valores son los siguientes: • LDAP: Autenticado a través de LDAP. • Cluster: Se autentica mediante un nombre de usuario y una contraseña almacenados en la base de datos del clúster. • IDP: Se autentica a través de un proveedor de identidades de terceros.	cadena
ClusterAdminIDs	Lista de ID de administración de clúster asociados con esta sesión. En el caso de sesiones relacionadas con LDAP o un proveedor de identidades (IDP) de terceros, se tratará de una lista de administradores de clústeres que coincidan asociados a esta sesión.	matriz en números enteros
Tiempo de espera final	Hora en la que la sesión deja de ser válida.esto se establece cuando se crea la sesión y no se puede cambiar.	cadena
IdpConfigVersion	La versión de configuración de IDP cuando se creó la sesión.	entero
LastAccessTimeout	Hora en la que la sesión deja de ser válida debido a la inactividad.se establece en un nuevo valor cuando se accede a la sesión para su uso, hasta el momento en que la sesión no es válida debido a que se alcanza el tiempo de espera final.	cadena
SessionCreationTime	Hora en la que se crea la sesión.	cadena
SessionID	UUID para esta sesión.	UUID

Nombre	Descripción	Tipo
nombre de usuario	Nombre de usuario asociado a esta sesión. Para las sesiones relacionadas con LDAP, será el DN LDAP del usuario. Para las sesiones relacionadas con un IDP de terceros, se tratará de un par de nombre-valor arbitrario que se utilizará para operaciones de auditoría dentro de la sesión. No coincidirán necesariamente con el nombre de administrador de clúster en el clúster. Por ejemplo, un ID de nombre de sujeto de SAML,pero esto estará dictado por la configuración del IDP y el contenido resultante de la aserción SAML.	cadena

BulkVolumeJob

El objeto bulkVolumeJob contiene información sobre operaciones masivas de lectura o escritura de volúmenes, como la clonación o la creación de copias Snapshot.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	Atributo JSON del trabajo de volumen masivo.	Objeto JSON
ID de volumen	El ID de trabajo del volumen masivo interno.	entero
CreateTime	La Marca de hora se creó para el trabajo de volumen masivo en formato UTC+0.	Cadena de fecha ISO 8601
Elatiempo	El número de segundos desde que se inició el trabajo.	cadena
formato	El formato de la operación de volumen masivo. Los posibles valores son los siguientes: • nativo • sin comprimir	cadena

Nombre	Descripción	Tipo
clave	La clave única que crea la sesión de volumen masivo.	cadena
Porcentaje completado	Porcentaje completado informado por la operación.	entero
RemasterHora	El tiempo estimado que queda en segundos.	entero
SrcVolumeID	El ID del volumen de origen.	entero
estado	El estado de la operación. Los posibles valores son los siguientes: • preparando • ejecutando • completado • error	cadena
guión	El nombre del script, si se proporciona alguno.	cadena
ID de copia Snapshot	El ID de la copia de Snapshot si una copia de Snapshot se encuentra en el origen del trabajo de volumen masivo.	entero
tipo	El tipo de operación a granel. Los posibles valores son los siguientes: • lea • escritura	cadena

vinculación (volúmenes virtuales)

El objeto de vinculación contiene información acerca de la vinculación de un volumen virtual. Puede recuperar una lista de esta información de todos los volúmenes virtuales mediante el `ListVirtualVolumeBindings` Método API.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ProtocolEndpointID	El ID único del extremo de protocolo.	UUID
ProtocolEndpointInBandID	El scentNAADeviceID del extremo de protocolo.	cadena
ProtocolEndpointType	El tipo de extremo de protocolo. SCSI es el único valor que se devuelve para el tipo de extremo de protocolo.	cadena
VirtualVolumeBindingID	El ID único del objeto de vinculación de volúmenes virtuales.	entero
VirtualVolumeHostID	El ID único del host del volumen virtual.	UUID
ID de volumen virtual	El ID exclusivo del volumen virtual.	UUID
VirtualVolumeSecondaryID	El ID secundario del volumen virtual.	cadena

Obtenga más información

- ListVirtualVolumeBindings
- ProtocolEndpoint

Detalles del certificado

El objeto certificateDetails contiene la información descodificada acerca de un certificado de seguridad.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
emisor	El nombre del emisor.	cadena
módulo	El módulo de la clave pública.	cadena
NotAfter	La fecha de caducidad del certificado.	Cadena ISO 8601
NotBefore	La fecha de inicio del certificado.	Cadena ISO 8601

Nombre	Descripción	Tipo
serie	El número de serie del certificado.	cadena
Sha1Fingerprint	El resumen de la versión del certificado codificada CON DER.	cadena
asunto	El nombre del asunto.	cadena

clúster

El objeto de clúster contiene información que el nodo utiliza para comunicarse con el clúster. Esta información se puede recuperar con el método API GetClusterConfig.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
cipi	La interfaz de red que se utiliza para la comunicación del clúster.	cadena
clúster	Nombre de clúster único.	cadena
Cifrado Capable	Indica si el nodo admite el cifrado de unidades.	booleano
conjunto	Los nodos que participan en el clúster.	matriz de cadenas
Configuración de fipsDriveConfiguration	Indica si el nodo es compatible con unidades certificadas con FIPS 140-2.	booleano
mipi	La interfaz de red utilizada para la gestión de nodos.	cadena
nombre	El nombre del clúster.	cadena
NodeID	El ID de nodo del nodo en el clúster.	cadena
PendingNodeID	El ID del nodo pendiente en el clúster.	entero
función	Identifica el rol del nodo.	entero

Nombre	Descripción	Tipo
sipi	La interfaz de red utilizada para el tráfico de almacenamiento.	cadena
estado	El estado actual del nodo. Los posibles valores son los siguientes: • Available: El nodo no se ha configurado con un nombre de clúster. • Pending: El nodo está pendiente para un clúster con nombre específico y se puede añadir. • Active: El nodo es un miembro activo de un clúster y no se puede añadir a otro clúster. • PendingActive: El nodo se está revirtiendo a la imagen de software de fábrica y aún no es miembro activo de un clúster. Cuando finalice, se realizará la transición al estado Active.	cadena
versión	La versión del software que se ejecuta en el nodo.	cadena

Modificación de miembros y estados de nodo

Esta tabla indica si los parámetros del objeto se pueden modificar en cada estado de nodo posible.

Nombre del parámetro	Estado disponible	Estado pendiente	Estado activo
cipi	No	No	No
clúster	Sí	Sí	No
Cifrado Capable	No	No	No
conjunto	No	No	No
mipi	Sí	Sí	No
nombre	Sí	Sí	Sí
NodeID	No	No	No

PendingNodeID	No	No	No
función	No	No	No
sipi	No	No	No
estado	No	No	No
versión	No	No	No

Obtenga más información

GetClusterConfig

ClusterAdmin

El objeto clusterAdmin contiene información acerca del usuario administrador actual del clúster. Puede recuperar información del usuario administrador con el método API GetCurrentClusterAdmin.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
acceso	Los métodos que puede utilizar este administrador de clúster.	matriz de cadenas
AuthMethod	El tipo de autorización que tiene el usuario administrador de clúster. Los posibles valores son los siguientes: • LDAP • Clúster • Local	cadena
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON
ClusterAdminID	El ID de administrador de clúster para este usuario administrador de clúster.	entero
nombre de usuario	Nombre de usuario para este administrador de clúster.	cadena

Obtenga más información

GetCurrentClusterAdmin

ClusterCapacity

El objeto clusterCapacity contiene mediciones de capacidad de alto nivel para el clúster. Es posible obtener información sobre la capacidad de clúster con el método API GetClusterCapacity. Las mediciones de espacio en los miembros del objeto se calculan en bytes.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ActiveBlockSpace	La cantidad de espacio en las unidades de bloques. Esto incluye información adicional, como entradas de metadatos y espacio que se puede limpiar.	entero
ActiveSessions	El número de sesiones iSCSI activas que se comunican con el clúster.	entero
AverageIOPS	El IOPS promedio para el clúster desde la hora universal coordinada (UTC) de la medianoche.	entero
ClusterRecentIOSize	El tamaño promedio de IOPS para todos los volúmenes del clúster.	entero
IOPS actuales	El IOPS promedio para todos los volúmenes del clúster durante los últimos 5 segundos.	entero
IOPS	La funcionalidad máxima estimada de IOPS del clúster actual.	entero

Nombre	Descripción	Tipo
MaxOverProvisionableSpace	La cantidad máxima de espacio de aprovisionamiento. Se trata de un valor calculado. No puede crear volúmenes nuevos si el espacio actual aprovisionado más el tamaño del nuevo volumen supera este número. El valor se calcula de la siguiente forma: `maxOverProvisionableSpace = maxProvisionedSpace * maxMetadataOverProvisionFactor`	entero
MaxProvisionedSpace	La cantidad total de espacio de aprovisionamiento si todos los volúmenes están llenos del 100% (sin metadatos de thin provisioning).	entero
MaxUsedMetadataSpace	La cantidad de bytes en las unidades de volúmenes que se usan para almacenar metadatos.	entero
MaxUsedSpace	La cantidad total de espacio en todas las unidades de bloques activas.	entero
No ZeroBlock	El número total de bloques de 4 KiB con datos después de haber completado la última operación de recopilación de basura.	entero
PeakActiveSessions	El número máximo de conexiones iSCSI desde la medianoche UTC.	entero
PeakIOPS	El valor más alto para IOPS actuales desde la medianoche de UTC.	entero
AprovisionadoSpace	La cantidad total de espacio aprovisionado en todos los volúmenes del clúster.	entero
fecha/hora	La fecha y la hora, en formato UTC+0, que se tomó esta muestra de capacidad de clúster.	Cadena ISO 8601

Nombre	Descripción	Tipo
TotalOps	La cantidad total de operaciones de I/o realizadas a lo largo de la vida útil del clúster.	entero
Juniorescandados	La cantidad total de bloques almacenados en las unidades de bloques. El valor incluye bloques replicados.	entero
UniqueBlocksUsedSpace	La cantidad total de datos que los uniqueBlocks tienen en las unidades de bloques. Consulte el método GetClusterCapacity para obtener información sobre la relación de este número con el valor unidoBlocks.	entero
UsedMetadataSpace	La cantidad total de bytes en las unidades de volúmenes que se usan para almacenar metadatos.	entero
UsedMetadataSpaceInSnapshots	La cantidad de bytes en unidades de volúmenes que se usan para almacenar datos únicos en las Snapshot. Este número calcula la cantidad de espacio de metadatos que se recuperaría si se eliminaran todas las instantáneas del sistema.	entero
UsedSpace	La cantidad total de espacio usado por todas las unidades de bloques del sistema.	entero
Cierres de ceros	El número total de bloques vacíos de 4 KiB sin datos después de haber completado la última ronda de recopilación de basura.	entero

Obtenga más información

GetClusterCapacity

ClusterConfig

El objeto ClusterConfig muestra información que el nodo utiliza para comunicarse con el clúster.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
cipi	La interfaz de red que se utiliza para la comunicación del clúster.	cadena
clúster	El nombre único del clúster.	cadena
Cifrado Capable	Especifica si el nodo admite cifrado.	booleano
conjunto	Los nodos que participan en el clúster.	matriz de cadenas
Configuración de fipsDriveConfiguration	Especifica si el nodo es compatible con unidades certificadas con FIPS 140-2.	booleano
HasLocalAdmin	Especifica si el clúster tiene un administrador local.	booleano
mipi	La interfaz de red utilizada para la gestión de nodos.	cadena
nombre	Identificador único del clúster.	cadena
NodeID	Identificador único del nodo.	entero
PendingNodeID	Identificador único del nodo pendiente.	entero
función	Identifica el rol del nodo.	cadena
sipi	La interfaz de red que se utiliza para el almacenamiento.	cadena
estado	Indica el estado del nodo.	cadena
versión	Indica la versión del nodo.	cadena

ClusterInfo

El objeto clusterInfo contiene información que el nodo utiliza para comunicarse con el clúster. Esta información se puede obtener con el método API GetClusterInfo.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON
DefaultProtectionScheme	El esquema de protección utilizado de forma predeterminada para volúmenes nuevos, a menos que se proporcione un esquema de protección con la CreateVolume llamada a método. Este esquema de protección debe estar siempre en el conjunto de esquemas de protección habilitados.	cadena
EnabledProtectionSchemes	Una lista de todos los esquemas de protección que se han habilitado en este clúster de almacenamiento.	matriz de cadenas
EncryptionAtRestState	El estado de la función Encryption at Rest. Los posibles valores son los siguientes: • Enabling: La opción Encryption at Rest se está habilitando. • Enabled: La opción Encryption at Rest está habilitada. • Disabling: La opción Encryption at Rest se está deshabilitando. • Disabled: La opción Encryption at Rest está deshabilitada.	cadena
conjunto	Los nodos que participan en el clúster.	matriz de cadenas
mivip	La dirección IP flotante (virtual) del clúster en la red de gestión.	cadena
MvipInterface	La interfaz física asociada con la dirección MVIP.	cadena
MvipNodeID	El nodo que contiene la dirección MVIP maestra.	entero

Nombre	Descripción	Tipo
MvipVlanTag	El identificador de VLAN de la dirección MVIP.	cadena
nombre	El nombre de clúster único.	cadena
RepCount	El número de réplicas de cada elemento de datos que se va a almacenar en el clúster. El valor válido es "2".	entero
Cifrar softwareAtRestState	Estado de cifrado basado en software en reposo.	cadena
SupportedProtectionSchemes	Una lista de todos los esquemas de protección que admiten este clúster de almacenamiento.	matriz de cadenas
svip	La dirección IP flotante (virtual) del clúster en la red de almacenamiento (iSCSI).	cadena
SvipInterface	La interfaz física asociada con la dirección SVIP maestra.	cadena
SvipNodeID	El nodo que contiene la dirección SVIP maestra.	entero
SvipVlanTag	El identificador de VLAN para la dirección SVIP maestra.	cadena
UniqueID	El ID único del clúster.	cadena
uuid	El identificador único del clúster.	UUID

Obtenga más información

- "GetClusterInfo"
- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

ClusterPair

El objeto clusterPair contiene información acerca de los clústeres emparejados con el clúster local. Se puede recuperar una lista de objetos clusterPair para el clúster local con el método ListClusterPairs.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Nombre del clúster	El nombre del otro clúster de la pareja.	cadena
ClusterPairID	Un ID único que se otorga a cada clúster en la pareja.	entero
ClusterPairUUID	El identificador único universal de la pareja de clústeres.	cadena
UUID	Identificador único del clúster remoto de la pareja de clústeres.	entero
latencia	La latencia, en milisegundos, entre clústeres.	entero
mivip	La dirección IP de la conexión de gestión para los clústeres emparejados.	cadena
estado	El estado de la conexión entre los clústeres emparejados. Los posibles valores son los siguientes: • Sin configurar • Conectado • Mal configurado • Desconectado	cadena
versión	La versión de Element del otro clúster en la pareja.	cadena

Obtenga más información

ListClusterPairs

ClusterStats

El objeto clusterStats contiene datos estadísticos para un clúster. Muchas de las estadísticas relacionadas con volúmenes que contiene el objeto presentan un promedio para todos los volúmenes del clúster. Puede usar el método GetClusterStats para recuperar esta información de un clúster.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Cálculo	Tipo
Actuales de IOPS	IOPS real actual para el clúster completo en los últimos 500 milisegundos.	Momento específico	entero
AverageIOPSize	Tamaño promedio en bytes de I/o reciente en el clúster en los últimos 500 milisegundos.	Momento específico	entero
Profundidad de clientQueueDepth	Número de operaciones de lectura y escritura pendientes en el clúster.	N.A.	entero
ClusterUtilización	El porcentaje de IOPS máximo del clúster que se está utilizando actualmente. Esto se computa como clusterUtilización = normalizedIOPS / maxIOPS (de GetClusterCapacity).	N.A.	flotante
LatencyUSec	El tiempo medio, en microsegundos, para completar operaciones a un clúster en los últimos 500 milisegundos.	Momento específico	entero
IOPS normalizadas	Número medio de IOPS para todo el clúster en los últimos 500 milisegundos.	Momento específico	entero
ReadBytes	Los bytes acumulativos totales leídos en el clúster desde la creación del clúster.	El incremento monotónicamente	entero
ReadBytesLastSample	La cantidad total de bytes leídos del clúster durante el último período de muestra.	Momento específico	entero

Nombre	Descripción	Cálculo	Tipo
ReadLatencyUSec	El tiempo medio, en microsegundos, para completar operaciones de lectura del clúster en los últimos 500 milisegundos.	Momento específico	entero
ReadLatencyUSectotal	El tiempo total dedicado a realizar operaciones de lectura desde la creación del clúster.	El incremento monotónicamente	entero
Operaciones de lectura	Las operaciones de lectura acumulativas totales en el clúster desde la creación del clúster.	El incremento monotónicamente	entero
ReadOpsLastSample	La cantidad total de operaciones de lectura durante el último periodo de muestra.	Momento específico	entero
SamplePeriodSec	La duración del período de la muestra, en milisegundos.	N.A.	entero
Servicios Count	El número de servicios que se ejecutan en el clúster. Si es igual a los servicios total, indica que se han recopilado estadísticas válidas de todos los nodos.	Momento específico	entero
Servicios totales	El número total de servicios esperados que se ejecutan en el clúster.	N.A.	entero
fecha/hora	La hora actual en formato UTC+0.	N.A.	Cadena de fecha ISO 8601
UnaligedReads	Las operaciones de lectura acumulativas totales no alineadas a un clúster desde la creación del clúster.	El incremento monotónicamente	entero

Nombre	Descripción	Cálculo	Tipo
UnaligedWrites	Las operaciones de escritura acumulativas totales no alineadas en un clúster desde la creación del clúster.	El incremento monotónicamente	entero
Bytes de escritura	Los bytes acumulativos totales escritos en el clúster desde la creación del clúster.	El incremento monotónicamente	entero
WriteBytesLastSample	La cantidad total de bytes escritos en el clúster durante el último período de muestra.	El incremento monotónicamente	entero
WriteLatencyUSec	El tiempo medio, en microsegundos, para completar operaciones de escritura a un clúster en los últimos 500 milisegundos.	Momento específico	entero
WriteLatencyUSectotal	El tiempo total dedicado a realizar operaciones de escritura desde la creación del clúster.	El incremento monotónicamente	entero
Operaciones de escritura	Las operaciones de escritura acumulativas totales en el clúster desde la creación del clúster.	El incremento monotónicamente	entero
WriteOpsLastSample	La cantidad total de operaciones de escritura durante el último periodo de muestra.	Momento específico	entero

Obtenga más información

GetClusterStats

ClusterStructure

El objeto clusterStructure contiene información de backup de configuración del clúster creada por el método GetClusterStructure. Puede utilizar el método SetClusterStructure para restaurar esta información en un clúster de almacenamiento que está reconstruyendo.

Miembros de objeto

Este objeto contiene la información de retorno combinada de los siguientes métodos:

- GetClusterInfo
- Cuentas de lista
- ListInitiators
- ListVolumes (Con includeVirtualVolumes=false)
- ListVolumeAccessGroups
- ListStorageContainers
- ListQoSPolicies
- GetSnmpInfo
- GetNtpInfo
- ListVirtualNetworks
- ListClusterAdmins
- ListSchedules
- ListSnapMirrorEndpoints
- GetFeatureStatus
- GetLdapConfiguration
- GetRemoteLoggingHosts
- GetDefaultQoS
- GetVolumeAccessGroupLunAssignments

Obtenga más información

- GetClusterStructure
- SetClusterStructure

unidad

El objeto de la unidad contiene información sobre las unidades individuales de los nodos activos del clúster. Este objeto contiene detalles sobre las unidades que se añadieron como metadatos de volúmenes o unidades de bloques, así como las unidades que todavía no se han añadido y están disponibles. Puede recuperar esta información con `ListDrives` Método API.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	La lista de pares nombre-valor en el formato de objetos JSON. Este objeto siempre es nulo y no se puede modificar.	Objeto JSON
capacidad	La capacidad total de la unidad, en bytes.	entero
Ranura de asistencia	En el caso de las plataformas HCI, este valor es la letra del nodo y el número de ranura en el chasis del servidor donde está ubicada esta unidad. En el caso de las plataformas de almacenamiento, el número de ranura es una representación de cadena del entero de "ranura".	cadena
DriveFailureDetail	Si el estado de una unidad es "Failed", este campo ofrece más detalles sobre por qué se marcó el error de la unidad.	cadena
ID de unidad	El ID de esta unidad.	entero
DriveSecurityFaultCausa	Si se habilita o se deshabilita la seguridad de la unidad con errores, el motivo por el que falló. Si el valor es "none", no se ha producido ningún error.	cadena
ID de clave	El ID de clave utilizado por el proveedor de claves para adquirir la clave de autenticación para desbloquear esta unidad.	UUID
KeyProviderID	Identifica el proveedor de la clave de autenticación para desbloquear esta unidad.	entero
NodeID	El ID del nodo que contiene esta unidad.	entero
Segmento Tamaño del archivo	El tamaño del archivo de segmento de la unidad, en bytes.	entero
serie	El número de serie de la unidad.	cadena

Nombre	Descripción	Tipo
ranura	El número de ranura en el chasis del servidor donde se encuentra esta unidad, o -1 si se utiliza un dispositivo SATADimm para la unidad de metadatos interna.	entero
estado	El estado de la unidad. Los posibles valores son los siguientes: • Available: Unidad disponible. • Active: Una unidad activa. • Erasing: Unidad que se está borrando de forma segura. Todos los datos de esa unidad se están quitando de forma permanente. • Failed: Unidad con errores. Todos los datos que anteriormente estuvieron en la unidad se migraron a otras unidades del clúster. • Removing: Unidad que se está quitando. Todos los datos que anteriormente estuvieron en la unidad se están migrando a otras unidades del clúster.	cadena
tipo	El tipo de unidad. Los posibles valores son los siguientes: • Volume: Almacena metadatos del volumen. • Bloque: Almacena datos de bloques. • Unknown: El tipo de unidad todavía no está activo y aún no se ha determinado.	cadena
UsableCapacity	La capacidad utilizable de la unidad, en bytes.	entero

Obtenga más información

ListDrives

DriveStats

El objeto driveStats contiene mediciones de actividad de alto nivel para una sola unidad. Con el método API, puede recuperar la información de medición `GetDriveStats`.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ActiveSessions	Cantidad de sesiones iSCSI que actualmente utilizan esta unidad (solo está presente para unidades de metadatos).	entero
ID de unidad	El ID único de la unidad en el clúster.	entero
FailedDieCount	Número de elementos de hardware de unidad con fallos.	entero
IosInProgress	La cantidad de I/O de esta unidad que se encuentran en curso.	entero
VidaRemainPercent	Indicador de desgaste de los medios de la unidad.	entero
Salvavidas ReadBytes	Los bytes totales que se leen en esta unidad durante la vida útil de la unidad.	entero
Salvavidas WriteBytes	Bytes totales escritos en esta unidad durante la vida útil de la unidad.	entero
PowerOnHours	Número de horas en las que se encendió esta unidad.	entero
lecturas	El número de llamadas de lectura () por segundo a esta unidad.	entero
ReadBytes	Bytes totales leídos desde la unidad debido a operaciones del cliente.	entero

Nombre	Descripción	Tipo
ReadsCombined	El número de llamadas read() a sectores adyacentes que podrían combinarse en una lectura más grande.	entero
ReadMseg	Núm. De milisegundos que se han empleado en la lectura.	entero
Operaciones de lectura	Operaciones de lectura totales en la unidad debido a operaciones de cliente.	entero
Agentes de propiedad	Número de sectores defectuosos sustituidos en esta unidad.	entero
ReserveCapacidadPercent	La capacidad de reserva disponible de la unidad.	entero
fecha/hora	La hora actual en formato UTC+0.	Cadena de fecha ISO 8601
Capacidad total	La capacidad total de la unidad, en bytes.	entero
Errores sin correcttableErrors	El valor de errores no corregibles del sistema DE supervisión automática, análisis y tecnología de informes (SMART) de la unidad.	entero
UsedCapacity	La capacidad en bytes utilizada de la unidad.	entero
Memoria usedMemory	Cantidad de memoria que actualmente utiliza el nodo que aloja esta unidad.	entero
escrituras	El número de llamadas write() por segundo a esta unidad.	entero
Bytes de escritura	Bytes totales escritos en la unidad debido a la actividad del cliente.	entero
WritesCombined	El número de llamadas write() a sectores adyacentes que podrían combinarse en una escritura más grande.	entero

Nombre	Descripción	Tipo
Escritura en segundo plano	Número de milisegundos dedicados a escribir.	entero
Operaciones de escritura	Operaciones de escritura totales en la unidad debido a la actividad de cliente.	entero

Obtenga más información

GetDriveStats

error

El objeto de error contiene un código de error y un mensaje si se produce un error durante una llamada al método. Todos los errores generados por el sistema tienen un código de error 500.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
codificación	Código numérico utilizado para identificar el error. Todos los errores generados por el sistema devuelven un código de 500.	entero
nombre	El identificador único para el error específico que se ha producido. Cada método devuelve un conjunto documentado de errores, aunque también debería estar preparado para tratar errores no reconocidos.	cadena
mensaje	Una descripción del error, posiblemente con detalles adicionales.	cadena

evento

El objeto event contiene detalles de los eventos que ocurren durante una llamada a un método API o mientras el sistema está realizando una operación.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
detalles	Información adicional sobre el evento.	Objeto JSON
ID de unidad	El ID de unidad de la unidad que notifica el fallo. 0 si no corresponde.	entero
ID de unidad	Una lista de los identificadores de unidades que notifican el fallo. Una lista vacía si no es aplicable.	matriz en números enteros
EventID	ID exclusivo asociado con cada evento.	entero
EventInfoType	El tipo de fallo.	cadena
mensaje	Descripción de cadena del evento que se ha producido.	cadena
NodeID	El ID de nodo del nodo que informa del error. 0 si no corresponde.	entero
ID de servicio	El ID de servicio del servicio que informa del error. 0 si no corresponde.	entero
gravedad	Gravedad el evento es el informe.	entero
TimeOfPublish	La hora en la que el registro de eventos del clúster recibió el evento, en formato UTC+0.	Cadena de fecha ISO 8601
TimeOfReport	La hora en la que ocurrió el evento en el clúster, en formato UTC+0.	Cadena de fecha ISO 8601

Nota: puede haber una ligera diferencia entre timeOfReport y timeOfPublish si el evento se ha producido y no se ha podido publicar inmediatamente.

Tipos de evento

La siguiente lista describe los posibles tipos de sucesos que puede contener el miembro eventInfoType:

- ApiEvent: Eventos iniciados a través de la API o la interfaz de usuario web que modifican la configuración.
- BinAssignmentEvent: Eventos relacionados con la asignación de datos a contenedores internos.
- BinSyncEvent: Eventos relacionados con una reasignación de datos entre servicios de bloques.
- BsCheckEvent: Eventos relacionados con comprobaciones de servicio de bloqueo.

- BsKillEvent: Eventos relacionados con terminaciones de servicios de bloques.
- BulkOpEvent: Eventos que funcionan en todo un volumen, como un backup de volumen, una restauración, una copia de Snapshot o un clon.
- ClonEvent: Eventos relacionados con la clonación de volúmenes.
- ClusterMasterEvent: Eventos de cambio en la configuración del clúster, como agregar o eliminar nodos.
- DataEvent: Eventos relacionados con la lectura y la escritura de datos.
- DbEvent: Eventos relacionados con la base de datos del nodo del conjunto.
- DriveEvent: Eventos relacionados con las operaciones de unidades.
- EncryptionAtRestEvent: Eventos relacionados con el cifrado de datos almacenados.
- EnsembleEvent: Eventos relacionados con el aumento o la disminución del tamaño del conjunto.
- FiberChannelEvent: Eventos relacionados con la configuración o conexiones del nodo Fibre Channel.
- GcEvent: Eventos relacionados con la recolección de basura. Estos procesos se ejecutan cada 60 minutos para reclamar almacenamiento en las unidades de bloques.
- IeEvent: Eventos relacionados con errores internos del sistema.
- InstallEvent: Eevnts relacionados con la instalación automática de software en nodos de almacenamiento pendientes.
- ISCSIEvent: Eventos relacionados con problemas de configuración o conexión iSCSI.
- LimitEvent: Eventos relacionados con el número de volúmenes o volúmenes virtuales en una cuenta o en el clúster que se acercan al máximo permitido.
- NetworkEvent: Eventos relacionados con redes virtuales.
- PlatformHardwarwareEvent: Eventos relacionados con problemas detectados en dispositivos de hardware.
- RemoteClusterEvent: Eventos relacionados con el emparejamiento de clústeres remotos.
- SchedulerEvent: Eventos relacionados con las capturas programadas.
- ServiceEvent: Eventos relacionados con el estado del servicio del sistema.
- StatEvent: Eventos relacionados con las estadísticas del sistema.
- SliceEvent: Eventos relacionados con el almacenamiento de metadatos.
- SnmpTrapEvent: Eventos relacionados con las capturas SNMP.
- TsEvent: Eventos del servicio de transporte del sistema.
- InmaculedException: Eventos relacionados con errores inesperados.
- VasaProviderEvent: Eventos relacionados con un proveedor VASA de VMware.

Obtenga más información

ListEvents

fallo

El objeto de fallo contiene información acerca de los errores que se han detectado en el clúster. La `ListClusterFaults` método devuelve información de errores del clúster.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ClusterFaultID	El ID único asociado con cada error de clúster.	entero
codificación	El código de avería del fallo específico detectado. Para obtener más información, consulte códigos de avería del clúster.	cadena
sql server	Información adicional específica de la avería.	Objeto JSON
fecha	La hora actual en formato UTC+0.	Cadena ISO 8601
detalles	La descripción del error con detalles adicionales.	cadena
ID de unidad	El primer ID de unidad de la lista driveIDs. Si la lista driveIDs está vacía (lo que significa que no se han devuelto errores que tratan con las unidades), este valor es 0.	entero
ID de unidad	Una lista de valores de DriveID para las unidades a las que hace referencia este error. Se incluye para fallos de manejo de unidades. Si no lo hace, se trata de una matriz vacía.	matriz en números enteros
NodeHardwarfwareFID	El identificador asignado a un error de hardware en el clúster.	entero
NodeID	El ID de nodo para el nodo al que hace referencia este error. Se incluye para los errores de nodo y de unidad; de lo contrario se establece como 0.	entero
resuelto	El estado resuelto del error. Los posibles valores son los siguientes: • True: El fallo ya no se detecta. • Falso: El fallo persiste.	booleano

Nombre	Descripción	Tipo
ResolvedDate	La fecha y la hora en la que se resolvió el error.	Cadena ISO 8601
ID de servicio	El servicio asociado al error. Este valor es "0" (cero) si el fallo no se asocia con un servicio.	entero
gravedad	La gravedad del error. Los posibles valores son los siguientes: • Warning: Un problema menor. El clúster está funcionando y las actualizaciones se permiten en este nivel de gravedad. • Error: Un error que generalmente no debe afectar al servicio (excepto la posible degradación del rendimiento o la pérdida de alta disponibilidad). Es posible que algunas funciones estén deshabilitadas. • Critical: Un error grave que afecta el servicio. El sistema no es capaz de atender las solicitudes de la API o I/o del cliente y está en riesgo de pérdida de datos. • BestPractice: Errores activados por una configuración del sistema sub-óptima.	cadena
tipo	El tipo de fallo. Los posibles valores son los siguientes: • Node: Error que afecta a un nodo en su totalidad. • Drive: Un error que afecta a una unidad individual. • Cluster: Un error que afecta a todo el clúster. • Service: Error que afecta a un servicio del clúster. • Volume: Un error que afecta a un volumen individual.	cadena

Obtenga más información

- ListClusterFaults
- "códigos de error de clúster"

Puerto de FiberChannelPort

El objeto FiberChannelPort contiene información acerca de los puertos individuales de un nodo o de un nodo entero del clúster. Puede recuperar esta información mediante `ListNodeFibreChannelPortInfo` método.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
firmware	La versión del firmware instalado en el puerto Fibre Channel.	entero
HBAPORT	El ID del puerto de adaptador de bus de host (HBA) individual.	entero
modelo	Modelo del HBA en el puerto.	cadena
NPortID	El ID único de nodo del puerto.	cadena
Pcigot	La ranura que contiene la tarjeta PCI en el chasis del nodo Fibre Channel.	entero
serie	El número de serie en el puerto Fibre Channel.	cadena
velocidad	La velocidad del HBA en el puerto.	cadena

Nombre	Descripción	Tipo
estado	Los posibles valores son los siguientes: • Desconocido • No disponible • En línea • Sin conexión • Bloqueado • Omitida • Diagnóstico • Linkdown • Error • Bucle invertido • Eliminado	cadena
Interruptor Wwn	El nombre World Wide Name del puerto del switch Fibre Channel.	cadena
wwnn	Nombre de nodo WWNN del nodo HBA.	cadena
wwpn	Nombre de puerto WWPN asignado al puerto físico del HBA.	cadena

Obtenga más información

ListNodeFiberChannelPortInfo

FipsErrorNodeReport

El objeto fipsErrorNodeReport contiene información de errores para cada nodo que no responde con información sobre la compatibilidad con FIPS 140-2 cuando se consulta con la `GetFipsReport` método.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
NodeID	El ID del nodo que no responde.	entero

Nombre	Descripción	Tipo
error	Un objeto JSON que contiene información sobre los errores.	Objeto JSON

FipsNodeReport

El objeto fipsNodeReport contiene información sobre la compatibilidad con FIPS 140-2 para un único nodo del clúster de almacenamiento. Puede recuperar esta información mediante `GetFipsReport` método.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
NodeID	El ID del nodo que informa de la información.	entero
PsDrives	Si el cifrado de unidades FIPS 140-2 está habilitado para este nodo o no. Los posibles valores son los siguientes: • None: Este nodo no es compatible con el cifrado de unidades FIPS. • Parcial: El nodo puede cifrar unidades FIPS, pero no todas las unidades presentes son unidades compatibles con FIPS. • Ready: El nodo es capaz de cifrar unidades FIPS y todas las unidades presentes son unidades compatibles con FIPS, o no hay unidades presentes.	FipsDrivesStatusType
Activa	Si el cifrado HTTPS FIPS 140-2 está habilitado para este nodo o no. Los posibles valores son los siguientes: • true: habilitado • false: desactivado	booleano

FipsReport

El objeto fipsReport contiene información acerca de la compatibilidad con FIPS 140-2 para todos los nodos del clúster de almacenamiento. Puede recuperar esta información mediante `GetFipsReport` método.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
nodos	Un informe sobre el estado de soporte de FIPS 140-2 para cada nodo del clúster de almacenamiento.	FipsNodeReport
ErrorNodes	Información de errores de cada nodo que no responde con el estado de soporte de FIPS 140-2-2.	FipsErrorNodeReport

GroupSnapshot

El objeto groupSnapshot contiene información sobre una snapshot de un grupo de volúmenes. Puede utilizar el `ListGroupSnapshots` Método API para recuperar la información de la snapshot de grupo.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON
CreateTime	El día y la hora con formato UTC+0 donde se creó la snapshot de grupo.	Cadena de fecha ISO 8601
EnableRemoteReplication	Identifica si la snapshot está habilitada para la replicación remota.	booleano
GroupSnapshotID	El ID único de la copia de Snapshot de grupo.	entero
GroupSnapshotUUID	El UUID de la snapshot de grupo.	cadena

Nombre	Descripción	Tipo
miembros	Una cabina de objetos que contienen información sobre cada miembro de la snapshot de grupo.	snapshot cabina
nombre	El nombre de la copia de Snapshot de grupo, o, si no se dio ninguna, el día y la hora con formato UTC en que se creó la copia de Snapshot.	Cadena o cadena de fecha ISO 8601
RemoteStatuses	Una cabina que contiene el identificador universal y el estado de replicación de cada snapshot remota en el clúster de destino como se ve en el clúster de origen.	RemoteClusterSnapshotStatus cabina
estado	Estado actual de la copia de Snapshot de grupo. Los posibles valores son los siguientes: • Unknown: Se produjo un error al obtener el estado de la snapshot. • Preparing: Esta copia de Snapshot se está preparando para poder usarla y aún no se puede escribir en ella. • RemoteSyncing: Esta snapshot se está replicando desde un clúster remoto. • Done: Esta snapshot se ha terminado de preparar o replicar y se puede usar. • Active: Esta copia de Snapshot es la rama activa. • Clonación: Esta instantánea está involucrada en una operación de copia de volumen.	cadena

Obtenga más información

ListGroupSnapshots

HardwareInfo

El objeto hardwareInfo contiene información detallada sobre el hardware y el estado de

cada nodo del clúster. Puede recuperar esta información con `GetHardwareInfo` Método API.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Serie de juntas	El número de serie de la placa DMI.	cadena
autobús	Información del bus multimedia de la placa base.	Objeto JSON
Serie de chassis	El número de serie del chasis.	cadena
Drivehardware	Una lista de información de cada unidad del nodo.	Cabina de objetos JSON
FiberChannelPorts	Una lista de los puertos Fibre Channel en el nodo.	matriz en números enteros
HardwareConfig	Información de configuración de periféricos de la placa base.	Objeto JSON
KerningelCrashDumpState	La configuración de volcado de bloqueo del núcleo del sistema operativo.	cadena
memoria	Información de hardware del firmware y de la memoria del sistema.	Objeto JSON
red	Descripciones del hardware de cada una de las interfaces de red del nodo.	Objeto JSON
Interfaces de red	El estado de las interfaces de red del nodo.	Objeto JSON
Ranura del nodo	Para las plataformas HCI, la letra que corresponde a la ranura del chasis de este nodo se encuentra en ("A", "B", "C" o "D"). En el caso de las plataformas de almacenamiento, este valor es nulo.	cadena

Nombre	Descripción	Tipo
nvram	Estadísticas de NVRAM para el nodo.	Objeto JSON
origen	El proveedor de la placa base.	cadena
plataforma	Una descripción de la plataforma del chasis.	Objeto JSON
serie	El número de serie del producto.	cadena
Reducida	Información de la controladora de almacenamiento.	Objeto JSON
Memoria del sistema	Información sobre el uso y el rendimiento de la memoria del sistema operativo.	Objeto JSON
sistema	El tipo de chasis del nodo.	Objeto JSON
uuid	El ID único del nodo.	UUID

Obtenga más información

GetHardwareInfo

host (volúmenes virtuales)

El objeto del host contiene información acerca de un host de volumen virtual. Puede utilizar el `ListVirtualVolumeHosts` método para obtener esta información para todos los hosts de volúmenes virtuales.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
vinculaciones	Una lista de objetos que describen los vinculaciones del host de volúmenes virtuales.	matriz en números enteros
ID de clúster	El ID único del clúster con el que está asociado este host.	UUID
Dirección de host	La dirección IP o el nombre DNS del host de volumen virtual.	cadena

Nombre	Descripción	Tipo
Nombres de iniciador	Una lista de IQN de iniciador para el host de volúmenes virtuales.	matriz de cadenas
VirtualVolumeHostID	El ID exclusivo de este host de volumen virtual.	UUID
VisibleProtocolEndpointID	Una lista de ID de extremos de protocolo visibles en este host.	Cabina de UUID

Obtenga más información

ListVirtualVolumeHosts

IdpConfigInfo

El objeto idpConfigInfo contiene detalles de configuración e integración relacionados con un proveedor de identidades (IDP) de terceros.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
activado	Especifica si esta configuración IdPConfiguration de terceros está habilitada.	booleano
IdpConfigurationID	UUID para la configuración de IDP de terceros.	UUID
IdpMetadata	Metadatos para detalles de configuración e integración para el inicio de sesión único de SAML 2.0.	cadena
IdpName	Nombre para recuperar el proveedor IDP para el inicio de sesión único SAML 2.0.	cadena
ServiceProviderCertificate	Un certificado PKCS#10 X.509 codificado en Base64 con formato PEM que se utilizará para la comunicación con este IDP.	cadena

Nombre	Descripción	Tipo
SpMetadataUrl	URL para recuperar los metadatos del proveedor de servicios (SP) del clúster para proporcionar al IDP para establecer una relación de confianza.	cadena

iniciador

El objeto iniciador contiene información acerca de un iniciador de iSCSI o Fibre Channel. Un objeto iniciador puede contener identificadores de IQN o WWPN. Puede utilizar el `ListInitiators` método para obtener una lista de todos los iniciadores conocidos en el sistema. Los objetos iniciadores se utilizan para configurar el acceso del iniciador SCSI a un conjunto de volúmenes mediante grupos de acceso de volúmenes. Un iniciador solo puede ser miembro de un grupo de acceso de volúmenes a la vez. Puede restringir el acceso del iniciador a una o varias VLAN especificando uno o varios virtualNetworkID mediante el `CreateInitiators` y.. `ModifyInitiators` métodos. Si no especifica ninguna red virtual, el iniciador puede acceder a todas las redes.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
alias	El nombre descriptivo asignado al iniciador, si los hay.	cadena
atributos	Un conjunto de atributos JSON asignados a este iniciador. Vacío si no hay atributos asignados.	Objeto JSON
ChapUsername	El nombre de usuario CHAP único para este iniciador.	cadena
ID de iniciador	El identificador numérico del iniciador.	entero
Nombre del iniciador	El nombre del iniciador, en formato IQN o WWPN.	cadena
InitiatorSecret	El secreto CHAP que se utiliza para autenticar el iniciador.	cadena
Requiredor	True si se requiere CHAP para este iniciador.	booleano

Nombre	Descripción	Tipo
TargetSecret	El secreto CHAP que se utiliza para autenticar el destino (cuando se utiliza la autenticación CHAP mutua).	cadena
VirtualNetworkIDs	La lista de identificadores de red virtual asociados con este iniciador. Si se define uno o más, este iniciador solo podrá iniciar sesión en las redes virtuales especificadas. Si no hay redes virtuales definidas, este iniciador puede iniciar sesión en todas las redes.	entero
VolumeAccessGroups	Una lista de los ID de grupo de acceso de volúmenes a los que pertenece este iniciador.	matriz en números enteros

Obtenga más información

ListInitiators

KeyProviderKmip

El objeto keyProviderKmip describe un proveedor de claves del protocolo de interoperabilidad de gestión de claves (KMIP). Un proveedor de claves es tanto un mecanismo como una ubicación para recuperar claves de autenticación que se deben usar con funciones del clúster como el cifrado en reposo.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
KeyProviderID	El ID del proveedor de claves KMIP. Este es un valor único que asigna el clúster durante la creación del proveedor de claves, el cual no se puede modificar.	entero

Nombre	Descripción	Tipo
KeyProviderIsActive	True si el proveedor de claves KMIP está activo. Un proveedor se considera activo si hay claves pendientes que se crearon pero que aún no se han eliminado y, por lo tanto, se supone que aún están en uso.	booleano
KeyProviderName	El nombre del proveedor de claves KMIP.	cadena
KeyServerID	Un ID de servidor de claves asociado a este proveedor. Debe agregar el servidor antes de que este proveedor pueda activarse. El servidor no se puede quitar mientras este proveedor está activo. Sólo se admite un ID de servidor para cada proveedor.	matriz en números enteros
KmipCapabilities	Las funcionalidades de este proveedor de claves KMIP incluyen detalles sobre la biblioteca subyacente, el cumplimiento de normativas FIPS, el proveedor SSL, etc.	cadena

KeyServerKmip

El objeto keyServerKmip describe un servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP), que es una ubicación para recuperar claves de autenticación para usarse con funciones del clúster como el cifrado en reposo.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
KeyProviderID	Si este servidor de claves KMIP se asigna a un proveedor, este miembro contiene el ID del proveedor de claves KMIP al que está asignado. De lo contrario, este miembro es nulo.	entero

Nombre	Descripción	Tipo
KeyServerID	El ID del servidor de claves KMIP. Este es un valor único que asigna el clúster durante la creación del servidor de claves. Este valor no se puede modificar.	entero
KmipAssignedProviderIsActive	Si este servidor de claves KMIP se asigna a un proveedor (keyProviderID no es nulo), este miembro indica si ese proveedor está activo (proporcionando claves que se están utilizando actualmente). De lo contrario, este miembro es nulo.	booleano
KmipCaCertificate	El certificado de clave pública de la CA raíz del servidor de claves externo. Esto se utiliza para verificar el certificado presentado por el servidor de claves externo en la comunicación TLS. Para los clústeres de servidores de claves en los que los servidores individuales utilizan CA diferentes, este miembro contiene una cadena concatenada de los certificados raíz de todas las CA.	cadena
KmipClientCertificate	Un certificado PKCS#10 X.509 codificado en formato PEM Base64 que utiliza el cliente KMIP de almacenamiento de Element.	cadena
KmipKeyServerHostnames	Los nombres de host o las direcciones IP asociados con este servidor de claves KMIP.	matriz de cadenas
KmipKeyServerName	El nombre del servidor de claves KMIP. Este nombre sólo se utiliza con fines de visualización y no necesita ser único.	cadena
KmipKeyServerPort	El número de puerto asociado con este servidor de claves KMIP (por lo general, 5696).	entero

LdapConfiguration

El objeto ldapConfiguration contiene información sobre la configuración de LDAP en el sistema de almacenamiento de. Puede recuperar la información LDAP con `GetLdapConfiguration` Método API.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Tipo de autorización	Identifica el método de autenticación de usuarios que se va a utilizar. Los posibles valores son los siguientes: • DirectBind • SearchAndBind	cadena
activado	Identifica si el sistema está configurado para LDAP o no. Los posibles valores son los siguientes: • verdadero • falso	booleano
GroupSearchBaseDN	El DN base del árbol para iniciar la búsqueda del grupo (el sistema realizará una búsqueda en el subárbol de aquí).	cadena
GroupSearchCustomFilter	Filtro de búsqueda personalizado utilizado.	cadena
GroupSearchType	Controla el filtro de búsqueda de grupos predeterminado que se utiliza. Los posibles valores son los siguientes: • NoGroups: Ningún soporte de grupo. • ActiveDirectory: Pertenencia anidada de todos los grupos de AD de un usuario. • MemberDN: Grupos del estilo MemberDN (un nivel).	cadena

Nombre	Descripción	Tipo
SearchBindDN	Un DN completo con el que se inicia sesión para realizar una búsqueda LDAP del usuario (necesita acceso de lectura al directorio LDAP).	cadena
URIs de servidor	Una lista separada por comas de los URI del servidor LDAP (por ejemplo, `ldap://1.2.3.4` y.. `ldaps://1.2.3.4:123`.)	cadena
UserDNTemplate	Cadena que se utiliza para formar un DN de usuario completo.	cadena
UserSearchBaseDN	El DN base de los tres que se usan para iniciar la búsqueda (realizará una búsqueda de subárbol de aquí).	cadena
UserSearchFilter	El filtro LDAP utilizado.	cadena

Obtenga más información

GetLdapConfiguration

LoggingServer

El objeto loggingServer contiene información sobre los hosts de registro configurados para el clúster de almacenamiento. Puede utilizar `GetRemoteLoggingHosts` para determinar cuáles son los hosts de registro actuales y, a continuación, utilizarlos `SetRemoteLoggingHosts` para definir la lista deseada de hosts de registro actuales y nuevos.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
host	Dirección IP del servidor de registro.	cadena
puerto	Número de puerto utilizado para comunicarse con el servidor de registro.	entero

red (interfaces unidas)

El objeto de red (interfaces ligadas) contiene información de configuración para las interfaces de red vinculadas en un nodo de almacenamiento. Puede utilizar el `GetConfig` y.. `GetNetworkConfig` métodos para obtener esta información para un nodo de almacenamiento.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
dirección	La dirección IPv4 asignada a esta interfaz en el nodo.	cadena
Dirección V6	La dirección de gestión de IPv6 asignada a la interfaz Bond1G en el nodo.	cadena
retraso de la bond-downdelay	Tiempo de espera, en milisegundos, antes de deshabilitar un esclavo tras haber detectado un fallo de enlace.	cadena
bond-fail_over_mac	La configuración de la dirección MAC de la interfaz de red.	cadena
bond-miimon	La frecuencia, en milisegundos, en la que se inspecciona el estado de enlace MII en busca de fallos de enlace.	cadena
bond-mode	El modo de pegado. Los posibles valores son los siguientes: • ActivePassive (predeterminado) • ALB • LACP (recomendado)	cadena

bond-primary_reselect	Especifica cuándo se elige el esclavo de vínculo primario como esclavo activo. Los posibles valores son los siguientes: • Siempre • Mejor • Fallo	cadena
esclavos de vínculo	La lista de interfaces esclavas para el enlace.	cadena
bond-lacp_rate	Cuando el modo Bond es LACP, la tasa puede cambiar a una de las siguientes: • LACP Fast (predeterminado) • LACP lento	cadena
retraso de la bond-updelay	El tiempo, en milisegundos, que se debe esperar antes de habilitar un esclavo tras la detección de un enlace.	cadena
servidores de nombres dns	Una lista de direcciones utilizadas para servicios de nombres de dominio, separada por comas o con espacio.	cadena
búsqueda dns	Una lista de dominios de búsqueda DNS separada por comas o con un espacio.	cadena
familia	Familia de direcciones que la interfaz está configurada para utilizar. Actualmente se admite "inet" para IPv4.	cadena
puerta de enlace	La dirección de red del enrutador IPv4 utilizada para enviar tráfico desde la red local.	cadena
GatewayV6	La dirección de red del enrutador IPv6 utilizada para enviar tráfico desde la red Bond1G local.	cadena

IpV6PrefixLength	La longitud del prefijo de subred para las rutas estáticas del tipo "net" para el tráfico de IPv6 en la red de Bond1G.	cadena
Dirección MAC	La dirección MAC real asignada a la interfaz y observada por la red.	cadena
MacAddressPermanente	Dirección MAC inmutable asignada por el fabricante a la interfaz.	cadena
método	El método que se utiliza para configurar la interfaz. Los posibles valores son los siguientes: • Loopback: Se utiliza para definir la interfaz de bucle invertido de IPv4. • Manual: Se utiliza para definir interfaces que no se configuran automáticamente. • dhcp: Se puede utilizar para obtener una dirección IP a través de DHCP. • Static: Se utiliza para definir interfaces Ethernet con direcciones IPv4 asignadas de forma estática.	cadena
mtu	El tamaño de paquete más grande (en bytes) que la interfaz puede transmitir. Debe ser mayor o igual que 1500; se admite un máximo de 9000.	cadena
máscara de red	La máscara de bits que especifica la subred de la interfaz.	cadena
red	Indica dónde comienza el rango de direcciones IP en función de la máscara de red.	cadena
rutas	Matriz separada por comas de cadenas de ruta que se van a aplicar a la tabla de enrutamiento.	matriz de cadenas

estado	El estado de la interfaz. Los posibles valores son los siguientes: • Down: La interfaz está inactiva. • Activo: La interfaz está lista, pero no tiene enlace. • UpAndRunning: La interfaz está lista y se ha establecido un vínculo.	cadena
SymmetricRouteRules	Reglas de enrutamiento simétricas configuradas en el nodo.	matriz de cadenas
UpAndRunning	Indica si la interfaz está lista y tiene un enlace.	booleano
VirtualNetworkTag	El identificador de red virtual de la interfaz (etiqueta VLAN).	cadena

Modificación de miembros y estados de nodo

Esta tabla indica si los parámetros del objeto se pueden modificar en cada estado de nodo posible.

Nombre del miembro	Estado disponible	Estado pendiente	Estado activo
dirección	Sí	Sí	No
Dirección V6	Sí	Sí	No
retraso de la bond-downdelay	Configurado por el sistema	N.A.	N.A.
bond-fail_over_mac	Configurado por el sistema	N.A.	N.A.
bond-miimon	Configurado por el sistema	N.A.	N.A.
bond-mode	Sí	Sí	Sí
bond-primary_reselect	Configurado por el sistema	N.A.	N.A.
esclavos de vínculo	Configurado por el sistema	N.A.	N.A.
bond-lacp_rate	Sí	Sí	Sí

retraso de la bond-updelay	Configurado por el sistema	N.A.	N.A.
servidores de nombres dns	Sí	Sí	Sí
búsqueda dns	Sí	Sí	Sí
familia	No	No	No
puerta de enlace	Sí	Sí	Sí
GatewayV6	Sí	Sí	Sí
IpV6PrefixLength	Sí	Sí	Sí
Dirección MAC	Configurado por el sistema	N.A.	N.A.
MacAddressPermanente	Configurado por el sistema	N.A.	N.A.
método	No	No	No
mtu	Sí	Sí	Sí
máscara de red	Sí	Sí	Sí
red	No	No	No
rutas	Sí	Sí	Sí
estado	Sí	Sí	Sí
SymmetricRouteRules	Configurado por el sistema	N.A.	N.A.
UpAndRunning	Configurado por el sistema	N.A.	N.A.
VirtualNetworkTag	Sí	Sí	Sí

Obtenga más información

- Getconfig
- GetNetworkConfig

red (todas las interfaces)

El objeto de red (todas las interfaces) recopila información sobre la configuración de la interfaz de red para un nodo de almacenamiento. Puede utilizar el `GetConfig` y.. `GetNetworkConfig` métodos para obtener esta información para un nodo de almacenamiento.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Bond10G	Información de configuración de la interfaz de unión rígida de Bond10G.	red (interfaces unidas)
Bond1G	Información de configuración de la interfaz de unión rígida.	red (interfaces unidas)
eth0-5	Un objeto para cada interfaz de Ethernet del nodo de almacenamiento, donde se describe la información de configuración de la interfaz. Estos objetos están numerados del 0 al 5 para que coincidan con el nombre de la interfaz.	Red (interfaces Ethernet)
lo	Información de configuración de la interfaz de bucle invertido.	red (interfaces locales)

Obtenga más información

- Getconfig
- GetNetworkConfig

Red (interfaces Ethernet)

El objeto network (interfaces Ethernet) contiene información de configuración para las interfaces Ethernet individuales. Puede utilizar el `GetConfig` y.. `GetNetworkConfig` métodos para obtener esta información para un nodo de almacenamiento.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo

bond-master	Especifica qué interfaz de unión rígida esta interfaz física se ha Unido como esclavo de enlace.	cadena
familia	Familia de direcciones que la interfaz está configurada para utilizar. Actualmente se admite "inet" para IPv4.	cadena
Dirección MAC	La dirección MAC real asignada a la interfaz y observada por la red.	cadena
MacAddressPermanente	Dirección MAC inmutable asignada por el fabricante a la interfaz.	cadena
método	El método que se utiliza para configurar la interfaz. Los posibles valores son los siguientes: • Loopback: Se utiliza para definir la interfaz de bucle invertido de IPv4. • Manual: Se utiliza para definir interfaces que no se configuran automáticamente. • dhcp: Se puede utilizar para obtener una dirección IP a través de DHCP. • Static: Se utiliza para definir interfaces Ethernet con direcciones IPv4 asignadas de forma estática.	cadena
estado	El estado de la interfaz. Los posibles valores son los siguientes: • Down: La interfaz está inactiva. • Activo: La interfaz está lista, pero no tiene enlace. • UpAndRunning: La interfaz está lista y se ha establecido un vínculo.	cadena
UpAndRunning	Indica si la interfaz está lista y tiene un enlace.	booleano

Modificación de miembros y estados de nodo

Esta tabla indica si los parámetros del objeto se pueden modificar en cada estado de nodo posible.

Nombre del parámetro	Estado disponible	Estado pendiente	Estado activo
bond-master	No	No	No
familia	No	No	No
Dirección MAC	Configurado por el sistema	N.A.	N.A.
MacAddressPermanente	Configurado por el sistema	N.A.	N.A.
método	No	No	No
estado	Sí	Sí	Sí
UpAndRunning	Configurado por el sistema	N.A.	N.A.

Obtenga más información

- Getconfig
- GetNetworkConfig

red (interfaces locales)

El objeto network (interfaces locales) contiene información de configuración para las interfaces de red locales, como la interfaz de bucle invertido, en un nodo de almacenamiento de. Puede utilizar el `GetConfig` y.. `GetNetworkConfig` métodos para obtener esta información para un nodo de almacenamiento.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
familia	Familia de direcciones que la interfaz está configurada para utilizar. Actualmente se admite "inet" para IPv4.	cadena
Dirección MAC	La dirección MAC real asignada a la interfaz y observada por la red.	cadena

MacAddressPermanente	Dirección MAC inmutable asignada por el fabricante a la interfaz.	cadena
método	El método que se utiliza para configurar la interfaz. Los posibles valores son los siguientes: • Loopback: Se utiliza para definir la interfaz de bucle invertido de IPv4. • Manual: Se utiliza para definir interfaces que no se configuran automáticamente. • dhcp: Se puede utilizar para obtener una dirección IP a través de DHCP. • Static: Se utiliza para definir interfaces Ethernet con direcciones IPv4 asignadas de forma estática.	cadena
estado	El estado de la interfaz. Los posibles valores son los siguientes: • Down: La interfaz está inactiva. • Activo: La interfaz está lista, pero no tiene enlace. • UpAndRunning: La interfaz está lista y se ha establecido un vínculo.	cadena
UpAndRunning	Indica si la interfaz está lista y tiene un enlace.	booleano

Modificación de miembros y estados de nodo

Esta tabla indica si los parámetros del objeto se pueden modificar en cada estado de nodo posible.

Nombre del parámetro	Estado disponible	Estado pendiente	Estado activo
familia	No	No	No
Dirección MAC	Configurado por el sistema	N.A.	N.A.
MacAddressPermanente	Configurado por el sistema	N.A.	N.A.

método	No	No	No
estado	Sí	Sí	Sí
UpAndRunning	Configurado por el sistema	N.A.	N.A.

Obtenga más información

- Getconfig
- GetNetworkConfig

Red (SNMP)

El objeto de red SNMP contiene información acerca de la configuración de SNMP v3 para los nodos del clúster.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
acceso	Tipo de acceso permitido para las solicitudes de información SNMP. Los posibles valores son los siguientes: • Ro: Acceso de sólo lectura. • rw: Acceso de lectura y escritura. • rosys: Acceso de sólo lectura a un conjunto restringido de información del sistema.	cadena
cidr	Una máscara de red CIDR. Esta máscara de red debe ser un entero mayor o igual que 0, e inferior o igual a 32. Tampoco debe ser igual a 31.	entero
comunidad netapp	La cadena de comunidad SNMP.	cadena

red	Este miembro, junto con el miembro cidr, controla a qué red se aplica el acceso y la cadena de comunidad. El valor especial "default" se utiliza para especificar una entrada que se aplica a todas las redes. La máscara CIDR se ignora cuando este miembro es un nombre de host o "predeterminado".	cadena

Obtenga más información

GetSnmpInfo

NetworkInterface

El objeto networkInterface contiene información de configuración para interfaces de red individuales en un nodo de almacenamiento.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
dirección	La dirección de gestión IPv4 de la interfaz.	cadena
Dirección V6	La dirección de gestión IPv6 de la interfaz.	cadena
emisión	La dirección de difusión de la interfaz.	cadena
Dirección MAC	La dirección MAC de la interfaz.	cadena
mtu	La unidad de transferencia máxima, en bytes, de la interfaz.	entero
nombre	Nombre de la interfaz.	cadena
espacio de nombres	Si esta interfaz tiene asignado un espacio de nombres de red virtual o no.	booleano
máscara de red	La máscara de subred de la interfaz.	cadena

estado	El estado operativo de la interfaz.	cadena
tipo	El tipo de interfaz (maestro de vínculo, esclavo de vínculo, etc.).	cadena
VirtualNetworkTag	El ID de VLAN asignado a la interfaz de en la red virtual.	entero

NetworkInterfaceStats

El objeto networkInterfaceStats contiene estadísticas de red, el número total de paquetes transmitidos y recibidos, e información sobre errores de interfaces de red individuales en un nodo de almacenamiento. Puede utilizar el `ListNetworkInterfaceStats` Método de API para enumerar esta información de las interfaces de red en un nodo de almacenamiento.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
colisiones	El número de colisiones detectadas.	entero
nombre	Nombre de la interfaz de red.	cadena
RxBytes	La cantidad total de bytes recibidos.	entero
RxCrcErrors	El número de paquetes recibidos con un error de CRC.	entero
RxDropped	El número de paquetes recibidos que se descartaron.	entero
RxErrors	El número de paquetes incorrectos o mal formados recibidos.	entero
RxFifoErrors	El número de errores de desbordamiento de FIFO en los datos recibidos.	entero
RxFrameErrors	El número de paquetes recibidos con errores de alineación de tramas.	entero
RxLengthErrors	El número de paquetes recibidos con un error de longitud.	entero
RxMissedErrors	El número de paquetes que ha perdido el receptor.	entero

Nombre	Descripción	Tipo
RxOverErrors	El número de errores de desbordamiento del búfer del anillo receptor para esta interfaz.	entero
RxPackets	El número total de paquetes recibidos.	entero
TxBytes	La cantidad total de bytes transmitidos.	entero
CarritxerErrors	El número de errores de portador para el lado de transmisión.	entero
TxErrors	El número de errores de transmisión de paquetes.	entero
FiftxoErrors	El número de errores de desbordamiento de FIFO en el lado de transmisión.	entero
Empaquetado txets	El número total de paquetes transmitidos.	entero

nodo

El objeto del nodo contiene información acerca de cada nodo del clúster. Puede recuperar esta información mediante `ListActiveNodes` y.. `ListAllNodes` métodos.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
AsociadosFServiceID	El ID de servicio de Fibre Channel para el nodo. "0" si el nodo no es un nodo Fibre Channel.	entero
AsociatedMasterServiceID	El ID de servicio principal del nodo.	entero
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON
Nombre de chassisName	Identifica de forma única un chasis; es idéntico para todos los nodos en un único chasis.	cadena
cip	La dirección IP del clúster asignada al nodo.	cadena

Nombre	Descripción	Tipo
cipi	La interfaz de red que se utiliza para la comunicación del clúster.	cadena
CustomProtectionDomainName	Identifica de forma exclusiva un dominio de protección personalizado. Este nombre es idéntico para todos los nodos de almacenamiento que conforman todo el chasis de un dominio de protección personalizado dado.	cadena
FiberChannelTargetPortGroup	El grupo de destino asociado con este nodo. "Null" si el nodo no es un nodo Fibre Channel.	entero
Modo de mantenimiento	Indica el modo en que está un nodo para mantenimiento.	n.a.
mip	La dirección IP utilizada para la gestión de nodos.	cadena
mipi	La interfaz de red utilizada para la gestión de nodos.	cadena
nombre	El nombre de host del nodo.	cadena
NodeID	NodeID para este nodo.	entero
Ranura del nodo	Para las plataformas HCI, la letra que corresponde a la ranura del chasis de este nodo se encuentra en ("A", "B", "C" o "D"). En el caso de las plataformas de almacenamiento, este valor es nulo.	cadena

Nombre	Descripción	Tipo
PlatformInfo	Información de hardware para el nodo. Miembros: • ChassisType: La plataforma de hardware del nodo. • CpuModel: El modelo de CPU de la plataforma de hardware. • NodeMemoryGB: La cantidad de memoria instalada en la plataforma física en GB. • NodeType: El nombre de modelo del nodo. • PlatformConfigVersion: La versión de software configurada para este hardware de nodo.	Objeto JSON
función	El rol del nodo en el clúster. Los posibles valores son los siguientes: • Gestión • Reducida • Informática • Testigo	
sip	La dirección IP de almacenamiento asignada al nodo.	cadena
sipi	La interfaz de red utilizada para el tráfico de almacenamiento.	cadena
SOFTWAREVERSION	Muestra la versión actual del software Element que se ejecuta en el nodo.	cadena
uuid	El identificador único universal asociado con este nodo.	cadena
Redes de virtualización	Objeto que contiene direcciones IP e ID de red virtual.	VirtualNetwork cabina

Obtenga más información

- ListActiveNodes
- ListAllNodes

ProtectionDomains de nodo

El objeto nodeProtectionDomains contiene información sobre la identificación de un nodo y de los dominios de protección asociados con dicho nodo.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
NodeID	Identificador único del nodo.	entero
ProtectionDomains	Lista de dominios de protección a los que pertenece el nodo.	"ProtectionDomain"

Estadísticas de nodos

El objeto nodeStats contiene mediciones de actividad de alto nivel para un nodo. Puede utilizar el `GetNodeStats` y.. `ListNodeStats` Métodos API para obtener algunos o todos los objetos nodeStats.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
cuente	El número total de muestras en el objeto nodeStats.	entero
cpu	Uso de CPU, en %.	entero
CpuTotal	Incremento monotónicamente del valor de la utilización de la cpu.	entero
CBytesIn	Bytes en la interfaz del clúster.	entero
CBytesOut	Bytes de salida en la interfaz del clúster.	entero
SBytesIn	Bytes en la interfaz de almacenamiento.	entero
SBytesOut	Bytes de la interfaz de almacenamiento.	entero
MBytesIn	Bytes en la interfaz de gestión.	entero

Nombre	Descripción	Tipo
MBytesOut	Los bytes se out en la interfaz de gestión.	entero
NetworkUtilationCluster	Utilización de interfaz de red (en %) para la interfaz de red del clúster.	entero
NetworkUtilationStorage	Utilización de interfaz de red (en %) para la interfaz de red de almacenamiento.	entero
ReadLatencyUSectotal	El valor monotónicamente aumenta del tiempo total dedicado a realizar operaciones de lectura en el nodo.	entero
Operaciones de lectura	Incremento monotónicamente del valor de las operaciones de lectura totales en un nodo.	entero
SLoadHistograma	Datos de histograma que ilustran la carga de servicios de segmentos con el tiempo.	Objeto JSON
fecha/hora	La hora actual en formato UTC+0.	Cadena de fecha ISO 8601
Memoria usedMemory	Uso total de memoria en bytes.	entero
WriteLatencyUSectotal	Incremento monotónicamente del valor del tiempo total dedicado a ejecutar operaciones de escritura en el nodo.	entero
Operaciones de escritura	Incremento monotónicamente del valor de las operaciones de escritura totales en un nodo.	entero

Obtenga más información

- GetNodeStats
- ListNodeStats

OntapVersionInfo

El objeto ontapVersionInfo contiene información acerca de la versión API del clúster ONTAP en una relación de SnapMirror. La interfaz de usuario web de Element utiliza el `GetOntapVersionInfo` Método API para obtener esta información.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
SnapMirrorEndpointID	El ID del sistema ONTAP de destino.	entero
ClientAPIMajorVesion	La versión principal de la API de ONTAP que utiliza el cliente API de Element.	cadena
ClientAPIMinorVesion	La versión secundaria de la API de ONTAP que utiliza el cliente API de Element.	cadena
OntapAPIMajorVersion	La versión principal de API actual compatible con el sistema ONTAP.	cadena
OntapAPIMinorVesion	La versión secundaria de la API actual compatible con el sistema ONTAP.	cadena
OntapVersion	La versión de software actual que se ejecuta en el clúster de ONTAP.	cadena

PendingActiveNode

El objeto pendingActiveNode contiene información acerca de un nodo que actualmente tiene el estado pendingActive, entre los estados pendiente y activo. Son nodos que se están revirtiendo a la imagen de software de fábrica. Utilice la `ListPendingActiveNodes` Método API para obtener una lista de esta información para todos los nodos pendingActive.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ActiveNodeKey	Una clave única que permite que el nodo se una al clúster automáticamente después de una instalación correcta del software.	cadena
NombreNodo asignado	El ID del nodo asignado para el nodo.	cadena

Nombre	Descripción	Tipo
Establish asyncHandle	Identificador de método asíncrono que puede utilizar para consultar el estado de la operación.	entero
cip	La dirección IP del clúster asignada al nodo.	cadena
mip	La dirección IP de gestión asignada al nodo.	cadena
Ranura del nodo	Para las plataformas HCI, la letra que corresponde a la ranura del chasis de este nodo se encuentra en ("A", "B", "C" o "D"). En el caso de las plataformas de almacenamiento, este valor es nulo.	cadena
PendingActiveNodeID	El ID de nodo pendiente del nodo.	entero
PlatformInfo	Información de hardware para el nodo. Miembros: • ChassisType: La plataforma de hardware del nodo. • CpuModel: El modelo de CPU de la plataforma de hardware. • NodeMemoryGB: La cantidad de memoria instalada en la plataforma física en GB. • NodeType: El nombre de modelo del nodo. • PlatformConfigVersion: La versión de software configurada para este hardware de nodo.	Objeto JSON
función	El rol del nodo en el clúster. Los posibles valores son los siguientes: • Gestión • Reducida • Informática • Testigo	

Nombre	Descripción	Tipo
sip	La dirección IP de almacenamiento (iSCSI) asignada al nodo.	cadena
SOFTWAREVERSION	La versión actual del software Element que se ejecuta en el nodo.	cadena

Obtenga más información

ListPendingActiveNodes

PendingNode

El objeto pendingNode contiene información sobre un nodo que se puede añadir a un clúster. Utilice la `ListPendingNodes` Método API para obtener una lista de esta información para todos los nodos pendientes. Puede añadir cualquiera de los nodos indicados a un clúster con el `AddNodes` Método API.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
cipi	La dirección IP del clúster asignada al nodo.	cadena
ActiveNodeKey	Una clave única que permite que el nodo se una al clúster automáticamente después de una instalación correcta del software.	cadena
NombreNodo asignado	El ID del nodo asignado para el nodo.	cadena
Establish asyncHandle	Identificador de método asíncrono que puede utilizar para consultar el estado de la operación.	entero
Nombre de chassisName	Identifica de forma única un chasis; es idéntico para todos los nodos en un único chasis.	cadena
cip	La dirección IP del clúster asignada al nodo.	cadena

Nombre	Descripción	Tipo
mip	La dirección IP de gestión asignada al nodo.	cadena
Ranura del nodo	Para las plataformas HCI, la letra que corresponde a la ranura del chasis de este nodo se encuentra en ("A", "B", "C" o "D"). En el caso de las plataformas de almacenamiento, este valor es nulo.	cadena
PendingActiveNodeID	El ID de nodo pendiente del nodo.	entero
PlatformInfo	Información de hardware para el nodo. Miembros: • ChassisType: La plataforma de hardware del nodo. • CpuModel: El modelo de CPU de la plataforma de hardware. • NodeMemoryGB: La cantidad de memoria instalada en la plataforma física en GB. • NodeType: El nombre de modelo del nodo. • PlatformConfigVersion: La versión de software configurada para este hardware de nodo.	Objeto JSON
función	El rol del nodo en el clúster. Los posibles valores son los siguientes: • Gestión • Reducida • Informática • Testigo	
sip	La dirección IP de almacenamiento (iSCSI) asignada al nodo.	cadena
SOFTWAREVERSION	La versión actual del software Element que se ejecuta en el nodo.	cadena

Obtenga más información

- AddNodes
- ListPendingNodes

ProtectionDomain

El objeto protectionDomain contiene los detalles de nombre y tipo de un dominio de protección.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ProtectionDomainName	El nombre del dominio de protección.	cadena
ProtectionDomainType	El tipo del dominio de protección. Los posibles valores son los siguientes: • Chassis: Todos los nodos de almacenamiento en un único chasis. • Custom: Todos los nodos de almacenamiento en un único dominio de protección definido por el cliente.	cadena

ProtectionDomainLevel

El objeto protectionDomainLevel contiene información acerca de la tolerancia actual y los niveles de resiliencia del clúster de almacenamiento. Los niveles de tolerancia indican la capacidad del clúster para seguir leyendo y escribiendo datos en el caso de un fallo, y los niveles de resiliencia indican la capacidad del clúster para recuperarse automáticamente de uno o más fallos dentro del tipo de dominio de protección asociado.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ProtectionDomainType	El tipo de dominio de protección que tiene la tolerancia y la resiliencia asociadas. Los posibles valores son los siguientes: • Node: Cualquier nodo individual. • Chassis: Cualquier nodo individual o todos los nodos de almacenamiento en un único chasis. • Custom: Todos los nodos de almacenamiento en un único dominio de protección definido por el cliente.	cadena
resiliencia	La resiliencia actual de este clúster desde la perspectiva de este tipo de dominio de protección.	ProtectionDomainResiliency
tolerancia	La tolerancia actual de este clúster desde la perspectiva de este tipo de dominio de protección.	ProtectionDomainTolerance

ProtectionDomainResiliency

El objeto protectionDomainResiliency contiene el estado de resiliencia de este clúster de almacenamiento. La resiliencia indica la capacidad del clúster de almacenamiento para recuperarse automáticamente de un fallo o varios en un único dominio de protección de su tipo de dominio de protección asociado. Un clúster de almacenamiento se considera curado cuando este pueda seguir leyendo y escribiendo datos mediante el fallo de cualquier otro nodo de almacenamiento (un estado conocido como tolerancia al nodo).

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ProtectionSchemeResiliencies	Una lista de objetos (uno para cada esquema de protección) que contienen información de resiliencia de fallos para el tipo asociado de dominio de protección.	ProtectionSchemeResiliency cabina

Nombre	Descripción	Tipo
SingleFailureThresholdBytesForBlockData	El número máximo de bytes que se pueden almacenar en el clúster de almacenamiento antes de perder la capacidad de recuperarse automáticamente en un estado de tolerancia de nodo.	entero
FailoidableForsemble	El número previsto de fallos simultáneos que se pueden producir sin perder la capacidad de recuperarse automáticamente a un estado de tolerancia de nodo para el quórum del conjunto.	entero

ProtectionDomainTolerance

El objeto protectionDomainTolerance contiene información sobre la capacidad del clúster de almacenamiento de seguir leyendo y escribiendo datos en caso de uno o más fallos. Todo ello dentro de un único dominio de protección de su tipo de dominio de protección asociado.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ProtectionSchemetolerancias	Una lista de objetos (uno para cada esquema de protección) que contienen información de tolerancia a fallos para el tipo de dominio de protección asociado.	ProtectionSchemeTolerance cabina
FailoidableForsemble	La cantidad de fallos simultáneos dentro del tipo asociado de dominio de protección que se puede producir sin perder el quórum del conjunto.	entero

ProtectionSchemeResiliency

El objeto protectionSchemeResiliency contiene información sobre si un clúster de almacenamiento, para un esquema de protección específico, puede recuperarse automáticamente de uno o varios fallos dentro de su protección asociada DomainType. Un clúster de almacenamiento se considera curado cuando este pueda seguir leyendo y escribiendo datos mediante el fallo de cualquier otro nodo de almacenamiento (un estado conocido como tolerancia al nodo).

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Esquema de protección	El esquema de protección actual de este clúster de almacenamiento. El único valor posible es doubleHelix.	cadena
FaillableFaiurForBlockData	El número previsto de fallos simultáneos que pueden producirse sin perder la capacidad de recuperarse automáticamente en un estado de tolerancia de nodo para los datos.	entero
SustentableFailuresForMetadata	El número previsto de fallos simultáneos que se pueden producir sin perder la capacidad de recuperarse automáticamente en un estado de tolerancia de nodo para metadatos.	entero

ProtectionSchemeTolerance

El objeto protectionSchemeTolerance contiene información sobre si un clúster de almacenamiento, para un esquema de protección específico, puede seguir leyendo y escribiendo datos después de un fallo.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Esquema de protección	El esquema de protección actual de este clúster de almacenamiento. El único valor posible es doubleHelix.	cadena
FaillableFaiurForBlockData	El número actual de errores simultáneos que se pueden producir sin perder la disponibilidad de datos de bloques para el esquema de protección asociado.	entero

Nombre	Descripción	Tipo
SustentableFailuresForMetadata	El número actual de errores simultáneos que se pueden producir sin perder la disponibilidad de metadatos para el esquema de protección asociado.	entero

ProtocolEndpoint

El objeto ProtocolEndpoint contiene los atributos de un extremo de protocolo. Puede recuperar esta información para todos los extremos de protocolo en el clúster mediante el `ListProtocolEndpoints` Método API.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Primario ProviderID	El ID del objeto de proveedor de extremo de protocolo principal para el extremo de protocolo.	entero
ProtocolEndpointID	El ID único del extremo de protocolo.	UUID
ProtocolEndpointState	El estado del extremo de protocolo. Los posibles valores son los siguientes: • Active: El extremo de protocolo está en uso. • Start: El extremo de protocolo se está iniciando. • Failover: El extremo de protocolo se conmutó al nodo de respaldo. • Reserved: El extremo de protocolo está reservado.	cadena
ProviderType	El tipo de proveedor del extremo de protocolo. Los posibles valores son los siguientes: • Primario • Secundario	cadena

Nombre	Descripción	Tipo
SsiNAADeviceID	El identificador exclusivo de dispositivo SCSI para el extremo de protocolo a nivel global en el formato extendido registrado de NAA según la norma IEEE.	cadena
Cód. Segundo Proder.	El ID del objeto de proveedor de extremo de protocolo secundario para el extremo de protocolo.	entero

Obtenga más información

ListProtocolEndpoints

Calidad de servicio

El objeto QoS contiene información acerca de la configuración de calidad de servicio de los volúmenes. Los volúmenes creados sin valores de calidad de servicio especificados se crean con los valores predeterminados. Puede encontrar los valores predeterminados mediante la `GetDefaultQoS` método.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
BurstIOPS	Se permiten IOPS máximo de 4 KB «pico» durante breves periodos de tiempo. Permite ráfagas de actividad de I/o con un valor normal de maxIOPS.	entero
Tiempo de burstTime	La cantidad de tiempo permitido para burstIOPS. El valor devuelto se representa en segundos. El sistema calcula este valor en función de las IOPS establecidas para la calidad de servicio.	entero

Nombre	Descripción	Tipo
curva	La curva es un conjunto de pares clave-valor. Las claves son tamaños de I/o en bytes. Los valores representan el coste de ejecutar un IOP en un tamaño de I/o específico. La curva se calcula en relación con una operación de 4096 bytes establecida en 100 IOPS.	Objeto JSON
IOPS	El número máximo de IOPS de 4 KB permitidas a lo largo de un periodo de tiempo prolongado.	entero
MinIOPS	Como garantía el mínimo de IOPS de 4 KB. Las IOPS permitidas solo se sitúan por debajo de este nivel si todos los volúmenes se han limitado a su valor de minIOPS y aún no hay suficiente capacidad de rendimiento.	entero

Obtenga más información

GetDefaultQoS

QoSPolicy

El objeto QoSPolicy contiene información sobre una directiva QoS en un clúster de almacenamiento que ejecuta el software Element.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
QosPolicyID	Identificador entero único para QoSPolicy asignado automáticamente por el clúster de almacenamiento.	entero
nombre	El nombre de la política de calidad de servicio. Por ejemplo: Oro, platino o plata.	cadena

Nombre	Descripción	Tipo
calidad de servicio	La configuración de la calidad de servicio que representa esta política.	Calidad de servicio
ID de volumen	Una lista de volúmenes asociados con esta política.	matriz en números enteros

Obtenga más información

GetQoSPolicy

RemoteClusterSnapshotStatus

La `remoteClusterSnapshotStatus` El objeto contiene el UUID y el estado de una snapshot almacenada en un clúster de almacenamiento remoto. Puede obtener esta información con el `ListSnapshots` o. `ListGroupSnapshots` Métodos de API.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
RemoteStatus	El estado de replicación de la snapshot remota en el clúster de destino como se ve en el clúster de origen. Los posibles valores son los siguientes: • Present: La copia de Snapshot existe en un clúster remoto. • NotPresent: La snapshot no existe en un clúster remoto. • Syncing: Este es un clúster de destino y que está replicando en este momento la snapshot. • Deleted: Es un clúster de destino. La copia de Snapshot se ha eliminado y sigue existiendo en el origen.	cadena
VolumePairUUID	El identificador universal de la pareja de volúmenes.	UUID

programación

El objeto de programación contiene información sobre una programación creada para realizar de forma autónoma una instantánea de un volumen. Puede recuperar la información de la programación de todas las programaciones con el `ListSchedules` Método API.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	Indica la frecuencia de la incidencia de la programación. Los posibles valores son los siguientes: • Día de la semana • Día del mes • Intervalo de tiempo	Objeto JSON
HasError	Indica si la programación tiene errores o no. Los posibles valores son los siguientes: • verdadero • falso	booleano
horas	Muestra las horas que transcurren antes de crear la siguiente snapshot. Los valores posibles están entre 0 y 24.	entero
LastRunStatus	Indica el estado de la última snapshot programada. Los posibles valores son los siguientes: • Correcto • Error	cadena
LastRunTimeStart	Indica la última vez que se inició la programación.	Cadena de fecha ISO 8601
minutos	Muestra los minutos que transcurrirán antes de que se cree la siguiente snapshot. Los valores posibles están entre 0 y 59.	entero

Nombre	Descripción	Tipo
mesdays	Indica los días del mes en que se realizará una copia de Snapshot.	cabina
en pausa	Indica si la programación se pausó o no. Los posibles valores son los siguientes: • verdadero • falso	booleano
recurrente	Indica si la programación se repite o no. Los posibles valores son los siguientes: • verdadero • falso	booleano
RunNextInterval	Indica si la programación se ejecutará la próxima vez que el programador esté activo. Si es verdadero, la programación se ejecutará la próxima vez que el programador esté activo y, a continuación, este valor se vuelva a definir como FALSE. Los posibles valores son los siguientes: • verdadero • falso	booleano
ID de intervalo	El ID único de la programación.	entero

Nombre	Descripción	Tipo
Info. De Lac	Incluye el nombre único que se le asignó a la programación, el período de retención de la snapshot que se creó y el ID de volumen del volumen a partir del cual se creó la copia de Snapshot. Valores válidos: • `enableRemoteReplication`: Indica si la instantánea debe incluirse en la replicación remota. (booleano) • `ensureSerialCreation`: Especifica si se debe permitir la creación de una nueva instantánea si se está realizando una replicación de instantánea anterior. (booleano) • `name`: El nombre de la instantánea que se va a utilizar. (cadena) • `retention`: La cantidad de tiempo que se retiene la instantánea. Dependiendo de la hora, se muestra en uno de los siguientes formatos: ◦ `fifo`: La instantánea se mantiene en base al primero en primero en salir (FIFO). Si está vacío, la copia de Snapshot se conserva siempre. (cadena) ◦ HH:mm:ss • `volumeID`: El ID del volumen que se incluirá en la instantánea. (entero) • `volumes`: Lista de ID de volumen que se incluirán en la instantánea de grupo. (matriz entera)	Objeto JSON
Nombre de la pila	El nombre único que se asigna a la programación.	cadena

Nombre	Descripción	Tipo
Tipo de columna	En este momento solo se admiten los tipos de programación de Snapshot.	cadena
SnapMirrorLabel	El snapMirrorLabel que se aplicará a la instantánea o instantánea de grupo creadas, incluidos en el documento LROInfo. Si no se establece, este valor es nulo.	cadena
Fecha de inicio	Indica la fecha la primera vez que se inició o empezará la programación; se le formateó la hora UTC.	Cadena de fecha ISO 8601
ToDeDeleted	Indica si la programación está marcada para eliminarse. Los posibles valores son los siguientes: • verdadero • falso	booleano
días laborables	Indica los días de la semana en que se realizará una copia de Snapshot.	cabina

Obtenga más información

ListSchedules

Sesión (Fibre Channel)

El objeto Session contiene información sobre cada sesión Fibre Channel que es visible para el clúster y en qué puertos de destino es visible. Puede recuperar esta información con `ListFibreChannelSessions` Método API.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
InitiatorWWPN	El nombre de puerto WWPN del iniciador que ha iniciado sesión en el puerto de destino.	cadena

Nombre	Descripción	Tipo
NodeID	El nodo a el que pertenece la sesión Fibre Channel.	entero
iniciador	Información sobre el iniciador del servidor de esta sesión Fibre Channel. Miembros: • Alias: El nombre descriptivo asignado al iniciador. • Atributos: Los atributos de este iniciador. • InitiatorID: El ID de este iniciador. • InitiatorName: El nombre de este iniciador. • VolumeAccessGroups: Una lista de los grupos de acceso de volúmenes asociados con este iniciador.	Objeto JSON
ID de servicio	El ID de servicio del puerto de destino implicado en esta sesión.	entero
TargetWWPN	El WWPN del puerto de destino involucrado en esta sesión.	cadena
VolumeAccessGroupID	El ID del grupo de acceso de volúmenes al que pertenece el WWPN de iniciador. Si no está en un grupo de acceso de volúmenes, este valor es nulo.	entero

Obtenga más información

ListFiberChannelSessions

Sesión (iSCSI)

El objeto Session (iSCSI) contiene información detallada sobre la sesión iSCSI de cada volumen. Es posible recuperar la información de la sesión iSCSI con `ListISCSISessions` Método API.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de cuenta	El ID de cuenta de la cuenta utilizada para la autenticación CHAP, si la hay.	entero
Nombre de cuenta	El nombre de la cuenta utilizada para la autenticación CHAP, si la hay.	cadena
CreateTime	La hora de creación de la sesión iSCSI, en formato UTC+0.	Cadena de fecha ISO 8601
ID de unidad	El DriveID asociado con el servicio de transporte en el que se celebra la sesión.	entero
ID de unidad	Una lista de los identificadores de unidades que notifican el fallo. Una lista vacía si no es aplicable.	matriz en números enteros
iniciador	Información sobre el iniciador del servidor de esta sesión iSCSI. Miembros: • Alias: El nombre descriptivo asignado al iniciador. • Atributos: Los atributos de este iniciador. • InitiatorID: El ID de este iniciador. • InitiatorName: El nombre de este iniciador. • VolumeAccessGroups: Una lista de los grupos de acceso de volúmenes asociados con este iniciador.	Objeto JSON
InitiatorIP	La dirección IP y el número de puerto del iniciador del servidor iSCSI.	cadena
Nombre del iniciador	El nombre completo de iSCSI (IQN) del iniciador del servidor iSCSI.	cadena

Nombre	Descripción	Tipo
InitiatorPortName	El initiatorName combinado con el initiatorSessionID; identifica el puerto del iniciador.	cadena
InitiatorSessionID	Un ID de 48 bits que proporciona el iniciador e identifica la sesión iSCSI como que pertenece a ese iniciador.	entero
MsSinceLastIscsiPDU	El tiempo, en milisegundos, desde que se recibió la última PDU iSCSI para esta sesión.	entero
MsSinceLastScsiCommand	La hora, en milisegundos, desde que se recibió el último comando SCSI para esta sesión.	entero
NodeID	El ID de nodo asociado con el servicio de transporte donde se aloja la sesión.	entero
ID de servicio	El ID de servicio del servicio de transporte que aloja la sesión.	entero
SessionID	El ID de sesión iSCSI.	entero
TargetIP	La dirección IP y el número de puerto del destino de almacenamiento iSCSI.	cadena
Nombre de targetName	El IQN del destino iSCSI.	cadena
TargetPortName	TargetName combinado con la etiqueta de grupo de portal de destino; identifica el puerto de destino.	cadena
Cód. Virtual	El ID de red virtual asociado con la sesión.	entero
ID de volumen	El ID de volumen del volumen asociado con la sesión, si lo hay.	entero
VolumeInstance	Identifica el objeto de volumen asociado con la sesión iSCSI, si lo hubiera.	entero

Obtenga más información

ListISCSISessions

SnapMirrorAggregate

El objeto snapMirrorAggregate contiene información sobre los agregados de ONTAP disponibles, que son colecciones de discos disponibles para los volúmenes como almacenamiento. Puede obtener esta información con el método API ListSnapMirrorAggregates.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
SnapMirrorEndpointID	El ID del sistema ONTAP de destino.	entero
AgregateName	El nombre del agregado.	cadena
Nombre de nodo	El nombre del nodo ONTAP al que pertenece este agregado.	cadena
Disponibles	La cantidad de bytes disponibles que quedan en el agregado.	entero
Tamaño detotal	El tamaño total (en bytes) del agregado.	entero
Porcentaje de capacidad	El porcentaje de espacio en disco actualmente en uso.	entero
Volumen total	La cantidad de volúmenes en el agregado.	entero

SnapMirrorClusterIdentity

El objeto snapMirrorClusterIdentity contiene información de identificación sobre el clúster de ONTAP remoto en una relación de SnapMirror.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
SnapMirrorEndpointID	El ID del sistema ONTAP de destino.	entero
Nombre del clúster	El nombre del clúster de ONTAP de destino.	cadena
ClusterUUID	El identificador único universal de 128 bits del clúster ONTAP de destino.	cadena
ClusterSerialNumber	El número de serie del clúster de ONTAP de destino.	cadena

SnapMirrorEndpoint

El objeto snapMirrorEndpoint contiene información sobre los sistemas de almacenamiento SnapMirror remotos que se comunican con el clúster de almacenamiento de Element. Puede recuperar esta información con el método API ListSnapMirrorEndpoints.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
SnapMirrorEndpointID	El identificador único del objeto del clúster local.	entero
Gestión de IP	La dirección IP de administración del clúster del extremo.	cadena
Nombre del clúster	El nombre del clúster ONTAP. Este valor se rellena automáticamente con el valor "'clustername'" del objeto snapMirrorClusterIdentity.	cadena
nombre de usuario	El nombre de usuario de gestión para el sistema ONTAP.	cadena
Direcciones IP	Lista de direcciones IP de almacenamiento entre clústeres para todos los nodos del clúster. Puede obtener estas direcciones IP con el método ListSnapMirrorNetworkinterfaces.	matriz de cadenas

Nombre	Descripción	Tipo
Conectado	El estado de conectividad del enlace de control al clúster de ONTAP.	booleano

SnapMirrorJobScheduleCronInfo

El objeto snapMirrorJobScheduleCronInfo contiene información sobre una programación de tareas de cron en el sistema ONTAP.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
SnapMirrorEndpointID	El ID del sistema ONTAP de destino.	entero
Nombredetrabajo	El nombre del programa de trabajo.	cadena
JobFinteDescription	Un resumen de la programación generado automáticamente por el usuario.	cadena

SnapMirrorLunInfo

El objeto snapMirrorLunInfo contiene información acerca del objeto de LUN de ONTAP.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
SnapMirrorEndpointID	El ID del sistema ONTAP de destino.	entero
CreationTimestamp	Hora de creación de la LUN.	Cadena de fecha ISO 8601
Nombre del almuerzo	El nombre de la LUN.	cadena
ruta	La ruta de la LUN.	cadena
tamaño	El tamaño en bytes de la LUN.	entero

Nombre	Descripción	Tipo
Dimensionado	La cantidad de bytes que utiliza la LUN.	entero
estado	Estado de acceso actual de la LUN. Los posibles valores son los siguientes: • en línea • sin conexión • lun_externa_error • nvfail • error_espacio	cadena
volumen	El nombre del volumen que contiene el LUN.	cadena
vserver	El Vserver que contiene la LUN.	cadena

SnapMirrorNetworkInterface

El objeto snapMirrorNetworkInterface contiene información acerca de las interfaces lógicas de interconexión de clústeres (LIF).

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
AdministrativeStatus	Si la interfaz lógica (LIF) está habilitada o deshabilitada de manera administrativa. Los posibles valores son los siguientes: • arriba • abajo	cadena
SnapMirrorEndpointID	El ID del sistema ONTAP de destino.	entero
Nombre de interfaz	El nombre de la LIF.	cadena
Dirección de red	La dirección IP de la LIF.	cadena
Máscara de red	La máscara de red del LIF.	cadena

Nombre	Descripción	Tipo
InterfaceRole	El rol de la LIF. Los posibles valores son los siguientes: • undef • clúster • sql server • gestión_nodo • interconexión de clústeres • gestión_clúster	cadena
OperationalStatus	El estado operativo de la LIF (independientemente de que haya formado o no una conexión correcta). Este estado puede diferir del estado administrativo si hay un problema de red que impide el funcionamiento de la interfaz. Los posibles valores son los siguientes: • arriba • abajo	cadena
Nombre del servidor virtual	El nombre del Vserver.	cadena

SnapMirrorNode

El objeto snapMirrorNode contiene información sobre los nodos del clúster de ONTAP de destino en una relación de SnapMirror.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
SnapMirrorEndpointID	El ID del sistema ONTAP de destino.	entero
nombre	El nombre del nodo ONTAP.	cadena
modelo	El modelo del nodo ONTAP.	cadena
SerialNumber	El número de serie del nodo ONTAP.	cadena

Nombre	Descripción	Tipo
ProductVersion	La versión del producto ONTAP.	cadena
IsNodesaludable	El estado de un nodo del clúster de ONTAP. Los posibles valores son los siguientes: • verdadero • falso	cadena
IsNodeadmisible	Tanto si el nodo es apto para participar en un clúster de ONTAP como si no lo es. Los posibles valores son los siguientes: • verdadero • falso	cadena

SnapMirrorPolicy

El objeto snapMirrorPolicy contiene información sobre una política de SnapMirror que se almacena en un sistema ONTAP.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
SnapMirrorEndpointID	El ID del sistema ONTAP de destino.	entero
PolicyName	El nombre único asignado a la política.	cadena
Tipo de póliza	El tipo de política. Los posibles valores son los siguientes: • async_mirror • mirror_vault	cadena
comentar	Una descripción legible asociada a la política de SnapMirror.	cadena

Nombre	Descripción	Tipo
Transferprioridad	Prioridad a la que se ejecuta una transferencia de SnapMirror. Los posibles valores son los siguientes: • Normal: La prioridad predeterminada. Estas transferencias se programan antes de que la mayoría de las transferencias de prioridad baja. • Low: Las transferencias tienen la prioridad más baja y se programan después de las transferencias de prioridad más normales.	cadena
Reglas de la póliza	Una lista de objetos que describen las reglas de políticas.	SnapMirrorPolicyRule cabina
TotKeepCount	El recuento de retención total para todas las reglas de la política.	entero
Reglas totales	El número total de reglas de la política.	entero
Nombre del servidor virtual	Nombre del Vserver para la normativa de SnapMirror.	cadena

SnapMirrorPolicyRule

El objeto snapMirrorPolicyRule contiene información sobre las reglas en una política de SnapMirror.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
SnapMirrorLabel	La etiqueta de la copia Snapshot, utilizada para la selección de copias Snapshot en relaciones de protección de datos ampliadas.	cadena

Nombre	Descripción	Tipo
Recuento de keepCount	Especifica la cantidad máxima de copias de Snapshot que se conservan en el volumen de destino de SnapMirror para una regla.	entero

SnapMirrorRelationship

El objeto snapMirrorRelationship contiene información sobre una relación de SnapMirror entre un volumen de Element y un volumen de ONTAP.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
SnapMirrorEndpointID	El ID del sistema ONTAP de destino.	entero
SnapMirrorRelationship ID	El identificador único de cada objeto snapMirrorRelationship de una cabina, tal y como se devolverá en ListSnapMirrorRelationship. Este UUID se crea y se devuelve en el sistema ONTAP.	cadena
Volumen de origen	Un objeto que describe el volumen de origen.	SnapMirrorVolumeInfo
DestationVolume	Un objeto que describe el volumen de destino.	SnapMirrorVolumeInfo
CurrentMaxTransferRate	La tasa máxima de transferencia actual entre los volúmenes de origen y destino, en kilobytes por segundo.	entero

Nombre	Descripción	Tipo
Es saludable	Si la relación es saludable o no. Los posibles valores son los siguientes: • Cierto: La relación es saludable. • Falso: La relación no es saludable. Esto puede deberse a que una actualización manual o programada falle o se anula, o a que se retrasa la última actualización programada.	booleano
tiempo de espera	La cantidad de tiempo en segundos por el que los datos en el volumen de destino están retrasados por los datos del volumen de origen.	entero
LastTransferDuration	La cantidad de tiempo en segundos que tardó en completarse la última transferencia.	entero
LastTransferError	Mensaje que describe la causa del último fallo de transferencia.	cadena
LastTransferSize	La cantidad total de bytes transferidos durante la última transferencia.	entero
LastTransferEndTimestamp	La Marca de hora del final de la última transferencia.	Cadena de fecha ISO 8601
LastTransferType	El tipo de transferencia anterior en la relación.	cadena
MaxTransferRate	Especifica la tasa máxima de transferencia de datos entre los volúmenes en kilobytes por segundo. El valor predeterminado, 0, es ilimitado y permite que la relación de SnapMirror utilice completamente el ancho de banda de red disponible.	entero

Nombre	Descripción	Tipo
Espejo de estado	El estado de mirroring de la relación de SnapMirror. Los posibles valores son los siguientes: • Inicializado: El volumen de destino no se ha inicializado. • snapmirror: El volumen de destino se ha inicializado y está listo para recibir actualizaciones de SnapMirror. • Broken-off: El volumen de destino es de lectura y escritura y existen snapshots.	cadena
NewestSnapshot	El nombre de la copia de Snapshot más reciente del volumen de destino.	cadena
PolicyName	Especifica el nombre de la política de SnapMirror de ONTAP para la relación. Se puede recuperar una lista de políticas disponibles con ListSnapMirrorPolicies. Los valores de ejemplo son «MirrorLatest» y «MirrorAndVault».	cadena
Tipo de póliza	El tipo de política de SnapMirror de ONTAP para la relación. Consulte ListSnapMirrorPolicies. Los ejemplos son: «'duplicación_asíncrona'» o «espejo_asíncrono».	cadena
RelationshiProgress	El número total de bytes que se han procesado hasta ahora para la actividad actual de la relación como devuelto en el estado relación. Esto se establece sólo cuando el miembro "relationsStatus" indica que una actividad está en curso.	entero

Nombre	Descripción	Tipo
Estado de las relaciones	El estado de la relación de SnapMirror. Los posibles valores son los siguientes: • inactivo • transfiriendo • comprobando • ralentización • en modo inactivo • en cola • preparando • finalizando • anulando • rompiendo	cadena
RelationshipType	El tipo de relación de SnapMirror. En los clústeres de almacenamiento que ejecutan el software Element, este valor siempre es «'Extended_data_protection».	cadena
Nombre de la pila	El nombre de la programación cron preexistente del sistema ONTAP que se utiliza para actualizar la relación SnapMirror. Se puede recuperar una lista de programaciones disponibles con ListSnapMirrorSchedules.	cadena
UnhealthyCausa	La razón por la que la relación no es saludable.	cadena

SnapMirrorVolume

El objeto snapMirrorVolume contiene información sobre un volumen ONTAP.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
SnapMirrorEndpointID	El ID del sistema ONTAP de destino.	entero

Nombre	Descripción	Tipo
nombre	El nombre del volumen.	cadena
tipo	El tipo de volumen. Los posibles valores son los siguientes: • rw: Volumen de lectura/escritura • ls: Volumen de carga compartida • dp: Volumen de protección de datos	cadena
vserver	El nombre del Vserver al que pertenece este volumen.	cadena
Nombre de aggrName	El nombre del agregado que contiene.	cadena
estado	El estado del volumen. Los posibles valores son los siguientes: • en línea • restringida • sin conexión • mixto	cadena
tamaño	El tamaño total del sistema de archivos (en bytes) del volumen.	cadena
Tamaño disponible	El tamaño (en bytes) del espacio disponible en el volumen.	cadena

SnapMirrorVolumeInfo

El objeto snapVolumeInfo contiene información sobre la ubicación de un volumen en una relación de SnapMirror, como su nombre y tipo.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
tipo	El tipo de volumen. Los posibles valores son los siguientes: • SolidFire: El volumen reside en un clúster de almacenamiento que ejecuta el software Element. • ONTAP: El volumen reside en un clúster de ONTAP remoto.	cadena
ID de volumen	El ID del volumen. Sólo válido si "type" es SolidFire.	entero
vserver	El nombre del Vserver al que pertenece este volumen. Sólo válido si "type" es ONTAP.	cadena
nombre	El nombre del volumen.	cadena

SnapMirrorVServer

El objeto snapMirrorVServer contiene información sobre las máquinas virtuales de almacenamiento (o vServers) en el clúster ONTAP de destino.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
SnapMirrorEndpointID	El ID del sistema ONTAP de destino.	entero
Nombre del servidor virtual	El nombre del Vserver.	cadena
VserverType	El tipo de Vserver. Los posibles valores son los siguientes: • sql server • admin • sistema • nodo	cadena

Nombre	Descripción	Tipo
VserverSubtype	Subtipo del Vserver. Los posibles valores son los siguientes: • predeterminado • dp_destino • sql server • origen_sinc • sync_destination	cadena
RootVolume	El volumen raíz del Vserver.	cadena
RootVolumeagregate	El agregado en el que se creará el volumen raíz.	cadena
VserveragregateInfo	Matriz de objetos snapMirrorVserveragregateInfo.	Objeto JSON
AdminState	Estado administrativo detallado del Vserver. Los posibles valores son los siguientes: • ejecutando • detenido • iniciando • parar • inicializando • eliminando	cadena
OperacionalState	Estado operativo básico del Vserver. Los posibles valores son los siguientes: • ejecutando • detenido	cadena

SnapMirrorVserveragregateInfo

El objeto snapMirrorVserveragregateInfo contiene información sobre los datos disponibles Storage Virtual Machines (también llamados vServers) en el clúster ONTAP de destino.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Nombre de aggrName	El nombre del agregado asignado a un Vserver.	cadena
AgAvailSize	El tamaño disponible del agregado asignado.	entero

snapshot

El objeto Snapshot contiene información sobre una snapshot realizada para un volumen. Puede utilizar el `ListSnapshots` Método API para recuperar una lista de información de snapshot de un volumen o de todos los volúmenes. El objeto incluye información sobre la snapshot activa, así como cada snapshot creada para un volumen.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON
suma de comprobación	Una pequeña representación de cadena de los datos de la instantánea almacenada. Esta suma de comprobación se puede utilizar más adelante para comparar otras instantáneas con el fin de detectar errores en los datos.	cadena
CreateTime	La hora a la que se formateó la copia de Snapshot en UTC+0.	Cadena de fecha ISO 8601
EnableRemoteReplication	Identifica si Snapshot está habilitada para la replicación remota.	booleano

Nombre	Descripción	Tipo
ExpiraciónCausa	Indica cómo se establece la caducidad de la instantánea. Los posibles valores son los siguientes: • API: El tiempo de caducidad se establece mediante la API. • Ninguno: No se establece el tiempo de caducidad. • Prueba: El tiempo de caducidad se establece para la prueba. • fifo: La caducidad se produce primero en salir.	cadena
Tiempo de caducidad	La hora en la que caducará esta snapshot y se purgará del clúster.	Cadena de fecha ISO 8601
ID de grupo	El ID de grupo si la copia de Snapshot forma parte de una copia de Snapshot de grupo.	entero
SnapgroupshotUUID	Contiene información sobre cada snapshot del grupo. Cada uno de estos miembros tendrá un parámetro UUID para el UUID de la snapshot.	cadena
InstanceCreateTime	La hora a la que se creó la snapshot en el clúster local.	Cadena de fecha ISO 8601
InstanceSnapshotUUID	El ID único universal de la snapshot en el clúster local. Este ID no se replica en otros clústeres.	cadena
nombre	El nombre exclusivo que se asigna a la copia de Snapshot. Si no se especifica ningún nombre, el nombre es la Marca de hora con formato UTC+0 del momento en que se creó la copia de Snapshot.	cadena
RemoteStatuses	Una cabina que contiene el identificador universal y el estado de replicación de cada snapshot remota en el clúster de destino como se ve en el clúster de origen.	RemoteClusterSnapshotStatus cabina

Nombre	Descripción	Tipo
SnapMirrorLabel	La etiqueta que utiliza el software SnapMirror para especificar la política de retención de snapshots en extremos de SnapMirror. Si no se establece, este valor es nulo.	cadena
ID de copia Snapshot	El ID exclusivo de una snapshot existente.	cadena
UUID de copia Snapshot	El ID único universal de una instantánea existente. Cuando la Snapshot se replica en los clústeres, este ID se replica junto con ella y se utiliza para identificar la copia de Snapshot entre los clústeres.	cadena
estado	Estado actual de la copia de Snapshot de grupo. Los posibles valores son los siguientes: • Unknown: Se produjo un error al obtener el estado de la snapshot. • Preparing: Esta copia de Snapshot se está preparando para poder usarla y aún no se puede escribir en ella. • RemoteSyncing: Esta snapshot se está replicando desde un clúster remoto. • Done: Esta snapshot se ha terminado de preparar o replicar y se puede usar. • Active: Esta copia de Snapshot es la rama activa. • Clonación: Esta instantánea está involucrada en una operación de copia de volumen.	cadena
Tamaño total	El tamaño total en bytes de la copia de Snapshot.	entero
ID de volumen virtual	El ID del volumen virtual asociado con esta copia de Snapshot.	UUID

Nombre	Descripción	Tipo
ID de volumen	El ID del volumen a partir del cual se creó la copia de Snapshot.	entero
Nombre de volumen	El nombre del volumen en el momento en que se creó la copia de Snapshot.	cadena

Obtenga más información

ListSnapshots

SnmpTrapRecipient

El objeto snmpTrapRecipient contiene información acerca de un host que está configurado para recibir capturas SNMP generadas por el clúster de almacenamiento. Puede utilizar el `GetSnmpTrapInfo` Método de API para obtener una lista de hosts configurados para recibir capturas SNMP.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
host	La dirección IP o el nombre de host del host de destino.	cadena
puerto	El número de puerto UDP del host en el que se debe enviar la captura. El intervalo válido es de 1 a 65535. 0 (cero) no es un número de puerto válido. El puerto predeterminado es 162.	entero
comunidad netapp	Cadena de comunidad SNMP.	cadena

Contenedor de almacenamiento

El objeto Storage Container contiene los atributos de un contenedor de almacenamiento de volúmenes virtuales. Puede recuperar esta información para cada contenedor de almacenamiento del clúster mediante el `ListStorageContainers` Método API.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de cuenta	El ID de la cuenta del sistema de almacenamiento asociada con el contenedor de almacenamiento.	entero
InitiatorSecret	El secreto de autenticación CHAP del iniciador asociado con el contenedor de almacenamiento.	cadena
nombre	El nombre del contenedor de almacenamiento.	cadena
ProtocolEndpointType	El tipo de extremo de protocolo del contenedor de almacenamiento. SCSI es el único valor válido.	cadena
estado	El estado del contenedor de almacenamiento. Los posibles valores son los siguientes: • Active: El contenedor de almacenamiento está en uso. • Locked: El contenedor de almacenamiento está bloqueado.	cadena
ID de almacenamiento ContainerID	El ID único del contenedor de almacenamiento.	UUID
TargetSecret	El secreto de autenticación CHAP para el destino asociado con el contenedor de almacenamiento.	cadena
VirtualVolumes	Una lista de ID de los volúmenes virtuales asociados con el contenedor de almacenamiento.	Cabina de UUID

Obtenga más información

ListStorageContainers

SyncJob

El objeto syncJob contiene información sobre los trabajos de clonado, replicación remota o sincronización de segmentos que se ejecutan en un clúster.

Puede recuperar la información de sincronización con `ListSyncJobs` Método API.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
BlocksPerSecond	La cantidad de bloques de datos que se transfieren por segundo del clúster de origen al clúster de destino. Presente sólo si el miembro del tipo está establecido en remoto.	entero
BranchType	Devuelto solo para trabajos de sincronización de replicación remota. Los posibles valores son los siguientes: • snapshot • volumen	cadena
BytesPerSecond	La cantidad de bytes que se procesa por segundo el clon. Presente solo si el miembro del tipo está establecido en clone o slice.	flotante
ClonID	El identificador de la operación de clonado en curso. Presente solo si el miembro del tipo está establecido en clone.	entero
Bytes de currentBytes	La cantidad de bytes que procesó el clon en el volumen de origen. Presente solo si el miembro del tipo está establecido en clone o slice.	entero
DstServiceID	El identificador de servicio que aloja la réplica principal del volumen. Presente sólo si el miembro del tipo está establecido en remoto.	entero
DstVolumeID	El ID del volumen de destino. Presente solo si el miembro del tipo está establecido en clone o remote.	entero

Nombre	Descripción	Tipo
Elatiempo	El tiempo transcurrido en segundos desde que se inició el trabajo de sincronización.	flotante o entero según el tipo de operación de sincronización
GroupCloneID	El ID de la operación de clonado de grupo en curso.	entero
NodeID	Especifica el nodo en el que se produce el clon. Presente solo si el miembro del tipo está establecido en clone.	entero
Porcentaje completado	El porcentaje de finalización del trabajo de sincronización.	flotante o entero según el tipo de operación de sincronización
RemasterHora	El tiempo estimado en segundos para completar la operación.	flotante
ID de sliceID	El ID de la unidad de segmentos que se está sincronizando.	entero
etapa	Presente solo si el miembro del tipo está establecido en remoto o clon. Los posibles valores son los siguientes: • Metadatos: La replicación está en proceso de determinar qué datos se deben transferir al clúster remoto. No se informa del estado para esta etapa del proceso de replicación. • Data: La replicación está en proceso de transferir la mayor parte de los datos al clúster remoto. • Entero: Indica la compatibilidad con versiones anteriores del corte para trabajos de sincronización de cortes.	cadena
ID de copia Snapshot	El ID de la copia de Snapshot a partir de la cual se creó el clon. Presente solo si el miembro del tipo está establecido en clone.	entero
SrcServiceID	El ID del servicio de origen.	entero

Nombre	Descripción	Tipo
SrcVolumeID	El ID del volumen de origen.	entero
Bytes en totalBytes	La cantidad total de bytes del clon. Presente solo si el miembro del tipo está establecido en clone o slice.	entero
tipo	El tipo de operación de sincronización. Los posibles valores son los siguientes: • clonar • corte • bloque • remoto	cadena

Obtenga más información

ListSyncJobs

tarea (volúmenes virtuales)

El objeto de la tarea contiene información acerca de una tarea de volumen virtual que se está ejecutando o finalizó en el sistema. Puede utilizar el `ListVirtualVolumeTasks` método para recuperar esta información de todas las tareas de volúmenes virtuales.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
cancelada	Indica si la tarea se ha cancelado o no. Los posibles valores son los siguientes: • verdadero • falso	booleano
VirtualVolumeID	El ID único de volumen virtual del volumen virtual que se está clonando (para tareas de clonado).	UUID

Nombre	Descripción	Tipo
PartentMetadata	Objeto que contiene metadatos del elemento principal para tareas que clonan o crean snapshots de un volumen virtual.	Objeto JSON
PartentTotalSize	El espacio total disponible (en bytes) en el elemento principal para tareas de clonado o snapshot.	entero
ParentUsedSize	El espacio utilizado del elemento principal (en bytes) para tareas de clonado o snapshot.	entero
funcionamiento	El tipo de operación que ejecuta la tarea. Los posibles valores son los siguientes: • Unknown: La operación de la tarea es desconocida. • Prepare: La tarea está preparando un volumen virtual. • Snapshot: La tarea está creando una copia de Snapshot de un volumen virtual. • Rollback: La tarea está revirtiendo un volumen virtual a una copia de Snapshot. • Clone: La tarea está creando un clon del volumen virtual. • FastClone: La tarea está creando un clon rápido de un volumen virtual. • CopyDiffs: La tarea está copiando bloques distintos en un volumen virtual.	cadena

Nombre	Descripción	Tipo
estado	El estado actual de la tarea de volumen virtual. Los posibles valores son los siguientes: • Error: La tarea no se realizó correctamente y devolvió un error. • Queued: La tarea está a la espera de ser ejecutada. • Running: La tarea se encuentra en ejecución. • Success: La tarea se completó correctamente.	cadena
VirtualVolumeHostID	El ID único del host que inició la tarea.	UUID
ID de volumen virtual	El nuevo ID exclusivo de volumen virtual (para tareas que crean un nuevo volumen virtual).	UUID
VirtualVolumeTaskID	El ID único de la tarea.	UUID

Obtenga más información

ListVirtualVolumeTasks

UsumUsuario

Puede utilizar el objeto usmUser de SNMP con `SetSnmpInfo` Método de API para configurar SNMP en el clúster de almacenamiento.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
acceso	Tipo de acceso SNMP para este usuario. Los posibles valores son los siguientes: • Rousser: Acceso de sólo lectura. • Rwuser: Acceso de lectura y escritura. Todos los objetos MIB del software Element son de solo lectura.	cadena
nombre	El nombre del usuario.	cadena
contraseña	La contraseña del usuario.	cadena
frase de contraseña	La frase de acceso del usuario.	cadena
SecLevel	El tipo de credenciales necesarias para este usuario. Los posibles valores son los siguientes: • Noauth: No se requiere contraseña ni frase de contraseña. • Auth: Se necesita una contraseña para el acceso de los usuarios. • priv: Se necesita una contraseña y una contraseña para el acceso del usuario.	cadena

Obtenga más información

SetSnmpInfo

VirtualNetwork

El objeto virtualNetwork contiene información acerca de una red virtual específica. Puede utilizar el `ListVirtualNetworks` Método API para recuperar una lista de esta información de todas las redes virtuales del sistema.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Bloqueos de direcciones	El rango de bloques de direcciones actualmente asignados a la red virtual. Miembros: • Disponible: Cadena binaria en "1"s y "0"s. "1" indica que la dirección IP está disponible y "0" indica que la dirección IP no está disponible. La cadena se lee de derecha a izquierda, siendo el dígito a la derecha la primera dirección IP de la lista de bloques de direcciones. • Size: El tamaño de este bloque de direcciones. • Start: La primera dirección IP del bloque.	Cabina de objetos JSON
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON
nombre	El nombre asignado a la red virtual.	cadena
máscara de red	La dirección IP de la máscara de red de la red virtual.	cadena
svip	La dirección IP de almacenamiento de la red virtual.	cadena
puerta de enlace	La puerta de enlace utilizada para la red virtual.	cadena
Cód. Virtual	El identificador único de una red virtual.	entero
VirtualNetworkTag	El identificador de etiqueta de VLAN.	entero

Obtenga más información

ListVirtualNetworks

Volumen virtual

El objeto virtualVolume contiene información de configuración acerca de un volumen virtual, así como información acerca de las instantáneas del volumen virtual. No incluye información sobre el tiempo de ejecución ni el uso. Puede utilizar el

`ListVirtualVolumes` método para recuperar esta información de un clúster.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
vinculaciones	Una lista de ID de vinculación para este volumen virtual.	Cabina de UUID
niños	Una lista de UUID de volumen virtual que son secundarios de este volumen virtual.	Cabina de UUID
descendientes	Cuando pasa recursivo: True al método ListVirtualVolumes, contiene una lista de UUID de volumen virtual que son descendientes de este volumen virtual.	Cabina de UUID
metadatos	Parejas clave-valor de los metadatos del volumen virtual, como el tipo de volumen virtual, el tipo de SO invitado, etc.	Objeto JSON
ID de parentVirtualVolumeID	El ID de volumen virtual del volumen virtual principal. Si el ID solo está formado por ceros, indica que se trata de un volumen virtual independiente y no tiene ningún enlace a un volumen principal.	UUID
ID de copia Snapshot	El ID de la snapshot de volumen subyacente. Este valor es "0" si el volumen virtual no representa una snapshot de.	entero
SnapshotInfo	Objeto de instantánea para la instantánea asociada (null si no ixestent).	snapshot

Nombre	Descripción	Tipo
estado	El estado actual del volumen virtual. Los posibles valores son los siguientes: • Clone: El volumen virtual se está procesando en respuesta a una operación de clon o snapshot. • Waiting: El volumen virtual está esperando a que se complete una operación Snapshot. • Ready: El volumen virtual está listo para uso general.	cadena
Contenedor de almacenamiento	Un objeto que describe el contenedor de almacenamiento que posee este volumen virtual.	Contenedor de almacenamiento
ID de volumen virtual	El ID exclusivo del volumen virtual.	UUID
VirtualVolumeType	El tipo de volumen virtual.	cadena
ID de volumen	El ID del volumen subyacente.	entero
VolumeInfo	Cuando pase detalles: True para el método ListVirtualVolumes, este miembro es un objeto que describe el volumen.	volumen

Obtenga más información

- ListVirtualVolumes
- snapshot
- Contenedor de almacenamiento
- volumen

volumen

El objeto de volumen contiene información de configuración acerca de los volúmenes emparejados o desemparejados. No incluye información de tiempo de ejecución ni de uso, y no contiene información acerca de los volúmenes virtuales.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
acceso	El tipo de acceso permitido para el volumen. Los posibles valores son los siguientes: • `readOnly`: Sólo se permiten operaciones de lectura. • `readWrite`: Se permiten lecturas y escrituras. • `locked`: No se permiten lecturas ni escrituras. • `replicationTarget`: Designado como volumen objetivo en un par de volúmenes replicado.	cadena
ID de cuenta	El ID de cuenta de la cuenta que contiene el volumen.	entero
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON
Tamaño del bloque	El tamaño de los bloques en el volumen.	entero
CreateTime	La hora con formato UTC+0 se creó el volumen.	Cadena ISO 8601
Plan de protección de currentScheme	El esquema de protección que se está utilizando para este volumen. Si un volumen se convierte de un esquema de protección a otro, este miembro refleja el esquema de protección al que se está convirtiendo el volumen.	cadena
DeleteTime	La hora con formato UTC+0 se eliminó el volumen.	Cadena ISO 8601
enable512e	Si se establece en TRUE, el volumen proporciona una emulación de sector de 512 bytes.	booleano
EnableSnapMirrorReplication	Tanto si el volumen se puede usar para la replicación con extremos de SnapMirror.	booleano

Nombre	Descripción	Tipo
Tamaño 50	Especifica la cantidad máxima de instantáneas del volumen que se mantendrán simultáneamente si se utiliza el modo de retención de snapshots First in-first-out (FIFO).	entero
iqn	El nombre completo de iSCSI correspondiente al volumen.	cadena
LastAccessTime	La última vez que se produjo cualquier acceso (incluidas las operaciones de I/o) al volumen (con el formato UTC+0). Si no se conoce la última hora de acceso, este valor es nulo.	Cadena ISO 8601
LastAccessTimeIO	La última vez que se produjo cualquier I/o en el volumen (con formato UTC+0). Si no se conoce la última hora de acceso, este valor es nulo.	Cadena ISO 8601
MinFioSize	Especifica la cantidad mínima de ranuras de snapshot reservadas simultáneamente por el volumen si se utiliza el modo de retención de snapshot del primero en entrar primero en salir (FIFO).	entero
nombre	El nombre del volumen según lo proporcionado en el momento de creación.	cadena
Esquema de protección previa	Si un volumen se convierte de un esquema de protección a otro, este miembro refleja el esquema de protección del que se está convirtiendo el volumen. Este miembro no cambia hasta que se inicia una conversión. Si un volumen nunca se convirtió, este miembro es nulo.	cadena
Tiempo purgable	La hora con formato UTC+0 se purgó el volumen del sistema.	Cadena ISO 8601
calidad de servicio	La configuración de calidad de servicio para este volumen.	Calidad de servicio

Nombre	Descripción	Tipo
QosPolicyID	El ID de política de calidad de servicio asociado con el volumen. El valor es nulo si el volumen no se asocia con una política.	entero
SsiEUIDeviceID	El identificador global exclusivo de dispositivo SCSI para el volumen en un formato de 16 bytes basado en EUI-64.	cadena
SsiNAADeviceID	El Identificador global exclusivo de dispositivo SCSI para el volumen en el formato extendido registrado de NAA según la norma IEEE.	cadena
Recuento de sliceos	El número de cortes en el volumen. Este valor es siempre "1".	entero
estado	El estado actual del volumen. Los posibles valores son los siguientes: • Init: Volumen que se está inicializando y no está listo para conexiones. • Active: Un volumen activo listo para las conexiones. • Deleted: Un volumen que se ha marcado para su eliminación, pero no se ha purgado todavía.	cadena
Tamaño total	Los bytes totales de capacidad aprovisionada.	entero
ID de volumen virtual	El ID único de volumen virtual asociado con el volumen, si lo hubiera.	UUID
VolumeAccessGroups	Lista de ID pf los grupos de acceso de volúmenes a los que pertenece un volumen. Este valor es una lista vacía si un volumen no pertenece a ningún grupo de acceso de volúmenes.	matriz en números enteros
VolumeConsistencyGroupUUID	El ID único universal del grupo de coherencia de volúmenes del que forma parte el volumen.	UUID

Nombre	Descripción	Tipo
ID de volumen	El ID de volumen único para el volumen.	entero
VolumePairs	Información acerca de un volumen emparejado. Solo es visible si un volumen está emparejado. Este valor es una lista vacía si el volumen no está emparejado.	Pareja de volúmenes cabina
VolumeUUID	El ID único universal del volumen.	UUID

Obtenga más información

- ListActiveVolumes
- ListDeletedVolumes
- ListVolumes
- ListVolumesForAccount
- Calidad de servicio

VolumeAccessGroup

El objeto volumeAccessGroup contiene información sobre un grupo de acceso de volúmenes específico. Se puede recuperar una lista de esta información para todos los grupos de acceso con el método API `ListVolumeAccessGroups`.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON
DeletedVolumes	La cabina de volúmenes que se eliminó del grupo de acceso de volúmenes que aún no se purgó del sistema.	matriz en números enteros
IniciatorID	Una lista de ID de iniciadores que se asignan al grupo de acceso de volúmenes.	matriz en números enteros

Nombre	Descripción	Tipo
iniciadores	Cabina de iniciadores IQN/WWPN únicos que se asignan al grupo de acceso de volúmenes.	matriz de cadenas
nombre	El nombre del grupo de acceso de volúmenes.	cadena
VolumeAccessGroupID	El identificador exclusivo de VolumeAccessGroupID para el grupo de acceso de volúmenes.	entero
volúmenes	Una lista de los ID de volumen que pertenecen al grupo de acceso de volúmenes.	matriz en números enteros

Obtenga más información

ListVolumeAccessGroups

Pareja de volúmenes

El objeto volumePair contiene información sobre un volumen que está emparejado con otro volumen en un clúster diferente. Si el volumen no está emparejado, este objeto está vacío. Puede utilizar el `ListActivePairedVolumes` y.. `ListActiveVolumes` Los métodos de API para obtener información acerca de los volúmenes emparejados.

Miembros de objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ClusterPairID	El clúster en el que está emparejado el volumen.	entero

Nombre	Descripción	Tipo
RemoteReplication	Detalles sobre la replicación de volúmenes. Miembros: • Mode: (Cadena) uno de los modos "asíncrono", "Sync" o "SnapshotsOnly". • PauseLimit: (Integer) sólo uso interno. • RemoteServiceID: (Entero) el ID del servicio de segmentos remotos. • ResumeDetails: (Cadena) reservado para uso futuro. • SnapshotReplication (objeto JSON) ◦ state: (Cadena) el estado de la replicación de snapshot en curso, si hay alguna en curso. ◦ StateDetails: (Cadena) reservado para uso futuro. • state: (Cadena) el estado de la replicación de volumen. • StateDetails: (Cadena) reservado para uso futuro.	Objeto JSON
RemoteSliceID	El ID de segmento definido por el clúster en el clúster remoto.	entero
ID de volumen remoto	El ID del volumen en el clúster remoto con el que se empareja el volumen local.	entero
RemoteVolumeName	El nombre del volumen remoto.	cadena
VolumePairUUID	Identificador único universal definido por el clúster para este emparejamiento en un formato canónico.	cadena

Obtenga más información

- ListActivePairedVolumes
- ListActiveVolumes

VolumeStats

El objeto volumeStats contiene datos estadísticos para un volumen individual.

Miembros de objeto

Es posible usar los siguientes métodos para obtener objetos volumeStats de algunos o todos los volúmenes:

- GetVolumeStats
- ListVolumeStatsByAccount
- ListVolumeStatsByVolume
- ListVolumeStatsByVolumeAccessGroup

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Cálculo	Tipo
ID de cuenta	El ID de la cuenta del propietario del volumen.	N.A.	entero
Actuales de IOPS	El IOPS real actual del volumen en los últimos 500 milisegundos.	Momento específico	entero
Establish asyncDelay	El tiempo transcurrido desde que el volumen se sincronizó por última vez con el clúster remoto. Si el volumen no se empareja, esto es nulo. **Nota:** un volumen de destino en un estado de replicación activo siempre tiene una recopilación de 0 (cero). Los volúmenes de destino tienen en cuenta los sistemas durante la replicación y suponen que establish asyncDelay es preciso en todo momento.	N.A.	Cadena de duración ISO 8601 o nula
AverageIOPSize	El tamaño promedio en bytes de I/o reciente en el volumen en los últimos 500 milisegundos.	Momento específico	entero

Nombre	Descripción	Cálculo	Tipo
BurstIOPSCredit	La cantidad total de créditos de IOP disponibles para el usuario. Cuando los volúmenes no utilizan el valor máximo de IOPS configurado, los créditos se acumulan.	N.A.	entero
Profundidad de clientQueueDepth	Número de operaciones de lectura y escritura pendientes en el volumen.	N.A.	entero
DesiredMetadataHosts	Los servicios de metadatos (slice) que se están migrando a si los metadatos del volumen se migran entre los servicios de metadatos. Un valor "nulo" significa que el volumen no se está migrando.	N.A.	Objeto JSON
LatencyUSec	El tiempo medio, en microsegundos, para completar operaciones al volumen en los últimos 500 milisegundos. Un valor de "0" (cero) significa que no hay operaciones de I/o en el volumen.	Momento específico	entero

Nombre	Descripción	Cálculo	Tipo
MetadataHosts	Los servicios de metadatos (slice) en los que reside los metadatos del volumen. Los posibles valores son los siguientes: • Primario: Los servicios de metadatos principales que alojan el volumen. • LiveSegundaries: Servicios de metadatos secundarios que están actualmente en un estado "vivo". • Servicios de metadatos secundarios que están en un estado muerto.	N.A.	Objeto JSON
IOPS normalizadas	Número medio de IOPS para todo el clúster en los últimos 500 milisegundos.	Momento específico	entero
No ZeroBlocks	El número total de bloques de 4 KiB con datos después de haber completado la última operación de recopilación de basura.	N.A.	entero
ReadBytes	Los bytes acumulativos totales leídos en el volumen desde la creación del volumen.	El incremento monotónicamente	entero
ReadBytesLastSample	La cantidad total de bytes leídos en el volumen durante el último período de muestra.	Momento específico	entero

Nombre	Descripción	Cálculo	Tipo
ReadLatencyUSec	El tiempo medio, en microsegundos, para completar operaciones de lectura del volumen en los últimos 500 milisegundos.	Momento específico	entero
ReadLatencyUSectotal	El tiempo total dedicado a realizar operaciones de lectura desde el volumen.	El incremento monotónicamente	entero
Operaciones de lectura	Las operaciones de lectura totales en el volumen desde la creación del volumen.	El incremento monotónicamente	entero
ReadOpsLastSample	La cantidad total de operaciones de lectura durante el último periodo de muestra.	Momento específico	entero
SamplePeriodSec	La duración del período de la muestra, en milisegundos.	N.A.	entero
acelerador	Un valor flotante entre 0 y 1 que representa cuánto regula el sistema a los clientes que están por debajo del valor máximo de IOPS debido a la repetición de la replicación de datos, errores puntuales y copias de Snapshot tomadas.	N.A.	flotante
fecha/hora	La hora actual en formato UTC+0.	N.A.	Cadena de fecha ISO 8601
UnaligedReads	Las operaciones de lectura no alineadas acumulativas totales en un volumen desde la creación del volumen.	El incremento monotónicamente	entero

Nombre	Descripción	Cálculo	Tipo
UnaligedWrites	Las operaciones de escritura acumulativas totales sin alinear en un volumen desde la creación del volumen.	El incremento monotónicamente	entero
VolumeAccessGroups	La lista de ID de los grupos de acceso de volúmenes a los que pertenece un volumen.	N.A.	matriz en números enteros
ID de volumen	El ID del volumen.	N.A.	entero
VolumeSize	La capacidad total aprovisionada en bytes.	N.A.	entero

Nombre	Descripción	Cálculo	Tipo
VolumeUtilización	Un valor de punto flotante que describe todas las funcionalidades de entrada/salida del cliente que están usando las funcionalidades de I/o del volumen en comparación con el valor de calidad de servicio máximo de ese volumen. Los posibles valores son los siguientes: • 0: El cliente no está usando el volumen. • 0.01 a 0.99: El cliente no utiliza por completo las funcionalidades de IOPS del volumen. • 1.00: El cliente está utilizando completamente el volumen hasta el límite de IOPS establecido por el valor de maxIOPS. • > 1.00: El cliente utiliza más del límite establecido por maxIOPS. Esto es posible cuando el valor de calidad de servicio de burstIOPS se establece en mayor que maxIOPS. Por ejemplo, si el valor de maxIOPS se establece en 1000 y el valor de burstIOPS se establece en 2000, el `volumeUtilizatio n` el valor sería 2.00 si el cliente utiliza el volumen por completo.	N.A.	flotante

Nombre	Descripción	Cálculo	Tipo
Bytes de escritura	Los bytes acumulativos totales escritos en el volumen desde la creación del volumen.	El incremento monotónicamente	entero
WriteBytesLastSample	La cantidad total de bytes escritos en el volumen durante el último período de muestra.	El incremento monotónicamente	entero
WriteLatencyUSec	El tiempo medio, en microsegundos, para completar operaciones de escritura a un volumen en los últimos 500 milisegundos.	Momento específico	entero
WriteLatencyUSectotal	El tiempo total dedicado a realizar operaciones de escritura en el volumen.	El incremento monotónicamente	entero
Operaciones de escritura	Las operaciones de escritura acumulativas totales en el volumen desde la creación del volumen.	El incremento monotónicamente	entero
WriteOpsLastSample	La cantidad total de operaciones de escritura durante el último periodo de muestra.	Momento específico	entero
Cierres de ceros	El número total de bloques vacíos de 4 KiB sin datos después de haber completado la última ronda de recopilación de basura.	Momento específico	entero

Métodos comunes

Los métodos comunes son los que se utilizan para recuperar información sobre el clúster de almacenamiento, la propia API o las operaciones de API continuas.

- GetAPI
- GetAsyncResult
- GetCompleteStats

- GetLimits
- GetOrigin
- GetRawStats
- ListAsyncResults

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

GetAPI

Puede utilizar el `GetAPI` Método para obtener una lista de todos los métodos de API y los extremos de API compatibles que se pueden usar en el sistema.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
<version>	Una lista de todos los métodos de API compatibles para esta versión de software, donde <version> es la versión de software actual que este sistema ejecuta.	matriz de cadenas
CurrentVersion	La versión actual del software de clúster de almacenamiento.	cadena
SoporteVersions	Una lista de todos los extremos de API que admite el sistema.	matriz de cadenas

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetAPI",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```
{
"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

Puede utilizar `GetAsyncResult` para recuperar el resultado de las llamadas de método asíncrono. Algunas llamadas a métodos requieren cierto tiempo para ejecutarse y es posible que no se hayan completado cuando el sistema envía la respuesta inicial. Para obtener el estado o el resultado de la llamada al método, utilice `GetAsyncResult` Para sondear el valor de la mano devuelto por el método.

`GetAsyncResult` devuelve el estado general de la operación (en curso, completado o error) de forma estándar, pero los datos reales devueltos para la operación dependen de la llamada al método original y los datos devueltos se documentan con cada método.

Si falta el parámetro keepResult o FALSE, el comando establish asyncHandle se desactiva cuando se devuelve el resultado, y más tarde intenta consultar que el comando establish devuelvan un error. Puede mantener activo el comando establish de la ley para consultas futuras estableciendo el parámetro keepResult en TRUE.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Establish asyncHandle	Valor devuelto por la llamada de método asíncrono original.	entero	Ninguno	Sí
KeepResult	Si es True, GetAsyncResult no elimina el resultado asíncrono al devolverlo, lo que permite consultas futuras a ese establish de generar datos.	booleano	falso	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
estado	Estado de la llamada de método asíncrono. Los posibles valores son los siguientes: • Running: El método se sigue ejecutando. • Completo: El método está completo y el resultado o error está disponible.	cadena
resultado	Si el método asíncrono se completó correctamente, esto es el resultado de la operación asíncrona. Si la operación asíncrona falla, este miembro no está presente.	cadena

Nombre	Descripción	Tipo
error	Si el estado es completo y el método asíncrono con errores, este miembro incluye los detalles del error. Si la operación asincrónica se realiza correctamente, este miembro no está presente.	cadena
ResultType	Tipo de operación que está realizando o estaba realizando la llamada de método asíncrono.	cadena
detalles	Si el estado es en ejecución, este miembro incluye información relevante para la operación actual del método. Si el método asíncrono no se está ejecutando, este miembro no está presente.	Objeto JSON
CreateTime	La hora a la que se llamó al método asíncrono, en formato UTC+0.	Cadena de fecha ISO 8601
LastUpdateTime	La hora a la que se actualizó por última vez el estado del método asíncrono, en formato UTC+0.	Cadena de fecha ISO 8601

Nota: el valor devuelto de GetAsyncResult es esencialmente una versión anidada de la respuesta JSON estándar con un campo de estado adicional.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetAsyncResult",
  "params": {
      "asyncHandle" : 389
},
"id" : 1
}
```

Ejemplo de respuesta: Error de método

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "error": {
      "code": 500,
      "message": "DBClient operation requested on a non-existent path at
[/asyncresults/1]",
      "name": "xDBNoSuchPath"
   },
   "id": 1
}
```

Si la "respuesta" fuera el objeto de respuesta JSON de la llamada GetAsyncResult, entonces "Response.error" correspondería a un error con el propio método GetAsyncResult (como consultar un handle no existente).

Ejemplo de respuesta: Error de tarea asíncrona

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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"
   }
}
```

El "esponse.result.error" correspondería a un resultado de error de la llamada al método original.

Ejemplo de respuesta: Tarea asíncrona correcta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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"
   }
}
```

"Esponse.result.result" es el valor devuelto por la llamada al método original si la llamada se ha completado correctamente.

Nuevo desde la versión

9.6

GetCompleteStats

La ingeniería de NetApp utiliza el `GetCompleteStats` Método API para probar nuevas funciones. Los datos devueltos de `GetCompleteStats` no está documentado, cambia con frecuencia y no se garantiza que sea preciso. No debe utilizar `GetCompleteStats` Para recoger datos de rendimiento o cualquier otra integración de gestión con un clúster de almacenamiento que ejecuta el software Element.

Utilice los siguientes métodos API compatibles para recuperar información estadística:

- GetVolumeStats
- GetClusterStats
- GetNodeStats
- GetDriveStats

Nuevo desde la versión

9.6

GetLimits

Puede utilizar el `GetLimits` Método para obtener los valores de límite definidos por la API. Estos valores pueden cambiar entre las versiones de elemento, pero no cambian sin una actualización del sistema. Conocer los valores de límite establecidos por la API

puede ser útil al escribir scripts de API para herramientas orientadas al usuario.

> La `GetLimits` Método devuelve los límites de la versión de software actual independientemente de la versión de extremo de API utilizada para pasar el método.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método devuelve un objeto JSON con parejas nombre-valor que contienen los límites de API.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetLimits",
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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
    }
}
```

Nuevo desde la versión

9.6

GetOrigin

Puede utilizar el `GetOrigin` método para obtener el certificado de origen para el lugar donde se creó el nodo.

Parámetros

Este método devuelve "null" si no hay ninguna certificación de origen.

Este método no tiene parámetros de entrada.

Valor de retorno

Este método devuelve información sobre la certificación de origen del proveedor.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
 "method": "GetOrigin",
 "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "integrator": "SolidFire",
  "<signature>": {
    "pubkey": [public key info],
    "version": 1,
    "data": [signature info]
  },
   "contract-id": "none",
   "location": "Boulder, CO",
   "organization": "Engineering",
   "type": "element-x"
  }
 ]
}
```

Nuevo desde la versión

9.6

GetRawStats

La ingeniería de NetApp utiliza el `GetRawStats` Método API para probar nuevas funciones. Los datos devueltos de `GetRawStats` no está documentado, cambia con frecuencia y no se garantiza que sea preciso. No debe utilizar `GetRawStats` Para recoger datos de rendimiento o cualquier otra integración de gestión con un clúster de almacenamiento que ejecuta el software Element.

Utilice los siguientes métodos API compatibles para recuperar información estadística:

- GetVolumeStats
- GetClusterStats
- GetNodeStats
- GetDriveStats

Nuevo desde la versión

9.6

ListAsyncResults

Puede utilizar `ListAsyncResults` para mostrar los resultados de todos los métodos asíncronos que se están ejecutando y se han completado actualmente en el sistema. Consulta de resultados asincrónicos con `ListAsyncResults` No hace que venza las manos completadas; puede usar `GetAsyncResult` Para consultar cualquiera de los controladores de generar devueltos por `ListAsyncResults`.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Establish asyncResultTypes	Una lista opcional de tipos de resultados. Puede utilizar esta lista para restringir los resultados solo a estos tipos de operaciones. Los posibles valores son los siguientes: • DriveAdd: Operaciones que involucran al sistema agregando una unidad al clúster. • BulkVolume: Operaciones de copia entre volúmenes, como backups o restauraciones. • Clone: Operaciones de clonado de volúmenes. • DriveRemoval: Operaciones relacionadas con el sistema que copia datos de una unidad en preparación para eliminarla del clúster. • RtfiPendingNode: Operaciones relacionadas con el sistema instalando software compatible en un nodo antes de añadirlo al clúster.	matriz de cadenas	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Establish asyncHandles	Una matriz de resultados del método asíncrono serializado.	Cabina de objetos JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListAsyncResults",
   "params": {
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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
      },
      ...]
   }
}
```

Nuevo desde la versión

9.6

Obtenga más información

GetAsyncResult

Métodos de API de cuenta

Los métodos de cuentas permiten agregar, quitar, ver y modificar la información de cuenta y seguridad.

- AddAccount
- GetAccountByID
- GetAccountByName
- GetAccountEfficiency
- Cuentas de lista
- ModificyAccount
- RemoveAccount

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

AddAccount

Puede utilizar `AddAccount` para agregar una nueva cuenta al sistema. También se puede usar este método para crear volúmenes nuevos en la cuenta nueva cuando se crea la cuenta. La configuración de protocolo de autenticación por desafío mutuo (CHAP) especificada para la cuenta se aplica a todos los volúmenes que pertenecen a la cuenta.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`attributes`	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`enableChap`	Especifica si un iniciador puede utilizar las credenciales de la cuenta CHAP para acceder a volúmenes.	booleano	verdadero	No
`initiatorSecret`	El secreto CHAP que se utiliza para el iniciador. Este secreto debe tener entre 12 y 16 caracteres, y ser impenetrable. El secreto CHAP del iniciador debe ser único y no puede ser igual al secreto CHAP objetivo. Si no se especifica, se crea un secreto aleatorio.	cadena	Ninguno	No
`targetSecret`	El secreto CHAP que se utiliza para el objetivo (autenticación CHAP mutua). Este secreto debe tener entre 12 y 16 caracteres, y ser impenetrable. El secreto CHAP objetivo debe ser único y no puede ser igual al secreto CHAP del iniciador. Si no se especifica, se crea un secreto aleatorio.	cadena	Ninguno	No
`username`	El nombre de usuario único para esta cuenta. (Debe tener entre 1 y 64 caracteres de longitud).	cadena	Ninguno	Sí

Valor de retorno

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
cuenta	Objeto que contiene información acerca de la cuenta recién creada.	cuenta
ID de cuenta	El ID del objeto de cuenta recién creado.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "AddAccount",
    "params": {
     "username"  : "bobsmith",
     "initiatorSecret" : "168[#5A757ru268)",
     "targetSecret" : "tlt&lt;,8TUYa7bC",
     "attributes" : {
       "billingcode" : 2345
     }
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
  }
}
```


Nuevo desde la versión

9.6

GetAccountByID

Puede utilizar `GetAccountByID` Para obtener detalles sobre una cuenta específica, dada su ID de cuenta.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de cuenta	El ID de cuenta de la cuenta para la que se obtendrá información.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
cuenta	Detalles de cuentas.	cuenta

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetAccountByID",
   "params": {
     "accountID"  : 3
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "account": {
        "attributes": {},
        "username": "account3",
        "targetSecret": "targetsecret",
        "volumes": [],
        "enableChap": true,
        "status": "active",
        "accountID": 3,
        "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
        "initiatorSecret": "initiatorsecret"
    }
}
```

Nuevo desde la versión

9.6

GetAccountByName

Puede utilizar `GetAccountByName` para obtener detalles sobre una cuenta específica, dada su nombre de usuario.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nombre de usuario	Nombre de usuario de la cuenta.	cadena	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
cuenta	Detalles de cuentas.	cuenta

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetAccountByName",
   "params": {
     "username"  : "jimmyd"
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "account": {
        "attributes": {},
        "username": "jimmyd",
        "targetSecret": "targetsecret",
        "volumes": [],
        "enableChap": true,
        "status": "active",
        "accountID": 1,
        "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
        "initiatorSecret": "initiatorsecret"
    }
}
```

Nuevo desde la versión

9.6

GetAccountEfficiency

Puede utilizar `GetAccountEfficiency` para obtener estadísticas de eficiencia sobre una cuenta de volumen. Este método devuelve información de eficiencia sólo para la cuenta que se da como parámetro.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de cuenta	Especifica la cuenta de volumen para la cual se devuelven estadísticas de eficiencia.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
compresión	La cantidad de espacio que ahorra la compresión de datos en todos los volúmenes de la cuenta. Se afirma como una relación en la que el valor "1" significa que los datos se han almacenado sin compresión.	flotante
deduplicación	La cantidad de espacio ahorrado no duplicando datos para todos los volúmenes de la cuenta. Se indica como una relación.	flotante
Volúmenes missingVolumes	Los volúmenes que no se pudieron consultar para los datos de eficiencia. Los volúmenes que faltan pueden deberse a que el ciclo de recolección de elementos no utilizados (GC) tiene menos de una hora de antigüedad, a una pérdida temporal de conectividad de red o a servicios reiniciados desde el ciclo de GC.	matriz en números enteros
Thin Provisioning	La relación entre el espacio utilizado y la cantidad de espacio asignado para almacenar datos. Se indica como una relación.	flotante
fecha/hora	La última vez que se recopilaron los datos de eficiencia después de la recolección de basura (GC), en formato UTC+0.	Cadena de fecha ISO 8601

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetAccountEfficiency",
   "params": {
     "accountID": 3
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {
       "compression": 2.020468042933262,
       "deduplication": 2.042488619119879,
       "missingVolumes": [],
       "thinProvisioning": 1.010087163391013,
       "timestamp": "2014-03-10T14:06:02Z"
   }
}
```

Nuevo desde la versión

9.6

Cuentas de lista

Puede utilizar `ListAccounts` para obtener la lista completa de cuentas de inquilino de almacenamiento, con soporte de paginación opcional. Las cuentas de Element permiten el acceso a los volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IncludeStorageContainers	De forma predeterminada, se incluyen contenedores de almacenamiento de volúmenes virtuales en la respuesta. Para excluir contenedores de almacenamiento, establezca el valor false.	booleano	verdadero	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
StartAccountID	Iniciando código de cuenta para devolver. Si no existe ninguna cuenta con este ID de cuenta, la siguiente cuenta por orden de ID de cuenta se utiliza como inicio de la lista. Para desplazarse por la lista, pase el ID de cuenta de la última cuenta en la respuesta anterior + 1.	entero	Ninguno	No
límite	Número máximo de objetos de cuenta que devolver.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
cuentas	La lista de cuentas.	cuenta cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListAccounts",
   "params": {
     "startAccountID"  : 0,
     "limit" : 1000
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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"
    }
  ]
}
}
```

Nuevo desde la versión

9.6

ModificyAccount

Puede utilizar el `ModifyAccount` método para modificar una cuenta existente.

Cuando se bloquea una cuenta, las conexiones existentes de esa cuenta se finalizan inmediatamente. Cuando se cambia la configuración de CHAP de una cuenta, las conexiones existentes permanecen activas y la nueva configuración de CHAP se utiliza en conexiones o reconexiones posteriores. Para borrar los atributos de una cuenta, especifique {} para el parámetro Attributes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de cuenta	ID de cuenta de la cuenta que se va a modificar.	entero	Ninguno	Sí
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
EnableChap	Especifica si un iniciador puede utilizar las credenciales de la cuenta CHAP para acceder a volúmenes.	booleano	Ninguno	No
InitiatorSecret	El secreto CHAP que se utiliza para el iniciador. Este secreto debe tener entre 12-16 y 16 caracteres, y ser impenetrable. El secreto CHAP del iniciador debe ser único y no puede ser igual al secreto CHAP objetivo.	cadena	Ninguno	No
estado	Estado de la cuenta. Los posibles valores son los siguientes: • Active: La cuenta está activa y se permiten las conexiones. • Locked: La cuenta está bloqueada y las conexiones se rechazan.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
TargetSecret	El secreto CHAP que se utiliza para el objetivo (autenticación CHAP mutua). Este secreto debe tener entre 12-16 y 16 caracteres, y ser impenetrable. El secreto CHAP objetivo debe ser único y no puede ser igual al secreto CHAP del iniciador.	cadena	Ninguno	No
nombre de usuario	Se utiliza para cambiar el nombre de usuario asociado a la cuenta. (Debe tener entre 1 y 64 caracteres de longitud).	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
cuenta	Objeto que contiene información acerca de la cuenta modificada.	cuenta

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente. En este ejemplo, los atributos se borran especificando {} para ellos:

```
{
   "method": "ModifyAccount",
   "params": {
     "accountID"  : 25,
     "status"    : "locked",
     "attributes" : {}
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "account": {
        "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
        "username": "user1",
        "accountID": 1,
        "volumes": [
        ],
        "enableChap": true,
        "initiatorSecret": "txz123456q890",
        "attributes": {
        },
        "status": active",
        "targetSecret": "rxe123b567890"
    }
}
```

Nuevo desde la versión

9.6

RemoveAccount

Puede utilizar el `RemoveAccount` método para quitar una cuenta existente. Debe eliminar y purgar todos los volúmenes asociados con la cuenta mediante `DeleteVolume` antes de poder eliminar la cuenta. Si los volúmenes de la cuenta siguen pendientes de eliminación, no podrá utilizar `RemoveAccount` para quitar la cuenta.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de cuenta	ID de la cuenta que se va a quitar.	entero	Ninguno	Sí

Valor de retorno

Este método no tiene ningún valor devuelto.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente.

```
{
   "method": "RemoveAccount",
   "params": {
     "accountID"  : 25
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
 "id" : 1,
 "result" : { }
}
```

Nuevo desde la versión

9.6

Obtenga más información

DeleteVolume

Métodos API de administrador

Es posible usar métodos de API de administrador para crear, modificar, ver y quitar administradores de clústeres de almacenamiento, así como para asignar niveles de acceso y privilegios a los que tienen acceso a un clúster de almacenamiento.

- AddClusterAdmin
- GetCurrentClusterAdmin
- GetLoginBanner
- ListClusterAdmins
- ModifyClusterAdmin
- RemoveClusterAdmin
- SetLoginBanner

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

AddClusterAdmin

Puede utilizar el `AddClusterAdmin` método para añadir una nueva cuenta de administrador de clúster. Un administrador de clúster puede gestionar el clúster a través de la API y las herramientas de gestión. Los administradores de clústeres están completamente separados y no guardan relación con las cuentas de cliente estándar.

Cada administrador de clúster puede restringirse a un subconjunto de la API. Debe utilizar varias cuentas de administrador de clúster para diferentes usuarios y aplicaciones. Como práctica recomendada, proporcione a cada administrador de clúster los permisos mínimos necesarios; esto reduce el impacto potencial de comprometer las credenciales.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
acceso	Controla los métodos que puede utilizar el administrador de clúster.	matriz de cadenas	Ninguno	Sí
AceptEula	Acepte el contrato de licencia para usuario final. Establezca esta opción en true para añadir una cuenta de administrador de clúster al sistema. Si se omite o se establece en falso, la llamada al método falla.	booleano	Ninguno	Sí
atributos	La lista de parejas nombre/valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
contraseña	La contraseña que se utiliza para autenticar este administrador de clúster.	cadena	Ninguno	Sí
nombre de usuario	Nombre de usuario único para este administrador de clúster. Debe tener entre 1 y 1024 caracteres.	cadena	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
ClusterAdminID	ClusterAdminID para el administrador de clúster recién creado.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "AddClusterAdmin",
  "params": {
    "username": "joeadmin",
    "password": "68!5Aru268)$",
    "attributes": {},
    "acceptEula": true,
    "access": ["volumes", "reporting", "read"]
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id":1,
  "result" : {
    "clusterAdminID": 2
   }
}
```

Nuevo desde la versión

9.6

Obtenga más información

Control de acceso

GetCurrentClusterAdmin

Puede utilizar el `GetCurrentClusterAdmin` Método para obtener información del administrador de clúster principal actual El administrador de clúster principal se creó cuando se creó el clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
ClusterAdmin	Información acerca del administrador de clúster.	ClusterAdmin

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method": "GetCurrentClusterAdmin",
"id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"id": 1,
"result": {
    "clusterAdmin":
        "access": [
           "administrator"
        ],
         "attributes": null,
         "authMethod": "Cluster"
         "clusterAdminID": 1,
         "username": "admin"
     }
   }
}
```

Nuevo desde la versión

10.0

GetLoginBanner

Puede utilizar el `GetLoginBanner` Método para obtener el banner de las condiciones de uso actualmente activas que los usuarios ven cuando inician sesión en la interfaz web de Element.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
banner	El texto actual del banner con las condiciones de uso. Este valor puede contener texto incluso cuando el banner está desactivado.	cadena

Nombre	Descripción	Tipo
activado	El estado del banner con las condiciones de uso. Los posibles valores son los siguientes: • True: El banner con las condiciones de uso se muestra cuando el inicio de sesión de la interfaz web. • False: El banner con las condiciones de uso no se muestra cuando el inicio de sesión de la interfaz web.	booleano

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 3411,
  "method": "GetLoginBanner",
  "params": {}
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 3411,
  "result": {
    "loginBanner": {
      "banner": "Welcome to NetApp!",
      "enabled": false
    }
  }
}
```

Nuevo desde la versión

10.0

ListClusterAdmins

Puede utilizar el `ListClusterAdmins` método para obtener la lista de todos los

administradores de clúster del clúster.

Puede haber varias cuentas de administrador de clúster con diferentes niveles de permisos. Solo puede haber un administrador de clúster principal en el sistema. El administrador de clúster principal es el administrador que se creó cuando se creó el clúster. Los administradores de LDAP también se pueden crear al configurar un sistema LDAP en el clúster.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ShowHidden	Muestra usuarios ocultos del administrador de clústeres, como el administrador SNMP.	booleano	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Administradores de clústeres	Información sobre todos los administradores de clústeres y LDAP que existen para un clúster.	ClusterAdmin cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListClusterAdmins",
   "params": {},
    "showHidden": true
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"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"
       }
     ]
   }
}
```


Nuevo desde la versión

9.6

ModifyClusterAdmin

Puede utilizar el `ModifyClusterAdmin` Método para cambiar la configuración de un administrador de clúster, un administrador de clúster LDAP o un administrador de clúster de proveedor de identidades (IDP) de terceros. No se puede modificar el acceso de la cuenta de administrador de clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
acceso	Controla qué métodos puede utilizar este administrador de clúster.	matriz de cadenas	Ninguno	No
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
ClusterAdminID	ClusterAdminID para el administrador del clúster, administrador de clúster LDAP o administrador de clúster IDP que se deben modificar.	entero	Ninguno	Sí
contraseña	La contraseña que se utiliza para autenticar este administrador de clúster. Este parámetro no se aplica a un administrador de clúster LDAP o IDP.	cadena	Ninguno	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ModifyClusterAdmin",
   "params": {
     "clusterAdminID"  : 2,
     "password"    : "7925Brc429a"
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
 "id" : 1
 "result" : { }
}
```

Nuevo desde la versión

9.6

Obtenga más información

Control de acceso

RemoveClusterAdmin

Puede utilizar el `RemoveClusterAdmin` Método para quitar un administrador de clúster, un administrador de clúster LDAP o un administrador de clúster de proveedor de identidades (IDP) de terceros. No es posible quitar la cuenta "admin" Cluster Admin.

Parámetro

Cuando se elimina un administrador de clúster IDP que tiene sesiones autenticadas asociadas a un IDP de proveedor de identidades de terceros, dichas sesiones se llevarán a cabo o, posiblemente, experimentarán una pérdida de derechos de acceso dentro de su sesión actual. La pérdida de derechos de acceso dependerá de si el administrador del clúster IDP que se quitó coincidan con uno de los varios administradores de clúster IDP de los atributos SAML de un usuario determinado. El conjunto restante de administradores de clústeres IDP correspondientes da como resultado un conjunto reducido de derechos de acceso a agregados. Otros tipos de usuario administrador del clúster se cerrará la sesión cuando se eliminen sus administradores de clúster.

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ClusterAdminID	ClusterAdminID para que se quite el administrador de clúster.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "RemoveClusterAdmin",
   "params": {
     "clusterAdminID"  : 2
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
 "id" : 1
 "result" : { }
}
```

Nuevo desde la versión

9.6

SetLoginBanner

Puede utilizar el `SetLoginBanner` Método para configurar el banner de las condiciones de uso que ven los usuarios cuando inician sesión en la interfaz web de Element.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
banner	El texto deseado del banner con las condiciones de uso. La longitud máxima permitida es de 4,096 caracteres.	cadena	Ninguno	No
activado	El estado del banner con las condiciones de uso. Los posibles valores son los siguientes: • `true`: El banner de los Términos de uso se muestra al iniciar sesión en la interfaz web. • `false`: El banner de los Términos de uso no se muestra al iniciar sesión en la interfaz web.	booleano	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
banner	El texto actual del banner con las condiciones de uso. Este valor puede contener texto incluso cuando el banner está desactivado.	cadena

Nombre	Descripción	Tipo
activado	El estado del banner con las condiciones de uso. Los posibles valores son los siguientes: • True: El banner con las condiciones de uso se muestra cuando el inicio de sesión de la interfaz web. • False: El banner con las condiciones de uso no se muestra cuando el inicio de sesión de la interfaz web.	booleano

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 3920,
  "method": "SetLoginBanner",
  "params": {
    "banner": "Welcome to NetApp!",
    "enabled": true
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 3920,
  "result": {
    "loginBanner": {
      "banner": "Welcome to NetApp!",
      "enabled": true
    }
  }
}
```

Nuevo desde la versión

10.0

Métodos de API de clúster

Los métodos de API de clústeres del software Element permiten gestionar la configuración y la topología del clúster de almacenamiento y los nodos que pertenecen a un clúster de almacenamiento.

Algunos métodos de API de clúster funcionan en nodos que forman parte de un clúster o que se han configurado para unirse a un clúster. Puede añadir nodos a un clúster nuevo o a un clúster existente. Los nodos que están listos para añadirse a un clúster están en estado "pendiente", lo que significa que se han configurado pero que todavía no se han añadido al clúster.

- AddNodes
- ClearClusterFaults
- CreateClusterInterfacePreference
- DeleteClusterInterfacePreference
- EnableFeature
- GetClusterCapacity
- GetClusterFullThreshold
- GetClusterHardwareInfo
- GetClusterInfo
- GetClusterInterfacePreference
- GetClusterMasterNodeID
- GetClusterStats
- GetClusterVersionInfo
- GetFeatureStatus
- GetLoginSessionInfo
- GetNodeHardwareInfo
- GetNodeStats
- ListActiveNodes
- ListAllNodes
- ListClusterFaults
- ListClusterInterfacePreferences
- ListEvents
- ListNodeStats
- ListISCSISessions
- Servicios de listas
- ListPendingNodes
- ListPendingActiveNodes
- ModifyClusterFullThreshold
- ModifyClusterInterfacePreference

- RemoveNodes
- SetLoginSessionInfo
- Apagado

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

AddNodes

Puede utilizar el `AddNodes` método para añadir uno o varios nodos nuevos a un clúster de.

Cuando un nodo que no está configurado se inicia por primera vez, se le solicita que configure el nodo. Una vez que configura el nodo, está registrado como un "nodo pendiente" con el clúster. Los clústeres de almacenamiento que ejecutan el software Element crean automáticamente la imagen de un nodo en la versión del clúster. Cuando se agrega un nodo pendiente, la respuesta del método incluye un valor de establish asyncHandle que se puede utilizar con `GetAsyncResult` método para consultar el estado del proceso automático de obtención de imágenes.

El proceso de añadir un nodo Fibre Channel es igual que añadir nodos de almacenamiento iSCSI de Element a un clúster. Los nodos Fibre Channel se registran en el sistema con un NodeID. Cuando son accesibles, se ponen en estado de "nodo pendiente". La `ListAllNodes` El método devolverá el pendingNodeID para los nodos iSCSI, así como los nodos Fibre Channel que están disponibles para agregarse al clúster.

Cuando añade un nodo a un clúster que ha configurado para redes virtuales, el sistema necesita un número suficiente de direcciones IP de almacenamiento virtual para asignar una IP virtual al nodo nuevo. Si no hay direcciones IP virtuales disponibles para el nodo nuevo, el `AddNode` error en la operación. Utilice la `ModifyVirtualNetwork` Método para añadir más direcciones IP de almacenamiento a la red virtual.

Una vez que se añade un nodo, queda disponibles las unidades del nodo y puede añadirlas con el `AddDrives` método para aumentar la capacidad de almacenamiento del clúster.

> Es posible que luego de añadir un nuevo nodo tarde varios segundos para arrancar y registrar las unidades como disponibles.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Instalación automática	Si es verdadero, se realizará un retorno a la imagen de fábrica (RTFI) en el nodo tras la adición. El comportamiento predeterminado es realizar RTFI. Si la `cEnableAutoInstall` la constante del clúster es falsa, tiene prioridad sobre este parámetro. Si hay una actualización en curso, el proceso de RTFI no tendrá lugar independientemente del valor de este parámetro.	booleano	Ninguno	No
PendingNodes	Los identificadores de nodo pendientes que se agregarán. Puede enumerar todos los nodos pendientes mediante el método ListPendingNodes.	matriz en números enteros	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Instalación automática	Si los nodos añadidos vuelven o no a la imagen de fábrica.	booleano

nodos	Una matriz de objetos que asigna el "pendingNodeID" anterior a "nodeID". Cuando se agrega un nodo pendiente que ejecuta una versión de software incompatible, esta matriz incluye un valor de establish de la ley que se puede utilizar con el método GetAsyncResult para consultar el estado del proceso automático de obtención de imágenes.	Cabina de objetos JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "AddNodes",
   "params": {
     "autoInstall" : true,
     "pendingNodes" : [1]
   },
   "id":1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  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"
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

Obtenga más información

- AddDrives
- GetAsyncResult
- ListAllNodes
- ModificyVirtualNetwork

ClearClusterFaults

Puede utilizar el `ClearClusterFaults` método para borrar información sobre fallos tanto actuales como detectados previamente. Se pueden borrar tanto los fallos resueltos como los no resueltos.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Intachable	Determina los tipos de fallos que se van a borrar. Los posibles valores son los siguientes: • actual: Fallos que se detectan actualmente y que no se han resuelto. • Resuelto: Fallos detectados y resueltos anteriormente. • All: Fallos tanto actuales como resueltos. El estado del fallo puede ser determinado por el campo "resolucionado" del objeto de fallo.	cadena	resuelto	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ClearClusterFaults",
   "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
    "result" : {}
}
```

Nuevo desde la versión

9.6

CreateClusterInterfacePreference

La `CreateClusterInterfacePreference` Método permite a los sistemas integrados con los clústeres de almacenamiento que ejecutan el software Element crear y almacenar información arbitraria en el clúster de almacenamiento. Este método es para uso interno.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nombre	El nombre de la interfaz del clúster preferido.	cadena	Ninguno	Sí
valor	El valor de la interfaz de clúster preferida.	cadena	Ninguno	Sí

Valor de retorno

Este método no tiene ningún valor devuelto.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
        "method": "CreateClusterInterfacePreference",
        "params": {
            "name": "prefname",
            "value": "testvalue"
        },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {}
}
```

Nuevo desde la versión

11.0

DeleteClusterInterfacePreference

La `DeleteClusterInterfacePreference` Método permite que los sistemas se integren con los clústeres de almacenamiento que ejecutan el software Element para eliminar una preferencia de interfaz de clúster existente. Este método es para uso interno.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nombre	El nombre de la interfaz del clúster preferencia de que se elimine.	cadena	Ninguno	Sí

Valores devueltos

Este método no tiene ningún valor devuelto.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "DeleteClusterInterfacePreference",
    "params": {
        "name": "prefname"
        },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {}
}
```

Nuevo desde la versión

11.0

EnableFeature

Puede utilizar el `EnableFeature` Método para habilitar funciones de clúster como VVol deshabilitados de forma predeterminada.

Parámetro

Este método tiene el siguiente parámetro de entrada.

> Para los sistemas que ejecutan el software Element 11.x, al habilitar Virtual Volumes o después de establecer la supervisión de dominios de protección, la función de dominios de protección del clúster solo opera en el nivel del nodo.

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
función	Habilite una función de clúster. Los posibles valores son los siguientes: • `fips`: Habilite el cifrado certificado FIPS 140-2 para las comunicaciones HTTPS. • `FipsDrives`: Habilite el soporte de unidades FIPS 140-2 para el clúster de almacenamiento . • `SnapMirror`: Active la función de clúster de replicación de SnapMirror. • `vvols`: Active la función de clúster VVols del software Element.	cadena	Ninguno	Sí

Valor de retorno

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "vvols"
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nuevo desde la versión

9.6

GetClusterCapacity

Puede utilizar el `GetClusterCapacity` para devolver mediciones de capacidad a grandes niveles para todo un clúster de almacenamiento. Este método muestra campos que se pueden usar para calcular las tasas de eficiencia que se muestran en la interfaz de usuario web de Element. Puede utilizar los cálculos de eficiencia de los scripts para obtener las tasas de eficiencia de thin provisioning, deduplicación, compresión y eficiencia general.

Cálculos de eficiencia

Utilice las siguientes ecuaciones para calcular el thin provisioning, la deduplicación y la compresión. Estas ecuaciones se aplican al elemento 8.2 y posterior.

- ThinProvisioningfactor = (nonZeroBlocks + zeroBlocks) / nonZeroBlocks
- DuplicationFactor = (nonZeroBlocks + snapshotNonZeroBlocks) / unicqueBlocks
- Compressionfactor = (unidoBlocks * 4096) / (uniqueBlocksUsedSpace * 0.93)

Cálculo general de la tasa de eficiencia

Use la siguiente ecuación para calcular la eficiencia general del clúster utilizando los resultados del cálculo de eficiencia de thin provisioning, deduplicación y compresión.

- Efficiencyfactor = thinProvisioningfactor * debDuplicationfactor * compressionfactor

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
ClusterCapacity	Mediciones de la capacidad para el clúster de almacenamiento.	ClusterCapacity

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetClusterCapacity",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
    }
  }
}
```


Nuevo desde la versión

9.6

GetClusterFullThreshold

Puede utilizar el `GetClusterFullThreshold` método para ver las fases establecidas para los niveles de ocupación del clúster. Este método muestra todas las métricas de ocupación del clúster.

> Cuando un clúster alcanza la etapa de error en la ocupación del clúster en bloque, las IOPS máximas en todos los volúmenes se reducen linealmente a la IOPS mínima del volumen cuando el clúster se acerca a la etapa crítica. Esto ayuda a evitar que el clúster alcance la etapa crítica de ocupación del clúster de bloques.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
BlockFullness	El nivel calculado actual de ocupación del bloque del clúster. • Stage1Happy: Sin alertas ni condiciones de error. Corresponde al estado **saludable** de la interfaz de usuario web. • Stage2Aware: Sin alertas ni condiciones de error. Corresponde al estado **saludable** de la interfaz de usuario web. • Stage3Low: El sistema no puede brindar protección de datos redundante contra dos fallos de nodo sin simultáneo. Corresponde al estado **Warning** de la interfaz de usuario web. Es posible configurar este nivel en la interfaz de usuario web (el sistema activa esta alerta de forma predeterminada cuando la capacidad es un 3 % inferior al estado error). • Stage4Critical: El sistema no es capaz de brindar protección de datos redundante desde un fallo de nodo único. No se pueden crear volúmenes o clones nuevos. Corresponde al estado **error** en la interfaz de usuario del elemento. • Stage5CompletelyConsumed: Totalmente consumido. El clúster es de solo lectura; se mantienen las conexiones iSCSI, pero se suspenden todas las escrituras. Corresponde al estado **Critical** de la interfaz de usuario de elemento.	cadena
plenitud	Refleja el nivel más alto de plenitud entre "blockFullness" y "metadataFullness".	cadena

Nombre	Descripción	Tipo
MaxMetadataOverProvisionFactor	Un representante de valor del número de veces que el espacio de metadatos se puede aprovisionar en exceso en relación con la cantidad de espacio disponible. Por ejemplo, si había suficiente espacio de metadatos para almacenar 100 TIB de volúmenes y este número se estableció en 5, se podría crear un valor de 500 TIB de volúmenes.	entero

Nombre	Descripción	Tipo
MetadataFullness	El nivel calculado actual de ocupación de metadatos del clúster. • Stage1Happy: Sin alertas ni condiciones de error. Corresponde al estado **saludable** de la interfaz de usuario web. • Stage2Aware: Sin alertas ni condiciones de error. Corresponde al estado **saludable** de la interfaz de usuario web. • Stage3Low: El sistema no puede brindar protección de datos redundante contra dos fallos de nodo sin simultáneo. Corresponde al estado **Warning** de la interfaz de usuario web. Es posible configurar este nivel en la interfaz de usuario web (el sistema activa esta alerta de forma predeterminada cuando la capacidad es un 3 % inferior al estado error). • Stage4Critical: El sistema no es capaz de brindar protección de datos redundante desde un fallo de nodo único. No se pueden crear volúmenes o clones nuevos. Corresponde al estado **error** en la interfaz de usuario del elemento. • Stage5CompletelyConsumed: Totalmente consumido. El clúster es de solo lectura; se mantienen las conexiones iSCSI, pero se suspenden todas las escrituras. Corresponde al estado **Critical** de la interfaz de usuario de elemento.	cadena
SliceReserveUsedThresholdPct	Condición de error. Se activa una alerta del sistema si el uso de segmentos reservados es mayor que este valor.	entero

Nombre	Descripción	Tipo
Stage2AwareThreshold	Condición de conciencia. El valor que se establece para el nivel de umbral del clúster de la etapa 2.	entero
Stage2BlockThresholdBytes	El número de bytes que utiliza el clúster en el que existirá una condición de fase 2.	entero
Stage2MetadataThresholdBytes	El número de bytes de metadatos que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 2.	
Stage3BlockThresholdBytes	El número de bytes de almacenamiento que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 3.	entero
Stage3BlockThresholdPercent	El valor porcentual establecido para la etapa 3. En este porcentaje lleno, se publica una advertencia en el registro de alertas.	entero
Stage3LowThreshold	Condición de error. El umbral en el que se crea una alerta del sistema debido a la baja capacidad de un clúster.	entero
Stage3MetadataThresholdBytes	El número de bytes de metadatos que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 3.	entero
Stage3MetadataThresholdPercent	El valor porcentual establecido para el stage3 de ocupación de metadatos. En este porcentaje lleno, se publicará una advertencia en el registro de alertas.	entero
Stage4BlockThresholdBytes	El número de bytes de almacenamiento que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 4.	entero

Nombre	Descripción	Tipo
Stage4Critical Threshold	Condición de error. El umbral en el que se crea una alerta del sistema para informar sobre una capacidad extremadamente baja en un clúster.	entero
Stage4MetadataThresholdBytes	El número de bytes de metadatos que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 4.	entero
Stage5BlockThresholdBytes	El número de bytes de almacenamiento que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 5.	entero
Stage5MetadataThresholdBytes	El número de bytes de metadatos que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 5.	entero
SumTotalClusterBytes	La capacidad física del clúster, medida en bytes.	entero
SumTotalMetadataClusterBytes	La cantidad total de espacio que se puede utilizar para almacenar metadatos.	entero
SumUsedClusterBytes	La cantidad de bytes de almacenamiento que se utiliza en el clúster.	entero
SUUsedMetadataClusterBytes	La cantidad de espacio usado en las unidades de volúmenes para almacenar metadatos.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method" : "GetClusterFullThreshold",
   "params" : {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```
{
  "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
  }
}
```


Nuevo desde la versión

9.6

Obtenga más información

ModifyClusterFullThreshold

GetClusterHardwareInfo

Puede utilizar el `GetClusterHardwareInfo` Método para recuperar la información y el estado de hardware de todos los nodos Fibre Channel, los nodos iSCSI y las unidades del clúster. Generalmente, se incluyen los fabricantes, los proveedores, las versiones y otra información de identificación de hardware asociada.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
tipo	Incluya sólo uno de los siguientes tipos de información de hardware en la respuesta. Los posibles valores son los siguientes: • unidades: Muestra sólo información de unidad en la respuesta. • Nodes: Muestra sólo la información del nodo en la respuesta. • All: Incluye información tanto de la unidad como de los nodos en la respuesta. Si se omite este parámetro, se asume un tipo de todo.	cadena	todo	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
ClusterHardwareInfo	Información de hardware para todos los nodos y unidades en el clúster. Cada objeto de esta salida se etiqueta con el ID de nodo del nodo especificado.	HardwareInfo

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetClusterHardwareInfo",
    "params": {
        "type": "all"
    },
    "id": 1
}
```

Ejemplo de respuesta

Debido a la longitud de este ejemplo de respuesta, se documenta en un tema complementario.

Nuevo desde la versión

9.6

Obtenga más información

GetClusterHardwareInfo

GetClusterInfo

Puede utilizar el `GetClusterInfo` método para obtener información de configuración del clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
ClusterInfo	Información del clúster.	ClusterInfo

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetClusterInfo",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```
{
    "id": 1,
    "result": {
        "clusterInfo": {
            "attributes": {},
            "defaultProtectionScheme": "doubleHelix",
            "enabledProtectionSchemes": [
                "doubleHelix"
            ],
            "encryptionAtRestState": "disabled",
            "ensemble": [
                "10.10.10.32",
                "10.10.10.34",
                "10.10.10.35",
                "10.10.10.36",
                "10.10.10.37"
            ],
            "mvip": "10.10.11.225",
            "mvipInterface": "team1G",
            "mvipNodeID": 3,
            "mvipVlanTag": "0",
            "name": "ClusterName",
            "repCount": 2,
            "softwareEncryptionAtRestState": "enabled",
            "supportedProtectionSchemes": [
                "doubleHelix"
            ],
            "svip": "10.10.10.111",
            "svipInterface": "team10G",
            "svipNodeID": 3,
            "svipVlanTag": "0",
            "uniqueID": "psmp",
            "uuid": "2f575d0c-36fe-406d-9d10-dbc1c306ade7"
        }
    }
}
```


Nuevo desde la versión

9.6

GetClusterInterfacePreference

La `GetClusterInterfacePreference` Método permite que los sistemas se integren con los clústeres de almacenamiento que ejecutan el software Element para obtener información acerca de una preferencia de interfaz de clúster existente. Este método es para uso interno.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nombre	El nombre de la interfaz del clúster preferido.	cadena	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
preferencia	El nombre y el valor de la preferencia de la interfaz de clúster solicitada.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "GetClusterInterfacePreference",
    "params": {
        "name": "prefname"
        },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "preference": {
            "name": "prefname",
            "value": "testvalue"
        }
    }
}
```

Nuevo desde la versión

11.0

GetClusterMasterNodeID

Puede utilizar el `GetClusterMasterNodeID` Método para recuperar el ID del nodo que realiza tareas de administración en todo el clúster y contiene la dirección IP virtual de almacenamiento (SVIP) y la dirección IP virtual de gestión (MVIP).

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
NodeID	ID del nodo maestro.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetClusterMasterNodeID",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1
  "result": {
    "nodeID": 1
   }
}
```

Nuevo desde la versión

9.6

GetClusterStats

Puede utilizar el `GetClusterStats` método para recuperar mediciones de actividad de alto nivel para el clúster. Los valores devueltos se acumulan a partir de la creación del clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
ClusterStats	Información de la actividad del clúster.	ClusterStats

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetClusterStats",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
    }
  }
}
```


Nuevo desde la versión

9.6

GetClusterVersionInfo

Puede utilizar el `GetClusterVersionInfo` Método para recuperar información acerca de la versión del software Element que se ejecuta en cada nodo del clúster. Este método también muestra información acerca de los nodos que se encuentran actualmente en proceso de actualización de software.

Miembros del objeto de información de la versión del clúster

Este método tiene los siguientes miembros de objeto:

Nombre	Descripción	Tipo
NodeID	El ID del nodo.	entero
NodeInternalRevision	La versión interna del software del nodo.	cadena
Versión de nodo	La versión de software del nodo.	cadena

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
ClusterAPIVersion	La versión de API actual en el clúster.	cadena
ClusterVersion	La versión del software Element que se ejecuta actualmente en el clúster.	cadena
ClusterVersionInfo	Lista de nodos del clúster con información de versión de cada nodo.	Cabina de objetos JSON
PendingClusterVersion	En caso de existir, esta es la versión a la que se está actualizando o volviendo a la versión del software del clúster.	cadena

Nombre	Descripción	Tipo
SoftwareVersionInfo	El estado de una actualización. Miembros del objeto: • Versión de CurrentVersion: La versión de software actual de un nodo. • NodeID: ID del nodo que se está actualizando desde CurrentVersion a pendingVersion. Este campo es 0 (cero) si no hay ninguna actualización en curso. • Nombrepaquete: Nombre del paquete de software que se está instalando. • PendingVersion: Versión del software que se está instalando. • StartTime: La fecha y la hora en que se inició la instalación, en formato UTC+0.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetClusterVersionInfo",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
 "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": ""
    }
  }
}
```

Nuevo desde la versión

9.6

GetFeatureStatus

Puede utilizar el `GetFeatureStatus` método para recuperar el estado de una función de clúster.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
función	El estado de una función de clúster. Si no se proporciona ningún valor, el sistema devuelve el estado de todas las características. Los posibles valores son los siguientes: • Vvols: Recupere el estado de la función de clúster VVol. • SnapMirror: Recupere el estado de la función de clúster de replicación de SnapMirror. • FIPS: Recupere el estado del cifrado FIPS 140-2 para la función de comunicación HTTPS. • FipsDrives: Recupere el estado de la función de cifrado de unidades FIPS 140-2-2.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
funciones	Matriz de objetos de operación que indica el nombre de la operación y su estado. Miembros del objeto: • Característica: (Cadena) el nombre de la operación. • Enabled: (booleano) tanto si la función está habilitada como si no.	Cabina de objetos JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetFeatureStatus",
    "params": {
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "features": [
            {
                "enabled": true,
                "feature": "Vvols"
            },
            {
                "enabled": true,
                "feature": "SnapMirror"
            },
            {
                "enabled": true,
                "feature": "Fips"
            },
            {
                "enabled": true,
                "feature": "FipsDrives"
            }
        ]
    }
}
```


Nuevo desde la versión

9.6

GetLoginSessionInfo

Puede utilizar el `GetLoginSessionInfo` Método para devolver el periodo de tiempo en el que una sesión de autenticación de inicio de sesión es válida tanto para los shell de inicio de sesión como para la TUI.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
LoginSessionInfo	Objeto que contiene el período de caducidad de la autenticación. Objetos posibles devueltos: • tiempo de espera: El tiempo, en minutos, cuando se agotará el tiempo de espera y vencerá esta sesión. Formateado en H:mm:ss Por ejemplo: 1:30:00, 20:00, 5:00. Todos los ceros iniciales y los dos puntos se eliminan independientemente del formato en el que se haya introducido el tiempo de espera.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetLoginSessionInfo",
    "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"id": 1,
  "result" : {
    "loginSessionInfo" : {
      "timeout" : "30:00"
    }
  }
}
```

Nuevo desde la versión

9.6

GetNodeHardwareInfo

Puede utilizar el `GetNodeHardwareInfo` método para obtener toda la información y el estado de hardware del nodo especificado. Generalmente, se incluyen los fabricantes, los proveedores, las versiones y otra información de identificación de hardware asociada.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
NodeID	ID del nodo para el que se está solicitando información del hardware. La información sobre un nodo Fibre Channel se devuelve si se especifica un nodo Fibre Channel.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
NodeHardwareInfo	Información de hardware para el ID de nodo especificado. Cada objeto de esta salida se etiqueta con el ID de nodo del nodo especificado.	HardwareInfo

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetNodeHardwareInfo",
   "params": {
     "nodeID": 1
   },
"id" : 1
}
```

Ejemplo de respuesta

Debido a la longitud de este ejemplo de respuesta, se documenta en un tema complementario.

Nuevo desde la versión

9.6

Obtenga más información

GetNodeHardwareInfo (salida para nodos Fibre Channel)

GetNodeHardwareInfo (salida para iSCSI)

GetNodeStats

Puede utilizar el `GetNodeStats` método para recuperar las mediciones de actividad de alto nivel de un único nodo.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
NodeID	Especifica el ID del nodo para el cual se devolverán las estadísticas.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Estadísticas de nodos	Información de la actividad del nodo.	Estadísticas de nodos

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetNodeStats",
   "params": {
     "nodeID": 5
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id" : 1,
   "result" : {
     "nodeStats" : {
       "cBytesIn" : 9725856460404,
       "cBytesOut" : 16730049266858,
       "cpu" : 98,
       "mBytesIn" : 50808519,
       "mBytesOut" : 52040158,
       "networkUtilizationCluster" : 84,
       "networkUtilizationStorage" : 0,
       "sBytesIn" : 9725856460404,
       "sBytesOut" : 16730049266858,
       "timestamp" : "2012-05-16T19:14:37.167521Z",
       "usedMemory" : 41195708000
     }
   }
}
```

Nuevo desde la versión

9.6

ListActiveNodes

Puede utilizar el `ListActiveNodes` método para obtener la lista de los nodos activos actualmente que se encuentran en el clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
nodos	La lista de nodos activos del clúster.	nodo cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListActiveNodes",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Debido a la longitud de este ejemplo de respuesta, se documenta en un tema complementario.

Nuevo desde la versión

9.6

Obtenga más información

ListActiveNodes

ListAllNodes

Puede utilizar el `ListAllNodes` método para enumerar los nodos activos y pendientes en el clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
nodos	Lista de objetos que describen los nodos activos en el clúster.	nodo

Nombre	Descripción	Tipo
PendingActiveNodes	Lista de objetos que describen nodos activos pendientes para el clúster.	PendingActiveNode cabina
PendingNodes	Lista de objetos que describen nodos pendientes para el clúster.	PendingNode cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListAllNodes",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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": []
    }
}
```


Nuevo desde la versión

9.6

ListClusterFaults

Puede utilizar el `ListClusterFaults` método para enumerar información sobre cualquier error detectado en el clúster. Con este método, puede enumerar tanto los fallos actuales como los que se han resuelto. El sistema almacena en caché los fallos cada 30

segundos.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Prácticas más eficaces	Incluir fallos activados por una configuración del sistema no óptima. Los posibles valores son los siguientes: • verdadero • falso	booleano	Ninguno	No
Intachable	Determina los tipos de fallos devueltos. Los posibles valores son los siguientes: • Actual: Lista de fallos activos sin resolver. • Resuelto: Lista de fallos detectados y resueltos con anterioridad. • All: Enumera los fallos actuales y resueltos. El estado del fallo puede verse en el miembro "relativamente solucionado" del objeto de fallo.	cadena	todo	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
fallos	Un objeto que describe los errores solicitados del clúster.	fallo

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListClusterFaults",
    "params": {
      "faultTypes": "current",
      "bestPractices": true
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "faults": [
      {
        "clusterFaultID": 1,
        "code": "notUsingLACPBondMode",
        "data": null,
        "date": "2016-04-26T14:57:04.275286Z",
        "details": "Bond1G interfaces found not using LACP bond mode.
Nodes not set to LACP bond mode: {1,2,4,5}",
        "driveID": 0,
        "driveIDs": [],
        "nodeHardwareFaultID": 0,
        "nodeID": 0,
        "resolved": false,
        "resolvedDate": "",
        "serviceID": 0,
        "severity": "bestPractice",
        "type": "cluster"
      },
      {
        "clusterFaultID": 9,
        "code": "disconnectedClusterPair",
        "data": null,
        "date": "2016-04-26T20:40:08.736597Z",
        "details": "One of the clusters in a pair may have become
misconfigured or disconnected.  Remove the local pairing and retry pairing
the clusters. Disconnected Cluster Pairs: []. Misconfigured Cluster Pairs:
[3]",
        "driveID": 0,
        "driveIDs": [],
        "nodeHardwareFaultID": 0,
        "nodeID": 0,
        "resolved": false,
        "resolvedDate": "",
        "serviceID": 0,
        "severity": "warning",
        "type": "cluster"
      }
    ]
  }
}
```

Nuevo desde la versión

9.6

ListClusterInterfacePreferences

La `ListClusterInterfacePreference` Method permite a los sistemas integrados con los clústeres de almacenamiento que ejecutan el software Element mostrar las preferencias de la interfaz de clúster existentes almacenadas en el sistema. Este método es para uso interno.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
preferencias	Una lista de objetos de interfaz de clúster almacenados actualmente en el clúster de almacenamiento, cada uno de los cuales contiene el nombre y el valor de la preferencia.	Cabina de objetos JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "ListClusterInterfacePreferences",
    "params": {
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "preferences": [
            {
                "name": "prefname",
                "value": "testvalue"
            }
        ]
    }
}
```

Nuevo desde la versión

11.0

ListEvents

Puede utilizar el `ListEvents` método para mostrar los eventos detectados en el clúster, ordenados de la más antigua a la más reciente.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de unidad	Especifica que solo se devolverán los eventos con este ID de unidad.	entero	0	No
EndEventID	Identifica el final de un intervalo de ID de evento que se deben devolver.	entero	(ilimitada)	No
EndPublishTime	Especifica que sólo se devolverán los eventos publicados antes de esta hora.	cadena	0	No
EndReportTime	Especifica que sólo se devolverán los eventos notificados antes de esta hora.	cadena	0	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Tipo de evento	Especifica el tipo de eventos que se van a devolver. Consulte evento para los posibles tipos de evento.	cadena	0	No
Maxevents	Especifica el número máximo de eventos que se devolverán.	entero	(ilimitada)	No
NodeID	Especifica que solo se devolverán los eventos con este ID de nodo.	entero		
ID de servicio	Especifica que sólo se devolverán los eventos con este ID de servicio.			
StartEventID	Identifica el comienzo de un intervalo de eventos que se van a devolver.	entero	0	No
StartPublishTime	Especifica que sólo se devolverán los eventos publicados después de este tiempo.	cadena	0	No
StartReportTime	Especifica que sólo se devolverán los eventos informados después de este tiempo.	cadena	0	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
eventos	Lista de eventos.	evento cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListEvents",
   "params": {
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
         }
      ]
   }
}
```


Nuevo desde la versión

9.6

ListNodeStats

Puede utilizar el `ListNodeStats` método para ver las mediciones de actividad de alto nivel para todos los nodos de almacenamiento de un clúster de almacenamiento.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Estadísticas de nodos	Información de la actividad del nodo de almacenamiento.	Estadísticas de nodos

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListNodeStats",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {
     "nodeStats": {
       "nodes": [
         {
         "cBytesIn": 46480366124,
         "cBytesOut": 46601523187,
         "cpu": 0,
         "mBytesIn": 59934129,
         "mBytesOut": 41620976,
         "networkUtilizationCluster": 0,
         "networkUtilizationStorage": 0,
         "nodeID": 1,
         "sBytesIn": 46480366124,
         "sBytesOut": 46601523187,
         "timestamp": 1895558254814,
         "usedMemory": 31608135680
         }
       ]
     }
 }
```

Nuevo desde la versión

9.6

ListISCSISessions

Puede utilizar el `ListISCSISessions` Método para enumerar la información de conexión iSCSI de los volúmenes en el clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
sesiones	Información sobre cada sesión iSCSI.	sesión

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListISCSISessions",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
 {
  "id": 1,
  "result": {
    "sessions": [
      {
        "accountID": 1,
        "accountName": "account1",
        "createTime": "2017-04-11T03:39:32.030291Z",
        "driveID": 23,
        "driveIDs": [23],
        "initiator": null,
        "initiatorIP": "10.1.1.1:37138",
        "initiatorName": "iqn.2010-01.net.solidfire.eng:c",
        "initiatorPortName": "iqn.2010-
01.net.solidfire.eng:c,i,0x23d860000",
        "initiatorSessionID": 9622126592,
        "msSinceLastIscsiPDU": 243,
        "msSinceLastScsiCommand": 141535021,
        "nodeID": 3,
        "serviceID": 6,
        "sessionID": 25769804943,
        "targetIP": "10.1.1.2:3260",
        "targetName": "iqn.2010-01.com.solidfire:a7sd.3",
        "targetPortName": "iqn.2010-01.com.solidfire:a7sd.3,t,0x1",
        "virtualNetworkID": 0,
        "volumeID": 3,
        "volumeInstance": 140327214758656
      }
     ...
    ]
  }
}
```


Nuevo desde la versión

9.6

Servicios de listas

Puede utilizar el `ListServices` método para enumerar la información de servicios de los nodos, las unidades, el software actual y otros servicios que se ejecutan en el clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
servicios	Los servicios que se ejecutan en las unidades y los nodos.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListServices",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
"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"
            }
        }
    ]
}
```


Nuevo desde la versión

9.6

ListPendingNodes

Puede utilizar el `ListPendingNodes` método para enumerar los nodos de almacenamiento pendientes en el sistema. Los nodos pendientes son nodos de almacenamiento que se ejecutan y se configuran para unirse al clúster de almacenamiento, pero aún no se añadieron mediante el método API AddNodes.

Direcciones de gestión IPv4 e IPv6

Tenga en cuenta que `ListPendingNodes` No enumera los nodos pendientes que tienen diferentes tipos de dirección para la dirección IP de gestión (MIP) y la dirección IP virtual de gestión (MVIP). Por ejemplo, si un nodo pendiente tiene una MVIP IPv6 y una MIP de IPv4, `ListPendingNodes` no incluirá el nodo como parte del resultado.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
PendingNodes	La lista de nodos pendientes del clúster.	PendingNode cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListPendingNodes",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}
```

Nuevo desde la versión

9.6

Obtenga más información

AddNodes

ListPendingActiveNodes

Puede utilizar el `ListPendingActiveNodes` Método para enumerar los nodos del clúster que están en el estado PendingActive, entre los estados pendiente y activo. Los nodos en este estado se devuelven a la imagen de fábrica.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
PendingActiveNodes	Lista de objetos, donde se detalla información acerca de todos los nodos PendingActive del sistema.	PendingActiveNode cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListPendingActiveNodes",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  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"
    }
    ]
  }
}
```

Nuevo desde la versión

9.6

ModifyClusterFullThreshold

Puede utilizar el `ModifyClusterFullThreshold` método para cambiar el nivel en el que el sistema genera un evento cuando el clúster de almacenamiento se acerca a un determinado uso de la capacidad. La configuración de umbral se puede utilizar para indicar la cantidad aceptable de almacenamiento en bloques utilizado antes de que el sistema genere una advertencia.

Por ejemplo, si desea recibir una alerta cuando el sistema alcance un 3 % por debajo del uso de almacenamiento en bloque de nivel "error", introduzca el valor "3" para el parámetro stage3BlockThreholdPercent. Si se alcanza este nivel, el sistema envía una alerta al registro de eventos en la Consola de administración de clústeres.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Debe seleccionar al menos un parámetro.

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
MaxMetadataOverProvisionFactor	Un representante de valor del número de veces que el espacio de metadatos se puede aprovisionar en exceso en relación con la cantidad de espacio disponible. Por ejemplo, si había suficiente espacio de metadatos para almacenar 100 TIB de volúmenes y este número se estableció en 5, se podría crear un valor de 500 TIB de volúmenes.	entero	5	No
Stage2AwareThreshold	El número de nodos de capacidad que queda en el clúster antes de que el sistema active una notificación de capacidad.	entero	Ninguno	No
Stage3BlockThresholdPercent	El porcentaje de uso del almacenamiento en bloque es inferior al umbral "error" que hace que el sistema active una alerta de "advertencia" de clúster.	entero	Ninguno	No
Stage3MetadataThresholdPercent	El porcentaje de utilización del almacenamiento de metadatos por debajo del umbral "'error'" que hace que el sistema active una alerta de clúster "'Advertencia'".	entero	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
BlockFullness	El nivel calculado actual de ocupación del bloque del clúster. • Stage1Happy: Sin alertas ni condiciones de error. Corresponde al estado **saludable** de la interfaz de usuario web. • Stage2Aware: Sin alertas ni condiciones de error. Corresponde al estado **saludable** de la interfaz de usuario web. • Stage3Low: El sistema no puede brindar protección de datos redundante contra dos fallos de nodo sin simultáneo. Corresponde al estado **Warning** de la interfaz de usuario web. Es posible configurar este nivel en la interfaz de usuario web (el sistema activa esta alerta de forma predeterminada cuando la capacidad es un 3 % inferior al estado error). • Stage4Critical: El sistema no es capaz de brindar protección de datos redundante desde un fallo de nodo único. No se pueden crear volúmenes o clones nuevos. Corresponde al estado **error** en la interfaz de usuario del elemento. • Stage5CompletelyConsumed: Totalmente consumido. El clúster es de solo lectura; se mantienen las conexiones iSCSI, pero se suspenden todas las escrituras. Corresponde al estado **Critical** de la interfaz de usuario de elemento.	cadena

plenitud	Refleja el nivel más alto de plenitud entre "blockFullness" y "metadataFullness".	cadena
MaxMetadataOverProvisionFactor	Un representante de valor del número de veces que el espacio de metadatos se puede aprovisionar en exceso en relación con la cantidad de espacio disponible. Por ejemplo, si había suficiente espacio de metadatos para almacenar 100 TIB de volúmenes y este número se estableció en 5, se podría crear un valor de 500 TIB de volúmenes.	entero

MetadataFullness	El nivel calculado actual de ocupación de metadatos del clúster. • Stage1Happy: Sin alertas ni condiciones de error. Corresponde al estado **saludable** de la interfaz de usuario web. • Stage2Aware: Sin alertas ni condiciones de error. Corresponde al estado **saludable** de la interfaz de usuario web. • Stage3Low: El sistema no puede brindar protección de datos redundante contra dos fallos de nodo sin simultáneo. Corresponde al estado **Warning** de la interfaz de usuario web. Es posible configurar este nivel en la interfaz de usuario web (el sistema activa esta alerta de forma predeterminada cuando la capacidad es un 3 % inferior al estado error). • Stage4Critical: El sistema no es capaz de brindar protección de datos redundante desde un fallo de nodo único. No se pueden crear volúmenes o clones nuevos. Corresponde al estado **error** en la interfaz de usuario del elemento. • Stage5CompletelyConsumed: Totalmente consumido. El clúster es de solo lectura; se mantienen las conexiones iSCSI, pero se suspenden todas las escrituras. Corresponde al estado **Critical** de la interfaz de usuario de elemento.	cadena
SliceReserveUsedThresholdPct	Condición de error. Se activa una alerta del sistema si el uso del segmento de umbral reservado es mayor que el valor devuelto por sliceReserveUsedholdPct .	entero

Stage2AwareThreshold	Condición de conciencia. El valor que se establece para el nivel de umbral del clúster "fase 2".	entero
Stage2BlockThresholdBytes	El número de bytes que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 2.	entero
Stage2MetadataThresholdBytes	El número de bytes de metadatos que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 2.	
Stage3BlockThresholdBytes	El número de bytes de almacenamiento que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 3.	entero
Stage3BlockThresholdPercent	El valor porcentual establecido para la etapa 3. En este porcentaje lleno, se publica una advertencia en el registro de alertas.	entero
Stage3LowThreshold	Condición de error. El umbral en el que se crea una alerta del sistema debido a la baja capacidad de un clúster.	entero
Stage3MetadataThresholdBytes	El número de bytes de metadatos que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 3.	
Stage4BlockThresholdBytes	El número de bytes de almacenamiento que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 4.	entero
Stage4Critical Threshold	Condición de error. El umbral en el que se crea una alerta del sistema para informar sobre una capacidad extremadamente baja en un clúster.	entero

Stage4MetadataThresholdBytes	El número de bytes de metadatos que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 4.	
Stage5BlockThresholdBytes	El número de bytes de almacenamiento que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 5.	entero
Stage5MetadataThresholdBytes	El número de bytes de metadatos que utiliza el clúster en el cual existirá una condición de ocupación de la etapa 5.	
SumTotalClusterBytes	La capacidad física del clúster, medida en bytes.	entero
SumTotalMetadataClusterBytes	La cantidad total de espacio que se puede utilizar para almacenar metadatos.	entero
SumUsedClusterBytes	La cantidad de bytes de almacenamiento que se utiliza en el clúster.	entero
SUUsedMetadataClusterBytes	La cantidad de espacio usado en las unidades de volúmenes para almacenar metadatos.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method" : "ModifyClusterFullThreshold",
   "params" : {
               "stage3BlockThresholdPercent" : 3
               },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
  }
}
```


Nuevo desde la versión

9.6

ModifyClusterInterfacePreference

La `ModifyClusterInterfacePreference` Método permite que los sistemas se integren con los clústeres de almacenamiento que ejecutan el software Element para cambiar una preferencia de interfaz de clúster existente. Este método es para uso interno.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nombre	El nombre de la interfaz del clúster preferida que se debe modificar.	cadena	Ninguno	Sí

valor	El nuevo valor de la interfaz de clúster preferida.	cadena	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "ModifyClusterInterfacePreference",
    "params": {
    "name": "testname",
    "value": "newvalue"
},
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {}
}
```

Nuevo desde la versión

11.0

RemoveNodes

Puede utilizar `RemoveNodes` para quitar uno o varios nodos que ya no deberían participar en el clúster.

Antes de quitar un nodo, debe quitar todas las unidades que contiene el nodo mediante el `RemoveDrives` método. No se puede quitar un nodo hasta que el `RemoveDrives` el proceso ha finalizado y todos los datos se han migrado del nodo. Después de quitar un nodo, este se registra a sí mismo como un nodo pendiente. Puede volver a añadir el nodo o apagarlo (apagar el nodo lo elimina de la lista de nodos pendientes).

Eliminación de nodo maestro de clústeres

Si utiliza `RemoveNodes` para quitar el nodo maestro de clúster, es posible que se agote el tiempo de espera del método antes de devolver una respuesta. Si la llamada al método no puede eliminar el nodo, vuelva a realizar la llamada al método. Tenga en cuenta que si va a quitar el nodo de maestro de clústeres junto con otros nodos, debe usar una llamada independiente para quitar el nodo maestro de clústeres por sí mismo.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IgnoroEnsemlletolerancia Cambiar	Ignore los cambios en la tolerancia de fallo del nodo del conjunto cuando quite los nodos. Si el clúster de almacenamiento utiliza esquemas de protección de datos que toleran varios fallos de nodo y la eliminación de los nodos disminuye la tolerancia de fallo del nodo del conjunto, la eliminación del nodo se produce un error normalmente. Es posible establecer este parámetro en TRUE para deshabilitar la comprobación de tolerancia del conjunto con el fin de que la eliminación del nodo se complete correctamente.	booleano	falso	No
nodos	Lista de NodeIDs para los nodos que se van a quitar.	matriz en números enteros	Ninguno	Sí

Valor de retorno

Este método no tiene ningún valor devuelto.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "RemoveNodes",
   "params": {
     "nodes"  : [3,4,5]
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1
  "result" : {},
}
```

Nuevo desde la versión

9.6

SetLoginSessionInfo

Puede utilizar el `SetLoginSessionInfo` método para establecer el período de tiempo que es válido una autenticación de inicio de sesión para una sesión. Una vez transcurrido el período de inicio de sesión sin actividad en el sistema, caduca la autenticación. Se requieren nuevas credenciales de inicio de sesión para permitir un acceso constante al clúster una vez transcurrido el período de inicio de sesión.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
tiempo de espera	Período de vencimiento de la autenticación en clúster. Con formato HH:mm:ss Por ejemplo: 01:30:00, 00:90:00, y 00:00:5400 pueden utilizarse todos para igualar un periodo de tiempo de espera de 90 minutos. El valor de tiempo de espera mínimo es 1 minuto. Cuando no se proporciona un valor, o se configura a cero, la sesión de inicio de sesión no tiene valor de tiempo de espera.	cadena	30 minutos	No

Valor de retorno

Este método no tiene ningún valor devuelto.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "SetLoginSessionInfo",
  "params": {
    "timeout" : "01:30:00"
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuevo desde la versión

9.6

Apagado

Puede utilizar el `Shutdown` método para reiniciar o apagar los nodos de un clúster. Puede apagar un único nodo, varios nodos o todos los nodos del clúster mediante este método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nodos	Lista de NodeIDs para los nodos que se van a reiniciar o apagar.	matriz en números enteros	Ninguno	Sí
opción	Acción que se debe realizar para el clúster. Valores posibles: * Restart: Reinicia el clúster. * Detener: Realiza un apagado completo.	cadena	reiniciar	No

Valor de retorno

Este método no tiene ningún valor devuelto. == las solicitudes de ejemplo para este método son similares al ejemplo siguiente:

```
{
   "method": "Shutdown",
   "params": {
     "nodes": [
       2,
       3,
       4
     ],
     "option": "halt"
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {
     "failed": [],
     "successful": [
          6
      [
   }
}
```

Nuevo desde la versión

9.6

Métodos API de creación de clúster

Puede usar estos métodos API para crear un clúster de almacenamiento de. Todos estos métodos se deben usar contra el extremo de API en un solo nodo.

- Clúster de propuesta de CheckedCluster
- CreateCluster
- GetBootstrapConfig

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Clúster de propuesta de CheckedCluster

Puede utilizar el `CheckProposedCluster` método para probar un conjunto de nodos de almacenamiento antes de crear un clúster de almacenamiento con ellos para identificar posibles errores o errores que se produzcan desde el intento, como funcionalidades de nodos mixtos desequilibradas o tipos de nodos que no son compatibles con los clústeres de almacenamiento de dos nodos.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nodos	Una lista de direcciones IP de almacenamiento del conjunto inicial de nodos de almacenamiento que forman el clúster de almacenamiento.	matriz de cadenas	Ninguno	Sí
fuerza	Establezca esta opción en true para ejecutar todos los nodos de almacenamiento en el clúster de almacenamiento.	booleano	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
ProposedClusterValid	Indica si los nodos de almacenamiento propuestos componen un clúster de almacenamiento válido o no. Los posibles valores son los siguientes: • verdadero • falso	booleano

ProposedClusterErrors	Errores que se producirían si se creara un clúster de almacenamiento mediante los nodos de almacenamiento propuestos.	matriz de cadenas

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "CheckProposedCluster",
    "params": {
    "nodes": [
        "192.168.1.11",
        "192.168.1.12",
        "192.168.1.13",
        "192.168.1.14"
    ]
},
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "proposedClusterValid": true,
        "proposedClusterErrors": [ ]
    }
}
```

Nuevo desde la versión

11.0

CreateCluster

Puede utilizar el `CreateCluster` método para inicializar el nodo en un clúster que tenga la propiedad de las direcciones "mvip" y "svip". Cada clúster nuevo se inicializa mediante la IP de gestión (MIP) del primer nodo del clúster. Este método también añade automáticamente todos los nodos que se están configurando en el clúster. Solo tiene que

utilizar este método una vez cada vez que se inicializa un clúster nuevo.

Después de iniciar sesión en el nodo maestro del clúster y ejecutar el GetBootStrapConfig Método para obtener las direcciones IP del resto de los nodos que se desean incluir en el clúster, es posible ejecutar el método CreateCluster en el nodo maestro para el clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
AceptEula	Indique su aceptación del contrato de licencia para usuario final al crear este clúster. Para aceptar el CLUF, establezca este parámetro en TRUE.	booleano	Ninguno	Sí
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
EnableSoftwareEncryptionAtest	Habilite este parámetro para utilizar el cifrado basado en software en reposo. De forma predeterminada es FALSE en todos los clústeres. Después de habilitar el cifrado de software en reposo, no se puede deshabilitar en el clúster.	booleano	verdadero	No
mivip	La dirección IP flotante (virtual) del clúster en la red de gestión.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nodos	Direcciones CIP/SIP del conjunto inicial de nodos que forman el clúster. La dirección IP de este nodo debe estar en la lista.	matriz de cadenas	Ninguno	Sí
Número de pedido	Número de pedido de venta alfanumérico. Necesario en plataformas basadas en software.	cadena	Ninguno	No (plataformas basadas en hardware) Sí (plataformas basadas en software)
contraseña	La contraseña inicial de la cuenta de administrador del clúster.	cadena	Ninguno	Sí
SerialNumber	Número de serie alfanumérico de nueve dígitos. Puede ser necesario en plataformas basadas en software.	cadena	Ninguno	No (plataformas basadas en hardware) Sí (plataformas basadas en software)
svip	La dirección IP flotante (virtual) del clúster en la red de almacenamiento (iSCSI).	cadena	Ninguno	Sí
nombre de usuario	Nombre de usuario del administrador del clúster.	cadena	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "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
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"id" : 1,
"result" : {}
}
```

Nuevo desde la versión

9.6

Obtenga más información

- "GetBootstrapConfig"
- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

GetBootstrapConfig

Puede utilizar el `GetBootstrapConfig` método para obtener información de clúster y nodo desde el archivo de configuración bootstrap. Utilice este método API en un nodo individual antes de que se haya Unido a un clúster. La información que devuelve este

método se utiliza en la interfaz de configuración de clústeres cuando se crea un clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
Nombre del clúster	El nombre del clúster.	cadena
mivip	Dirección MVIP del clúster. Vacío si el nodo no forma parte de un clúster.	cadena
Nombre de nodo	El nombre del nodo.	cadena
nodos	Lista de información sobre cada nodo que está esperando activamente para unirse al clúster. Los posibles valores son los siguientes: • ChassisType: (Cadena) Plataforma de hardware del nodo. • cip: (Cadena) Dirección IP de clúster del nodo. • Compatible: (booleano) indica si el nodo es compatible con el nodo en el que se ejecutó la llamada API. • Nombre de host: (Cadena) Nombre de host del nodo. • mip: (Cadena) la dirección IP de gestión de IPv4 del nodo. • MipV6: (Cadena) la dirección IP de gestión de IPv6 del nodo. • NodeType: (Cadena)Nombre del modelo del nodo. • Versión: (String)Versión del software actualmente instalado en el nodo.	Cabina de objetos JSON

Nombre	Descripción	Tipo
svip	La dirección SVIP del clúster. NULL si el nodo no forma parte de un clúster.	cadena
versión	La versión del software Element que se encuentra instalada actualmente en el nodo que se denominó con este método de API.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetBootstrapConfig",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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"
    }
}
```

Nuevo desde la versión

9.6

Obtenga más información

CreateCluster

Métodos de API de unidad

Es posible usar los métodos de API de unidad para añadir y gestionar unidades que están disponibles para un clúster de almacenamiento. Cuando se añade un nodo de almacenamiento al clúster de almacenamiento o se instalan unidades nuevas en un nodo de almacenamiento existente, las unidades se pueden añadir al clúster de almacenamiento.

- AddDrives
- GetDriveHardwarwareInfo
- GetDriveStats
- ListDrives
- ListDriveStats
- RemoveDrives
- SecureEraseDrives

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

AddDrives

Puede utilizar el `AddDrives` método para añadir una o varias unidades disponibles al clúster, lo cual permite que las unidades alojen una parte de los datos del clúster.

Cuando se añade un nodo de almacenamiento al clúster o se instalan unidades nuevas en un nodo existente, las unidades nuevas se marcan como disponibles y se deben añadir mediante AddDrives antes de que se puedan utilizar. Utilice la ListDrives método para mostrar las unidades disponibles para añadir. Cuando se añade una unidad, el sistema determina automáticamente el tipo de unidad que debería ser.

El método es asíncrono y devuelve tan pronto como se inician los procesos para reequilibrar las unidades del clúster. Sin embargo, puede tardar más tiempo en que los datos del clúster se reequilibren utilizando las unidades que se acaban de añadir; el reequilibrado continuará incluso después de que finalice la llamada al método AddDrives. Puede utilizar el GetAsyncResult Método para consultar el comando establish devuelto por el método. Una vez que se devuelve el método AddDrives, puede utilizar ListSyncJobs método para ver el progreso del reequilibrado de los datos con las nuevas unidades.

Cuando se agregan varias unidades, es más eficaz agregarlas en una sola llamada al método AddDrives en lugar de varios métodos individuales con una sola unidad cada uno. Esto reduce la cantidad de equilibrio de datos que se debe producir para estabilizar la carga de almacenamiento en el clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
unidades	Información sobre cada unidad que se va a añadir al clúster. Los posibles valores son los siguientes: • DriveID: El ID de la unidad que se va a añadir (número entero). • Type: El tipo de unidad que se va a añadir (cadena). Los valores válidos son "slice", "block" o "volume". Si se omite, el sistema asigna el tipo correcto.	Cabina de objetos JSON	Ninguno	Sí (el tipo es opcional)

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Establish asyncHandle	Valor de mango utilizado para obtener el resultado de la operación.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 1,
  "method": "AddDrives",
  "params": {
    "drives": [
      {
        "driveID": 1,
        "type": "slice"
      },
      {
        "driveID": 2,
        "type": "block"
      },
      {
        "driveID": 3,
        "type": "block"
      }
    ]
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result" : {
    "asyncHandle": 1
  }
}
```

Nuevo desde la versión

9.6

Obtenga más información

- GetAsyncResult
- ListDrives
- ListSyncJobs

GetDriveHardwarwareInfo

Puede utilizar el `GetDriveHardwareInfo` método para obtener toda la información de

hardware para la unidad dada. Generalmente, se incluyen los fabricantes, los proveedores, las versiones y otra información de identificación de hardware asociada.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de unidad	ID de la unidad para la solicitud.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
resultado	Se devolvió la información de hardware para el DriveID especificado.	HardwareInfo

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetDriveHardwareInfo",
   "params": {
     "driveID": 5
   },
   "id" : 100
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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"
     }
   }
}
```


Nuevo desde la versión

9.6

Obtenga más información

ListDrives

GetDriveStats

Puede utilizar el `GetDriveStats` método para obtener mediciones de actividad de alto nivel para una sola unidad. Los valores se acumulan desde la adición de la unidad al clúster. Algunos valores son específicos de las unidades de bloques. Cuando se ejecuta este método, se devuelven datos estadísticos para los tipos de unidades de metadatos o bloque.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de unidad	ID de la unidad para la solicitud.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
DriveStats	Información de la actividad de la unidad para el DriveID especificado.	DriveStats

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetDriveStats",
   "params": {
     "driveID": 3
   },
   "id" : 1
}
```

Ejemplo de respuesta (unidad de bloque)

Este método devuelve una respuesta similar al siguiente ejemplo para una unidad de bloque:

```
{
  "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
    }
  }
}
```


Ejemplo de respuesta (unidad de metadatos de volumen)

Este método devuelve una respuesta similar al siguiente ejemplo de una unidad de metadatos de un volumen:

```
{
  "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
    }
  }
}
```


Nuevo desde la versión

9.6

Obtenga más información

ListDrives

ListDrives

Puede utilizar el `ListDrives` método para enumerar las unidades que existen en los nodos activos del clúster. Este método muestra las unidades que se añadieron como metadatos de volumen o unidades de bloques, así como las unidades que no se añadieron y están disponibles.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
unidades	La lista de unidades del clúster.	unidad cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListDrives",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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"
       }
     }
   ]
}
```


Nuevo desde la versión

9.6

ListDriveStats

Puede utilizar el `ListDriveStats` método para enumerar las mediciones de actividad de alto nivel para varias unidades en el clúster. De forma predeterminada, este método muestra las estadísticas de todas las unidades del clúster, mientras que estas mediciones se acumulan a partir de la adición de la unidad al clúster. Algunos valores que muestra este método son específicos de las unidades de bloques, y otros son específicos de las unidades de metadatos.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
unidades	Lista de ID de unidad (DriveID) para los que se devolverán estadísticas de unidad. Si omite este parámetro, se muestran mediciones de todas las unidades.	matriz en números enteros	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
DriveStats	Lista de información de actividades de la unidad de cada unidad.	DriveStats cabina
errores	Esta lista contiene el DriveID y el mensaje de error asociado. Siempre está presente y vacío si no hay errores.	Cabina de objetos JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 1,
  "method": "ListDriveStats",
  "params": {
    "drives":[22,23]
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
        }
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

Obtenga más información

GetDriveStats

RemoveDrives

Puede utilizar el `RemoveDrives` método para quitar de forma proactiva unidades que

forman parte del clúster. Se recomienda usar este método al reducir la capacidad de un clúster o como preparación para reemplazar unidades que se acercan al final de su vida útil. `RemoveDrives` Crea una tercera copia de los datos del bloque en los otros nodos del clúster y espera a que se complete la sincronización antes de mover las unidades a la lista «Available». Las unidades de la lista «Disponible» se eliminan por completo del sistema y no tienen servicios en ejecución ni datos activos.

`RemoveDrives` es un método asíncrono. Según la capacidad total de las unidades que se estén quitando, es posible que se deban tardar varios minutos migrar todos los datos.

Cuando se quitan varias unidades, se usa un único `RemoveDrives` llamada a método en lugar de varios métodos individuales con una sola unidad cada uno. Esto reduce la cantidad de equilibrio de datos que debe producirse para estabilizar uniformemente la carga de almacenamiento del clúster.

También es posible quitar unidades con estado "Failed" mediante `RemoveDrives`. Cuando se retira una unidad con el estado «fallido», la unidad no se devuelve a un estado «disponible» o «activo». La unidad no está disponible para usar en el clúster.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
unidades	Lista de identificadores de unidades que se van a quitar del clúster.	matriz en números enteros	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Establish asyncHandle	Valor de mango utilizado para obtener el resultado de la operación.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "RemoveDrives",
   "params": {
      "drives"  : [3, 4, 5]
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result" : {
     "asyncHandle": 1
   }
}
```

Nuevo desde la versión

9.6

Obtenga más información

- GetAsyncResult
- ListDrives

SecureEraseDrives

Puede utilizar el `SecureEraseDrives` método para eliminar todos los datos residuales de las unidades que tienen el estado "available". Se recomienda usar este método cuando se reemplaza una unidad que se acerca al final de su vida útil que contenía datos confidenciales. Este método utiliza un comando de la unidad de borrado de seguridad para escribir un patrón predeterminado en la unidad y restablece la clave de cifrado en la unidad. Este método asíncrono puede tardar varios minutos en completarse.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
unidades	Lista de ID de unidad que se van a borrar de forma segura.	matriz en números enteros	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Establish asyncHandle	Valor de mango utilizado para obtener el resultado de la operación.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "SecureEraseDrives",
   "params": {
     "drives"  : [3, 4, 5]
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id" : 1
   "result" : {
     "asyncHandle" : 1
   }
}
```

Nuevo desde la versión

9.6

Obtenga más información

- GetAsyncResult
- ListDrives

Métodos de API de Fibre Channel

Es posible usar métodos de API Fibre Channel para añadir, modificar o quitar miembros de nodos Fibre Channel de un clúster de almacenamiento.

- GetVolumeAccessGroupLunAssignments
- ListFiberChannelPortInfo
- ListFiberChannelSessions
- ListNodeFiberChannelPortInfo
- ModifyVolumeAccessGroupLunAssignments

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

GetVolumeAccessGroupLunAssignments

Puede utilizar el `GetVolumeAccessGroupLunAssignments` Método para recuperar detalles de las asignaciones de LUN de un grupo de acceso de volúmenes especificado.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VolumeAccessGroupID	Un ID de grupo de acceso de volúmenes único que se utiliza para mostrar información.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumeAccessGroupLunAssignments	Una lista de todos los puertos Fibre Channel físicos o un puerto para un único nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetVolumeAccessGroupLunAssignments",
   "params": {
      "volumeAccessGroupID": 5
    },
  "id" : 1
   }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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}
       ]
    }
  }
}
```

Nuevo desde la versión

9.6

ListFiberChannelPortInfo

Puede utilizar el `ListFibreChannelPortInfo` Método para ver información acerca de los puertos Fibre Channel.

Este método de API está pensado para usar en nodos individuales; se necesitan un ID de usuario y una contraseña para acceder a nodos Fibre Channel individuales. Sin embargo, este método se puede usar en el

clúster si el parámetro force está establecido en true. Cuando se usa en el clúster, se muestran todas las interfaces de Fibre Channel.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
fuerza	Establezca esta opción en true para ejecutarse en todos los nodos del clúster.	booleano	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
FiberChannelPorts	Una lista de todos los puertos Fibre Channel físicos o un puerto para un único nodo.	Puerto de FiberChannelPort cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListFibreChannelPortInfo",
    "params": {},
    "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
         }
      ]
     }
    }
   }
  }
}
```


Nuevo desde la versión

9.6

ListFiberChannelSessions

Puede utilizar el `ListFibreChannelSessions` Método para ver información acerca de las sesiones Fibre Channel en un clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
sesiones	Una lista de objetos que describen sesiones Fibre Channel activas en el clúster.	sesión cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListFibreChannelSessions",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
    }
    ]
  }
}
```

Nuevo desde la versión

9.6

ListNodeFiberChannelPortInfo

Puede utilizar el `ListNodeFibreChannelPortInfo` Método para ver información acerca de los puertos Fibre Channel en un nodo.

Este método de API está pensado para usar en nodos individuales; se necesitan un ID de usuario y una

contraseña para acceder a nodos Fibre Channel individuales. Cuando se usa en el clúster, se muestran todas las interfaces de Fibre Channel.

Parámetro

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
FiberChannelPorts	Una lista de todos los puertos Fibre Channel físicos o un puerto para un único nodo.	Puerto de FiberChannelPort cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListNodeFibreChannelPortInfo",
   "params": {
       "nodeID": 5,
       "force": true
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}
```

Nuevo desde la versión

9.6

ModifyVolumeAccessGroupLunAssignments

Puede utilizar el `ModifyVolumeAccessGroupLunAssignments` Método para definir asignaciones de LUN personalizadas para volúmenes específicos.

Este método solo cambia los valores de LUN establecidos en el parámetro lunAssignments en el grupo de acceso de volúmenes. El resto de las asignaciones de LUN no han cambiado.

Los valores de asignación de LUN deben ser únicos para los volúmenes de un grupo de acceso de volúmenes. No se pueden definir valores de LUN duplicados dentro de un grupo de acceso de volúmenes. Sin embargo, puede volver a utilizar los mismos valores de LUN en diferentes grupos de acceso de volúmenes.

> Los valores válidos de LUN abarcan de 0 a 16383. El sistema genera una excepción si pasa un valor de LUN fuera de este rango. Ninguna de las asignaciones de LUN especificadas se modifica si hay una excepción.

PRECAUCIÓN:

Si cambia una asignación de LUN para un volumen con I/o activas, es posible interrumpir las operaciones de I/O. Debe cambiar la configuración del servidor antes de cambiar las asignaciones de LUN de volumen.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VolumeAccessGroupID	ID de grupo de acceso de volúmenes único para el que se modificarán las asignaciones de LUN.	entero	Ninguno	Sí
LunAssignments	Los ID de volumen con nuevos valores de LUN asignados.	matriz en números enteros	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo

VolumeAccessGroupLunAssignments	Objeto que contiene detalles de las asignaciones de LUN de grupos de acceso de volúmenes modificadas.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ModifyVolumeAccessGroupLunAssignments",
   "params": {
       "volumeAccessGroupID" : 218,
       "lunAssignments" : [
           {"volumeID" : 832, "lun" : 0},
           {"volumeID" : 834, "lun" : 1}
        ]
    },
    "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "volumeAccessGroupLunAssignments": {
      "deletedLunAssignments": [],
      "lunAssignments": [
        {
          "lun": 0,
          "volumeID": 832
        },
        {
          "lun": 1,
          "volumeID": 834
        }
      ],
      "volumeAccessGroupID": 218
    }
  }
}
```

Nuevo desde la versión

9.6

Métodos de API del iniciador

Los métodos de iniciador permiten añadir, quitar, ver y modificar objetos de iniciador iSCSI, que controlan la comunicación entre el sistema de almacenamiento y los clientes de almacenamiento externos.

- CreateInitiators
- DeleteInitiators
- ListInitiators
- ModificyInitiators

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

CreateInitiators

Puede utilizar `CreateInitiators` Para crear varios IQN de iniciador nuevos o nombres de puerto WWPN y, de manera opcional, asignarles alias y atributos. Cuando utilice `CreateInitiators` para crear nuevos iniciadores, también puede añadirlos a grupos de acceso de volúmenes.

Si la operación no puede crear uno de los iniciadores proporcionados en el parámetro, el método devuelve un error y no crea ningún iniciador (no es posible completar parcialmente).

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
iniciadores	Una lista de objetos que contienen características de cada iniciador nuevo. Objetos: • `alias`: (Opcional) el nombre descriptivo que se debe asignar a este iniciador. (cadena) • `attributes`: (Opcional) un conjunto de atributos JSON que se asignarán a este iniciador. (Objeto JSON) • `chapUsername`: (Opcional) el nombre de usuario CHAP único para este iniciador. Los valores predeterminados del nombre del iniciador (IQN) si no se especifican durante la creación y requiredChap son true. (cadena) • `initiatorSecret`: (Opcional) el secreto CHAP utilizado para autenticar el iniciador. Por defecto, es un secreto generado aleatoriamente si no se especifica durante la creación y requiredChap es true. (cadena)	Cabina de objetos JSON	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
iniciadores	Lista de objetos que describen los iniciadores recién creados.	iniciador cabina

Error

Este método puede devolver el siguiente error:

Nombre	Descripción
XInitiatorExists	Devuelto si el nombre del iniciador que ha elegido ya existe.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "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"
      }
    ]
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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": []
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

Obtenga más información

ListInitiators

DeleteInitiators

Puede utilizar `DeleteInitiators` para eliminar uno o más iniciadores del sistema (y de todos los volúmenes o grupos de acceso de volúmenes asociados).

Si `DeleteInitiators` error al eliminar uno de los iniciadores proporcionados en el parámetro, el sistema devuelve un error y no elimina ningún iniciador (no es posible realizar una finalización parcial).

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
iniciadores	Una matriz de ID de iniciadores que se van a eliminar.	matriz en números enteros	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Error

Este método puede devolver el siguiente error:

Nombre	Descripción
XInitiatorDoesNotExist	Devuelto si el nombre del iniciador que ha elegido no existe.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 5101,
  "method": "DeleteInitiators",
  "params": {
    "initiators": [
      145,
      147
    ]
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 5101,
  "result": {}
}
```

Nuevo desde la versión

9.6

ListInitiators

Puede utilizar el `ListInitiators` Método para obtener la lista de IQN de iniciador o nombres de puerto WWPN.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
iniciadores	Una lista de ID de iniciador que se desea recuperar. Puede proporcionar este parámetro o el parámetro startInitiatorID, pero no ambos.	matriz en números enteros	Ninguno	No
StartInitiatorID	El ID del iniciador en el que comenzar el listado. Puede proporcionar este parámetro o el parámetro Initiators, pero no ambos.	entero	0	No
límite	El número máximo de objetos iniciador que se van a devolver.	entero	(ilimitada)	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
iniciadores	Lista de la información del iniciador.	iniciador cabina

Excepciones

Este método puede tener la siguiente excepción:

Nombre	Descripción
XInvalidParameter	Emitido si incluye el startInitiatorID y los parámetros de iniciadores en la misma llamada de método.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListInitiators",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "initiators": [
      {
        "alias": "",
        "attributes": {},
        "initiatorID": 2,
        "initiatorName": "iqn.1993-08.org.debian:01:c84ffd71216",
        "volumeAccessGroups": [
          1
        ]
      }
    ]
  }
}
```

Nuevo desde la versión

9.6

ModificyInitiators

Puede utilizar el `ModifyInitiators` método para cambiar los atributos de uno o más iniciadores existentes.

No puede cambiar el nombre de un iniciador existente. Si necesita cambiar el nombre de un iniciador,

elimínelo primero con el DeleteInitiators y cree uno nuevo con el CreateInitiators método.

Si ModifyInitiators no cambia uno de los iniciadores proporcionados en el parámetro, el método devuelve un error y no modifica ningún iniciador (no es posible completar parcialmente).

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio

iniciadores	Una lista de objetos que contienen características de cada iniciador que se va a modificar. Objetos posibles: • `alias`: (Opcional) un nuevo nombre descriptivo que se debe asignar al iniciador. (cadena) • `attributes`: (Opcional) un nuevo conjunto de atributos JSON que se asignarán al iniciador. (Objeto JSON) • `chapUsername`: (Opcional) un nuevo nombre de usuario CHAP único para este iniciador. (cadena) • `forceDuringUpgrade`: Complete la modificación del iniciador durante una actualización. • `initiatorID`: (Obligatorio) el ID del iniciador que se va a modificar. (entero) • `initiatorSecret`: (Opcional) un nuevo secreto CHAP utilizado para autenticar al iniciador. (cadena) `requireChap`: (Opcional) True si se requiere	Cabina de objetos JSON	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
iniciadores	Lista de objetos que describen los iniciadores recién modificados.	iniciador cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 6683,
  "method": "ModifyInitiators",
  "params": {
    "initiators": [
      {
        "initiatorID": 2,
        "alias": "alias1",
        "volumeAccessGroupID": null
      },
      {
        "initiatorID": 3,
        "alias": "alias2",
        "volumeAccessGroupID": 1
      }
    ]
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

- CHAP para este iniciador. (booleano)
- el destino (al utilizar la autenticación CHAP mutua). (cadena)
- `GroupID`: (Opcional) el ID del grupo de acceso de volúmenes al que se debe añadir el iniciador. Si el iniciador se encontraba previamente en un grupo de acceso de volúmenes diferente, se elimina del grupo de acceso de volúmenes antiguo. Si esta clave está presente pero es

```
{
  "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
        ]
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

Obtenga más información

- CreateInitiators
- DeleteInitiators

Métodos de API de LDAP

Puede usar el protocolo ligero de acceso a directorios (LDAP) para autenticar el acceso al almacenamiento de Element. Los métodos de API de LDAP que se describen en esta sección le permiten configurar el acceso LDAP al clúster de almacenamiento.

- AddLdapClusterAdmin
- EnableLdapAuthentication
- Autenticación DisableLdapAuthentication
- GetLdapConfiguration
- TestLdapAuthentication

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

AddLdapClusterAdmin

Puede utilizar el `AddLdapClusterAdmin` Para añadir un nuevo usuario administrador de clúster LDAP. Un administrador de clúster LDAP puede gestionar el clúster mediante las herramientas API y de gestión. Las cuentas de administrador de clúster LDAP están completamente separadas y no están relacionadas con las cuentas de cliente estándar.

Parámetros

También puede utilizar este método para agregar un grupo LDAP definido en Active Directory®. El nivel de acceso que se da al grupo se pasa a los usuarios individuales del grupo LDAP.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
acceso	Controla qué métodos puede utilizar este administrador de clúster.	matriz de cadenas	Ninguno	Sí
AceptEula	Acepte el contrato de licencia para usuario final. Establezca esta opción en true para añadir una cuenta de administrador de clúster al sistema. Si se omite o se establece en falso, la llamada al método falla.	booleano	Ninguno	Sí
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
nombre de usuario	El nombre de usuario distintivo del nuevo administrador de clúster LDAP.	cadena	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "AddLdapClusterAdmin",
  "params": {"username":"cn=mike
jones,ou=ptusers,dc=prodtest,dc=solidfire,dc=net",
    "access": ["administrator", "read"
    ]
  },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
 "id": 1,
 "result": {}
}
```

Nuevo desde la versión

9.6

Obtenga más información

Control de acceso

EnableLdapAuthentication

Puede utilizar el `EnableLdapAuthentication` Método para configurar una conexión de directorio LDAP para la autenticación LDAP de un clúster de. Los usuarios que son miembros del directorio LDAP pueden iniciar sesión en el sistema de almacenamiento con sus credenciales de LDAP.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Tipo de autorización	Identifica el método de autenticación de usuarios que se va a utilizar. Los posibles valores son los siguientes: • `DirectBind` • `SearchAndBind`	cadena	SearchAndBind	No
GroupSearchBaseDN	El DN base del árbol para iniciar la búsqueda del subárbol del grupo.	cadena	Ninguno	No
GroupSearchType	Controla el filtro de búsqueda de grupos predeterminado que se utiliza. Los posibles valores son los siguientes: • NoGroups: Ningún soporte de grupo. • ActiveDirectory: Pertenencia anidada de todos los grupos de directorios activos de un usuario. • MemberDN: Grupos del estilo MemberDN (un nivel).	cadena	ActiveDirectory	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
URIs de servidor	Lista separada por comas de URI de servidor LDAP o LDAPS. Puede agregar un puerto personalizado al final de un URI LDAP o LDAPS usando un punto y dos puntos seguidos por el número de puerto. Por ejemplo, el URI "ldap://1.2.3.4" utiliza el puerto predeterminado y el URI "ldaps://1.2.3.4:123" utiliza el puerto personalizado 123.	matriz de cadenas	Ninguno	Sí
UserSearchBaseDN	El DN base del árbol para iniciar la búsqueda del subárbol. Este parámetro es obligatorio cuando se utiliza AuthType de SearchAndBind.	cadena	Ninguno	No
SearchBindDN	Un DN completo con el que se inicia sesión para realizar una búsqueda LDAP del usuario. El DN requiere acceso de lectura al directorio LDAP. Este parámetro es obligatorio cuando se utiliza AuthType de SearchAndBind.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SearchBindPassword	La contraseña de la cuenta searchBindDN utilizada para realizar la búsqueda. Este parámetro es obligatorio cuando se utiliza AuthType de SearchAndBind.	cadena	Ninguno	Sí
UserSearchFilter	Filtro de búsqueda LDAP que se va a utilizar al consultar el servidor LDAP. La cadena debe tener el texto de marcador de posición "%USERNAME%" que se sustituye por el nombre de usuario del usuario que se va a autenticar. Por ejemplo, (&(objectClass=person)(sAMAccountName=%USERNAME%)) utilizará el campo sAMAccountName de Active Directory para que coincida con el nombre de usuario introducido al iniciar sesión en el clúster. Este parámetro es obligatorio cuando se utiliza AuthType de SearchAndBind.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
UserDNTemplate	Plantilla de cadena utilizada para definir un patrón para construir un nombre completo (DN) de usuario. La cadena debe tener el texto de marcador de posición "%USERNAME%" que se sustituye por el nombre de usuario del usuario que se va a autenticar. Este parámetro es necesario cuando se utiliza AuthType de DirectBind.	cadena	Ninguno	Sí
GroupSearchCustomFilter	Para utilizarlo con el tipo de búsqueda CustomFilter, un filtro LDAP que se utilizará para devolver el DNS de los grupos de un usuario. La cadena puede tener texto de marcador de posición de %USERNAME% y %USERDN% para ser reemplazado por su nombre de usuario y su DN de usuario completo según sea necesario.	cadena	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "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
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"id": 1,
"result": {
  }
}
```

Nuevo desde la versión

9.6

Autenticación DisableLdapAuthentication

Puede utilizar el `DisableLdapAuthentication` Método para deshabilitar la autenticación LDAP y quitar todas las opciones de configuración de LDAP. Este método no quita ninguna cuenta de administrador de clúster configurada para los usuarios o los grupos. Una vez deshabilitada la autenticación LDAP, los administradores de clúster que se configuran para usar la autenticación LDAP ya no pueden acceder al clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DisableLdapAuthentication",
  "params": {},
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"id": 1,
"result": {}
}
```

Nuevo desde la versión

9.6

GetLdapConfiguration

Puede utilizar el `GetLdapConfiguration` Método para obtener la configuración de LDAP activa actualmente en el clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto.

Nombre	Descripción	Tipo
LdapConfiguration	Lista de las opciones de configuración de LDAP actuales. Esta llamada API no devuelve el texto sin formato de la contraseña de la cuenta de búsqueda. **Nota:** Si la autenticación LDAP está deshabilitada actualmente, todas las configuraciones devueltas están vacías con la excepción de "AuthType" y "groupSearchType", que se establecen en "SearchAndBind" y "ActiveDirectory" respectivamente.	LdapConfiguration

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetLdapConfiguration",
  "params": {},
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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%))"
     }
   }
}
```

Nuevo desde la versión

9.6

TestLdapAuthentication

Puede utilizar el `TestLdapAuthentication` Método para validar la configuración de autenticación LDAP habilitada actualmente. Si la configuración es correcta, la llamada API devuelve la pertenencia al grupo del usuario probado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nombre de usuario	Nombre de usuario que se va a probar.	cadena	Ninguno	Sí
contraseña	La contraseña para probar el nombre de usuario.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
LdapConfiguration	Objeto ldapConfiguration que se va a probar. Si se proporciona este parámetro, el sistema prueba la configuración proporcionada aunque la autenticación de LDAP esté deshabilitada actualmente.	LdapConfiguration	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
grupos	Lista de grupos LDAP que incluyen al usuario probado como miembro.	cabina
DN de usuario	Nombre completo LDAP del usuario probado.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method": "TestLdapAuthentication",
"params": {"username":"admin1",
           "password":"admin1PASS"
      },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
 "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"
  }
}
```

Nuevo desde la versión

9.6

Métodos de API de autenticación multifactor

Puede usar la autenticación multifactor (MFA) para gestionar las sesiones de usuario usando un proveedor de identidades (IDP) de terceros a través del lenguaje de marcado de aserción de seguridad (SAML).

- AddIdpClusterAdmin
- CreateIdpConfiguration
- DeleteAuthSession
- DeleteAuthSessionsByClusterAdmin
- DeleteAuthSessionsByUsername
- DeleteIdpConfiguration
- DisableIdpAuthentication
- EnableIdpAuthentication
- GetIdpAuthenticationState
- ListActiveAuthSessions
- ListIdpConfigurations
- UpdateIdpConfiguration

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

AddIdpClusterAdmin

Puede utilizar el `AddIpdClusterAdmin` Método para añadir un usuario administrador de clúster autenticado por un proveedor de identidades (IDP) de terceros. Las cuentas

de administrador del clúster de IDP se configuran según la información de valor de atributos de SAML que se proporciona dentro de la afirmación de SAML del IDP asociada con el usuario. Si un usuario se autentica correctamente con el IDP y tiene declaraciones de atributos SAML dentro de las afirmaciones de SAML que coinciden con varias cuentas de administrador de clúster IDP, el usuario tendrá el nivel de acceso combinado de las cuentas de administrador de clúster de IDP que coincidan.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
acceso	Controla qué métodos puede usar este administrador de clúster de IDP.	matriz de cadenas	Ninguno	Sí
AceptEula	Acepte el contrato de licencia para usuario final. Establezca esta opción en true para añadir una cuenta de administrador de clúster al sistema. Si se omite o se establece en falso, la llamada al método falla.	booleano	Ninguno	Sí
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nombre de usuario	Asignación de atributo-valor de SAML a un administrador del clúster IDP (por ejemplo, email=test@example.com). Puede definirse mediante un asunto SAML específico `NameID` O como una entrada en la declaración de atributo SAML, como `eduPersonAffiliation`.	cadena	Ninguno	Sí

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
ClusterAdminID	Identificador único para el administrador de clúster recién creado.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "AddIdpClusterAdmin",
    "params": {
        "username": "email=test@example.com",
        "acceptEula": true,
        "access": ["administrator"]
    }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "result": {
        "clusterAdminID": 13
    }
}
```

Nuevo desde la versión

12.0

CreateIdpConfiguration

Puede utilizar el `CreateIpdConfiguration` Método para crear una relación de confianza potencial para la autenticación mediante un proveedor de identidades (IDP) de terceros para el clúster. Se requiere un certificado de proveedor de servicios SAML para la comunicación de IDP. Este certificado se genera según sea necesario y se devuelve mediante esta llamada a la API.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IdpMetadata	Metadatos de IDP para almacenar.	cadena	Ninguno	Sí
IdpName	Nombre utilizado para identificar un proveedor de IDP para el inicio de sesión único SAML 2.0.	cadena	Ninguno	Sí

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
IdpConfigInfo	Información acerca de la configuración del proveedor de identidades (IDP) de terceros.	"IdpConfigInfo"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "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"
    },
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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"
        }
    }
}
```

Nuevo desde la versión

12.0

DeleteAuthSession

Puede utilizar el `DeleteAuthSession` método para eliminar una sesión de autenticación de usuario individual. Si el usuario que llama no está en ClusterAdmins / Administrator AccessGroup, sólo se puede eliminar la sesión de autenticación que pertenece al usuario que realiza la llamada.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SessionID	Identificador único para la sesión de autenticación que se va a eliminar.	UUID	Ninguno	Sí

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
sesión	Información de sesión para la sesión de autenticación de eliminación.	"AuthSessionInfo"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "DeleteAuthSession",
    "params": {
        "sessionID": "a862a8bb-2c5b-4774-a592-2148e2304713"
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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"
        }
    }
}
```


Nuevo desde la versión

12.0

DeleteAuthSessionsByClusterAdmin

Puede utilizar el `DeleteAuthSessionsByClusterAdmin` método para eliminar todas las sesiones de autenticación asociadas con el especificado `ClusterAdminID`. Si el ClusterAdminID especificado se asigna a un grupo de usuarios, se eliminarán todas las sesiones de autenticación de todos los miembros de ese grupo. Para ver una lista de sesiones que pueden eliminarse, utilice el método ListAuthSessionsByClusterAdmin con el `ClusterAdminID` parámetro.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ClusterAdminID	Identificador único del administrador de clúster.	entero	Ninguno	Sí

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
sesiones	Información de la sesión para las sesiones de autenticación eliminadas.	"AuthSessionInfo"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DeleteAuthSessionsByClusterAdmin",
  "params": {
    "clusterAdminID": 1
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"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"
      }
    ]
}
```

Nuevo desde la versión

12.0

DeleteAuthSessionsByUsername

Puede utilizar el `DeleteAuthSessionsByUsername` método para eliminar todas las sesiones de autenticación de un usuario determinado. Un llamante que no esté en AccessGroup ClusterAdmins/Administrator sólo puede eliminar sus propias sesiones. Una persona que llama con privilegios de Administrador de clúster puede eliminar sesiones que pertenecen a cualquier usuario. Para ver la lista de sesiones que se podrían eliminar, utilice `ListAuthSessionsByUsername` con los mismos parámetros. Para ver una lista de sesiones para su posible eliminación, utilice `ListAuthSessionsByUsername` método con el mismo parámetro.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
AuthMethod	Método de autenticación de las sesiones de usuario que se van a eliminar. Sólo un llamante del ClusterAdmins/Administrator AccessGroup puede proporcionar este parámetro. Los valores posibles son: • **AuthMethod=Cluster** especifica el nombre de usuario ClusterAdmin. • **AuthMethod=LDAP** especifica el DN LDAP del usuario. • **AuthMethod=IDP** especifica el UUID de IDP del usuario o NameID. Si el IDP no está configurado para devolver ninguna de las dos opciones, esto especifica un UUID aleatorio emitido al crear la sesión.	AuthMethod	Ninguno	No
nombre de usuario	Identificador único del usuario.	cadena	Ninguno	No

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo

sesiones	Información de la sesión para las sesiones de autenticación eliminadas.	"AuthSessionInfo"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DeleteAuthSessionsByUsername",
  "params": {
    "authMethod": "Cluster",
    "username": "admin"
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"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"
      }
    ]
}
```

Nuevo desde la versión

12.0

DeleteIdpConfiguration

Puede utilizar el `DeleteIdpConfiguration` Método para eliminar una configuración existente de un IDP de terceros para el clúster. Al eliminar la última configuración de IDP, se quita el certificado de proveedor de servicios SAML del clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IdpConfigurationID	UUID para la configuración de IDP de terceros.	UUID	Ninguno	No
IdpName	Nombre utilizado para identificar y recuperar un proveedor de IDP para el inicio de sesión único SAML 2.0.	cadena	Ninguno	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DeleteIdpConfiguration",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
    "idpName": "https://provider.name.url.com"
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "result":{}
}
```

Nuevo desde la versión

12.0

DisableIdpAuthentication

Puede utilizar el `DisableIdpAuthentication` Método para deshabilitar la compatibilidad con la autenticación mediante PDI de terceros para el clúster. Una vez deshabilitada, los usuarios autenticados por PDI de terceros ya no pueden acceder al clúster y todas las sesiones autenticadas activas se invalidan o desconectan. Los administradores de LDAP y clúster pueden acceder al clúster a través de interfaces de usuario compatibles.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DisableIdpAuthentication",
  "params": {}
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"result": {}
}
```

Nuevo desde la versión

12.0

EnableIdpAuthentication

Puede utilizar el `EnableIdpAuthentication` Método para habilitar la compatibilidad con la autenticación mediante PDI de terceros para el clúster. Una vez habilitada la autenticación de IDP, los administradores de LDAP y clúster ya no pueden acceder al clúster a través de IU compatibles y todas las sesiones autenticadas activas quedan invalidadas o desconectadas. Sólo los usuarios autenticados por PDI de terceros pueden acceder al clúster a través de interfaces de usuario admitidas.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IdpConfigurationID	UUID para la configuración de IDP de terceros. Si solo existe una configuración de IDP, la opción predeterminada es habilitar dicha configuración. Si sólo tiene una configuración IdpConfiguration única, no es necesario proporcionar el parámetro idpConfigurationID.	UUID	Ninguno	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "EnableIdpAuthentication",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"result": {}
}
```

Nuevo desde la versión

12.0

GetIdpAuthenticationState

Puede utilizar el `GetIdpAuthenticationState` Método para devolver información sobre el estado de la autenticación mediante PDI de terceros.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
activado	Indica si la autenticación IDP de terceros está habilitada.	booleano

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetIdpAuthenticationState"
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "result": {"enabled": true}
}
```

Nuevo desde la versión

12.0

ListActiveAuthSessions

Puede utilizar el `ListActiveAuthSessions` método para enumerar todas las sesiones autenticadas activas. Sólo los usuarios con derechos de acceso administrativo pueden llamar a este método.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
sesiones	Información de sesión para las sesiones de autenticación.	"AuthSessionInfo"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListActiveAuthSessions"
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"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"
      }
    ]
}
```


Nuevo desde la versión

12.0

ListIdpConfigurations

Puede utilizar el `ListIdpConfigurations` Método para enumerar configuraciones para PDI de terceros. Opcionalmente, puede proporcionar cualquiera de los dos `enabledOnly` Marque para recuperar la configuración de IDP habilitada actualmente o un UUID de metadatos IDP o el nombre IDP para consultar información de una configuración de IDP específica.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
EnabledOnly	Filtra el resultado para devolver la configuración de IDP habilitada actualmente.	booleano	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IdpConfigurationID	UUID para la configuración de IDP de terceros.	UUID	Ninguno	No
IdpName	Recupera la información de configuración de IDP para un nombre de IDP específico.	cadena	Ninguno	No

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
IdpConfigInfos	Información sobre las configuraciones de IDP de terceros.	"IdpConfigInfo" cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListIdpConfigurations",
  "params": {}
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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"
        }
    }
}
```


Nuevo desde la versión

12.0

UpdateIdpConfiguration

Puede utilizar el `UpdateIdpConfiguration` Método para actualizar una configuración existente con un IDP de terceros para el clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
GenerateNewCertificate	Cuando se especifica como TRUE, se genera una clave SAML y un certificado nuevos y reemplaza la pareja existente. Nota: La sustitución del certificado existente interrumpirá la confianza establecida entre el clúster y el IDP hasta que se vuelvan a cargar los metadatos del proveedor de servicios del clúster en el IDP. Si no se proporciona o se establece en FALSE, el certificado y la clave SAML siguen sin cambios.	booleano	Ninguno	No
IdpConfigurationID	UUID para la configuración de IDP de terceros.	UUID	Ninguno	No
IdpMetadata	Metadatos IDP para los detalles de configuración e integración para el inicio de sesión único SAML 2.0.	cadena	Ninguno	No
IdpName	Nombre utilizado para identificar y recuperar un proveedor de IDP para el inicio de sesión único SAML 2.0.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
NewIdpName	Si se especifica, este nombre sustituye el nombre del IDP anterior.	cadena	Ninguno	No

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
IdpConfigInfo	Información sobre la configuración de IDP de terceros.	"IdpConfigInfo"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method": "UpdateIdpConfiguration",
"params": {
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "generateNewCertificate": true
    }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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"
        }
    }
}
```


Nuevo desde la versión

12.0

Métodos API de autenticación de sesión

Es posible usar la autenticación basada en sesiones para gestionar sesiones de usuario.

- ListAuthSessionsByClusterAdmin
- ListAuthSessionsByUsername

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

ListAuthSessionsByClusterAdmin

Puede utilizar el `ListAuthSessionsByClusterAdmin` método para enumerar todas las sesiones de autenticación asociadas con el especificado `ClusterAdminID`. Si se especifica `ClusterAdminID` se asigna a un grupo de usuarios, se enumerarán todas las sesiones de autenticación de todos los miembros de ese grupo.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ClusterAdminID	Identificador único del administrador de clúster.	entero	Ninguno	Sí

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
sesiones	Lista de información de sesión para las sesiones de autenticación.	"AuthSessionInfo"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "ListAuthSessionsByClusterAdmin",
    "clusterAdminID": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"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"
      }
    ]
}
```


Nuevo desde la versión

12.0

ListAuthSessionsByUsername

Puede utilizar el `ListAuthSessionsByUsername` método para mostrar todas las sesiones de autenticación del usuario especificado. Un llamante que no esté en los privilegios de administrador/administradores de clúster de AccessGroup sólo puede enumerar sus propias sesiones. Una persona que llama con privilegios de administrador/administradores de clúster puede mostrar las sesiones que pertenecen a cualquier usuario.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
AuthMethod	Método de autenticación de las sesiones de usuario que se mostrarán en la lista. Sólo un llamante del ClusterAdmins/Administrator AccessGroup puede proporcionar este parámetro. Los valores posibles son: • **AuthMethod=Cluster** especifica el nombre de usuario ClusterAdmin. • **AuthMethod=LDAP** especifica el DN LDAP del usuario. • **AuthMethod=IDP** especifica el UUID de IDP del usuario o NameID. Si el IDP no está configurado para devolver ninguna de las dos opciones, esto especifica un UUID aleatorio emitido al crear la sesión.	AuthMethod	Ninguno	Sí
nombre de usuario	Identificador único del usuario.	cadena	Ninguno	Sí

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo

sesiones	Lista de información de sesión para las sesiones de autenticación.	"AuthSessionInfo"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "ListAuthSessionsByUsername",
    "authMethod": "Cluster",
    "username": "admin"
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"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"
      }
    ]
}
```

Nuevo desde la versión

12.0

Métodos de API de nodo

Puede usar métodos API de nodo para configurar nodos individuales. Estos métodos

funcionan en nodos únicos que se deben configurar, se han configurado pero que aún no participan en un clúster o que participan activamente en un clúster. Los métodos de API de nodos le permiten ver y modificar la configuración de los nodos individuales y la red de clústeres que se usa para comunicarse con el nodo. Debe ejecutar estos métodos en nodos individuales; no puede ejecutar métodos de API por nodo en comparación con la dirección del clúster.

- CheckPingOnVlan
- CheckboedNodeAdditions
- CreateClusterSupportBundle
- CreateSupportBundle
- DeleteAllSupportBundles
- Modo de mantenimiento disableMaintenanceMode
- DisableSsh
- EnableMaintenanceMode
- EnableSsh
- GetClusterConfig
- Estado GetClusterState
- Getconfig
- GetDriveConfig
- GetHardwarConfig
- GetHardwareInfo
- GetIpmiConfig
- GetIpmiInfo
- GetNetworkConfig
- GetNetworkInterface
- GetNodeActiveTlsCiphers
- GetNodeFipsDrivesReport
- GetNodeSSLCertificate
- GetNodeSupportedTlsCiphers
- GetPendingOperation
- GetSshInfo
- ListDrivehardware
- ListNetworkinterfaces
- ListTests
- ListUtilities
- RemoveNodeSSLCertificate
- ResetDrives
- ResetNode

- ResetNodeSupplementalTlsCiphers
- RestartNetworking
- Servicios de RestartServices
- SetClusterConfig
- Config
- SetNetworkConfig
- SetNodeSSLCertificate
- SetNodeSupplementalTlsCiphers
- Apagado
- TestConnectEnsemble
- TestConnectMvip
- TestConnectSvip
- TestDrives
- TestHardwarConfig
- TestLocateCluster
- TestLocalConnectivity
- TestNetworkConfig
- Pruebas de ping
- TestRemoteConnectivity

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

CheckPingOnVlan

Puede utilizar el `CheckPingOnVlan` Método para probar la conectividad de red en una VLAN temporal al realizar la validación de red previa a la implementación. `CheckPingOnVlan` Crea una interfaz de VLAN temporal, envía paquetes ICMP a todos los nodos del clúster de almacenamiento mediante la interfaz de VLAN y, a continuación, elimina la interfaz.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
intentos	Especifica el número de veces que el sistema debe repetir el ping de prueba.	entero	5	No
hosts	Especifica una lista separada por comas de direcciones o nombres de host de dispositivos para hacer ping.	cadena	Los nodos del clúster	No
interfaz	La interfaz existente (base) desde la que se deben enviar los pings. Los posibles valores son los siguientes: • Bond10G: Envíe ping desde la interfaz de Bond10G. • Bond1G: Envíe ping desde la interfaz de Bond1G.	cadena	Ninguno	Sí
Tamaño del paquete	Especifica el número de bytes que se enviarán en el paquete ICMP que se envía a cada IP. El número de bytes debe ser inferior al MTU máximo especificado en la configuración de red.	entero	Ninguno	No
PingTimeoutMsec	Especifica el número de milisegundos que se deben esperar por cada respuesta ping individual.	entero	500 ms	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ProhibiitFragmentación	Activa el indicador DF (no fragment) para los paquetes ICMP.	booleano	falso	No
SourceAddressV4	La dirección IPv4 de origen que se va a usar en los paquetes ping ICMP.	cadena	Ninguno	Sí
SourceAddressV6	La dirección IPv6 de origen que se va a usar en los paquetes ping ICMP.	cadena	Ninguno	Sí
TotalTimeoutSec	Especifica el tiempo en segundos que el ping debe esperar a que se produzca una respuesta del sistema antes de emitir el siguiente intento de ping o de finalizar el proceso.	entero	5	No
VirtualNetworkTag	El identificador de VLAN que se va a utilizar al enviar los paquetes ping.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
detalles	Lista de cada IP con la que el nodo pudo comunicarse y las estadísticas de respuesta ping.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "CheckPingOnVlan",
    "params": {
        "interface": "Bond10G",
        "virtualNetworkTag": 4001,
        "sourceAddressV4": "192.168.41.4",
        "hosts": "192.168.41.2"
},
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "details": {
      "192.168.41.2": {
        "individualResponseCodes": [
          "Success",
          "Success",
          "Success",
          "Success",
          "Success"
        ],
        "individualResponseTimes": [
          "00:00:00.000373",
          "00:00:00.000098",
          "00:00:00.000097",
          "00:00:00.000074",
          "00:00:00.000075"
        ],
        "individualStatus": [
          true,
          true,
          true,
          true,
          true
        ],
        "interface": "Bond10G",
        "responseTime": "00:00:00.000143",
        "sourceAddressV4": "192.168.41.4",
        "successful": true,
        "virtualNetworkTag": 4001
      }
    },
    "duration": "00:00:00.244379",
    "result": "Passed"
  }
}
```


Nuevo desde la versión

11.1

CheckboedNodeAdditions

Puede utilizar el `CheckProposedNodeAdditions` método para probar un conjunto de

nodos de almacenamiento a fin de ver si puede añadirlos a un clúster de almacenamiento sin errores ni violaciones de prácticas recomendadas.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nodos	Una lista de direcciones IP de almacenamiento de nodos de almacenamiento que están listos para añadir a un clúster de almacenamiento.	matriz de cadenas	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
ProposedClusterValid	Indica si los nodos de almacenamiento propuestos componen un clúster de almacenamiento válido o no. Los posibles valores son los siguientes: • verdadero • falso	booleano

ProposedClusterErrors	Errores que se producirían si se creara un clúster de almacenamiento mediante los nodos de almacenamiento propuestos. posibles códigos de error: • `nodesNoCapacity`: Los nodos no tienen ninguna capacidad utilizable. • `nodesTooLarge`: Los nodos constituyen una parte demasiado grande de la capacidad del grupo para el esquema de protección activo. • `nodesConnectFailed`: No se ha podido conectar a los nodos para consultar la configuración de hardware. • `nodesQueryFailed`: No se pudo consultar los nodos para la configuración de hardware. • `nodesClusterMember`: Las direcciones IP de los nodos ya están en uso en el clúster. • `nonFipsNodeCapable`: No se puede agregar un nodo no compatible con FIPS al clúster de almacenamiento mientras la función de cifrado de unidades FIPS 140-2 está habilitada. • `nonFipsDrivesCapable`: No se puede agregar un nodo con unidades no compatibles con FIPS al clúster mientras la función de cifrado de unidades FIPS 140-2 está habilitada.	matriz de cadenas

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "CheckProposedNodeAdditions",
    "params": {
    "nodes": [
        "192.168.1.11",
        "192.168.1.12",
        "192.168.1.13",
        "192.168.1.14"
    ]
},
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "proposedClusterValid": true,
        "proposedClusterErrors": [ ]
    }
}
```

Nuevo desde la versión

11.0

CreateClusterSupportBundle

Puede utilizar el `CreateClusterSupportBundle` en el nodo de gestión para formar paquetes de soporte de todos los nodos de un clúster. Los paquetes de soporte de nodo individual se comprimen como archivos tar.gz. El paquete de soporte del clúster es un archivo tar que contiene los paquetes de soporte del nodo. Solo puede ejecutar este método en un nodo de gestión, no funciona cuando se ejecuta en un nodo de almacenamiento.

Parámetros

Debe llamar a este método contra el nodo de gestión. Por ejemplo:

```
https://<management node IP>:442/json-rpc/10.0
```

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
AllowIncomplete	Permite que el script continúe ejecutándose si los paquetes no se pueden recopilar a partir de uno o más nodos.	booleano	Ninguno	No
Nombre de paquete	Nombre único para cada paquete de soporte creado. Si no se proporciona ningún nombre, "supportBundle" y el nombre de nodo se utilizan como nombre de archivo	cadena	Ninguno	No
mivip	La dirección MVIP del clúster. Los paquetes se agrupan en todos los nodos del clúster. Este parámetro es obligatorio si no se especifica el parámetro Nodes.	cadena	Ninguno	Sí
nodos	Las direcciones IP de los nodos desde los cuales se van a formar paquetes. Use nodos o mvip, pero no ambos, para especificar los nodos a partir de los cuales se van a formar paquetes. Este parámetro es obligatorio si no se especifica mvip.	matriz de cadenas	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
contraseña	La contraseña de administrador del clúster. **Nota:** esta contraseña es visible como texto cuando se introduce.	cadena	Ninguno	Sí
nombre de usuario	El nombre de usuario administrador del clúster.	cadena	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method": "CreateClusterSupportBundle",
"params": {
          "bundlename": "clusterbundle",
          "mvip": "132.119.120.100"
      }
   },
 "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
    }
}
```


Nuevo desde la versión

9.6

CreateSupportBundle

Puede utilizar `CreateSupportBundle` para crear un archivo de bundle de soporte dentro del directorio del nodo. Tras su creación, el paquete se almacena en el nodo como archivo tar (la opción de compresión gz está disponible a través del parámetro extraArgs).

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Nombre de paquete	Nombre único del bundle de soporte. Si no se proporciona ningún nombre, "supportBundle" y el nombre de nodo se utilizan como nombre de archivo.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Extrargs	Utilice '--compress gz' para crear el paquete de soporte como un archivo tar.gz.	cadena	Ninguno	No
TimeoutSec	La cantidad de segundos que se ejecuta el script del bundle de soporte.	entero	1500	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
detalles	Los detalles del bundle de soporte. Los posibles valores son los siguientes: • BundleName: El nombre especificado en el método CreateSupportBundleAPI. Si no se especifica ningún nombre, se utiliza "supportBundle". • ExtraArgs: Los argumentos aprobados con este método. • Files: Una lista de los archivos del bundle de soporte que creó el sistema. • Output: El resultado de la línea de comandos desde el script que creó el bundle de soporte. • TimeoutSec: Cantidad de segundos que se ejecuta la secuencia de comandos del bundle de soporte antes de detenerse. • url: Se creó la URL del bundle de soporte.	Objeto JSON
duración	El tiempo utilizado para crear el bundle de soporte con el formato: HH:MM:SS.ssssss.	cadena

resultado	El éxito o el fallo de la operación del bundle de soporte.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
 "method": "CreateSupportBundle",
"params": {
  "extraArgs": "--compress gz"
 },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"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"
  }
}
```

Nuevo desde la versión

9.6

DeleteAllSupportBundles

Puede utilizar el `DeleteAllSupportBundles` método para eliminar todos los paquetes de soporte generados con la `CreateSupportBundle` Método API.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "DeleteAllSupportBundles",
   "params": {}
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
 }
}
```

Nuevo desde la versión

9.6

Modo de mantenimiento disableMaintenanceMode

Puede utilizar el `DisableMaintenanceMode` método para sacar un nodo de almacenamiento del modo de mantenimiento. Solo debe deshabilitar el modo de mantenimiento después de completar el mantenimiento y el nodo está en línea.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nodos	Lista de ID de nodos de almacenamiento que se van a quitar del modo de mantenimiento.	matriz en números enteros	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
Establish asyncHandle	Puede utilizar el método GetAsyncResult para recuperar este comando establish de la escritura y determinar cuándo se completa la transición del modo de mantenimiento.	entero
Modo CurrentMode	El estado actual del modo de mantenimiento del nodo. Los posibles valores son los siguientes: • Disabled: No se ha solicitado ningún mantenimiento. • FailedToRecover: El nodo no pudo recuperarse del modo de mantenimiento. • Inesperado: Se encontró que el nodo estaba sin conexión, pero estaba en el modo deshabilitado. • RecoveringFromMaintenance: El nodo se está recuperando del modo de mantenimiento. • PreparaciónForMaintenance: Se están llevando a cabo acciones para preparar un nodo para realizar tareas de mantenimiento. • ReadyForMaintenance: El nodo está listo para realizar tareas de mantenimiento.	Modo de mantenimiento (cadena)

Modo requestedMode	El estado del modo de mantenimiento solicitado del nodo. Los posibles valores son los siguientes: • Disabled: No se ha solicitado ningún mantenimiento. • FailedToRecover: El nodo no pudo recuperarse del modo de mantenimiento. • Inesperado: Se encontró que el nodo estaba sin conexión, pero estaba en el modo deshabilitado. • RecoveringFromMaintenance: El nodo se está recuperando del modo de mantenimiento. • PreparaciónForMaintenance: Se están llevando a cabo acciones para preparar un nodo para realizar tareas de mantenimiento. • ReadyForMaintenance: El nodo está listo para realizar tareas de mantenimiento.	Modo de mantenimiento (cadena)

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DisableMaintenanceMode",
  "params": {
    "nodes": [6]
  },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
      {
        "requestedMode": "Disabled",
        "asyncHandle": 1,
        "currentMode": "Enabled"
     }
}
```

Nuevo desde la versión

12.2

Obtenga más información

"Conceptos del modo de mantenimiento del almacenamiento de NetApp HCI"

DisableSsh

Puede utilizar el `DisableSsh` Método para deshabilitar el servicio SSH para un solo nodo de almacenamiento. Este método no afecta la duración del tiempo de espera del servicio SSH para todo el clúster.

Parámetro

Este método no tiene parámetro de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
activado	El estado del servicio SSH de este nodo.	booleano

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DisableSsh",
  "params": {
      },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {"enabled": false}
}
```

EnableMaintenanceMode

Puede utilizar el `EnableMaintenanceMode` método para preparar un nodo de almacenamiento para el mantenimiento. Los escenarios de mantenimiento incluyen cualquier tarea que requiera que el nodo se apague o se reinicie.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ForceWithUnresolvedFaults	Fuerce el modo de mantenimiento para habilitar para este nodo incluso con fallos de clúster de bloqueo presentes.	booleano	Falso	No
nodos	La lista de ID de nodo que se van a poner en modo de mantenimiento. Solo se admite un nodo cada vez.	matriz en números enteros	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
PerMinutePrimarySwapLimit	El número de cortes principales que se van a intercambiar por minuto. Si no se especifica, todos los cortes primarios se intercambiarán a la vez.	entero	Ninguno	No
tiempo de espera	Especifica cuánto tiempo debe permanecer activado el modo de mantenimiento antes de que se desactive automáticamente. Con formato de cadena de tiempo (por ejemplo, HH:mm:ss). Si no se especifica, el modo de mantenimiento permanecerá habilitado hasta que se deshabilite explícitamente.	cadena	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
Establish asyncHandle	Puede utilizar el método GetAsyncResult para recuperar este comando establish de la escritura y determinar cuándo se completa la transición del modo de mantenimiento.	entero

Modo CurrentMode	El estado actual del modo de mantenimiento del nodo. Los posibles valores son los siguientes: • Disabled: No se ha solicitado ningún mantenimiento. • FailedToRecover: El nodo no pudo recuperarse del modo de mantenimiento. • RecoveringFromMaintenance: El nodo se está recuperando del modo de mantenimiento. • PreparaciónForMaintenance: Se están llevando a cabo acciones para preparar un nodo para realizar tareas de mantenimiento. • ReadyForMaintenance: El nodo está listo para realizar tareas de mantenimiento.	Modo de mantenimiento (cadena)
Modo requestedMode	El estado del modo de mantenimiento solicitado del nodo. Los posibles valores son los siguientes: • Disabled: No se ha solicitado ningún mantenimiento. • FailedToRecover: El nodo no pudo recuperarse del modo de mantenimiento. • RecoveringFromMaintenance: El nodo se está recuperando del modo de mantenimiento. • PreparaciónForMaintenance: Se están llevando a cabo acciones para preparar un nodo para realizar tareas de mantenimiento. • ReadyForMaintenance: El nodo está listo para realizar tareas de mantenimiento.	Modo de mantenimiento (cadena)

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "EnableMaintenanceMode",
  "params": {
    "forceWithUnresolvedFaults": False,
    "nodes": [6],
    "perMinutePrimarySwapLimit" : 40,
    "timeout" : "01:00:05"
  },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
      {
        "requestedMode": "ReadyForMaintenance",
        "asyncHandle": 1,
        "currentMode": "Disabled"
     }
}
```

Nuevo desde la versión

12.2

Obtenga más información

"Conceptos del modo de mantenimiento del almacenamiento de NetApp HCI"

EnableSsh

Puede utilizar el `EnableSsh` Método para habilitar el servicio Secure Shell (SSH) para un solo nodo. Este método no afecta a la duración del tiempo de espera de SSH para todo el clúster y no exime al nodo de que SSH esté deshabilitado por el tiempo de espera global de SSH.

Parámetro

Este método no tiene parámetro de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
activado	El estado del servicio SSH de este nodo.	booleano

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "EnableSsh",
  "params": {
     },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {"enabled": true}
}
```

GetClusterConfig

Puede utilizar el `GetClusterConfig` Método API para obtener información acerca de la configuración de clúster que el nodo utiliza para comunicarse con su clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
clúster	Información de configuración de clúster que el nodo utiliza para comunicarse con el clúster.	clúster

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetClusterConfig",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
    }
  }
}
```

Nuevo desde la versión

9.6

Estado GetClusterState

Puede utilizar el `GetClusterState` Método API para indicar si un nodo forma parte de un clúster o no.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
clúster	El nombre del clúster.	cadena
estado	• Available: No se configuró el nodo con un nombre de clúster. • Pending: Nodo está pendiente para un clúster con nombre específico y se puede añadir. • Active: El nodo es un miembro activo de un clúster y es posible que no se pueda añadir a otro clúster.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetClusterState",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id" : 1,
   "result" :
      "cluster" :  "Cluster101"
      "state" : "Active"
}
```

Nuevo desde la versión

9.6

Getconfig

Puede utilizar el `GetConfig` Método API para obtener toda la información de configuración de un nodo. Este método API incluye la misma información disponible en ambos `GetClusterConfig` y.. `GetNetworkConfig` Métodos de API.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
gestión de	Los detalles de configuración del clúster. Este objeto contiene: • clúster: Información del clúster que identifica cómo se comunica el nodo de almacenamiento con el clúster de almacenamiento al que está asociado. • red (todas las interfaces): Tipos de conexión de red y configuración actual para cada interfaz de red del nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetConfig",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Debido a la longitud de este ejemplo de respuesta, se documenta en un tema complementario.

Nuevo desde la versión

9.6

Obtenga más información

- GetClusterConfig
- GetNetworkConfig
- Getconfig

GetDriveConfig

Puede utilizar el `GetDriveConfig` método para obtener información de la unidad para los números de unidades de bloques y segmentos esperados, así como el número de unidades de bloque y segmentos conectados actualmente al nodo.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
DriveConfig	La información de las unidades que están conectadas al nodo.	unidad

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetDriveConfig",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Las respuestas para este método son similares al ejemplo siguiente. Debido al tamaño, la respuesta contiene información de una unidad de un solo nodo de almacenamiento.

```
{
    "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
            }
    }
}
```

GetHardwarConfig

Puede utilizar el `GetHardwareConfig` método para obtener la información de configuración de hardware para un nodo. Estos datos de configuración están destinados al uso interno. Para obtener un inventario más útil de componentes de hardware del sistema en tiempo real, utilice `GetHardwareInfo` en su lugar, el método.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
HardwareConfig	Lista de información de hardware y configuración actual.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetHardwareConfig",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Las respuestas para este método son similares al ejemplo siguiente.

```
{
    "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
            }
        }
    }
}
```


Nuevo desde la versión

9.6

GetHardwareInfo

Puede utilizar el `GetHardwareInfo` método para obtener información y estado del hardware activo de un único nodo. La información de hardware suele incluir a los fabricantes, proveedores, versiones, unidades y otra información de identificación asociada.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
fuerza	Establezca este parámetro «force» en TRUE para que se ejecute en todos los nodos del clúster.	booleano	falso	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
HardwareInfo	Información de hardware para el nodo.	HardwareInfo

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetHardwareInfo",
   "params": {
   },
"id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
        },
      ...
      ]
    }
  }
}
```


Nuevo desde la versión

9.6

GetIpmiConfig

Puede utilizar el `GetIpmiConfig` método para recuperar información del sensor de hardware de sensores que están en su nodo.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo
ChassisType	Se utiliza para mostrar información sobre cada tipo de chasis del nodo. Los posibles valores son los siguientes: • all: devuelve información del sensor para cada tipo de chasis. • {chassis type}: devuelve la información del sensor de un tipo de chasis especificado.	cadena

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
SensorName	Nombre del sensor que se ha encontrado.	cadena
UniqueSensorID	Identificador único del sensor.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetIpmiConfig",
  "params": {
     "chassisType"; "all"
     },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
 "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"
                }
            ],
        }
```

Nuevo desde la versión

9.6

GetIpmiInfo

Puede utilizar el `GetIpmiInfo` método para mostrar un informe detallado de los sensores (objetos) de los ventiladores de los nodos, las temperaturas de admisión y escape y las fuentes de alimentación que supervisa el sistema.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
sensores	Información detallada de cada sensor dentro de un nodo.	Cabina de objetos JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetIpmiInfo",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Debido a la duración de la respuesta devuelta para este método API, partes de la respuesta han sido eliminadas intencionalmente de este documento. Lo que se incluye son las partes de la información de hardware que supervisa el sistema para garantizar que el nodo se ejecute con un rendimiento óptimo.

```
{
  "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"
            },
              .
              .
              .
            }
          ]
        }
      }
    }
```


Nuevo desde la versión

9.6

GetNetworkConfig

Puede utilizar el `GetNetworkConfig` método para mostrar la información de configuración de red de un nodo.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
red	Los tipos de conexión de red y la configuración actual de cada interfaz de red del nodo.	red (todas las interfaces)

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetNetworkConfig",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Debido a la longitud de este ejemplo de respuesta, se documenta en un tema complementario.

Nuevo desde la versión

9.6

Obtenga más información

GetNetworkConfig

GetNetworkInterface

Puede utilizar el `GetNetworkInterface` método para obtener información sobre una interfaz de red en un nodo.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
interfaz	El nombre de la interfaz para obtener información acerca de cada nodo. Los posibles valores son los siguientes: • Bond1G • Bond10G	cadena	Ninguno	No
fuerza	Establezca este parámetro en TRUE para ejecutarse en todos los nodos del clúster.	booleano	falso	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
nodos	Una cabina de objetos que describen la interfaz para cada nodo de almacenamiento del clúster de almacenamiento. Cada objeto dentro de la matriz contiene los siguientes elementos: • NodeID: (Entero) el ID del nodo de almacenamiento en el clúster de almacenamiento al que se aplica la información de la interfaz. • resultado: (NetworkInterface) Información de configuración de la interfaz para este nodo de almacenamiento.	Cabina de objetos JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "GetNetworkInterface",
    "params": {
        "interface": "Bond1G",
        "force": true
        },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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
                }
            }
        }
    ]
}
```

```
}
```

Nuevo desde la versión

9.6

GetNodeActiveTlsCiphers

Puede utilizar el `GetNodeActiveTlsCiphers` Método en un solo nodo para obtener una lista de los cifrados TLS que se han aceptado actualmente en este nodo. Puede usar este método para los nodos de almacenamiento y de gestión.

Parámetro

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
MandatoryCiphers	Lista de conjuntos de cifrado TLS obligatorios para el nodo. Estos son cifrados que siempre están activos en el nodo.	cadena
SupplesCiphers	Lista de conjuntos de cifrado TLS complementarios para el nodo.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetNodeActiveTlsCiphers",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
      "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

Puede utilizar el `GetNodeFipsDrivesReport` Método para comprobar el estado de la funcionalidad de cifrado de unidades FIPS 140-2 de un solo nodo en el clúster de almacenamiento. Se debe ejecutar este método contra un nodo de almacenamiento individual.

Parámetro

Este método no tiene parámetro de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
PsDrives	Un objeto JSON que contiene el estado de la compatibilidad con la función FIPS 140-2 para este nodo. Los posibles valores son los siguientes: • None: El nodo no es compatible con FIPS. • Parcial: El nodo es compatible con FIPS, pero no todas las unidades del nodo son unidades FIPS. • Ready: El nodo es compatible con FIPS y todas las unidades del nodo son unidades FIPS (o no existen unidades).	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetNodeFipsDrivesReport",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "fipsDrives": "None"
    }
}
```

Nuevo desde la versión

11.5

GetNodeSSLCertificate

Puede utilizar el `GetNodeSSLCertificate` Método para recuperar el certificado SSL

que está activo actualmente en el nodo de gestión.

Parámetros

Debe llamar a este método contra el nodo de gestión. Por ejemplo:

```
https://<management node IP>:442/json-rpc/10.0
```

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
certificado	El texto completo codificado con PEM del certificado.	cadena
detalles	La información descodificada del certificado.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method" : "GetNodeSSLCertificate",
    "params" : {},
    "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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

Puede utilizar el `GetNodeSupportedTlsCiphers` Método en un solo nodo para obtener una lista de los cifrados TLS que actualmente son compatibles con este nodo. Puede usar este método para los nodos de almacenamiento y de gestión.

Parámetro

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
MandatoryCiphers	Lista de conjuntos de cifrado TLS obligatorios para el nodo. Estos son cifrados que siempre están activos en el nodo.	cadena
DefaultSupplementalCiphers	Lista de conjuntos de cifrado TLS suplementarios predeterminados para el nodo. Los cifrados complementarios se restauran en esta lista cuando se ejecuta el método API ResetNodeSupplementalTlsCiphers.	cadena
SoportedSupplementalCiphers	Lista de conjuntos de cifrado TLS complementarios disponibles que puede configurar con el método API SetNodeSupplementTlsCiphers.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetNodeSupportedTlsCiphers",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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

Puede utilizar el `GetPatchInfo` Método para obtener información sobre las revisiones del software Element instaladas en un nodo de almacenamiento.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`force`	Fuerce el método para que se ejecute en todos los nodos del clúster de almacenamiento. Solo se necesita esto cuando emita la API a una dirección IP de clúster en lugar de a un solo nodo. Los posibles valores son los siguientes: • `true` • `false`	booleano	`false`	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
parches	Objeto que contiene información acerca de las revisiones instaladas en este nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetPatchInfo",
   "params": {
      "force": false,
      },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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"
          ]
          }
        }
    }
}
```

Nuevo desde la versión

12.3

GetPendingOperation

Puede utilizar el `GetPendingOperation` método para detectar una operación en un nodo que se encuentra actualmente en curso. Este método también se puede utilizar para informar cuando se ha completado una operación.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
pendiente	Los posibles valores son los siguientes: • True: La operación sigue en curso. • falso: La operación ya no está en curso.	booleano
funcionamiento	Nombre de la operación que está en curso o que se ha completado.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetPendingOperation",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id" : 1,
   "result" : {
      "pendingOperation" : {
         "pending" : "true",
         "operation" : "TestDrivesInternal",
      }
   }
}
```

Nuevo desde la versión

9.6

GetSshInfo

Puede utilizar el `GetSshInfo` Método para consultar el estado del servicio SSH en un

solo nodo.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
resultado	El estado del servicio SSH de este nodo.	booleano

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method" : "GetSshInfo",
    "params" : {},
    "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "enabled": false
    }
}
```

ListDrivehardware

Puede utilizar el `ListDriveHardware` método para enumerar todas las unidades conectadas a un nodo. Cuando se usa en nodos individuales, este método muestra información de hardware de la unidad. Cuando se utiliza en la MVIP del nodo maestro de clúster, este método muestra información de todas las unidades de todos los nodos.

Parámetros

"SecuritySupported": La línea verdadera de la respuesta del método no implica que las unidades sean capaces de cifrar; solo que se pueda consultar el estado de seguridad. Si tiene un tipo de nodo con un número de modelo que finaliza en "-NE", se producirá un error en los comandos para habilitar las funciones de seguridad en estas unidades.

Este método tiene el siguiente parámetro:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
fuerza	Establezca esta opción en true para ejecutar este método en todos los nodos.	booleano	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Drivehardware	Se devolvió información de hardware de la unidad para el nodo.	Cabina de objetos JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method": "ListDriveHardware",
"params": {},
"id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
      }
    ]
}
```


Nuevo desde la versión

9.6

Obtenga más información

EnableEncryptionAtest

ListNetworkinterfaces

Puede utilizar el `ListNetworkInterfaces` método para enumerar la información de cada interfaz de red en un nodo. Este método de API está pensado para usar en nodos individuales; se necesitan ID de usuario y autenticación de contraseña para acceder a nodos individuales. Sin embargo, puede usar este método en el clúster si se da el valor TRUE al parámetro force en la llamada al método. Cuando se utiliza el parámetro en el clúster, se muestran todas las interfaces.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
fuerza	Los posibles valores son los siguientes: • True: Se muestra información sobre todas las interfaces de red del clúster. • Falso: No se devuelve información.	booleano	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
interfaces	Una lista de información de configuración para cada interfaz de red del nodo de almacenamiento (o de todo el clúster de almacenamiento, si se fuerza = `true`).	NetworkInterface cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method": "ListNetworkInterfaces",
"params": {},
"id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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
                        }
                    ]
                }
            }
        ]
    }
}
```


Nuevo desde la versión

9.6

ListNetworkInterfaceStats

Puede utilizar el `ListNetworkInterfaceStats` método para enumerar estadísticas como el número de paquetes descartados y varios tipos de errores para cada interfaz de red en un nodo. Este método de API está pensado para usar en nodos individuales; se necesitan ID de usuario y autenticación de contraseña para acceder a nodos individuales. Sin embargo, puede usar este método en el clúster si se da el valor TRUE al parámetro force en la llamada al método. Cuando se utiliza el parámetro en el clúster, se muestran las estadísticas de red de todas las interfaces.

Parámetro

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
NetworkInterfaceStats	Una lista de información de estadísticas de red, como el número de paquetes eliminados y diversos tipos de errores de red, para cada interfaz de red de un nodo de almacenamiento.	NetworkInterfaceStats cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method": "ListNetworkInterfaceStats",
"params": {},
"id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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
        }
    ]
}
```


Nuevo desde la versión

12.3

ListTests

Puede utilizar el `ListTests` método para enumerar las pruebas que están disponibles para ejecutarse en un nodo.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
pruebas	Lista de pruebas que se pueden realizar en el nodo.	matriz de cadenas

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListTests",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
   "tests": [
             "TestConnectEnsemble",
             "TestConnectMvip",
             "TestConnectSvip",
             "TestDrives",
             "TestHardwareConfig",
             "TestLocateCluster",
             "TestPing",
             "TestLocalConnectivity",
             "TestRemoteConnectivity",
             "TestNetworkConfig"
           ]
      }
}
```

Nuevo desde la versión

9.6

ListUtilities

Puede utilizar el `ListUtilities` método para enumerar las operaciones que están disponibles para ejecutarse en un nodo.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
servicios públicos	Lista de utilidades disponibles actualmente para ejecutarse en el nodo.	matriz de cadenas

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListUtilities",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "utilities": [
      "ResetDrives",
      "ResetNode",
      "RestartNetworking",
      "RestartServices",
      "CreateSupportBundle",
      "DeleteAllSupportBundles",
      "CreateClusterSupportBundle"
    ]
  }
}
```

Nuevo desde la versión

9.6

RemoveNodeSSLCertificate

Puede utilizar el `RemoveNodeSSLCertificate` Método para quitar el certificado SSL

de usuario y la clave privada para el nodo de gestión. Después de eliminar el certificado y la clave privada, el nodo de gestión se configura para usar el certificado y la clave privada predeterminados.

Parámetros

Debe llamar a este método contra el nodo de gestión. Por ejemplo:

```
https://<management node IP>:442/json-rpc/10.0
```

Este método no tiene parámetros de entrada.

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method" : "RemoveNodeSSLCertificate",
    "params" : {},
    "id" : 3
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id" : 3,
    "result" : {}
}
```

ResetDrives

Puede utilizar el `ResetDrives` método para inicializar unidades de forma proactiva y quitar todos los datos que residen actualmente en una unidad. La unidad se puede volver a usar en un nodo existente o se puede usar en un nodo actualizado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
unidades	Lista de nombres de dispositivos (no identificadores de unidades) que se van a restablecer.	cadena	Ninguno	Sí
fuerza	Configure en TRUE para restablecer la unidad.	booleano	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
detalles	Detalles de las unidades que se están restableciendo.	Cabina de objetos JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ResetDrives",
   "params": {
      "drives" : "slot3",
      "force" : true
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
  }
}
```


Nuevo desde la versión

9.6

ResetNode

Puede utilizar el `ResetNode` método para restablecer un nodo a la configuración de fábrica. Cuando llama a este método, se eliminan todos los datos, paquetes (actualizaciones de software, etc.), configuraciones y archivos de registro del nodo. Sin embargo, la configuración de red del nodo se conserva durante esta operación. Los nodos que participan en un clúster no se pueden restablecer a la configuración de fábrica.

Parámetros

La API ResetNode sólo se puede utilizar en los nodos en estado "disponible". No se puede usar en los nodos que están "activos" en un clúster ni en el estado "Pending".

PRECAUCIÓN:

Este método borra todos los datos de clientes que están en el nodo.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
cree	Se utiliza para especificar la dirección URL de una imagen de software de elemento remoto a la que se restablecerá el nodo.	URL	Ninguno	No
fuerza	Establezca esta opción en true para restablecer el nodo.	booleano	Ninguno	Sí
opciones	Se utiliza para introducir especificaciones para ejecutar las operaciones de restablecimiento. El soporte de NetApp puede proporcionar detalles si es necesario.	Objeto JSON	Ninguno	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ResetNode",
   "params": {
      "build" : "file:///sf/rtfi/image/filesystem.squashfs",
      "force" : true
              },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
```

```
    }
  }
}
```

Nuevo desde la versión

9.6

ResetNodeSupplementalTlsCiphers

Puede utilizar el `ResetNodeSupplementalTlsCiphers` Método para restaurar la lista de cifrados adicionales TLS al valor predeterminado. Este comando se puede usar en nodos de gestión.

Parámetro

Debe llamar a este método contra el nodo de gestión. Por ejemplo:

```
https://<management node IP>:442/json-rpc/10.0
```

Este método no tiene parámetros de entrada.

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ResetNodeSupplementalTlsCiphers",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

RestartNetworking

Puede utilizar el `RestartNetworking` método para reiniciar los servicios de red en un nodo.

PRECAUCIÓN:

Este método reinicia todos los servicios de red en un nodo, lo que produce una pérdida temporal de conectividad de red.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
fuerza	Establezca esta opción en true para reiniciar los servicios de red en un nodo.	booleano	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "RestartNetworking",
   "params": {
              "force" : true
             },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{ "id" : 1,
  "result" : {}
}
```

Nuevo desde la versión

9.6

Servicios de RestartServices

Puede utilizar el `RestartServices` método para reiniciar los servicios en un nodo.

Parámetros

PRECAUCIÓN:

Este método provoca una interrupción temporal de los servicios de los nodos.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
fuerza	Establezca esta opción en true para reiniciar los servicios en un nodo.	booleano	Ninguno	Sí
servicio	Nombre del servicio que se va a reiniciar.	cadena	Ninguno	No
acción	Acción que se debe realizar en el servicio (inicio, parada, reinicio).	cadena	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
detalles	El resultado del procedimiento de reinicio del servicio, incluidos los errores (si los hay).	Objeto JSON
duración	El tiempo, en segundos, se tardó en reiniciar los servicios al nodo.	cadena
resultado	Resultados del reinicio.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "RestartServices",
   "params": {
              "force" : true
              "action" : restart,
             }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "details": "solidfire stop/waiting\nsolidfire start/running, process
7284\n",
    "duration": "00:00:02.541594",
    "result": "Passed"
  }
}
```

Nuevo desde la versión

9.6

SetClusterConfig

Puede utilizar el `SetClusterConfig` método para establecer la configuración que un nodo utiliza para comunicarse con el clúster con el que está asociado. Para mostrar la configuración de interfaz del clúster actual de un nodo, ejecute el `GetClusterConfig` Método API.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
clúster	Atributos de configuración que deben cambiarse durante esta llamada de método. Sólo es necesario agregar a este método los campos que desee modificar como miembros de este parámetro.	clúster	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
clúster	Información de configuración que el nodo utiliza para comunicarse con el clúster.	clúster

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "SetClusterConfig",
   "params": {
      "cluster": {
         "name": "myhost",
         "mipi": "Bond10G"
      },
    "id" : 1
   }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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"
      }
   }
}
```

Nuevo desde la versión

9.6

Config

Puede utilizar el `SetConfig` método para establecer la información de red y clúster del nodo. Este método incluye la misma configuración en un único método API que está disponible mediante ambos `SetClusterConfig` y.. `SetNetworkConfig` métodos. Sólo es necesario incluir con este método los campos que desee modificar.

Parámetro

PRECAUCIÓN:

Si se cambia el modo de enlace en un nodo, se puede producir una pérdida temporal de conectividad de red.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
clúster	Información de clúster que identifica la forma en que el nodo de almacenamiento se comunica con el clúster de almacenamiento con el que está asociado.	clúster	Ninguno	No
red	Los tipos de conexión de red y la configuración actual de cada interfaz de red del nodo.	red (todas las interfaces)	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
gestión de	La configuración nueva y actual del nodo. Este objeto contiene: • clúster: Información del clúster que identifica cómo se comunica el nodo de almacenamiento con el clúster de almacenamiento al que está asociado. • red (todas las interfaces): Tipos de conexión de red y configuración actual para cada interfaz de red del nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "SetConfig",
    "params": {
        "cluster": {
            "name": "MyHostname"
        },
        "network": {
            "Bond10G": {
                "bond-mode": "ALB"
            }
        }
    }
}
```

Ejemplo de respuesta

La respuesta de este método es la misma que la del método getconfig. Todos los campos del objeto se muestran y se actualizan los valores cuando se utiliza SetConfig.

Nuevo desde la versión

9.6

Obtenga más información

- SetClusterConfig
- SetNetworkConfig
- Getconfig

SetNetworkConfig

Puede utilizar el `SetNetworkConfig` método para establecer la configuración de red para un nodo. Para mostrar la configuración de red actual de un nodo, ejecute el `GetNetworkConfig` Método API.

Parámetro

PRECAUCIÓN:

Si se cambia el modo de enlace en un nodo, se puede producir una pérdida temporal de conectividad de red.

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
red	Un objeto que contiene la configuración de red de los nodos que se va a modificar. Sólo tiene que agregar los campos que desea cambiar a este método como atributos en este parámetro.	red (todas las interfaces)	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
red	La configuración de red nueva y actual del nodo.	red (todas las interfaces)

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "SetNetworkConfig",
        "params": {
            "network": {
                "Bond10G": {
                    "bond-mode": "ALB"
                },
                "Bond1G": {
                    "netmask": "255.255.224.0"
                },
                "eth0": {
                    "method": "bond"
                },
                "lo": {
                    "method": "loopback"
                }
            }
        }
}
```

Ejemplo de respuesta

La respuesta de este método es la misma que la del método GetNetworkConfig . El método muestra todos los miembros de cada objeto e incluye los nuevos valores para los miembros modificados.

Nuevo desde la versión

9.6

Obtenga más información

- GetNetworkConfig
- GetNetworkConfig

SetNodeSSLCertificate

Puede utilizar el `SetNodeSSLCertificate` Método para establecer un certificado SSL de usuario y una clave privada para el nodo de gestión.

Después de usar la API, debe reiniciar el nodo de gestión.

Parámetros

Debe llamar a este método contra el nodo de gestión. Por ejemplo:

```
https://<management node IP>:442/json-rpc/10.0
```

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
certificado	Versión de texto codificado con PEM del certificado.**Nota:** cuando se establece un certificado de nodo o clúster, el certificado debe incluir la extensión extendedKeyUsage para serverAuth. Esta extensión permite utilizar el certificado sin errores en los sistemas operativos y exploradores comunes. Si la extensión no está presente, la API rechazará el certificado como no válido.	cadena	Ninguno	Sí
Privatekey	La versión de texto codificada con PEM de la clave privada.	cadena	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "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
}
```


Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id" : 2,
    "result" : {}
}
```

SetNodeSupplementalTlsCiphers

Puede utilizar el `SetNodeSupplementalTlsCiphers` Método para especificar la lista de cifrados TLS suplementarios. Este comando se puede usar en nodos de gestión.

Parámetro

Debe llamar a este método contra el nodo de gestión. Por ejemplo:

```
https://<management node IP>:442/json-rpc/10.0
```

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SupplesCiphers	Los nombres suplementarios de las suites de cifrado utilizando el esquema de nomenclatura OpenSSL. El uso de nombres de paquete cifrado no distingue mayúsculas y minúsculas.	cadena	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
MandatoryCiphers	Lista de conjuntos de cifrado TLS obligatorios para el nodo. Estos son cifrados que siempre están activos en el nodo.	cadena
SupplesCiphers	Lista de conjuntos de cifrado TLS complementarios para el nodo.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "SetNodeSupplementalTlsCiphers",
   "params": {
        "supplementalCiphers": [
            "DHE-RSA-AES128-SHA256",
            "DHE-RSA-AES128-GCM-SHA256",
            "ECDHE-RSA-AES128-SHA256",
            "ECDHE-RSA-AES128-GCM-SHA256"
        ]
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
        ]
    }
}
```

Apagado

Puede utilizar el `Shutdown` método para reiniciar o apagar los nodos de un clúster. Puede apagar un único nodo, varios nodos o todos los nodos del clúster mediante este método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nodos	Lista de NodeIDs para los nodos que se van a reiniciar o apagar.	matriz en números enteros	Ninguno	Sí
opción	Acción que se debe realizar para el clúster. Valores posibles: * Restart: Reinicia el clúster. * Detener: Realiza un apagado completo.	cadena	reiniciar	No

Valor de retorno

Este método no tiene ningún valor devuelto. == las solicitudes de ejemplo para este método son similares al ejemplo siguiente:

```
{
   "method": "Shutdown",
   "params": {
     "nodes": [
       2,
       3,
       4
     ],
     "option": "halt"
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {
     "failed": [],
     "successful": [
          6
      [
   }
}
```

Nuevo desde la versión

9.6

TestConnectEnsemble

Puede utilizar el `TestConnectEnsemble` método para verificar la conectividad con un conjunto de bases de datos especificado. De forma predeterminada, utiliza el conjunto para el clúster con el que está asociado el nodo. Como alternativa, puede proporcionar un conjunto diferente para probar la conectividad.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
conjunto	Una lista separada por comas de direcciones IP de clúster de nodos del conjunto para realizar las pruebas de conectividad.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
detalles	Objetos devueltos: • `nodes`: (Objeto) una lista de cada nodo del conjunto en la prueba y los resultados de las pruebas. • `duration`: (Cadena) el tiempo necesario para ejecutar la prueba. • `result`: (Cadena) los resultados de la prueba completa.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "TestConnectEnsemble",
  "params": {},
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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"
   }
}
```

Nuevo desde la versión

9.6

TestConnectMvip

Puede utilizar el `TestConnectMvip` método para probar la conexión de gestión con el clúster de almacenamiento. La prueba hace ping en la dirección MVIP y ejecuta un método API sencillo para verificar la conectividad.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
mivip	Es posible pasar este valor para probar la conexión de gestión de una MVIP diferente. No es necesario utilizar este valor cuando se prueba la conexión con el clúster de destino.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
detalles	Información acerca de la operación de prueba (objeto JSON): • `connected`: Indica si la prueba podría conectarse a la MVIP (booleano) • `mvip`: La MVIP probada en (cadena) • `pingBytes`: Detalles de las pruebas ping con 56 bytes y 1500 bytes (objeto) ◦ `56`: Resultados de la prueba ping de 56 bytes (objeto JSON): ▪ `individualResponseTimes`: Lista de tiempos de respuesta de cada nodo del conjunto (matriz de cadenas) ▪ `individualStatus`: Lista del estado de ping de cada nodo del conjunto (matriz booleana) ▪ `responseTime`: Tiempo medio de respuesta de ping (cadena) ▪ `successful`: Indica si la prueba ping se realizó correctamente (booleano). ◦ `1500`: Resultados de la prueba ping de 1500 bytes (objeto JSON): ▪ `individualResponseTimes`: Lista de tiempos de respuesta de cada nodo del conjunto (matriz de cadenas) ▪ `individualStatus`: Lista del estado de ping de cada nodo del conjunto (matriz booleana) `responseTime`: Tiempo medio de respuesta de ping	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "TestConnectMvip",
   "params": {
       "mvip" : "172.27.62.50"
       },
    "id":1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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",
```

- (cadena)
- successful: Si la prueba en su conjunto (cadena)

```
            "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"
  }
}
```


Nuevo desde la versión

9.6

TestConnectSvip

Puede utilizar el `TestConnectSvip` método para probar la conexión de almacenamiento con el clúster de almacenamiento. La prueba hace ping en la dirección SVIP mediante paquetes ICMP y, cuando se realiza correctamente, se conecta como un iniciador iSCSI.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
svip	Puede pasar este valor para probar la conexión de gestión de una SVIP diferente. No es necesario utilizar este valor cuando se prueba la conexión con el clúster de destino.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
detalles	Información acerca de la operación de prueba (objeto JSON): • `connected`: Indica si la prueba podría conectarse a la SVIP (booleano) • `svip`: El SVIP probado contra (cadena) • `pingBytes`: Detalles de las pruebas ping con 56 bytes y 9000 bytes (objeto) ◦ `56`: Resultados de la prueba ping de 56 bytes (objeto JSON): ▪ `individualResponseTimes`: Lista de tiempos de respuesta de cada nodo del conjunto (matriz de cadenas) ▪ `individualStatus`: Lista del estado de ping de cada nodo del conjunto (matriz booleana) ▪ `responseTime`: Tiempo medio de respuesta de ping (cadena) ▪ `successful`: Indica si la prueba ping se realizó correctamente (booleano). ◦ `9000`: Resultados de la prueba ping de 9000 bytes (objeto JSON): ▪ `individualResponseTimes`: Lista de tiempos de respuesta de cada nodo del conjunto (matriz de cadenas) ▪ `individualStatus`: Lista del estado de ping de cada nodo del conjunto (matriz booleana) `responseTime`: Tiempo medio de respuesta de ping	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "TestConnectSvip",
   "params": {
      "svip" : "172.27.62.50"
      },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "details": {
      "connected": true,
      "pingBytes": {
           "56": {
               "individualResponseTimes": [
                   "00:00:00.000152",
                   "00:00:00.000132",
                   "00:00:00.000119",
                   "00:00:00.000114",
                   "00:00:00.000112"
              ],
              "individualStatus": [
                  true,
                  true,
                  true,
                  true,
                  true
              ],
              "responseTime": "00:00:00.000126",
              "successful": true
           },
          "9000": {
                "individualResponseTimes": [
                    "00:00:00.000295",
                    "00:00:00.000257",
                    "00:00:00.000172",
                    "00:00:00.000172",
```

```
                    "00:00:00.000267"
                ],
                "individualStatus": [
                    true,
                    true,
                    true,
                    true,
                    true
                ],
                "responseTime": "00:00:00.000233",
                "successful": true
            }
          },
          "svip": "172.27.62.50"
        },
        "duration": "00:00:00.421907",
        "result": "Passed"
    }
}
```


Nuevo desde la versión

9.6

TestDrives

Puede utilizar el `TestDrives` método para ejecutar una validación de hardware en todas las unidades del nodo. Este método detecta fallos de hardware en las unidades e informa de cualquiera de los resultados de las pruebas de validación.

Parámetros

Sólo puede utilizar el `TestDrives` Método en nodos que no están "activos" en un clúster.

Esta prueba dura aproximadamente 10 minutos.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
fuerza	Establezca esta opción en true para probar las unidades en el nodo.	booleano	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
minutos	Especifica la cantidad de minutos para que se ejecute la prueba.	entero	10	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
detalles	Información sobre el éxito o el fallo de la operación de prueba.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "TestDrives",
   "params": {
               "force": true,
               "minutes" : 10
              },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una tabla con los resultados de prueba de cada unidad del nodo.

Nuevo desde la versión

9.6

TestHardwarConfig

Puede utilizar el `TestHardwareConfig` método para realizar pruebas de hardware en un nodo. Las opciones de prueba incluyen verificar las configuraciones de hardware, las versiones de firmware y la presencia de todas las unidades.

Parámetros

Esta prueba no se realiza con la intención de detectar fallos de hardware.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
limpio	Inicia la prueba de configuración de hardware con una caché limpia. Los posibles valores son los siguientes: • Verdadero: Elimina el archivo de resultados de la prueba en caché y vuelve a ejecutar las pruebas. • False: Recupera los resultados de una prueba en caché.	booleano	falso	No
fuerza	El parámetro force debe estar incluido en este método para restablecer correctamente el nodo.	booleano	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
detalles	Detalles de configuración de hardware.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "TestHardwareConfig",
   "params": {
      "force": true
     },
   "id" : 1
}
```

Ejemplo de respuesta

Debido a la longitud de este ejemplo de respuesta, se documenta en un tema complementario.

Nuevo desde la versión

9.6

Obtenga más información

TestHardwarConfig

TestLocateCluster

Puede utilizar el `TestLocateCluster` método para validar que el nodo puede localizar el clúster especificado en la configuración de clúster. El resultado valida que el clúster se ha creado y enumera los nodos en el conjunto del clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
detalles	Información sobre el éxito o el fallo de la operación de prueba.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "TestLocateCluster",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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"
   }
}
```

Nuevo desde la versión

9.6

TestLocalConnectivity

Puede utilizar el `TestLocalConnectivity` Método para hacer ping en la IP de clúster

(CIP) de cada nodo en un clúster activo.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
detalles	Tiempos de respuesta ping individuales para cada nodo del clúster activo local.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "TestLocalConnectivity",
   "params": {},
   "id": 1
}
```

Ejemplo de respuesta

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "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"
  }
}
```


Nuevo desde la versión

9.6

TestNetworkConfig

Puede utilizar el `TestNetworkConfig` método para probar que los ajustes de red configurados coinciden con la configuración de red que se está usando en el sistema.

Parámetros

Cuando configura un nodo con el método SetNetworkConfig, en la interfaz de usuario o en la TUI, la configuración se valida y almacena. La prueba de API TestNetworkConfig utiliza la configuración almacenada para la lógica posterior a la validación. Por ejemplo, en el caso de que se produzca una interrupción del servicio de alimentación o un error de red, puede usar este método API para garantizar que un nodo se ejecute con la configuración de red más almacenada actualmente. Esto valida que no haya errores en la configuración y que la configuración actual esté en uso.

Esta prueba está diseñada para mostrar sólo fallos en el resultado de respuesta. Si no hay errores, esta prueba no devuelve ningún resultado. Consulte los siguientes ejemplos de respuesta.

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
detalles	Contiene los errores encontrados al validar los ajustes de red almacenados actualmente con la configuración de red en ejecución.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "TestNetworkConfig",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta 1

Si no se detecta ningún error, no se devuelve ninguna respuesta.

```
{
   "id" : 1,
   "result": {
   "details": {
   "network": {...}
  },
   "duration": "00:00:00.144514",
   "result": "Passed"
  }
}
```

Ejemplo de respuesta 2

Ejemplo de discrepancia de MTU.

```
{
  "id" : 1,
  "result":
  {
     "details" :
     {
        "error":
        {
           "message" : "Network configuration mismatch on Bond10G:
Incorrect MTU expectedMTU=[1500]  actualMTU=[9600]", name:
"xAssertionFailure"
        }
     },
     "duration": "0.125213sec",
     "result": "Failed"
  }
}
```

Ejemplo de respuesta 3

Ejemplo de una ruta estática que falta.

```
{
  "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"
  }
}
```

Nuevo desde la versión

9.6

Obtenga más información

SetNetworkConfig

Pruebas de ping

Puede utilizar el `TestPing` Método para probar la conectividad de red a todos los nodos del clúster en las interfaces 1G y 10G mediante paquetes ICMP. La prueba utiliza los tamaños de MTU adecuados para cada paquete en función de los ajustes de MTU en la configuración de red. `TestPing` No crea una interfaz de VLAN temporal.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
intentos	Especifica el número de veces que el sistema debe repetir el ping de prueba.	entero	5	No
hosts	Especifica una lista separada por comas de direcciones o nombres de host de dispositivos para hacer ping. Si no se especifican hosts, el método hace ping a los hosts en el clúster de almacenamiento.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
interfaz	La interfaz existente (base) desde la que se deben enviar los pings. Los posibles valores son los siguientes: • `Bond10G`: Permite enviar pings desde la interfaz Bond10G. • `Bond1G`: Permite enviar pings desde la interfaz Bond1G.	cadena	Ninguno	No
Tamaño del paquete	Especifica el número de bytes que se enviarán en el paquete ICMP que se envía a cada IP. El número de bytes debe ser inferior al MTU máximo especificado en la configuración de red.	entero	Ninguno	No
PingTimeoutMsec	Especifica el número de milisegundos que se deben esperar por cada respuesta ping individual.	entero	500 milisegundos	No
ProhibiitFragmentación	Activa el indicador DF (no fragment) para los paquetes ICMP.	booleano	falso	No
SourceAddressV4	La dirección IPv4 de origen que se va a usar en los paquetes ping ICMP.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SourceAddressV6	La dirección IPv6 de origen que se va a usar en los paquetes ping ICMP.	cadena	Ninguno	No
TotalTimeoutSec	Especifica el tiempo en segundos que el ping debe esperar a que se produzca una respuesta del sistema antes de emitir el siguiente intento de ping o de finalizar el proceso.	entero	5	No
VirtualNetworkTag	El identificador de VLAN que se va a utilizar al enviar los paquetes ping.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
detalles	Lista de cada IP con la que el nodo pudo comunicarse y las estadísticas de respuesta ping.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "TestPing",
    "params": {
        "interface": "Bond1G",
        "hosts": "192.168.0.1"
    },
    "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```
{
  "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"
  }
}
```


Nuevo desde la versión

5.0

TestRemoteConnectivity

Puede utilizar `TestRemoteConnectivity` método para hacer ping en cada nodo del clúster remoto y comprobar la conexión de la base de datos del conjunto remoto. Los clústeres deben emparejarse para devolver resultados útiles con este método. Si la conexión de base de datos remota falla, la respuesta del sistema muestra las excepciones.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
detalles	Tiempos de respuesta ping individuales para cada nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "TestRemoteConnectivity",
    "params": {
      "force": "true"
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
  }
}
```


Nuevo desde la versión

9.6

Métodos de API de replicación

Los métodos de API de replicación permiten conectar dos clústeres para la protección continua de datos (CDP). Cuando se conectan dos clústeres, los volúmenes activos en un clúster se pueden replicar de manera continua en un segundo clúster para proporcionar recuperación de datos. Al emparejar volúmenes para la replicación, es posible proteger los datos de eventos que podrían no ser accesibles.

- Orden de operaciones de emparejamiento de clústeres
- Orden de las operaciones de emparejamiento de volúmenes

- Modos de replicación compatibles para clústeres emparejados
- CompleteClusterPairing
- CompleteVolumePairing
- ListClusterPairs
- ListActivePairedVolumes
- ModifyVolumePair
- RemoveClusterPair
- RemoveVolumePair
- StartClusterPairing
- StartVolumePairing

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Orden de operaciones de emparejamiento de clústeres

Es necesario establecer una conexión entre una pareja de clústeres de almacenamiento que ejecutan el software Element para poder utilizar la replicación remota.

Use el siguiente conjunto de métodos API para establecer una conexión de clúster:

- StartClusterPairing:

  Este método de API crea y devuelve una clave de emparejamiento que se utiliza para establecer una pareja de clústeres. La clave está codificada y contiene información que se utiliza para establecer comunicaciones entre clústeres. Un único clúster se puede emparejar con hasta cuatro clústeres. Sin embargo, se debe generar una nueva clave para cada emparejamiento de clústeres. La StartClusterPairing método genera una nueva clave cada vez que se llama al método. Utilice cada clave única con CompleteClusterPairing método para emparejar cada clúster adicional.

  > Por motivos de seguridad, la clave de emparejamiento no se debe enviar a otros usuarios por correo electrónico. La clave contiene un nombre de usuario y una contraseña.

- CompleteClusterPairing:

  Este método utiliza la clave de emparejamiento creada con el StartClusterPairing Método API para crear una pareja de clústeres. Emita el CompleteClusterPairing Método API con el parámetro clusterPairingKey en el destino. El clúster de origen es el clúster que creó la clave.

Obtenga más información

- StartClusterPairing
- CompleteClusterPairing

Orden de las operaciones de emparejamiento de volúmenes

Para poder emparejar los volúmenes, es necesario crear una pareja de clústeres entre dos clústeres correspondientes.

Use el siguiente conjunto de métodos API para establecer una conexión de clúster:

- StartVolumePairing:

  Este método de API crea y devuelve una clave de emparejamiento de volúmenes que se utiliza para crear una pareja de volúmenes. La clave contiene información que se utiliza para establecer comunicaciones entre volúmenes.

- CompleteVolumePairing:

  Este método utiliza la clave de emparejamiento creada con el StartVolumePairing Método API para crear una pareja de volúmenes. Emita el CompleteVolumePairing Método API con los parámetros volumeID y volumePairingKey para el volumen de destino.

Solo se puede identificar uno de los volúmenes emparejados como un volumen de destino de replicación. Utilice la ModifyVolumePair Método API para establecer la dirección de la replicación de datos del volumen identificando el volumen que es el destino. Los datos se replican del volumen de origen al volumen de destino.

Obtenga más información

- StartVolumePairing
- CompleteVolumePairing
- ModifyVolumePair

Modos de replicación compatibles para clústeres emparejados

Los siguientes modos de replicación se admiten en los clústeres emparejados:

- Replicación asíncrona de datos: Los datos que se envían al volumen de destino de replicación se envían de forma asíncrona. El sistema no espera que se envíe un acuse de recibo antes de escribir datos.
- Replicación síncrona de datos: Los datos que se envían al volumen de destino de replicación se envían de forma síncrona. Cuando el sistema reconoce las operaciones de I/o enviadas desde el host, el reconocimiento del sistema se envía de nuevo al host y los datos se envían al volumen de destino de replicación.
- Replicación de los datos solo con snapshots: Solo se replican las copias de Snapshot de volumen en el clúster de destino.

CompleteClusterPairing

La `CompleteClusterPairing` el método es el segundo paso del proceso de emparejamiento de clústeres. Utilice este método con la clave codificada recibida de `StartClusterPairing` método para completar el proceso de emparejamiento de clústeres.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ClusterPairingKey	Una cadena de caracteres que se devuelve del StartClusterPairing Método API.	cadena	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
ClusterPairID	Identificador único de la pareja de clústeres.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "CompleteClusterPairing",
   "params": {
        "clusterPairingKey" :
"7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223
a2231636561313336322d346338662d343631612d626537322d373435363661393533643263
6222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d6330755
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a393133313432363439 2c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id" : 1,
   "result" : {
       "clusterPairID" : 1
   }
}
```

Nuevo desde la versión

9.6

Obtenga más información

StartClusterPairing

CompleteVolumePairing

Puede utilizar `CompleteVolumePairing` para completar el emparejamiento de dos volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	El ID de volumen que completará la pareja de volúmenes.	entero	Ninguno	Sí
VolumePairingKey	La clave ha vuelto de la StartVolumePairing Método API.	cadena	Ninguno	Sí

Valor de retorno

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "CompleteVolumePairing",
   "params": {
        "volumeID" : 12,
        "volumePairingKey" :
"7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223
a2231636561313336322d346338662d343631612d626537322d373435363661393533643263
6222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d6330755
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a393133313432363439 2c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
        },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
"id": 1,
"result": {}
}
```

Nuevo desde la versión

9.6

Obtenga más información

StartVolumePairing

ListClusterPairs

Puede utilizar el `ListClusterPairs` método para enumerar todos los clústeres que se emparejan con el clúster actual. Este método muestra información acerca de los emparejamientos de clústeres activos y pendientes, como estadísticas del emparejamiento actual, así como la conectividad y la latencia (en milisegundos) del emparejamiento de clústeres.

Parámetro

Este método no tiene parámetro de entrada:

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
ClusterPairs	Información sobre cada clúster emparejado.	ClusterPair cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListClusterPairs",
   "params": {
      },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
 "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"
     }
   ]
 }
```


Nuevo desde la versión

9.6

ListActivePairedVolumes

Puede utilizar el `ListActivePairedVolumes` método para enumerar todos los volúmenes activos emparejados con un volumen. Este método muestra información acerca de los volúmenes con emparejamientos activos y pendientes.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
volúmenes	Información de volumen de los volúmenes emparejados.	Pareja de volúmenes cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListActivePairedVolumes",
   "params": {
      },
   "id" : 1
}
```

Ejemplo de respuesta

Las respuestas para este método son similares al ejemplo siguiente:

```
{
    "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"
                    }
                ]
            }
        ]
    }
}
```


Nuevo desde la versión

9.6

ModifyVolumePair

Puede utilizar el `ModifyVolumePair` método para pausar o reiniciar la replicación entre un par de volúmenes. Este método se establece en el volumen de origen (el volumen con acceso de lectura/escritura).

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	Número de identificación del volumen que se va a modificar.	entero	Ninguno	Sí
Manual de instrucciones	La replicación remota se puede pausar o reiniciar en el volumen de origen (lectura/escritura). Los posibles valores son los siguientes: • True: Pausa la replicación de volúmenes. • False: Reinicie la replicación de volúmenes. Si no se especifica ningún valor, no se realiza ningún cambio en la replicación.	booleano	Ninguno	No

modo	Modo de replicación del volumen. Los posibles valores son los siguientes: • Asincrónica: Las escrituras se reconocen cuando se completan localmente. El clúster no espera a que se repliquen las escrituras en el clúster de destino. • Sync: El origen reconoce la escritura cuando los datos se almacenan localmente y en el clúster remoto. • SnapshotsOnly: Solo se replican las copias de Snapshot que se crearon en el clúster de origen. No se replican las escrituras activas del volumen de origen.	cadena	Ninguno	No

Valor de retorno

Este método no tiene ningún valor devuelto.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ModifyVolumePair",
  "params": {
    "pausedManual": false,
    "volumeID": 5,
    "mode": "sync"
   },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id" : 1,
   "result" : {}
}
```

Nuevo desde la versión

9.6

RemoveClusterPair

Puede utilizar el `RemoveClusterPair` método para cerrar las conexiones abiertas entre dos clústeres emparejados.

Parámetro

> Antes de quitar una pareja de clústeres, primero se debe quitar todo el emparejamiento de volúmenes a los clústeres con el método API RemoveVolumePair.

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ClusterPairID	Identificador único que se utiliza para emparejar dos clústeres.	entero	Ninguno	Sí

Valor de retorno

Este método no tiene ningún valor devuelto.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "RemoveClusterPair",
   "params": {
              "clusterPairID": 1
      },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {}
}
```

Nuevo desde la versión

9.6

RemoveVolumePair

Puede utilizar el `RemoveVolumePair` método para quitar el emparejamiento remoto entre dos volúmenes. Use este método en los volúmenes de origen y objetivo emparejados. Cuando se quita la información de emparejamiento de volúmenes, los datos ya no se replican en el volumen o desde él.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	El ID del volumen en el que se detiene el proceso de replicación.	entero	Ninguno	Sí

Valor de retorno

Este método no tiene ningún valor devuelto.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "RemoveVolumePair",
   "params": {
      "volumeID": 5
   "id" : 1
   }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {
   }
}
```

Nuevo desde la versión

9.6

StartClusterPairing

Puede utilizar el `StartClusterPairing` método para crear una clave codificada desde un clúster que se utilice para emparejarla con otro clúster. La clave creada a partir de este método de API se utiliza en la `CompleteClusterPairing` método para establecer el emparejamiento de clústeres. Un clúster se puede emparejar con un máximo de otros cuatro clústeres.

Parámetro

Este método no tiene parámetro de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
ClusterPairingKey	Una cadena de caracteres que utiliza el CompleteClusterPairing Método API.	cadena

Nombre	Descripción	Tipo
ClusterPairID	Identificador único de la pareja de clústeres.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "StartClusterPairing",
   "params": {
      },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {
     "clusterPairID": 1,
     "clusterPairingKey":
"7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223
a2231636561313336322d346338662d343631612d626537322d373435363661393536432
6222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d6330755
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a393133313432363439 2c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
   }
}
```

Nuevo desde la versión

9.6

Obtenga más información

CompleteClusterPairing

StartVolumePairing

Puede utilizar el `StartVolumePairing` método para crear una clave codificada desde

un volumen que se utilice para emparejarlo con otro volumen. La clave que crea este método se utiliza en la `CompleteVolumePairing` método para establecer un emparejamiento de volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
modo	El modo del volumen en el que se inicia el proceso de emparejamiento. El modo solo se puede establecer si el volumen es el volumen de origen. Los posibles valores son los siguientes: • `Async`: Las escrituras se reconocen cuando se completan localmente. El clúster no espera a que se repliquen las escrituras en el clúster de destino. (Predeterminado si no se especifica ningún parámetro de modo.) • `Sync`: Source confirma la escritura cuando los datos se almacenan localmente y en el clúster remoto. • `SnapshotsOnly`: Sólo se replican las instantáneas creadas en el clúster de origen. No se replican las escrituras activas del volumen de origen.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	El ID del volumen en el que se inicia el proceso de emparejamiento.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumePairingKey	Una cadena de caracteres que utiliza el CompleteVolumePairing Método API.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "StartVolumePairing",
   "params": {
         "mode": "Async",
     "volumeID" : 14
      },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id" : 1,
   "result" : {
      "volumePairingKey" :
"7b226d766970223a223139322e3136382e3133392e313232222c22766f6c756d654944223
a312c22766f6c756d654e616d65223a2254657374222c22766f6c756d65506169725555494
4223a22363936323466636 22d323032652d343332352d613536392d6563396336353563376
23561227d"
      }
}
```

Nuevo desde la versión

9.6

Obtenga más información

CompleteVolumePairing

Métodos de API de seguridad

Es posible integrar el software Element con servicios relacionados con la seguridad externos, como un servidor de gestión de claves externo. Estos métodos relacionados con la seguridad permiten configurar funciones de seguridad de Element, como la gestión de claves externa para el cifrado en reposo.

- AddKeyServerToProviderKmip
- CreateKeyProviderKmip
- CreateKeyServerKmip
- CreatePublicPrivateKeyPair
- DeleteKeyProviderKmip
- DeleteKeyServerKmip
- DisableEncryptionAtest
- EnableEncryptionAtest
- GetClientCertificateSignRequest
- GetKeyProviderKmip
- GetKeyServerKmip
- ListKeyProvidersKmip
- ListKeyServersKmip
- ModifyKeyServerKmip
- RemoveKeyServerFromProviderKmip
- TestKeyProviderKmip
- TestKeyServerKmip

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

AddKeyServerToProviderKmip

Puede utilizar el `AddKeyServerToProviderKmip` Método para asignar un servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) al proveedor de claves especificado. Durante la asignación, se contacta con el servidor para verificar la funcionalidad. Si el servidor de claves especificado ya está asignado al proveedor de

claves especificado, no se realiza ninguna acción y no se devuelve ningún error. Puede quitar la asignación mediante `RemoveKeyServerFromProviderKmip` método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderID	El ID del proveedor de claves al que se asignará el servidor de claves.	entero	Ninguno	Sí
KeyServerID	El ID del servidor de claves que se asignará.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene ningún valor devuelto. La asignación se considera correcta siempre que no se devuelva ningún error.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "AddKeyServerToProviderKmip",
  "params": {
    "keyProviderID": 1,
    "keyServerID": 15
    },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
      {}
    }
}
```

Nuevo desde la versión

11.7

CreateKeyProviderKmip

Puede utilizar el `CreateKeyProviderKmip` Método para crear un proveedor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) con el nombre especificado. Un proveedor de claves define un mecanismo y una ubicación para recuperar claves de autenticación. Cuando se crea un proveedor de claves KMIP nuevo, no tiene ningún servidor de claves KMIP asignado. Para crear un servidor de claves KMIP, use el `CreateKeyServerKmip` método. Para asignarlo a un proveedor, consulte `AddKeyServerToProviderKmip`.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderName	El nombre que se asignará al proveedor de claves KMIP creado. Este nombre sólo se utiliza con fines de visualización y no necesita ser único.	cadena	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyProvider	Objeto que contiene detalles acerca del proveedor de claves recién creado.	"KeyProviderKmip"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "CreateKeyProviderKmip",
  "params": {
    "keyProviderName": "ProviderName",
    },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
      {
    "kmipKeyProvider": {
        "keyProviderName": "ProviderName",
        "keyProviderIsActive": true,
        "kmipCapabilities": "SSL",
        "keyServerIDs": [
            15
        ],
        "keyProviderID": 1
    }
}
}
```

Nuevo desde la versión

11.7

CreateKeyServerKmip

Puede utilizar el `CreateKeyServerKmip` Método para crear un servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) con los atributos especificados. Durante la creación, no se contacta con el servidor; no es necesario que exista antes de utilizar este método. Para configuraciones de servidor de claves en clúster, debe proporcionar los nombres de host o direcciones IP de todos los nodos de servidor en el parámetro kmipKeyServerHostnames. Puede utilizar el `TestKeyServerKmip` método para probar un servidor de claves.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KmipCaCertificate	El certificado de clave pública de la CA raíz del servidor de claves externo. Esto se utilizará para verificar el certificado presentado por el servidor de claves externo en la comunicación TLS. Para los clústeres de servidores de claves en los que los servidores individuales utilizan distintas CA, proporcione una cadena concatenada que contenga los certificados raíz de todas las CA.	cadena	Ninguno	Sí
KmipClientCertificate	Un certificado PKCS#10 X.509 codificado en Base64 con formato PEM que utiliza el cliente KMIP de SolidFire.	cadena	Ninguno	Sí
KmipKeyServerHostnames	Cabina de los nombres de host o las direcciones IP asociadas con este servidor de claves KMIP. Sólo se deben proporcionar varios nombres de host o direcciones IP si los servidores de claves se encuentran en una configuración en clúster.	matriz de cadenas	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KmipKeyServerName	El nombre del servidor de claves KMIP. Este nombre sólo se utiliza con fines de visualización y no necesita ser único.	cadena	Ninguno	Sí
KmipKeyServerPort	El número de puerto asociado con este servidor de claves KMIP (por lo general, 5696).	entero	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyServer	Objeto que contiene detalles acerca del servidor de claves recién creado.	"KeyServerKmip"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "CreateKeyServerKmip",
  "params": {
    "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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
        }
     }
}
```

Nuevo desde la versión

11.7

CreatePublicPrivateKeyPair

Puede utilizar el `CreatePublicPrivateKeyPair` Método para crear claves SSL públicas y privadas. Es posible usar estas claves para generar solicitudes de firma de certificados. Solo puede haber una pareja de claves en uso para cada clúster de almacenamiento. Antes de utilizar este método para reemplazar las claves existentes, asegúrese de que ningún proveedor ya utilice las claves.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
CommonName	El campo X.509 Nombre distintivo **Nombre común** (CN).	cadena	Ninguno	No
país	El campo X 509 de nombre completo **país** ©.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Dirección de correo electrónico	El campo X 509 Nombre distintivo **Dirección de correo electrónico** (CORREO).	cadena	Ninguno	No
localidad	El campo X 509 Nombre distintivo **Nombre de localidad** (L).	cadena	Ninguno	No
organización	El campo X 509 Nombre distintivo **Nombre de organización** (o).	cadena	Ninguno	No
Unidad organizativa	El campo X.509 Nombre distintivo **Nombre de unidad organizativa** (OU).	cadena	Ninguno	No
estado	El campo X 509 Nombre distinguido **Estado** o **Nombre de provincia** (ST o SP o S).	cadena	Ninguno	No

Valores devueltos

Este método no tiene valores devueltos. Si no hay ningún error, la creación de claves se considera correcta.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "CreatePublicPrivateKeyPair",
  "params": {
    "commonName": "Name",
    "country": "US",
    "emailAddress" : "email@domain.com"
   },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
      {}
}
```

Nuevo desde la versión

11.7

DeleteKeyProviderKmip

Puede utilizar el `DeleteKeyProviderKmip` Método para eliminar el proveedor de claves de interoperabilidad de gestión de claves inactiva especificado (KMIP).

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderID	El ID del proveedor de claves que se eliminará.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos. La operación de eliminación se considera correcta siempre que no haya error.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DeleteKeyProviderKmip",
  "params": {
    "keyProviderID": "1"
    },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
      {}
}
```

Nuevo desde la versión

11.7

DeleteKeyServerKmip

Puede utilizar el `DeleteKeyServerKmip` Método para eliminar un servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) existente. Puede eliminar un servidor de claves a menos que sea el último asignado a su proveedor, y ese proveedor proporciona claves que están en uso actualmente.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyServerID	El ID del servidor de claves KMIP que se desea eliminar.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los valores no return. La operación de eliminación se considera correcta si no hay errores.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DeleteKeyServerKmip",
  "params": {
     "keyServerID": 15
  },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
      {}
}
```

Nuevo desde la versión

11.7

DisableEncryptionAtest

Puede utilizar el `DisableEncryptionAtRest` método para quitar el cifrado que se aplicó previamente al clúster mediante el `EnableEncryptionAtRest` método. Este método disable es asíncrono y devuelve una respuesta antes de que se deshabilite el cifrado. Puede utilizar el `GetClusterInfo` método para sondear el sistema para ver cuándo se ha completado el proceso.

Para ver el estado actual del cifrado en reposo y/o el cifrado de software en reposo en el clúster, use el "obtenga el método de información del clúster". Puede utilizar el `GetSoftwareEncryptionAtRestInfo` "método para obtener información que utiliza el clúster para cifrar datos en reposo".

No se puede usar este método para deshabilitar el cifrado de software en reposo. Para deshabilitar el cifrado de software en reposo, debe hacerlo "cree un nuevo clúster" con el cifrado de software en reposo deshabilitado.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "DisableEncryptionAtRest",
   "params": {},
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id" : 1,
  "result" : {}
}
```

Nuevo desde la versión

9.6

Obtenga más información

- "GetClusterInfo"
- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

EnableEncryptionAtest

Puede utilizar el `EnableEncryptionAtRest` Método para habilitar el cifrado AES (estándar de cifrado avanzado) de 256 bits en reposo en el clúster de manera que el clúster pueda gestionar la clave de cifrado utilizada para las unidades de cada nodo. Esta función no está habilitada de forma predeterminada.

Para ver el estado actual del cifrado en reposo y/o el cifrado de software en reposo en el clúster, use el "obtenga el método de información del clúster". Puede utilizar el `GetSoftwareEncryptionAtRestInfo` "método para obtener información que utiliza el clúster para cifrar datos en reposo".

Este método no habilita el cifrado de software en reposo. Esto sólo se puede hacer usando "cree el método de clúster" con `enableSoftwareEncryptionAtRest` establezca en `true`.

Cuando habilita el cifrado en reposo, el clúster gestiona automáticamente las claves de cifrado internamente para las unidades de cada nodo del clúster.

Si se especifica un keyProviderID, la contraseña se genera y recupera según el tipo de proveedor de claves. Esto suele realizarse mediante un servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) en el caso de un proveedor de claves KMIP. Después de esta operación, el proveedor especificado se

considera activo y no se puede eliminar hasta que se deshabilite el cifrado en reposo con el `DisableEncryptionAtRest` método.

> Si tiene un tipo de nodo con un número de modelo que termina en "-NE", la `EnableEncryptionAtRest` La llamada al método fallará y la respuesta será "no se permite el cifrado. Cluster detectado nodo no encriptable".

> Solo tendrá que habilitar o deshabilitar el cifrado cuando el clúster se ejecute y esté en buen estado. Puede activar o desactivar el cifrado a su discreción y con la frecuencia que necesite.

> Este proceso es asíncrono y devuelve una respuesta antes de activar el cifrado. Puede utilizar el `GetClusterInfo` método para sondear el sistema para ver cuándo se ha completado el proceso.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderID	El ID de un proveedor de claves KMIP que se debe usar.	entero	Ninguno	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "EnableEncryptionAtRest",
   "params": {},
   "id": 1
}
```

Ejemplos de respuestas

Este método devuelve una respuesta similar al siguiente ejemplo del método EnableEncryptionAtRest. No hay resultados para informar.

```
{
   "id": 1,
   "result": {}
}
```

Mientras que el cifrado en reposo se está habilitado en un clúster, GetClusterInfo muestra un resultado que describe el estado del cifrado en reposo ("cifrado AtRestState") como "habilitado". Una vez que el cifrado en reposo está completamente habilitado, el estado devuelto cambia a "habilitado".

```
{
   "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"
      }
   }
}
```

Nuevo desde la versión

9.6

Obtenga más información

- "SecureEraseDrives"
- "GetClusterInfo"
- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

GetClientCertificateSignRequest

Puede utilizar el `GetClientCertificateSignRequest` método para generar una

solicitud de firma de certificación que puede estar firmada por una entidad de certificación a fin de generar un certificado de cliente para el clúster. Los certificados firmados son necesarios para establecer una relación de confianza para interactuar con servicios externos.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
ClientCertificadosSignRequest	Una solicitud de firma de certificado de cliente PKCS#10 X.509 codificada con PEM Base64.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetClientCertificateSignRequest",
  "params": {
  },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
      {
        "clientCertificateSignRequest":
"MIIByjCCATMCAQAwgYkxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
   }
}
```

Nuevo desde la versión

11.7

GetKeyProviderKmip

Puede utilizar el `GetKeyProviderKmip` Método para recuperar información sobre el proveedor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) especificado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderID	El ID del objeto de proveedor de claves KMIP que se va a devolver.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyProvider	Objeto que contiene detalles sobre el proveedor de claves solicitado.	"KeyProviderKmip"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetKeyProviderKmip",
  "params": {
    "keyProviderID": 15
    },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
    {
    "kmipKeyProvider": {
        "keyProviderID": 15,
        "kmipCapabilities": "SSL",
        "keyProviderIsActive": true,
        "keyServerIDs": [
            1
        ],
        "keyProviderName": "ProviderName"
    }
   }
}
```

Nuevo desde la versión

11.7

GetKeyServerKmip

Puede utilizar el `GetKeyServerKmip` Método para obtener información sobre el servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) especificado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyServerID	El ID del servidor de claves KMIP acerca de la cual se desea obtener información.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyServer	Objeto que contiene detalles acerca del servidor de claves solicitado.	"KeyServerKmip"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetKeyServerKmip",
  "params": {
     "keyServerID": 15
  },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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
        }
    }
}
```

Nuevo desde la versión

11.7

GetSoftwareEncryptionAtRestInfo

Puede utilizar el `GetSoftwareEncryptionAtRestInfo` método para obtener información de cifrado por software que el clúster utiliza para cifrar datos en reposo.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Parámetro	Descripción	Tipo	Opcional
MasterKeyInfo	Información acerca de la clave maestra actual de cifrado en reposo de software.	Cifrar KeyInfo	Verdadero
RekeyMasterKeyAsyncResultID	El ID de resultado asíncrono de la operación de reclave actual o más reciente (si existe), si aún no se ha eliminado. `GetAsyncResult` la salida incluirá una `newKey` campo que contiene información acerca de la nueva clave maestra y un `keyToDecommission` campo que contiene información acerca de la clave anterior.	entero	Verdadero
estado	El estado actual del cifrado de software en reposo. Los valores posibles son `disabled` o. `enabled`.	cadena	Falso
versión	Un número de versión que aumenta cada vez que se habilita el cifrado de software en reposo.	entero	Falso

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
 "method": "getsoftwareencryptionatrestinfo"
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "masterKeyInfo": {
            "keyCreatedTime": "2021-09-20T23:15:56Z",
            "keyID": "4d80a629-a11b-40ab-8b30-d66dd5647cfd",
            "keyManagementType": "internal"
        },
        "state": "enabled",
        "version": 1
    }
}
```


Nuevo desde la versión

12.3

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

ListKeyProvidersKmip

Puede utilizar el `ListKeyProvidersKmip` Método para recuperar una lista de todos los proveedores de claves del protocolo de interoperabilidad de gestión de claves (KMIP) existentes. Puede filtrar la lista especificando parámetros adicionales.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderIsActive	Los filtros regresaron objetos del servidor de claves KMIP en función de si están activos. Los posibles valores son los siguientes: • True: Devuelve solo los proveedores de claves KMIP activos (que proporcionan claves en uso actualmente). • False: Devuelve solo los proveedores de claves KMIP inactivos (sin ofrecer ninguna clave y sin poder eliminarla). Si se omite, los proveedores de claves KMIP que se devuelven no se filtran en función de si están activos.	booleano	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KmipKeyProviderHasServerAssigned	Los filtros devuelven proveedores de claves KMIP en función de si tienen asignado un servidor de claves KMIP. Los posibles valores son los siguientes: • True: Solo devuelve los proveedores de claves KMIP que tienen asignado un servidor de claves KMIP. • False: Devuelve solo los proveedores de claves KMIP que no tienen asignado un servidor de claves KMIP. Si se omite, los proveedores de claves KMIP que se devuelven no se filtran en función de si tienen asignado un servidor de claves KMIP.	booleano	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyProviders	Una lista de los proveedores de claves KMIP que se hayan creado.	"KeyProviderKmip" cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListKeyProvidersKmip",
  "params": {},
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
    {
    "kmipKeyProviders": [
        {
            "keyProviderID": 15,
            "kmipCapabilities": "SSL",
            "keyProviderIsActive": true,
            "keyServerIDs": [
                1
            ],
            "keyProviderName": "KeyProvider1"
        }
    ]
}
}
```

Nuevo desde la versión

11.7

ListKeyServersKmip

Puede utilizar el `ListKeyServersKmip` Método para enumerar todos los servidores de claves de protocolo de interoperabilidad de gestión de claves (KMIP) creados. Los resultados se pueden filtrar especificando parámetros adicionales.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderID	Cuando se especifica, el método solo devuelve los servidores de claves KMIP asignados al proveedor de claves KMIP especificado. Si se omite, los servidores de claves KMIP devueltos no se filtrarán en función de si se asignan al proveedor de claves KMIP especificado.	entero	Ninguno	No
KmipAssignedProviderIsActive	Los filtros regresaron objetos del servidor de claves KMIP en función de si están activos. Los posibles valores son los siguientes: • True: Devuelve solo los servidores de claves KMIP activos (que proporcionan claves en uso actualmente). • False: Devuelve solo los servidores de claves KMIP inactivos (sin proporcionar ninguna clave y sin poder eliminarse). Si se omite, los servidores de claves KMIP devueltos no se filtran en función de si están activos.	booleano	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KmipHasProviderAssigned	Los filtros devuelven servidores de claves KMIP en función de si tienen asignado un proveedor de claves KMIP. Los posibles valores son los siguientes: • True: Solo devuelve los servidores de claves KMIP que tienen asignado un proveedor de claves KMIP. • False: Devuelve solo los servidores de claves KMIP que no tienen asignado un proveedor de claves KMIP. Si se omite, los servidores de claves KMIP que se devuelven no se filtran en función de si tienen asignado un proveedor de claves KMIP.	booleano	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyServers	La lista completa de los servidores de claves KMIP que se crearon.	"KeyServerKmip" cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListKeyServersKmip",
  "params": {},
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "kmipKeyServers": [
        {
            "kmipKeyServerName": "keyserverName",
            "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
            "keyServerID": 15,
            "kmipAssignedProviderIsActive": true,
            "kmipKeyServerPort": 5696,
            "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames": [
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID": 1
        }
    ]
}
```

Nuevo desde la versión

11.7

ModifyKeyServerKmip

Puede utilizar el `ModifyKeyServerKmip` Método para modificar un servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) existente en los atributos especificados. Aunque el único parámetro requerido es keyServerID, una solicitud que contiene sólo el keyServerID no realizará ninguna acción y no devolverá ningún error. Cualquier otro parámetro que especifique reemplazará los valores existentes para el servidor de claves con el keyServerID especificado. Se contacta con el servidor de claves durante la operación para garantizar que funciona. Puede proporcionar varios nombres de host o direcciones IP con el parámetro kmipKeyServerHostnames, pero sólo si los servidores de claves están en una configuración en clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyServerID	El ID del servidor de claves KMIP que se desea modificar.	entero	Ninguno	Sí
KmipCaCertificate	El certificado de clave pública de la CA raíz del servidor de claves externo. Esto se utilizará para verificar el certificado presentado por el servidor de claves externo en la comunicación TLS. Para los clústeres de servidores de claves en los que los servidores individuales utilizan distintas CA, proporcione una cadena concatenada que contenga los certificados raíz de todas las CA.	cadena	Ninguno	No
KmipClientCertificate	Un certificado PKCS#10 X.509 codificado en Base64 con formato PEM que utiliza el cliente KMIP de SolidFire.	cadena	Ninguno	No

KmipKeyServerHostnames	Cabina de los nombres de host o las direcciones IP asociadas con este servidor de claves KMIP. Sólo se deben proporcionar varios nombres de host o direcciones IP si los servidores de claves se encuentran en una configuración en clúster.	matriz de cadenas	Ninguno	No
KmipKeyServerName	El nombre del servidor de claves KMIP. Este nombre sólo se utiliza con fines de visualización y no necesita ser único.	cadena	Ninguno	No
KmipKeyServerPort	El número de puerto asociado con este servidor de claves KMIP (por lo general, 5696).	entero	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyServer	Un objeto que contiene detalles acerca del servidor de claves recién modificado.	"KeyServerKmip"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ModifyKeyServerKmip",
  "params": {
    "keyServerID": 15
    "kmipCaCertificate": "CPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "kirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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
        }
    }
}
```

Nuevo desde la versión

11.7

RekeySoftwareEncryptionAtRestMasterKey

Puede utilizar el `RekeySoftwareEncryptionAtRestMasterKey` Método para volver a introducir la clave maestra de cifrado en reposo de software utilizada para cifrar los

depósitos (claves de cifrado de datos). Durante la creación de clústeres, el cifrado de software en reposo se configura para utilizar Internal Key Management (IKM). Este método de nueva clave se puede utilizar después de la creación de un clúster para utilizar IKM o Gestión de claves externas (EKM).

Parámetros

Este método tiene los siguientes parámetros de entrada. Si la `keyManagementType` no se especifica el parámetro; la operación de nueva clave se realiza mediante la configuración de gestión de claves existente. Si la `keyManagementType` se especifica y el proveedor de claves es externo, el `keyProviderID` también se debe utilizar el parámetro.

Parámetro	Descripción	Tipo	Opcional
Tipo de material de la columna	El tipo de gestión de claves utilizado para gestionar la clave maestra. Los valores posibles son: `Internal`: ReKey utilizando la gestión de claves internas. `External`: ReKey mediante la gestión de claves externas. Si no se especifica este parámetro, se ejecuta la operación de nueva clave mediante la configuración de gestión de claves existente.	cadena	Verdadero
KeyProviderID	El ID del proveedor de claves que se utilizará. Se trata de un valor único devuelto como parte de uno de los `CreateKeyProvider` métodos. El ID sólo es necesario cuando `keyManagementType` es `External` y, de lo contrario, no es válido.	entero	Verdadero

Valores devueltos

Este método tiene los siguientes valores devueltos:

Parámetro	Descripción	Tipo	Opcional
Establish asyncHandle	Determine el estado de la operación de reclaves con este método `asyncHandle` valor con `GetAsyncResult`. `GetAsyncResult` la salida incluirá una `newKey` campo que contiene información acerca de la nueva clave maestra y un `keyToDecommission` campo que contiene información acerca de la clave anterior.	entero	Falso

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "asyncHandle": 1
}
```

Nuevo desde la versión

12.3

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

RemoveKeyServerFromProviderKmip

Puede utilizar el `RemoveKeyServerFromProviderKmip` Método para anular la asignación del servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) especificado del proveedor al que se asignó. Puede anular la asignación de un servidor de claves de su proveedor a menos que sea el último y su proveedor esté activo (proporcionando claves que estén en uso actualmente). Si el servidor de claves especificado no está asignado a un proveedor, no se realiza ninguna acción y no se devuelve ningún error.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyServerID	El ID del servidor de claves KMIP para anular la asignación.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos. La eliminación se considera correcta siempre que no se devuelva ningún error.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "RemoveKeyServerFromProviderKmip",
  "params": {
    "keyServerID": 1
   },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
      {}
    }
}
```

Nuevo desde la versión

11.7

TestKeyProviderKmip

Puede utilizar el `TestKeyProviderKmip` Método para probar si el proveedor de claves del protocolo de interoperabilidad de gestión de claves (KMIP) especificado es accesible y funciona normalmente.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderID	El ID del proveedor de claves que se probará.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos. La prueba se considera correcta mientras no se devuelve ningún error.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "TestKeyProviderKmip",
  "params": {
    "keyProviderID": 15
  },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
      {}
    }
}
```

Nuevo desde la versión

11.7

TestKeyServerKmip

Puede utilizar el `TestKeyServerKmip` Método para probar si el servidor de claves del protocolo de interoperabilidad de gestión de claves (KMIP) especificado es accesible y funciona con normalidad.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyServerID	El ID del servidor de claves KMIP que se probará.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos. La prueba se considera correcta si no se devuelve ningún error.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "TestKeyServerKmip",
  "params": {
    "keyServerID": 15
  },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
      {}
    }
```

Nuevo desde la versión

11.7

Métodos de API de SnapMirror

La interfaz de usuario web de Element utiliza los métodos de API de SnapMirror para gestionar copias de Snapshot reflejadas con sistemas ONTAP remotos. Estos métodos están destinados únicamente a su uso en la interfaz de usuario web de Element. Si necesita acceso mediante API a la funcionalidad SnapMirror, utilice las API de ONTAP. No se proporcionan ejemplos de solicitud y devolución para los métodos de API de SnapMirror.

- AbrortSnapMirrorRelationship
- SnapBreakMirrorRelationship
- SnapBreakMirrorVolume
- CreateSnapMirrorEndpoint
- CreateSnapMirrorEndpointUnmanaged
- CreateSnapMirrorRelationship
- CreateSnapMirrorVolume
- DeleteSnapMirrorEndpoints
- DeleteSnapMirrorrelationships
- GetOntapVersionInfo
- GetSnapMirrorClusterIdentity
- InitializeSnapMirrorRelationship
- ListSnapMirrorAggregates
- ListSnapMirrorEndpoints
- ListSnapMirrorLuns
- ListSnapMirrorNetworkinterfaces
- ListSnapMirrorNodes
- ListSnapMirrorPolicies

- ListSnapMirrorSchedules
- ListSnapMirrorRelationship
- ListSnapMirrorVolumes
- ListSnapMirrorservidores
- ModificySnapMirrorEndpoint
- ModificySnapMirrorEndpoint (no administrado)
- ModificySnapMirrorRelationship
- UpdateSnapMirrorRelationship
- QuiesceSnapMirrorRelationship
- ReumeSnapMirrorRelationship
- ResyncSnapMirrorRelationship

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

AbrortSnapMirrorRelationship

La interfaz de usuario web del software Element utiliza el `AbortSnapMirrorRelationship` Método para detener las transferencias de SnapMirror que han comenzado pero que aún no están completas.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	El ID de extremo del sistema de almacenamiento remoto de ONTAP se comunica con el clúster de almacenamiento de Element.	entero	Ninguno	Sí
DestationVolume	El volumen de destino de la relación de SnapMirror.	SnapMirrorVolumeInfo	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ClearCheckpoint	Determina si se borra o no el punto de control de reinicio. Los posibles valores son los siguientes: • verdadero • falso	booleano	falso	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
SnapMirrorRelationship	Objeto que contiene información sobre la relación de SnapMirror anulada.	SnapMirrorRelationship

Nuevo desde la versión

10.1

SnapBreakMirrorRelationship

La interfaz de usuario web de Element utiliza el `BreakSnapMirrorRelationship` Método para romper una relación de SnapMirror. Cuando se interrumpe una relación de SnapMirror, el volumen de destino se hace de lectura y escritura independiente, y a continuación, se puede desviar del origen. Puede restablecer la relación con `ResyncSnapMirrorRelationship` Método API. Para utilizar este método, el clúster de ONTAP debe estar disponible.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	El ID de extremo del sistema de almacenamiento remoto de ONTAP se comunica con el clúster de almacenamiento de Element.	entero	Ninguno	Sí
DestationVolume	El volumen de destino de la relación de SnapMirror.	SnapMirrorVolumeInfo	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
SnapMirrorRelationship	Objeto que contiene información acerca de la relación SnapMirror rota.	SnapMirrorRelationship

Nuevo desde la versión

10.1

Obtenga más información

SnapBreakMirrorVolume

SnapBreakMirrorVolume

La interfaz de usuario web de Element utiliza el `BreakSnapMirrorVolume` Método para interrumpir la relación de SnapMirror entre un contenedor de origen de ONTAP y el volumen de destino de Element. Romper un volumen de SnapMirror de Element es útil si un sistema ONTAP deja de estar disponible al replicar los datos en un volumen de Element. Con esta función, un administrador de almacenamiento puede tomar el control de un volumen de Element SnapMirror, romper su relación con el sistema ONTAP remoto y revertir el volumen a una copia Snapshot anterior.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	El volumen donde se ejecuta la operación de interrupción. El modo de acceso de volúmenes debe ser snapMirrorTarget.	entero	Ninguno	Sí
ID de copia Snapshot	Revertir el volumen a la snapshot identificada mediante este ID. El comportamiento predeterminado es revertir a la instantánea más reciente.	entero	Ninguno	No
conservar	Conserve las Snapshot más recientes que la snapshot identificada mediante el ID de copia de Snapshot. Los posibles valores son los siguientes: • True: Conserve las copias de Snapshot más recientes que el ID de copia Snapshot. • False: No se conservan las snapshots más recientes que el ID de copia Snapshot. Si es false, se eliminan las Snapshot más recientes que el ID de copia Snapshot.	booleano	falso	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
acceso	Modo de acceso de volumen resultante. Los posibles valores son los siguientes: • READWRITE • Sólo lectura • bloqueado	cadena	READWRITE	No

Valores devueltos

Este método no tiene valores devueltos.

Nuevo desde la versión

10.0

Obtenga más información

SnapBreakMirrorRelationship

CreateSnapMirrorEndpoint

La interfaz de usuario web de Element utiliza el `CreateSnapMirrorEndpoint` Método para crear una relación con un extremo de SnapMirror remoto.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Gestión de IP	La dirección IP de gestión del extremo de SnapMirror remoto.	cadena	Ninguno	Sí
nombre de usuario	El nombre de usuario de gestión para el sistema ONTAP.	cadena	Ninguno	Sí
contraseña	La contraseña de gestión para el sistema ONTAP.	cadena	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
SnapMirrorEndpoint	El extremo de SnapMirror recién creado.	SnapMirrorEndpoint

Nuevo desde la versión

10.0

CreateSnapMirrorEndpointUnmanaged

El sistema de almacenamiento del software Element utiliza `CreateSnapMirrorEndpointUnmanaged` Método para habilitar extremos de SnapMirror remotos y sin gestionar para comunicarse con un clúster de almacenamiento de Element. No se pueden administrar extremos no gestionados mediante las API de SnapMirror de Element. Deben gestionarse con las API o el software de gestión de ONTAP.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Nombre del clúster	Nombre del extremo.	cadena	Ninguno	Sí
Direcciones IP	La lista de direcciones IP para un clúster de sistemas de almacenamiento ONTAP que se deben comunicar con este clúster de almacenamiento de Element.	matriz de cadenas	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo

SnapMirrorEndpoint	El extremo de SnapMirror recién creado.	SnapMirrorEndpoint

Nuevo desde la versión

10.3

CreateSnapMirrorRelationship

La interfaz de usuario web de Element utiliza el `CreateSnapMirrorRelationship` Método para crear una relación de protección de datos ampliada de SnapMirror entre un extremo de origen y de destino.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	El ID de extremo del sistema de almacenamiento remoto de ONTAP se comunica con el clúster de almacenamiento de Element.	entero	Ninguno	Sí
Volumen de origen	El volumen de origen de la relación.	SnapMirrorVolumeInfo	Ninguno	Sí
DestationVolume	El volumen de destino de la relación.	SnapMirrorVolumeInfo	Ninguno	Sí
RelationshipType	Tipo de relación. En los sistemas de almacenamiento que ejecutan el software Element, este valor siempre es «'Extended_data_protection».	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
PolicyName	Especifica el nombre de la política de SnapMirror de ONTAP para la relación. Si no se especifica, el nombre de la política predeterminada es MirrorLatest.	cadena	Ninguno	No
Nombre de la pila	El nombre de la programación cron preexistente del sistema ONTAP que se utiliza para actualizar la relación SnapMirror. Si no se designa ninguna programación, las actualizaciones de SnapMirror no se programan y deben actualizarse manualmente.	cadena	Ninguno	No
MaxTransferRate	Especifica la tasa máxima de transferencia de datos entre los volúmenes en kilobytes por segundo. El valor predeterminado, 0, es ilimitado y permite que la relación de SnapMirror utilice completamente el ancho de banda de red disponible.	entero	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo

SnapMirrorRelationship	Información acerca de la relación de SnapMirror recién creada.	SnapMirrorRelationship

Nuevo desde la versión

10.1

CreateSnapMirrorVolume

La interfaz de usuario web de Element utiliza el `CreateSnapMirrorVolume` Método para crear un volumen en el sistema ONTAP remoto.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	El ID de extremo del sistema de almacenamiento remoto de ONTAP se comunica con el clúster de almacenamiento de Element.	entero	Ninguno	Sí
vserver	El nombre del Vserver.	cadena	Ninguno	Sí
nombre	El nombre del volumen ONTAP de destino.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
tipo	El tipo de volumen. Los posibles valores son los siguientes: • rw: Volumen de lectura/escritura • ls: Volumen de carga compartida • dp: Volumen de protección de datos Si no se proporciona ningún tipo, el tipo predeterminado es dp.	cadena	Ninguno	No
agregado	El agregado de ONTAP que contiene en el que se creará el volumen. Puede utilizar ListSnapMirrorAggregates para obtener información sobre los agregados de ONTAP disponibles.	cadena	Ninguno	Sí
tamaño	El tamaño en bytes del volumen.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
SnapMirrorVolume	Información acerca de un volumen de SnapMirror.	SnapMirrorVolume

Nuevo desde la versión

10.1

DeleteSnapMirrorEndpoints

Utiliza la interfaz de usuario web de Element `DeleteSnapMirrorEndpoints` Para eliminar uno o varios extremos de SnapMirror del sistema.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Una cabina de ID de extremos de SnapMirror que se van a eliminar.	matriz en números enteros	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Nuevo desde la versión

10.0

DeleteSnapMirrorrelationships

La interfaz de usuario web de Element utiliza el `DeleteSnapMirrorRelationships` Método para quitar una o varias relaciones de SnapMirror entre un extremo de origen y destino.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	El ID de extremo del sistema de almacenamiento remoto de ONTAP se comunica con el clúster de almacenamiento de Element.	entero	Ninguno	Sí
DestinationVolumes	Los volúmenes de destino o la relación de SnapMirror.	SnapMirrorVolumeInfo cabina	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
resultado	Si la acción de eliminación se ha realizado correctamente, este objeto contiene un mensaje de éxito. Si la acción ha fallado, contiene un mensaje de error.	Objeto JSON

Nuevo desde la versión

10.1

GetOntapVersionInfo

Utiliza la interfaz de usuario web de Element `GetOntapVersionInfo` Para obtener información sobre la compatibilidad de versiones de API desde el clúster de ONTAP en una relación de SnapMirror.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Si se proporciona, el sistema enumera la información de versión del extremo con el snapMirrorEndpointID especificado. Si no se proporciona, el sistema enumera la información de la versión de todos los extremos de SnapMirror conocidos.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
OntapVersionInfo	La información de la versión de software del extremo de ONTAP.	OntapVersionInfo cabina

Nuevo desde la versión

10.1

GetSnapMirrorClusterIdentity

La interfaz de usuario web del software Element utiliza `GetSnapMirrorClusterIdentity` Para obtener información sobre la identidad del clúster de ONTAP.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Si se proporciona, el sistema enumera la identidad del clúster del extremo con el snapMirrorEndpointID especificado. Si no se proporciona, el sistema enumera la identidad del clúster de todos los extremos de SnapMirror conocidos.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorClusterIdentity	Una lista de las identidades de los clústeres de los extremos de SnapMirror.	SnapMirrorClusterIdentity cabina

Nuevo desde la versión

10.1

InitializeSnapMirrorRelationship

La interfaz de usuario web del software Element utiliza el `InitializeSnapMirrorRelationship` Método para inicializar el volumen de destino en una relación de SnapMirror mediante una transferencia inicial de referencia entre clústeres.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	El ID del sistema de ONTAP remoto.	entero	Ninguno	Sí
DestationVolume	El volumen de destino de la relación de SnapMirror.	SnapMirrorVolumeInfo	Ninguno	Sí
MaxTransferRate	Especifica la tasa máxima de transferencia de datos entre los volúmenes en kilobytes por segundo. El valor predeterminado, 0, es ilimitado y permite que la relación de SnapMirror utilice completamente el ancho de banda de red disponible.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorRelationship	Información acerca de la relación de SnapMirror inicializada	SnapMirrorRelationship

Nuevo desde la versión

10.1

ListSnapMirrorAggregates

La interfaz de usuario web del software Element utiliza el `ListSnapMirrorAggregates` Método para enumerar todos los agregados de SnapMirror que están disponibles en el sistema remoto de ONTAP. Un agregado describe un conjunto de recursos de almacenamiento físicos.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Devuelve solo los agregados asociados con el ID de extremo especificado. Si no se proporciona ningún ID de extremo, el sistema enumera los agregados de todos los extremos de SnapMirror conocidos.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorAggregates	Una lista de los agregados disponibles en el sistema de almacenamiento ONTAP.	SnapMirrorAggregate cabina

Nuevo desde la versión

10.1

ListSnapMirrorEndpoints

La interfaz de usuario web del software Element utiliza el `ListSnapMirrorEndpoints` Método para enumerar todos los extremos de SnapMirror con los que se comunica el clúster de almacenamiento de Element.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Devolver sólo los objetos asociados a estos ID. Si no se proporcionan ID o la cabina está vacía, el método devuelve todos los ID de extremo de SnapMirror.	matriz en números enteros	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorEndpoints	Una lista de extremos de SnapMirror existentes.	SnapMirrorEndpoint cabina

Nuevo desde la versión

10.0

ListSnapMirrorLuns

La interfaz de usuario web del software Element utiliza el `ListSnapMirrorLuns` Método para enumerar la información de LUN para la relación de SnapMirror desde el clúster de ONTAP remoto.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Enumere solo la información de LUN asociada con el ID de extremo especificado.	entero	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
DestationVolume	El volumen de destino de la relación de SnapMirror.	SnapMirrorVolumeInfo	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
SnapMirrorLunInfos	Una lista de objetos que contienen información acerca de LUN de SnapMirror.	SnapMirrorLunInfo cabina

Nuevo desde la versión

10.1

ListSnapMirrorNetworkinterfaces

La interfaz de usuario web del software Element utiliza el `ListSnapMirrorNetworkInterfaces` Método para enumerar todas las interfaces de SnapMirror disponibles en un sistema ONTAP remoto.

Parámetro

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Devuelve sólo las interfaces de red asociadas con el identificador de punto final especificado. Si no se proporciona ningún ID de extremo, el sistema enumera las interfaces de todos los extremos de SnapMirror conocidos.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
InterfaceRole	Enumere sólo la interfaz de red que sirve la función especificada.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorNetworkinterfaces	Una lista de las interfaces de red de SnapMirror disponibles en el sistema de almacenamiento remoto de ONTAP.	SnapMirrornetworkInterface cabina

Nuevo desde la versión

10.1

ListSnapMirrorNodes

La interfaz de usuario web del software Element utiliza el `ListSnapMirrorNodes` Método para obtener una lista de nodos en un clúster de ONTAP remoto.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Si se proporciona, el sistema enumera los nodos del extremo con el snapMirrorEndpointID especificado. Si no se proporciona, el sistema enumera los nodos de todos los extremos de SnapMirror conocidos.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorNodes	Una lista de los nodos del clúster de ONTAP.	SnapMirrorNode cabina

Nuevo desde la versión

10.1

ListSnapMirrorPolicies

La interfaz de usuario web del software Element utiliza el `ListSnapMirrorPolicies` Método para enumerar todas las políticas de SnapMirror en un sistema de ONTAP remoto.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Enumere sólo las políticas asociadas al identificador de extremo especificado. Si no se proporciona ningún ID de extremo, el sistema enumera las políticas de todos los extremos de SnapMirror conocidos.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorPolicies	Una lista de políticas de SnapMirror en el sistema de almacenamiento de ONTAP.	SnapMirrorPolicy cabina

Nuevo desde la versión

10.1

ListSnapMirrorSchedules

La interfaz de usuario web del software Element utiliza el `ListSnapMirrorSchedules` Método para obtener una lista de las programaciones disponibles en un clúster de ONTAP remoto.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Si se proporciona, el sistema enumera las programaciones del extremo con el identificador de extremo de SnapMirror especificado. Si no se proporciona esta opción, el sistema enumera las programaciones de todos los extremos de SnapMirror conocidos.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorSchedules	Una lista de las programaciones de SnapMirror en el clúster de ONTAP remoto.	SnapMirrorJobScheduleCronInfo cabina

Nuevo desde la versión

10.1

ListSnapMirrorRelationship

La interfaz de usuario web del software Element utiliza el `ListSnapMirrorRelationships` Método para enumerar una o todas las relaciones

de SnapMirror en un clúster de almacenamiento de Element.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Enumere sólo las relaciones asociadas con el identificador de extremo especificado. Si no se proporciona ningún ID de extremo, el sistema enumera las relaciones de todos los extremos de SnapMirror conocidos.	entero	Ninguno	No
DestationVolume	Las relaciones de lista asociadas con el volumen de destino especificado.	SnapMirrorVolumeInfo	Ninguno	No
Volumen de origen	Enumere las relaciones asociadas con el volumen de origen especificado.	SnapMirrorVolumeInfo	Ninguno	No
vserver	Enumere las relaciones en el Vserver especificado.	cadena	Ninguno	No
ID de relación	Enumerar las relaciones asociadas con el ID de relación especificado.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorRelationship	Una lista de los objetos que contienen información acerca de las relaciones de SnapMirror.	SnapMirrorRelationship cabina

Nuevo desde la versión

10.1

ListSnapMirrorVolumes

La interfaz de usuario web del software Element utiliza el `ListSnapMirrorVolumes` Método para enumerar todos los volúmenes de SnapMirror disponibles en un sistema ONTAP remoto.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Enumere solo los volúmenes asociados con el ID de extremo especificado. Si no se proporciona ningún ID de extremo, el sistema enumera los volúmenes de todos los extremos de SnapMirror conocidos.	entero	Ninguno	No
vserver	Enumere los volúmenes alojados en el Vserver especificado. El Vserver debe ser del tipo "datos".	cadena	Ninguno	No
nombre	Enumere solo los volúmenes ONTAP con el nombre especificado.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
tipo	Enumere solo los volúmenes ONTAP del tipo especificado. Los posibles valores son los siguientes: • rw: Volúmenes de lectura y escritura • ls: Volúmenes de carga compartida • dp: Volúmenes de protección de datos	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorVolumes	Una lista de los volúmenes de SnapMirror disponibles en el sistema de almacenamiento ONTAP.	SnapMirrorVolume cabina

Nuevo desde la versión

10.1

ListSnapMirrorservidores

La interfaz de usuario web del software Element utiliza el `ListSnapMirrorVservers` Método para enumerar todos los vServers de SnapMirror disponibles en un sistema ONTAP remoto.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	Enumere sólo los vServers asociados con el identificador de extremo especificado. Si no se proporciona ningún ID de extremo, el sistema enumera los vServers de todos los extremos de SnapMirror conocidos.	entero	Ninguno	No
VserverType	Enumere solo los vServers del tipo especificado. Los posibles valores son los siguientes: • admin • sql server • nodo • sistema	cadena	Ninguno	No
Nombre del servidor virtual	Enumere solo los vServers con el nombre especificado.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorVServer	Una lista de vServers de SnapMirror disponibles en el sistema de almacenamiento de ONTAP.	SnapMirrorVServer cabina

Nuevo desde la versión

10.1

ModificySnapMirrorEndpoint

La interfaz de usuario web del software Element utiliza el `ModifySnapMirrorEndpoint` Método para cambiar el nombre y los atributos de gestión de un extremo de SnapMirror.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	El extremo de SnapMirror que se desea modificar.	entero	Ninguno	Sí
Gestión de IP	La nueva dirección IP de administración para el sistema ONTAP.	cadena	Ninguno	No
nombre de usuario	El nuevo nombre de usuario de gestión para el sistema ONTAP.	cadena	Ninguno	No
contraseña	La nueva contraseña de gestión para el sistema ONTAP.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorEndpoint	Información acerca del extremo de SnapMirror modificado.	SnapMirrorEndpoint

Nuevo desde la versión

10.0

ModificySnapMirrorEndpoint (no administrado)

El software Element utiliza esta versión de `ModifySnapMirrorEndpoint` Método para modificar los atributos del nombre o la dirección IP del clúster de almacenamiento de un extremo de SnapMirror no gestionado. No se pueden administrar extremos no

gestionados mediante las API de SnapMirror de Element. Deben gestionarse con las API o el software de gestión de ONTAP.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	El extremo de SnapMirror que se desea modificar.	entero	Ninguno	Sí
Nombre del clúster	Nuevo nombre del extremo.	cadena	Ninguno	No
Direcciones IP	La nueva lista de direcciones IP para un clúster de sistemas de almacenamiento ONTAP que se deben comunicar con este clúster de almacenamiento de Element.	matriz de cadenas	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorEndpoint	Información acerca del extremo de SnapMirror modificado.	SnapMirrorEndpoint

Nuevo desde la versión

10.3

ModificySnapMirrorRelationship

Puede utilizar `ModifySnapMirrorRelationship` cambiar los intervalos en los que se produce una snapshot programada. También puede eliminar o pausar una programación mediante este método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
DestationVolume	El volumen de destino de la relación de SnapMirror.	SnapMirrorVolumeinfo	Ninguno	Sí
MaxTransferRate	Especifica la tasa máxima de transferencia de datos entre los volúmenes en kilobytes por segundo. El valor predeterminado, 0, es ilimitado y permite que la relación de SnapMirror utilice completamente el ancho de banda de red disponible.	entero	Ninguno	No
PolicyName	Especifica el nombre de la política de SnapMirror de ONTAP para la relación.	cadena	Ninguno	No
Nombre de la pila	El nombre de la programación cron preexistente del sistema ONTAP que se utiliza para actualizar la relación SnapMirror.	cadena	Ninguno	No
SnapMirrorEndpointID	El ID de extremo del sistema de almacenamiento remoto de ONTAP se comunica con el clúster de almacenamiento de Element.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorRelationship	Objeto que contiene los atributos de relación de SnapMirror modificados.	SnapMirrorRelationship

Nuevo desde la versión

10.1

UpdateSnapMirrorRelationship

La interfaz de usuario web del software Element utiliza el `UpdateSnapMirrorRelationship` Método para que el volumen de destino de una relación de SnapMirror sea un reflejo actualizado del volumen de origen.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	El ID de extremo del sistema de almacenamiento remoto de ONTAP se comunica con el clúster de almacenamiento de Element.	entero	Ninguno	Sí
DestationVolume	El volumen de destino de la relación de SnapMirror.	SnapMirrorVolumeinfo	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
MaxTransferRate	Especifica la tasa máxima de transferencia de datos entre los volúmenes en kilobytes por segundo. El valor predeterminado, 0, es ilimitado y permite que la relación de SnapMirror utilice completamente el ancho de banda de red disponible.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorRelationship	Objeto que contiene información acerca de la relación actualizada de SnapMirror.	SnapMirrorRelationship

Nuevo desde la versión

10.1

QuiesceSnapMirrorRelationship

La interfaz de usuario web del software Element utiliza el `QuiesceSnapMirrorRelationship` Método para deshabilitar futuras transferencias de datos para una relación de SnapMirror. Si se está realizando una transferencia, el estado de la relación se convierte en "inactivo" hasta que se completa la transferencia. Si se cancela la transferencia actual, no se reiniciará. Puede volver a habilitar las transferencias de datos para la relación mediante el `ResumeSnapMirrorRelationship` Método API.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	El ID de extremo del sistema de almacenamiento remoto de ONTAP se comunica con el clúster de almacenamiento de Element.	entero	Ninguno	Sí
DestationVolume	El volumen de destino de la relación de SnapMirror.	SnapMirrorVolumeinfo	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorRelationship	Un objeto que contiene información acerca de la relación de SnapMirror en modo inactivo.	SnapMirrorRelationship

Nuevo desde la versión

10.1

ReumeSnapMirrorRelationship

La interfaz de usuario web del software Element utiliza el `ResumeSnapMirrorRelationship` Método para habilitar futuras transferencias para una relación de SnapMirror en modo inactivo.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	El ID de extremo del sistema de almacenamiento remoto de ONTAP se comunica con el clúster de almacenamiento de Element.	entero	Ninguno	Sí
DestationVolume	El volumen de destino de la relación de SnapMirror.	SnapMirrorVolumeinfo	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorRelationship	Objeto que contiene información acerca de la relación reanudada de SnapMirror.	SnapMirrorRelationship

Nuevo desde la versión

10.1

ResyncSnapMirrorRelationship

La interfaz de usuario web del software Element utiliza el `ResyncSnapMirrorRelationship` método para establecer o restablecer una relación de mirroring entre un extremo de origen y de destino. Cuando vuelve a sincronizar una relación, el sistema elimina las copias Snapshot en el volumen de destino que son más recientes que la copia Snapshot común y, a continuación, monta el volumen de destino como un volumen de protección de datos con la copia Snapshot común como la copia Snapshot exportada.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnapMirrorEndpointID	El ID de extremo del sistema de almacenamiento remoto de ONTAP se comunica con el clúster de almacenamiento de Element.	entero	Ninguno	Sí
DestationVolume	El volumen de destino de la relación de SnapMirror.	SnapMirrorVolumeinfo	Ninguno	Sí
MaxTransferRate	Especifica la tasa máxima de transferencia de datos entre los volúmenes en kilobytes por segundo. El valor predeterminado, 0, es ilimitado y permite que la relación de SnapMirror utilice completamente el ancho de banda de red disponible.	entero	Ninguno	No
Volumen de origen	El volumen de origen de la relación de SnapMirror.	SnapMirrorVolumeinfo	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SnapMirrorRelationship	Un objeto que contiene información sobre la relación de SnapMirror resynced.	SnapMirrorRelationship

Nuevo desde la versión

10.1

Métodos de la API de configuración del sistema

Los métodos de API de configuración del sistema le permiten obtener y establecer valores de configuración que se aplican a todos los nodos del clúster.

- DisablebmcColdReset
- DisableClusterSsh
- DisableSnmp
- EnablebmcColdReset
- EnableClusterSsh
- EnableSnmp
- GetBinAssignmentProperties
- GetClusterSshInfo
- GetClusterStructure
- GetFipsReport
- GetLldpConfig
- GetLldpInfo
- GetNodeFipsDrivesReport
- GetNtpInfo
- GetNvramInfo
- GetProtectionDomainLayout
- GetRemoteLoggingHosts
- GetSnmpACL
- GetSnmpInfo
- GetSnmpState
- GetSnmpTrapInfo
- GetSSLCertificate
- ListProtectionDomainLevels
- RemoveSSLCertificate
- ResetNetworkConfig
- ResetSupplementalTlsCiphers
- SetClusterStructure
- SetLldpConfig
- SetNtpInfo
- SetProtectionDomainLayout
- SetRemoteLoggingHosts
- SetSnmpACL
- SetSnmpInfo

- SetSnmpTrapInfo
- SetSSLCertificate
- SnmpSendTestTraps
- TestAddressAvailability

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

DisablebmcColdReset

Puede utilizar el `DisableBmcColdReset` Método para deshabilitar la tarea en segundo plano que restablece periódicamente el controlador de administración de placa base (BMC) para todos los nodos del clúster.

Parámetro

Este método no tiene parámetro de entrada.

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
CbmcResetDurationMinutes	Devuelve el tiempo transcurrido entre los intervalos de restablecimiento. El intervalo debe ser siempre 0 una vez que se complete el comando.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DisableBmcColdReset",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "cBmcResetDurationMinutes": 0
    }
}
```

Nuevo desde la versión

12.0

DisableClusterSsh

Puede utilizar el `DisableClusterSsh` Método para deshabilitar el servicio SSH para todo el clúster de almacenamiento. Cuando añada nodos al clúster de almacenamiento, los nuevos nodos heredan esta configuración en todo el clúster.

Parámetro

Este método no tiene parámetro de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
resultado	Un objeto JSON que contiene el estado del servicio SSH para el clúster de almacenamiento, el tiempo restante hasta que SSH esté deshabilitado y el estado del servicio SSH para cada nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DisableClusterSsh",
  "params": {
      },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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
    } ]
            }
    }
```

Nuevo desde la versión

10.3

DisableSnmp

Puede utilizar el `DisableSnmp` Método para deshabilitar SNMP en los nodos del clúster.

Parámetro

Este método no tiene parámetro de entrada.

Valor de retorno

Este método no tiene ningún valor devuelto.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DisableSnmp",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "result" : {},
  "id" : 1
}
```

Nuevo desde la versión

9.6

EnablebmcColdReset

Puede utilizar el `EnableBmcColdReset` Método para habilitar una tarea en segundo plano que restablece periódicamente el controlador de administración de placa base (BMC) para todos los nodos del clúster.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
tiempo de espera	El tiempo entre las operaciones de restablecimiento del BMC, en minutos.	entero	20160 minutos	No

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
CbmcResetDurationMinutes	Devuelve el tiempo transcurrido entre los intervalos de restablecimiento. El intervalo debe ser siempre 0 una vez que se complete el comando.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "EnableBmcColdReset",
    "params": {
                "timeout": 36000
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "cBmcResetDurationMinutes": 36000
    }
}
```

Nuevo desde la versión

12.0

EnableClusterSsh

Puede utilizar el `EnableClusterSsh` Método para habilitar el servicio SSH en todos los nodos del clúster de almacenamiento.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
duración	La cantidad de tiempo durante el cual se seguirá habilitando el servicio SSH.	cadena	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
resultado	Un objeto JSON que contiene el estado del servicio SSH para el clúster de almacenamiento, el tiempo restante hasta que SSH esté deshabilitado y el estado del servicio SSH para cada nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "EnableClusterSsh",
  "params": {
      "duration"  : "02:00:00.00"
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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
    } ]
            }
    }
```

Nuevo desde la versión

10.3

EnableSnmp

Puede utilizar el `EnableSnmp` Método para habilitar SNMP en nodos de clúster. Cuando habilita SNMP, la acción se aplica a todos los nodos del clúster, y los valores que se pasan sustituyen a todos los valores establecidos en cualquier llamada anterior a. `EnableSnmp`.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SnmpV3Enabled	Si se establece en true, SNMP v3 se habilita en cada nodo del clúster. Si se establece en false, se habilita SNMP v2.	booleano	falso	No

Valor de retorno

Este método no tiene ningún valor devuelto.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "EnableSnmp",
  "params": {
      "snmpV3Enabled"  : "true"
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuevo desde la versión

9.6

GetBinAssignmentProperties

Puede utilizar el `GetBinAssignmentProperties` método para recuperar las propiedades de asignación de bandeja en la base de datos.

Parámetro

Este método tiene los parámetros no input.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
propiedades	Detalla las propiedades de todas las asignaciones de bandejas actuales de la base de datos.	BinAssignmentProperties

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "GetBinAssignmentProperties",
    "params": {
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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": []
        }
    }
}
```


Nuevo desde la versión

12.0

GetClusterSshInfo

Puede utilizar el `GetClusterSshInfo` Método para consultar el estado del servicio SSH de todo el clúster de almacenamiento.

Parámetro

Este método no tiene parámetro de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
resultado	Un objeto JSON que contiene el estado del servicio SSH para el clúster de almacenamiento, el tiempo restante hasta que SSH esté deshabilitado y el estado del servicio SSH para cada nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:


```
{
  "method": "GetClusterSshInfo",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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
    } ]
            }
    }
```

Nuevo desde la versión

10.3

GetClusterStructure

Puede utilizar el `GetClusterStructure` método para realizar una copia de seguridad de la información de configuración actual del clúster de almacenamiento. Si la configuración del clúster de almacenamiento cambia mientras se ejecuta este método, el contenido del backup de configuración será impredecible. Puede guardar estos datos en un archivo de texto y restaurarlos en otros clústeres o el mismo clúster en caso de desastre.

Parámetro

Este método no tiene parámetro de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
resultado	Un objeto JSON que contiene la información de configuración del clúster de almacenamiento actual.	ClusterStructure

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetClusterStructure",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result" : <clusterStructure object containing configuration
information>
    }
```

Nuevo desde la versión

10.3

GetFipsReport

Puede utilizar el `GetFipsReport` Método para comprobar el estado de soporte de la función de cifrado FIPS 140-2 de todos los nodos del clúster de almacenamiento.

Parámetro

Este método no tiene parámetro de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
resultado	Un objeto JSON que contiene el estado de la compatibilidad con la función FIPS 140-2 para cada nodo e información sobre errores de cada nodo que no responde a la consulta.	FipsReport

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetFipsReport",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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"
               }
        }
    ]
    }
}
```


Nuevo desde la versión

10.3

GetLldpConfig

Puede utilizar el `GetLldpConfig` Método para obtener la configuración del protocolo de detección de nivel de enlace (LLDP) para cada nodo de un clúster de almacenamiento.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
LldpConfig	Información sobre la configuración de LLDP en el clúster de almacenamiento.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetLldpConfig",
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": null,
        "result": {
            "lldpConfig": {
                "enableLldp": true,
                "enableMed": false,
                "enableOtherProtocols": true
        }
    }
}
```

GetLldpInfo

Puede utilizar el `GetLldpInfo` Método para obtener la configuración del protocolo de detección de capa de enlace (LLDP) para cada nodo de un clúster de almacenamiento o un nodo de almacenamiento individual.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
LldpInfo	Información sobre el chasis, la interfaz y la configuración de LLDP vecinas para cada nodo de un clúster de almacenamiento.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetLldpInfo",
   "id" : 1
}
```

Ejemplo de respuesta

Debido a la longitud de este ejemplo de respuesta, se documenta en un tema complementario.

Nuevo desde la versión

11.0

Obtenga más información

GetLldpInfo

GetNodeFipsDrivesReport

Puede utilizar el `GetNodeFipsDrivesReport` Método para comprobar el estado de la funcionalidad de cifrado de unidades FIPS 140-2 de un solo nodo en el clúster de almacenamiento. Se debe ejecutar este método contra un nodo de almacenamiento individual.

Parámetro

Este método no tiene parámetro de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
PsDrives	Un objeto JSON que contiene el estado de la compatibilidad con la función FIPS 140-2 para este nodo. Los posibles valores son los siguientes: • None: El nodo no es compatible con FIPS. • Parcial: El nodo es compatible con FIPS, pero no todas las unidades del nodo son unidades FIPS. • Ready: El nodo es compatible con FIPS y todas las unidades del nodo son unidades FIPS (o no existen unidades).	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetNodeFipsDrivesReport",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "fipsDrives": "None"
    }
}
```

Nuevo desde la versión

11.5

GetNtpInfo

Puede utilizar el `GetNtpInfo` Método para obtener la información de configuración del

protocolo de hora de red (NTP) actual.

Parámetro

Este método no tiene parámetro de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
servidores	Lista de servidores NTP.	matriz de cadenas
cliente de envío	Indica si los nodos del clúster están escuchando mensajes de NTP de retransmisión. Los posibles valores son los siguientes: • verdadero • falso	booleano

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetNtpInfo",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {
    "broadcastclient" : false,
    "servers" : [ "us.pool.ntp.org" ]
   }
}
```

Nuevo desde la versión

9.6

GetNvramInfo

Puede utilizar el `GetNvramInfo` Método para obtener información de cada nodo acerca de la tarjeta NVRAM.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
fuerza	El parámetro force debe estar incluido en este método para poder ejecutarse correctamente en todos los nodos del clúster.	booleano	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
NvramInfo	Matrices de eventos y errores detectados en la tarjeta NVRAM.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetNvramInfo",
  "params": {
      "force": true
      },
  "id" : 1
}
```

Ejemplo de respuesta

Debido a la longitud de este ejemplo de respuesta, se documenta en un tema complementario.

Nuevo desde la versión

9.6

Obtenga más información

GetNvramInfo

GetProtectionDomainLayout

Puede utilizar el `GetProtectionDomainLayout` método para obtener toda la información del dominio de protección de un clúster, incluido el chasis y el dominio de protección personalizado en cada nodo.

Parámetro

Este método tiene los parámetros no input.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
ProtectionDomainLayout	Lista de nodos, cada uno con sus dominios de protección asociados.	Lista JSON de "ProtectionDomains de nodo" objetos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetProtectionDomainLayout",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
        }
      ]
    }
```

```
      ]
    }
}
```

Nuevo desde la versión

12.0

GetRemoteLoggingHosts

Puede utilizar el `GetRemoteLoggingHosts` método para obtener la lista actual de servidores de registro.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
RemoteHosts	Lista de direcciones IP e información de puerto sobre los hosts configurados para recibir información de registro reenviado.	LoggingServer cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "id": 3386609,
   "method": "GetRemoteLoggingHosts",
   "params": {}
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 3386609,
   "result": {
      "remoteHosts": [
         {
           "host": "172.16.1.20",
           "port": 10514
         },
         {
           "host": "172.16.1.25"
         }
      ]
   }
}
```

Nuevo desde la versión

9.6

Obtenga más información

SetRemoteLoggingHosts

GetSnmpACL

Puede utilizar el `GetSnmpACL` Método para obtener los permisos de acceso SNMP actuales en los nodos del clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
redes	Lista de redes y qué tipo de acceso tienen a los servidores SNMP que se ejecutan en los nodos del clúster. Este valor se presenta si SNMP v3 está deshabilitado.	red cabina

Nombre	Descripción	Tipo
UsmUsers	Lista de usuarios y el tipo de acceso que tienen a los servidores SNMP que se ejecutan en los nodos del clúster. Este valor se presenta si SNMP v3 está habilitado.	UsumUsuario cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method": "GetSnmpACL",
"params": {},
"id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {
     "usmUsers"  : [
       {
          "name": "jdoe",
          "access": "rouser",
          "secLevel": "priv",
          "password": "mypassword",
          "passphrase": "mypassphrase",
       }
     ]
   }
}
```

Nuevo desde la versión

9.6

GetSnmpInfo

Puede utilizar el `GetSnmpInfo` Método para obtener la información de configuración del protocolo simple de gestión de red (SNMP) actual.

Parámetros

GetSnmpInfo queda obsoleto para versiones posteriores a la versión 8.0 del elemento. La GetSnmpState y.. SetSnmpACL Los métodos sustituyen al método GetSnmpInfo.

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
redes	Lista de redes y tipos de acceso habilitados para SNMP. **Nota:** las redes sólo se muestran si SNMP v3 está desactivado.	red
activado	Indica si los nodos del clúster están configurados para SNMP. Los posibles valores son los siguientes: • verdadero • falso	booleano
SnmpV3Enabled	Si el nodo del clúster está configurado para SNMP v3. Los posibles valores son los siguientes: • verdadero • falso	booleano
UsmUsers	Si se habilita SNMP v3, se devuelve una lista con los parámetros de acceso de usuario para SNMP desde el clúster. Este se devuelve en lugar del parámetro Networks.	UsumUsuario

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetSnmpInfo",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id" : 1,
   "result" : {
      "enabled" : true,
      "networks" : [
         {
            "access" : "rosys",
            "cidr" : 0,
            "community" : "public",
            "network" : "localhost"
         }
      ]
   }
}
```

Nuevo desde la versión

9.6

Obtenga más información

- GetSnmpState
- SetSnmpACL

GetSnmpState

Puede utilizar el `GetSnmpState` Método para obtener el estado actual de la función SNMP.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
activado	Los posibles valores son los siguientes: • verdadero • falso El valor predeterminado es FALSE. Devuelve TRUE si los nodos del clúster se han configurado para SNMP.	booleano
SnmpV3Enabled	Los posibles valores son los siguientes: • verdadero • falso El valor predeterminado es FALSE. Devuelve TRUE si los nodos del clúster están configurados para SNMP v3.	booleano

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetSnmpState",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {
   "enabled": true,
   "snmpV3Enabled": false
   }
}
```

Nuevo desde la versión

9.6

Obtenga más información

SetSnmpACL

GetSnmpTrapInfo

Puede utilizar el `GetSnmpTrapInfo` Método para obtener información actual sobre la configuración de la captura SNMP.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
TrapRecipients	Lista de hosts que van a recibir los retos generados por el clúster.	SnmpTrapRecipient cabina
ClusterFaultTrapsEnabled	El valor true indica que se configura una notificación solidFireClusterFaultNotification para enviarse a la lista de destinatarios de capturas cuando se registra un fallo del clúster.	booleano
ClusterFaultResolvedTrapsEnabled	El valor true indica que una notificación solidFireClusterFaultResolvedNotification está configurada para enviarse a la lista de destinatarios de la captura cuando se resuelve un error del clúster.	booleano
ClusterEventTrapsEnabled	El valor true indica que se ha configurado solidFireClusterEventNotification para que se envíe a la lista de destinatarios de capturas cuando se registra un evento de clúster.	booleano

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method":"GetSnmpTrapInfo"
   "params":{},
   "id":1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
     }
   ]
 }
}
```

Nuevo desde la versión

9.6

GetSSLCertificate

Puede utilizar el `GetSSLCertificate` Método para recuperar el certificado SSL activo actualmente en los nodos de almacenamiento del clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
certificado	El texto completo codificado con PEM del certificado.	cadena
detalles	La información descodificada del certificado.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method" : "GetSSLCertificate",
    "params" : {},
    "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```
{
    "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"
        }
    }
}
```


Nuevo desde la versión

10.0

ListProtectionDomainLevels

Puede utilizar el `ListProtectionDomainLevels` método para enumerar los niveles de tolerancia y resiliencia del clúster de almacenamiento. Los niveles de tolerancia indican la capacidad del clúster para seguir leyendo y escribiendo datos en caso de fallo, y los niveles de resiliencia indican la capacidad del clúster de almacenamiento para recuperarse de forma automática a partir de uno o más fallos.

Parámetro

Este método no tiene parámetro de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
ProtectionDomainLevels	Una lista de los diferentes niveles de dominio de protección, donde cada uno proporciona información sobre la tolerancia y la resiliencia del clúster de almacenamiento.	ProtectionDomainLevel

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListProtectionDomainLevels",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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
                    }
                }
            ]
        }
}
```


Nuevo desde la versión

11.0

RemoveSSLCertificate

Puede utilizar el `RemoveSSLCertificate` Método para quitar el certificado SSL de usuario y la clave privada de los nodos de almacenamiento del clúster. Después de eliminar el certificado y la clave privada, los nodos de almacenamiento se configuran para usar el certificado predeterminado y la clave privada.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method" : "RemoveSSLCertificate",
    "params" : {},
    "id" : 3
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id" : 3,
    "result" : {}
}
```

Nuevo desde la versión

10.0

ResetNetworkConfig

Puede utilizar el `ResetNetworkConfig` método para ayudar a resolver problemas de configuración de red para un nodo individual. Este método restablece la configuración de red de un nodo individual a los valores predeterminados de fábrica.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ResetNetworkConfig",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método no devuelve una respuesta.

Nuevo desde la versión

11.0

ResetSupplementalTlsCiphers

Puede utilizar el `ResetSupplementalTlsCiphers` Método para restaurar la lista de cifrados adicionales TLS al valor predeterminado. Puede utilizar este método en el clúster completo.

Parámetro

Este método no tiene parámetros de entrada.

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ResetSupplementalTlsCiphers",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuevo desde la versión

11.3

SetClusterStructure

Puede utilizar el `SetClusterStructure` método para restaurar la información de configuración del clúster de almacenamiento desde un backup. Al llamar al método, pasa el objeto clusterStructure que contiene la información de configuración que desea restaurar como parámetro params.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo
parámetros	Un objeto JSON que contiene la información de configuración del clúster de almacenamiento actual.	ClusterStructure

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
resultado	Controlador de resultados asíncrono.	Establish asyncHandle

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "SetClusterStructure",
  "params": <insert clusterStructure object here>,
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result" : {
    "asyncHandle": 1
    }
}
```

Nuevo desde la versión

10.3

SetLldpConfig

Puede utilizar el `SetLldpConfig` Método para configurar la configuración del protocolo de detección de nivel de enlace (LLDP) para un clúster de almacenamiento.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
EnableOtherProtocols	Permite el uso automático de otros protocolos de detección: CDP, FDP, EDP y SONMP.	booleano	verdadero	No
EnableMed	Habilite Media Endpoint Discovery (LLDP-MED).	booleano	falso	No
EnableLldp	Habilite o deshabilite LLDP.	booleano	verdadero	No

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
LIdpConfig	Información sobre la configuración de LLDP actual del clúster de almacenamiento, incluida la configuración recientemente modificada.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 3920,
  "method":"SetLldpConfig",
    "params": {
        "lldpConfig": {
            "enableMed": true
        }
    }
  }
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 3920,
  "result": {
    "lldpConfig": {
        "enableLldp": true,
        "enableMed": true,
        "enableOtherProtocols": true
     }
  }
}
```

SetNtpInfo

Puede utilizar el `SetNtpInfo` Método para configurar NTP en los nodos del clúster. Los valores que establece con esta interfaz se aplican a todos los nodos del clúster. Si un servidor de retransmisión NTP transmite periódicamente información de hora a la red, los nodos se pueden configurar como clientes de retransmisión.

Parámetros

> Asegúrese de usar los servidores NTP internos a la red en lugar de los que vienen predeterminados en la instalación.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
servidores	La lista de servidores NTP que se van a añadir a cada configuración de NTP de nodo.	matriz de cadenas	Ninguno	Sí
cliente de envío	Habilita cada nodo del clúster como cliente de retransmisión.	booleano	falso	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "SetNtpInfo",
   "params": {
     "servers"  : [
       "ntpserver1.example.org",
       "ntpserver2.example.org",
       "ntpserver3.example.org"
     ],
     "broadcastclient" : false
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id" : 1,
    "result" : {}
}
```

Nuevo desde la versión

9.6

SetProtectionDomainLayout

Puede utilizar el `SetProtectionDomainLayout` método para asignar nodos a dominios de protección personalizados.

Debe proporcionarse información para todos los nodos activos del clúster. No se puede proporcionar información para los nodos inactivos. Todos los nodos de un chasis determinado deben asignarse al mismo dominio de protección personalizado. Debe proporcionarse el mismo protecDomainType para todos los nodos. ProtectionDomainTypes que no son personalizadas, como nodo y chasis, no deben incluirse. Si se proporciona alguna de estas opciones, se ignoran los dominios de protección personalizados y se devuelve un error adecuado.

Los dominios de protección personalizados no se admiten con las siguientes configuraciones:

- Los clústeres de almacenamiento que contienen un chasis compartido
- Clústeres de almacenamiento de dos nodos

El método devuelve un error cuando se utiliza en los clústeres de almacenamiento con estas configuraciones.

Parámetro

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ProtectionDomainLayout	Información de dominio de protección para cada nodo.	Lista JSON de "ProtectionDomains de nodo" objetos.	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
ProtectionDomainLayout	Lista de nodos, cada uno con sus dominios de protección asociados.	Lista JSON de "ProtectionDomains de nodo" objetos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "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"
          }
        ]
      }
    ]
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```
{
  "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"
            }
          ]
        }
      ]
    }
}
```

Nuevo desde la versión

12.0

SetRemoteLoggingHosts

Puede utilizar el `SetRemoteLoggingHosts` método para configurar el registro remoto de los nodos en el clúster de almacenamiento en un servidor de registro o servidores centralizados. El registro remoto se realiza a través de TCP utilizando el puerto predeterminado 514. Esta API no se añade a los hosts de registro existentes. En su lugar, sustituye lo que existe actualmente con nuevos valores especificados por este método API. Puede utilizar `GetRemoteLoggingHosts` para determinar cuáles son los hosts de registro actuales y, a continuación, utilizarlos `SetRemoteLoggingHosts` para definir la lista deseada de hosts de registro actuales y nuevos.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
RemoteHosts	Lista de hosts que son destinatarios de mensajes de registro.	LoggingServer cabina	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "id": 1,
   "method": "SetRemoteLoggingHosts",
   "params": {
     "remoteHosts": [
        {
          "host": "172.16.1.20",
          "port": 10514
        },
        {
          "host": "172.16.1.25"
        }
      ]
   }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id" : 1,
    "result" : {}
}
```

Nuevo desde la versión

9.6

Obtenga más información

GetRemoteLoggingHosts

SetSnmpACL

Puede utilizar el `SetSnmpACL` Método para configurar permisos de acceso SNMP en los nodos del clúster. Los valores establecidos con esta interfaz se aplican a todos los nodos del clúster y los valores que se pasan reemplazan a todos los valores establecidos en

cualquier llamada anterior a. `SetSnmpACL`. Tenga también en cuenta que los valores establecidos con esta interfaz reemplazan todos los valores de red o usmUsers establecidos con `SetSnmpInfo` método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
redes	Lista de redes y qué tipo de acceso tienen a los servidores SNMP que se ejecutan en los nodos del clúster. Consulte objeto de red SNMP para obtener los valores de red posibles. Este parámetro es necesario si SNMP v3 está deshabilitado.	red	Ninguno	No
UsmUsers	Lista de usuarios y el tipo de acceso que tienen a los servidores SNMP que se ejecutan en los nodos del clúster. Este parámetro es necesario si SNMP v3 está habilitado.	UsumUsuario	Ninguno	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "SetSnmpACL",
  "params": {
    "usmUsers"  : [
      {
         "name": "jdoe",
         "access": "rouser",
         "secLevel": "priv",
         "password": "mypassword",
         "passphrase": "mypassphrase",
      }
    ]
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuevo desde la versión

9.6

Obtenga más información

SetSnmpInfo

SetSnmpInfo

Puede utilizar el `SetSnmpInfo` Método para configurar las versiones 2 y 3 de SNMP en nodos de clúster. Los valores establecidos con esta interfaz se aplican a todos los nodos del clúster y los valores que se pasan reemplazan a todos los valores establecidos en cualquier llamada anterior a. `SetSnmpInfo`.

Parámetros

> SetSnmpInfo queda obsoleto para las versiones 6.0 y posteriores de los elementos. Utilice la EnableSnmp y.. SetSnmpACL en su lugar, los métodos.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
redes	Lista de redes y qué tipo de acceso tienen a los servidores SNMP que se ejecutan en los nodos del clúster. Consulte SNMP red objeto para los posibles valores. Este parámetro solo es necesario para SNMP v2.	red cabina	Ninguno	No
activado	Si se establece en true, se habilita SNMP en cada nodo del clúster.	booleano	falso	No
SnmpV3Enabled	Si se establece en true, SNMP v3 se habilita en cada nodo del clúster.	booleano	falso	No
UsmUsers	Si SNMP v3 está habilitado, este valor se debe pasar en lugar del parámetro Networks. Este parámetro es necesario únicamente para SNMP v3.	UsumUsuario	Ninguno	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud con SNMP v3 habilitado

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method":"SetSnmpInfo",
"params":{
    "enabled":true,
    "snmpV3Enabled":true,
    "usmUsers":[
      {
        "name":"user1",
        "access":"rouser",
        "secLevel":"auth",
        "password":"namex1",
        "passphrase":"yourpassphrase"
      }
    ]
  },
 "id":1
}
```

Ejemplo de solicitud con SNMP v2 habilitado

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method":"SetSnmpInfo",
"params":{
    "enabled":true,
    "snmpV3Enabled":false,
    "networks":[
      {
        "community":"public",
        "access":"ro",
        "network":"localhost",
      }
    ]
  },
  "id":1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1
  "result" :{
  }
}
```

Nuevo desde la versión

9.6

SetSnmpTrapInfo

Puede utilizar el `SetSnmpTrapInfo` Método para habilitar y deshabilitar la generación de notificaciones SNMP (capturas) del clúster y especificar el conjunto de hosts que reciben las notificaciones. Los valores que se pasan con cada uno de ellos `SetSnmpTrapInfo` llamada a método reemplaza todos los valores establecidos en cualquier llamada anterior.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo
TrapRecipients	Lista de hosts que reciben los retos generados por el clúster de almacenamiento. Se requiere al menos un objeto si se habilita alguno de los tipos de solapamiento. Este parámetro solo es necesario si alguno de los parámetros booleanos se establece en TRUE. (No hay un valor predeterminado. No es obligatorio).	SnmpTrapRecipient cabina
ClusterFaultTrapsEnabled	Si se establece en true, se envía una notificación de fallo del clúster correspondiente a la lista configurada de destinatarios de capturas cuando se registra un fallo en el clúster. (Valor predeterminado: FALSE. No es obligatorio).	booleano

Nombre	Descripción	Tipo
ClusterFaultResolvedTrapsEnabled	Si se establece en true, se envía una notificación de fallo resuelto del clúster correspondiente a la lista de destinatarios de capturas configurados cuando se resuelve un fallo del clúster. (Valor predeterminado: FALSE. No es obligatorio).	booleano
ClusterEventTrapsEnabled	Si se establece en true, se envía una notificación de eventos del clúster correspondiente a la lista configurada de destinatarios de capturas cuando se registra un evento del clúster. (Valor predeterminado: FALSE. No es obligatorio).	booleano

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method":"SetSnmpTrapInfo",
"params":{
    "clusterFaultTrapsEnabled":true,
    "clusterFaultResolvedTrapsEnabled":true,
    "clusterEventTrapsEnabled":true,
    "trapRecipients":[
    {
      "host":"192.30.0.10",
      "port":162,
      "community":"public"
    }
   ]
  },
  "id":1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id" : 1,
    "result" : {}
}
```

Nuevo desde la versión

9.6

SetSSLCertificate

Puede utilizar el `SetSSLCertificate` Método para establecer un certificado SSL de usuario y una clave privada para los nodos de almacenamiento del clúster.

Después de usar la API, debe reiniciar el nodo de gestión.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
certificado	La versión de texto codificada en PEM del certificado. **Nota:** al configurar un certificado de nodo o clúster, el certificado debe incluir la extensión extendedKeyUsage para serverAuth. Esta extensión permite utilizar el certificado sin errores en los sistemas operativos y exploradores comunes. Si la extensión no está presente, la API rechazará el certificado como no válido.	cadena	Ninguno	Sí
Privatekey	La versión de texto codificada con PEM de la clave privada.	cadena	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "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
}
```


Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```
{
    "id" : 2,
    "result" : {}
}
```


Nuevo desde la versión

10.0

SnmpSendTestTraps

`SnmpSendTestTraps` Permite probar la funcionalidad SNMP para un clúster. Este método indica al clúster que envíe capturas SNMP de prueba al administrador SNMP configurado actualmente.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
estado	Estado de la prueba.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "SnmpSendTestTraps",
    "params": {},
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {
      "status": "complete"
   }
}
```

Nuevo desde la versión

9.6

TestAddressAvailability

Puede utilizar el `TestAddressAvailability` Método para comprobar si hay una determinada dirección IP en uso en una interfaz dentro del clúster de almacenamiento.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
interfaz	La interfaz de red de destino (como eth0, Bond10G, etc.).	cadena	Ninguno	Sí
dirección	La dirección IP que se va a buscar en la interfaz de destino.	cadena	Ninguno	Sí
VirtualNetworkTag	El ID de VLAN de destino.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
tiempo de espera	Tiempo de espera en segundos para probar la dirección de destino.	entero	5	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
dirección	La dirección IP probada.	cadena
disponible	True si la dirección IP solicitada está en uso y FALSE si no lo está.	booleano

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "TestAddressAvailability",
    "params": {
        "interface": "Bond10G",
        "address": "10.0.0.1",
        "virtualNetworkTag": 1234
    }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "address":"10.0.0.1",
        "available": true
    }
}
```

Nuevo desde la versión

11.0

Métodos de API de redes múltiples inquilinos

Las redes multitenant en clústeres de almacenamiento de Element permiten que el tráfico entre varios clientes en redes lógicas independientes se conecten a un clúster de almacenamiento de Element sin enrutamiento de la capa 3.

Las conexiones al clúster de almacenamiento se separan en la pila de redes mediante el etiquetado de VLAN.

Requisitos previos para configurar una red virtual multitenant

- Se debe haber identificado el bloque de direcciones IP de red de cliente que se asignarán a las redes virtuales en los nodos de almacenamiento.
- Se debe haber identificado la dirección IP de red de almacenamiento de cliente (SVIP) que se usará como extremo para todo el tráfico de almacenamiento de.

Orden de operaciones de red virtual

1. Utilice el método AddVirtualNetwork para aprovisionar en lote las direcciones IP que introduzca.

   Después de añadir una red virtual, el clúster realiza de forma automática los siguientes pasos:

   - Cada nodo de almacenamiento crea una interfaz de red virtual.
   - A cada nodo de almacenamiento se le asigna una dirección VLAN que se puede enrutar con la SVIP virtual.
   - Las direcciones IP de VLAN persisten en cada nodo en el caso de que se reinicie un nodo.
2. Cuando se asignan la interfaz de red virtual y las direcciones VLAN, es posible asignar el tráfico de red de cliente a la SVIP virtual.

Obtenga más información

- Convenciones de nomenclatura de redes virtuales
- AddVirtualNetwork
- ModificyVirtualNetwork
- ListVirtualNetworks
- RemoveVirtualNetwork
- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Convenciones de nomenclatura de redes virtuales

Los sistemas de almacenamiento de NetApp Element utilizan números que aumentan monotónicamente como identificadores únicos para todos los objetos del sistema.

Cuando se crea un volumen nuevo, el nuevo volumeID es un incremento de exactamente 1. Esta convención

sucede con las redes virtuales en los clústeres de almacenamiento que ejecutan el software Element. La primera red virtual que se crea en un clúster de elementos tiene un VirtualNetworkID de 1. Este ID no es lo mismo que un número de etiqueta de VLAN.

Puede utilizar VirtualNetworkID y VirtualNetworkTag (etiqueta VLAN) indistintamente si se indica en los métodos API.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

AddVirtualNetwork

Puede utilizar el `AddVirtualNetwork` método para añadir una red virtual nueva a la configuración de un clúster.

Cuando se añade una red virtual, se crea una interfaz para cada nodo y cada interfaz requiere una dirección IP de red virtual. La cantidad de direcciones IP especificada como parámetro para este método API debe ser igual o mayor que la cantidad de nodos del clúster. El sistema aprovisiona de forma masiva direcciones de red virtual y las asigna a los nodos individuales de forma automática. No es necesario asignar direcciones de red virtual a los nodos de forma manual.

El método AddVirtualNetwork sólo se utiliza para crear una nueva red virtual. Si desea realizar cambios en una red virtual existente, utilice ModificyVirtualNetwork método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Bloqueos de direcciones	El rango exclusivo de direcciones IP que se incluirán en la red virtual. Miembros requeridos para el objeto: • Start: El inicio del rango de direcciones IP. (cadena) • Size: El número de direcciones IP que se van a incluir en el bloque. (entero)	Cabina de objetos JSON	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
puerta de enlace	La dirección IP de una puerta de enlace de la red virtual. Este parámetro solo es válido si el parámetro Namespace está configurado en TRUE.	cadena	Ninguno	No
nombre	Un nombre definido por el usuario para la nueva red virtual.	cadena	Ninguno	Sí
espacio de nombres	Cuando se establece en true, habilita la funcionalidad VLAN de almacenamiento enrutable mediante la creación y configuración de un espacio de nombres y la red virtual incluida en él.	booleano	Ninguno	No
máscara de red	Máscara de red exclusiva para la red virtual que se está creando.	cadena	Ninguno	Sí
svip	La dirección IP de almacenamiento exclusiva para la red virtual que se está creando.	cadena	Ninguno	Sí
VirtualNetworkTag	Una etiqueta de red virtual (VLAN) única. Los valores admitidos son de 1 a 4094.	entero	Ninguno	Sí

Nota: los parámetros de red virtual deben ser únicos para cada red virtual cuando se establece el espacio de nombres en FALSE.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Cód. Virtual	El ID de red virtual de la nueva red virtual.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "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
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result":
      {
        "virtualNetworkID": 5
   }
}
```

Nuevo desde la versión

9.6

ModificyVirtualNetwork

Puede utilizar el `ModifyVirtualNetwork` método para cambiar los atributos de una red virtual existente.

Este método permite agregar o quitar bloques de direcciones, cambiar la máscara de red o modificar el nombre o la descripción de la red virtual. También se puede utilizar para habilitar o deshabilitar espacios de nombres, así como para agregar o quitar una puerta de enlace si los espacios de nombres están habilitados en la red virtual.

Este método requiere virtualNetworkID o virtualNetworkTag como parámetro, pero no ambos.

PRECAUCIÓN:

Habilitar o deshabilitar la funcionalidad VLAN de almacenamiento enrutable para una red virtual existente cambiando el parámetro Namespace interrumpe cualquier tráfico gestionado por la red virtual. Lo mejor es cambiar el parámetro Namespace durante una ventana de mantenimiento programada.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Cód. Virtual	Identificador único de la red virtual que se va a modificar. Este es el ID de red virtual que asigna el clúster.	entero	Ninguno	No
VirtualNetworkTag	La etiqueta de red que identifica la red virtual que se desea modificar.	entero	Ninguno	No

Bloqueos de direcciones	El nuevo bloque de direcciones que se debe establecer para esta red virtual. Esto puede incluir nuevos bloques de direcciones para añadir al objeto existente o omitir los bloques de direcciones no utilizados que se deban eliminar. También puede ampliar o reducir el tamaño de los bloques de direcciones existentes. Sólo puede aumentar el tamaño de los bloqueos de direcciones iniciales de un objeto de red virtual; nunca puede reducirlo. Miembros requeridos para este objeto: • Start: El inicio del rango de direcciones IP. (cadena) • Size: El número de direcciones IP que se van a incluir en el bloque. (entero)	Objeto JSON	Ninguno	No
puerta de enlace	La dirección IP de una puerta de enlace de la red virtual. Este parámetro solo es válido si el parámetro Namespace está configurado en TRUE.	cadena	Ninguno	No

atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
nombre	El nuevo nombre de la red virtual.	cadena	Ninguno	No
espacio de nombres	Cuando se establece en true, habilita la funcionalidad VLAN de almacenamiento enrutable volviendo a la red virtual y configurando un espacio de nombres para que la contenga. Cuando se establece en false, se deshabilita la funcionalidad VRF para la red virtual. Si se cambia este valor, se interrumpe el tráfico que funciona con esta red virtual.	booleano	Ninguno	No
máscara de red	Nueva máscara de red para esta red virtual.	cadena	Ninguno	No
svip	La dirección IP virtual de almacenamiento para esta red virtual. La SVIP para una red virtual no se puede modificar. Debe crear una red virtual nueva para usar una dirección SVIP diferente.	cadena	Ninguno	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "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
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
  }
}
```

Nuevo desde la versión

9.6

ListVirtualNetworks

Puede utilizar el `ListVirtualNetworks` método para enumerar todas las redes virtuales configuradas para el clúster.

Puede utilizar este método para comprobar la configuración de red virtual en el clúster. No hay parámetros necesarios para este método. Sin embargo, para filtrar los resultados, puede pasar uno o más valores virtualNetworkID o virtualNetworkTag.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Cód. Virtual	ID de red para filtrar la lista de una sola red virtual.	entero	Ninguno	No
VirtualNetworkTag	Etiqueta de red para filtrar la lista de una sola red virtual.	entero	Ninguno	No
VirtualNetworkIDs	ID de red que se incluirán en la lista.	matriz en números enteros	Ninguno	No
VirtualNetworkTags	Etiqueta de red que se incluirá en la lista.	matriz en números enteros	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Redes de virtualización	Objeto que contiene direcciones IP de red virtual.	VirtualNetwork

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListVirtualNetworks",
  "params": {
     "virtualNetworkIDs": [5,6]
   },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```
{
  "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
     },
    {
   }
  ]
}
```


Nuevo desde la versión

9.6

RemoveVirtualNetwork

Puede utilizar el `RemoveVirtualNetwork` método para quitar una red virtual añadida previamente.

Este método requiere virtualNetworkID o virtualNetworkTag como parámetro, pero no ambos.

No puede quitar una red virtual si hay iniciadores asociados. En primer lugar, anule la asociación de los iniciadores y, a continuación, quite la red virtual.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Cód. Virtual	ID de red que identifica la red virtual que se desea quitar.	entero	Ninguno	Sí
VirtualNetworkTag	Etiqueta de red que identifica la red virtual que se va a quitar.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "RemoveVirtualNetwork",
  "params": {
     "virtualNetworkID": 5
    }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {}
}
```

Nuevo desde la versión

9.6

Métodos de API de volumen

Los métodos de la API de volúmenes del software Element permiten gestionar volúmenes que residen en un nodo de almacenamiento. Puede crear, modificar, clonar y eliminar volúmenes con estos métodos. También puede usar métodos de API de volúmenes para recopilar y mostrar mediciones de datos de un volumen.

- CancelClone
- CancelGroupClone
- CloneMultipleVolumes
- CloneVolume
- CopyVolume
- QoCreateSPolicy
- CreateVolume
- CreateBackupTarget
- QoDeleteSPolicy

- DeleteVolume
- DeleteVolumes
- GetBackupTarget
- GetVolumeStats
- GetDefaultQoS
- GetQoSPolicy
- GetVolumeCount
- GetVolumeEffect
- ListActiveVolumes
- ListBackupTargets
- ListBulkVolumeJobs
- ListDeletedVolumes
- ListQoSPolicies
- ListSyncJobs
- ListVolumeQoSHistogramas
- ListVolumes
- ListVolumeStats
- ListVolumesForAccount
- ListVolumeStatsByAccount
- ListVolumeStatsByVirtualVolume
- ListVolumeStatsByVolume
- ListVolumeStatsByVolumeAccessGroup
- ModifyBackupTarget
- ModifyQoSPolicy
- Volumen ModificíoVolume
- ModificyVolumes
- PurgeDeletedVolume
- PurgeDeletedVolumes
- RemoveBackupTarget
- RestoreDeletedVolume
- SetDefaultQoS
- StartBulkVolumeRead
- StartBulkVolumeWrite
- UpdateBulkVolumeStatus

Obtenga más información

- "Documentación de SolidFire y el software Element"

- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

CancelClone

Puede utilizar el `CancelClone` método para detener un clon de volumen o un proceso de copia de volumen en curso. Cuando se cancela una operación de clonado de grupo, el sistema completa y elimina la operación establish asociada a la operación.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ClonID	CloneIID para el proceso de clonado en curso.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "CancelClone",
   "params": {
      "cloneID" : 5,
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuevo desde la versión

9.6

CancelGroupClone

Puede utilizar el `CancelGroupClone` método para detener un proceso de clonado en curso que se produce en un grupo de volúmenes. Cuando se cancela una operación de clonado de grupo, el sistema completa y elimina la operación establish asociada a la operación.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
GroupCloneID	CloneIID para el proceso de clonado en curso.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "CancelGroupClone",
   "params": {
      "cloneID" : 5,
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuevo desde la versión

9.6

CloneMultipleVolumes

Puede utilizar el `CloneMultipleVolumes` método para crear un clon de un grupo de volúmenes especificados. Es posible asignar un conjunto coherente de características a un grupo de varios volúmenes cuando se clonan juntos.

Antes de usar el parámetro groupSnapshotID para clonar los volúmenes en una snapshot de grupo, primero se debe crear la snapshot de grupo mediante el CreateGroupSnapshot El método API o la interfaz de usuario web. El uso de groupSnapshotID es opcional cuando se clonan varios volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
acceso	Nuevo método de acceso predeterminado para los nuevos volúmenes si no se invalida con la información que se pasa en la cabina del volumen.	cadena	Ninguno	No
EnableSnapMirrorReplication	Determina si el volumen se puede usar para la replicación con extremos de SnapMirror. Los posibles valores son los siguientes: • verdadero • falso	booleano	falso	No
GroupSnapshotID	El ID de la snapshot de grupo que se utilizará como base para el clon.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
NewAccountID	Nuevo ID de cuenta de los volúmenes si no se anula mediante información que se transmite en la cabina de volúmenes.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
volúmenes	Recogida de miembros que se especifica para los nuevos volúmenes. Miembros: • Volumen ID: (Obligatorio) • Acceso: (Opcional) puede ser uno de readonly, READWRITE, bloqueado o replicationTarget . • Atributos: (Opcional) Lista de pares nombre-valor en formato de objeto JSON. • Nombre: (Opcional) Nuevo nombre para el clon. • NewAccountID: (Opcional) ID de cuenta de los nuevos volúmenes. • NewSize: (Opcional) Tamaño total del volumen, en bytes. El tamaño se redondea al megabyte más cercano. Si no se especifican miembros opcionales, los valores se heredan de los volúmenes de origen.	Cabina de objetos JSON	Ninguno	Sí (volumeID)

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
Establish asyncHandle	Valor devuelto por una llamada de método asíncrono.	entero
GroupCloneID	El ID único del clon del nuevo grupo.	entero
miembros	Lista de ID de volumen para las parejas de volúmenes de origen y destino.	Cabina de objetos JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "CloneMultipleVolumes",
   "params": {
       "volumes": [
           {
              "volumeID": 5
              "name":"foxhill",
              "access":"readOnly"
              },
           {
              "volumeID": 18
              },
           {
             "volumeID": 20
              }
     ]
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "asyncHandle": 12,
    "groupCloneID": 4,
    "members": [
     {
      "srcVolumeID": 5,
      "volumeID": 29
     },
     {
      "srcVolumeID": 18,
      "volumeID": 30
     },
     {
      "srcVolumeID": 20,
      "volumeID": 31
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

CloneVolume

Puede utilizar el `CloneVolume` método para crear una copia de un volumen. Este método es asíncrono y puede tardar una cantidad variable de tiempo en completarse.

El proceso de clonación comienza inmediatamente cuando hace el `CloneVolume` Solicite y es representativo del estado del volumen cuando se emite el método API. Puede utilizar el GetAsyncResult el método para determinar cuándo se completa el proceso de clonado y el nuevo volumen está disponible para las conexiones. Puede utilizar ListSyncJobs para ver el progreso de la creación del clon. Los atributos iniciales y la configuración de calidad de servicio del volumen se heredan del volumen que se clona. Puede cambiar esta configuración con Volumen ModificíoVolume.

> Los volúmenes clonados no heredan pertenencia al grupo de acceso de volúmenes en el volumen de origen.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
acceso	Acceso permitido para el volumen nuevo. Si no se especifica un valor, el valor de acceso no cambia. Los posibles valores son los siguientes: • `readOnly`: (Opcional) sólo se permiten operaciones de lectura. • `readWrite`: (Opcional) se permiten lecturas y escrituras. • `locked`: (Opcional) no se permiten lecturas ni escrituras. Si no se especifica, se utiliza el valor de acceso del volumen que se clona. • `replicationTarget`: (Opcional) identifique un volumen como volumen de destino para un conjunto de volúmenes emparejados. Si el volumen no está emparejado, el estado de acceso se bloquea.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
enable512e	Especifica si el nuevo volumen debe usar la emulación de sector de 512 bytes. Si no se especifica, se utiliza la configuración del volumen que se clona.	booleano	Ajuste del volumen original	No
EnableSnapMirrorReplication	Determina si el volumen se puede usar para la replicación con extremos de SnapMirror. Los posibles valores son los siguientes: • verdadero • falso	booleano	falso	No
nombre	Nombre del nuevo volumen clonado; debe tener entre 1 y 64 caracteres de longitud.	cadena	Ninguno	Sí
NewAccountID	AccountID del propietario del nuevo volumen. Si no se especifica, se utiliza el ID de cuenta del propietario del volumen que se va a clonar.	entero	ID de cuenta del propietario del volumen original	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
NuevoTamaño	El nuevo tamaño, en bytes. Puede ser mayor o menor que el tamaño del volumen que se clona. Si no se especifica, no se cambia el tamaño del volumen. El tamaño se redondea al tamaño de 1 MB más cercano.	entero	Ninguno	No
ID de copia Snapshot	ID de la copia de Snapshot que se utiliza como origen del clon. Si no se proporciona ningún ID, se utiliza el volumen activo actual.	entero	Ninguno	No
ID de volumen	ID de volumen del volumen que se va a clonar.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
Establish asyncHandle	El valor del mango utilizado para obtener el resultado de la operación.	entero
ClonID	ClonId para el volumen recién clonado.	entero
curva	Los valores de curva de calidad de servicio que se aplican al clon.	Objeto JSON
volumen	Un objeto que contiene información acerca del volumen que se acaba de clonar.	volumen

ID de volumen	VolumeID del volumen que se acaba de clonar.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "CloneVolume",
   "params": {
      "volumeID" : 5,
      "name"  : "mysqldata-snapshot1",
      "access" : "readOnly"
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
    }
}
```


Nuevo desde la versión

9.6

Obtenga más información

- GetAsyncResult
- ListSyncJobs
- Volumen ModificíoVolume

CopyVolume

Puede utilizar el `CopyVolume` método para sobrescribir el contenido de los datos de un volumen existente con el contenido de los datos de otro volumen (o snapshot). Los atributos del volumen de destino, como IQN, la configuración de calidad de servicio, el tamaño, la cuenta y la pertenencia a grupos de acceso de volúmenes no se modifican. El volumen de destino ya debe existir y debe tener el mismo tamaño que el volumen de origen.

Lo mejor es desmontar el volumen de destino antes de que se inicie la operación. Si el volumen de destino se modifica durante la operación, se pierden los cambios. Esta operación puede tardar una cantidad variable de tiempo en completarse. Puede utilizar el GetAsyncResult método para determinar cuándo ha finalizado el proceso, y. ListSyncJobs para ver el progreso de la copia.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
DstVolumeID	ID de volumen del volumen que se va a sobrescribir.	entero	Ninguno	Sí
ID de volumen	El ID de volumen del volumen del que se va a leer.	entero	Ninguno	Sí
ID de copia Snapshot	ID de la copia de Snapshot que se utiliza como origen del clon. Si no se proporciona ningún ID, se utiliza el volumen activo actual.	entero	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
Establish asyncHandle	Valor de mango utilizado para obtener el resultado de la operación.	entero
ClonID	CloneID para el volumen que se acaba de clonar.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "CopyVolume",
   "params": {
      "volumeID" : 3,
      "dstVolumeID" : 2
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "asyncHandle": 9,
    "cloneID": 5
  }
}
```

Nuevo desde la versión

9.6

Obtenga más información

- GetAsyncResult
- ListSyncJobs

QoCreateSPolicy

Puede utilizar el `CreateQoSPolicy` Método para crear un objeto QoSPolicy que posteriormente se puede aplicar a un volumen tras la creación o modificación. Una política de calidad de servicio tiene un ID único, un nombre y una configuración de calidad de servicio.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nombre	El nombre de la política QoS; por ejemplo, Gold, Platinum o Silver.	cadena	Ninguno	Sí
calidad de servicio	La configuración de la calidad de servicio que representa esta política.	Calidad de servicio	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
QosPolicy	El objeto QoSPolicy recién creado.	QoSPolicy

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 68,
  "method": "CreateQoSPolicy",
  "params": {
    "name": "bronze",
    "qos": {
      "minIOPS": 50,
      "maxIOPS": 15000,
      "burstIOPS": 15000
    }
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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": []
    }
  }
}
```


Nuevo desde la versión

10.0

CreateVolume

Puede utilizar el `CreateVolume` método para crear un nuevo volumen vacío en el clúster. Apenas se crea el volumen, el volumen está disponible para la conexión a través de iSCSI.

Los volúmenes creados sin valores de calidad de servicio especificados utilizan los valores predeterminados. Los valores predeterminados de un volumen se pueden ver con `GetDefaultQoS` método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`access`	El modo de acceso del volumen. Si se incluye este parámetro, el único valor admitido es `snapMirrorTarget`.	cadena	Ninguno	No
`accountID`	El ID de la cuenta a la que pertenece este volumen.	entero	Ninguno	Sí
`associateWithQoSPolicy`	Asocie el volumen con la política de calidad de servicio especificada. Los posibles valores son los siguientes: • `true`: Asocie el volumen con la directiva QoS especificada en el parámetro QoSPolicyID. • `false`: No asocie el volumen con la directiva QoS especificada en el parámetro QoSPolicyID. Cuando es false, se elimina cualquier asociación de directiva existente, independientemente de si se especifica una directiva QoS en el parámetro QoSPolicy.	booleano	verdadero	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`attributes`	La lista de pares nombre-valor en el formato de objetos JSON. El tamaño total del atributo debe ser menor que 1000B, o 1 KB, incluidos los caracteres de formato JSON.	Objeto JSON	Ninguno	No
`enable512e`	Habilitar la emulación de sector de 512 bytes. Los posibles valores son los siguientes: • `true`: El volumen proporciona emulación de sector de 512 bytes. • `false`: la emulación 512e no está habilitada.	booleano	Ninguno	Sí
`enableSnapMirrorReplication`	Determina si el volumen se puede usar para la replicación con extremos de SnapMirror. Los posibles valores son los siguientes: • `true` • `false`	booleano	falso	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`fifoSize`	Especifica el número máximo de instantáneas de primera entrada y salida (FIFO) admitidas por el volumen. Tenga en cuenta que las instantáneas FIFO y no FIFO utilizan el mismo pool de ranuras de instantánea disponibles en un volumen. Utilice esta opción para limitar el consumo de instantáneas FIFO de las ranuras de instantánea disponibles. Si se omite, el valor predeterminado es 24.	entero	24	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`minFifoSize`	Especifica la cantidad mínima de ranuras de snapshot reservadas por el volumen en primer lugar de salida (FIFO). De este modo, se garantiza que si se utilizan tanto instantáneas FIFO como instantáneas no FIFO en un volumen en el que las instantáneas que no son FIFO no consumen de forma accidental demasiadas ranuras FIFO. También garantiza que al menos estas instantáneas FIFO estén siempre disponibles. Puesto que las instantáneas FIFO y no FIFO comparten la misma agrupación, el `minFifoSize` Reduce el número total de instantáneas no FIFO posibles en la misma cantidad. Si se omite, el valor predeterminado es 0.	entero	0	No
`name`	Nombre del grupo de acceso de volúmenes (puede especificarse el usuario). No es necesario ser único, pero se recomienda. Debe tener entre 1 y 64 caracteres de longitud.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`qos`	La configuración de calidad inicial de servicio para este volumen. Los valores predeterminados se utilizan si no se especifica ninguno. Los posibles valores son los siguientes: • `minIOPS` • `maxIOPS` • `burstIOPS`	Objeto QoS	Ninguno	No
`qosPolicyID`	El ID de la política cuya configuración de calidad de servicio debe aplicarse a los volúmenes especificados. Este parámetro es mutuamente exclusivo con el `qos` parámetro.	entero	Ninguno	No
`totalSize`	El tamaño total del volumen, en bytes. El tamaño se redondea al megabyte más cercano.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
volumen	Objeto que contiene información acerca del volumen recién creado.	volumen
ID de volumen	El ID de volumen para el volumen recién creado.	entero

curva	La curva es un conjunto de pares clave-valor. Las claves son los tamaños de I/o en bytes. Los valores representan el coste de ejecutar un IOP en un tamaño de I/o específico. La curva se calcula en relación con una operación de 4096 bytes establecida en 100 IOPS.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "CreateVolume",
   "params": {
      "name": "mysqldata",
      "accountID": 1,
      "totalSize": 107374182400,
      "enable512e": false,
      "attributes": {
         "name1": "value1",
         "name2": "value2",
         "name3": "value3"
      },
      "qos": {
         "minIOPS": 50,
         "maxIOPS": 500,
         "burstIOPS": 1500,
         "burstTime": 60
      }
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "curve": {
            "4096": 100,
            "8192": 160,
```

```
            "16384": 270,
            "32768": 500,
            "65536": 1000,
            "131072": 1950,
            "262144": 3900,
            "524288": 7600,
            "1048576": 15000
        },
        "volume": {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {
                "name1": "value1",
                "name2": "value2",
                "name3": "value3"
            },
            "blockSize": 4096,
            "createTime": "2016-03-31T22:20:22Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:mysqldata.677",
            "name": "mysqldata",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 500,
                "minIOPS": 50
            },
            "scsiEUIDeviceID": "6a796179000002a5f47acc0100000000",
            "scsiNAADeviceID": "6f47acc1000000006a796179000002a5",
            "sliceCount": 0,
            "status": "active",
            "totalSize": 107374182400,
            "virtualVolumeID": null,
```

```
            "volumeAccessGroups": [],
            "volumeID": 677,
            "volumePairs": []
        },
        "volumeID": 677
    }
}
```

Nuevo desde la versión

9.6

Obtenga más información

GetDefaultQoS

CreateBackupTarget

Puede utilizar `CreateBackupTarget` para crear y almacenar información de destino de copia de seguridad de modo que no sea necesario volver a introducirla cada vez que se crea una copia de seguridad.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nombre	Nombre del destino del backup.	cadena	Ninguno	Sí
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	Sí (pero puede estar vacío)

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
BackupTargetID	Identificador único asignado al destino de backup nuevo.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "CreateBackupTarget",
   "params": {
      "name": "mytargetbackup"
   },
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {
      "backupTargetID": 1
   }
}
```

Nuevo desde la versión

9.6

QoDeleteSPolicy

Puede utilizar el `DeleteQoSPolicy` Método para eliminar una política de calidad de servicio del sistema. La configuración de calidad de servicio de todos los volúmenes creados o modificados con esta política no se ve afectada.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
QosPolicyID	El ID de la política de calidad de servicio que se eliminará.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 663,
  "method": "DeleteQoSPolicy",
  "params": {
    "qosPolicyID": 4
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 663,
  "result": {}
}
```

Nuevo desde la versión

9.6

DeleteVolume

Puede utilizar el `DeleteVolume` método para marcar un volumen activo para su eliminación. Una vez marcado, el volumen se purga (se elimina permanentemente) después de que transcurre un intervalo de limpieza.

Una vez que se realiza una solicitud para eliminar un volumen, todas las conexiones iSCSI activas con el volumen se finalizan inmediatamente y no se permiten más conexiones mientras el volumen está en este estado. No se devuelve un volumen marcado en las solicitudes de detección de objetivos.

Las copias de Snapshot de un volumen marcadas para eliminación no se ven afectadas. Las Snapshot se conservan hasta que se purga el volumen del sistema. Si se Marca un volumen para eliminación y tiene una operación de lectura masiva de volúmenes o escritura masiva en curso, se detiene la operación de lectura o escritura masiva de volúmenes.

Si el volumen que se elimina se empareja con un volumen, la replicación entre los volúmenes emparejados se suspende y no se transfieren datos a él o de ella mientras se encuentra en estado eliminado. El volumen remoto al que se emparejó el volumen eliminado con los entra en estado PausedMisconfigured y ya no se envían los datos ni desde el volumen eliminado. Hasta que se purga el volumen eliminado, este se puede restaurar y se pueden reanudar las transferencias de datos. Si el volumen eliminado se purga del sistema, el volumen con el que se emparejó entra en el estado StoppedMisconfigured y se elimina el estado del emparejamiento de volúmenes. El volumen purgado deja de estar disponible de forma permanente.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	El ID del volumen que se desea eliminar.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
volumen	Objeto que contiene información acerca del volumen eliminado.	volumen
ID de volumen	El ID de volumen del volumen eliminado.	entero
curva	La curva es un conjunto de pares clave-valor. Las claves son los tamaños de I/o en bytes. Los valores representan el coste de ejecutar un IOP en un tamaño de I/o específico. La curva se calcula en relación con una operación de 4096 bytes establecida en 100 IOPS.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "DeleteVolume",
   "params": {
      "volumeID"  : 5
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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": []
```

```
      }
    }
  }
```

Nuevo desde la versión

9.6

DeleteVolumes

Puede utilizar el `DeleteVolumes` método para marcar varios (hasta 500) volúmenes activos para su eliminación. Una vez marcado, el volumen se purga (se elimina permanentemente) después de que transcurre un intervalo de limpieza.

Una vez que se realiza una solicitud para eliminar volúmenes, todas las conexiones iSCSI activas con los volúmenes se finalizan inmediatamente y no se permiten más conexiones mientras los volúmenes están en este estado. No se devuelve un volumen marcado en las solicitudes de detección de objetivos.

Las copias de Snapshot de un volumen marcadas para eliminación no se ven afectadas. Las Snapshot se conservan hasta que se purga el volumen del sistema. Si se Marca un volumen para eliminación y tiene una operación de lectura masiva de volúmenes o escritura masiva en curso, se detiene la operación de lectura o escritura masiva de volúmenes.

Si los volúmenes que se eliminan se emparejan con un volumen, la replicación entre los volúmenes emparejados se suspende y no se transfieren datos a ellos o de ellos mientras se encuentran en estado eliminado. Los volúmenes remotos cuyos volúmenes eliminados se emparejaron con entran en estado PausedMisconfigured y ya no se envían los datos a ellos o desde los volúmenes eliminados. Hasta que se purguen los volúmenes eliminados, se pueden restaurar y se pueden reanudar las transferencias de datos. Si los volúmenes eliminados se purgan del sistema, los volúmenes se emparejaron con se introducen en el estado StoppedMisconfigured y se elimina el estado del emparejamiento de volúmenes. Los volúmenes purgados dejan de estar disponibles de forma permanente.

Parámetros

Este método tiene los siguientes parámetros de entrada.

Se requiere al menos uno de los siguientes parámetros, y debe usar solo uno de ellos (todos se excluyen uno al otro).

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	La lista de ID de los volúmenes que se van a eliminar del sistema.	matriz en números enteros	Ninguno	Consulte Nota.

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VolumeAccessGroupID	Una lista de los ID de grupo de acceso de volúmenes. Todos los volúmenes de todos los grupos de acceso de volúmenes especificados en esta lista se eliminan del sistema.	matriz en números enteros	Ninguno	Consulte Nota.
ID de cuenta	Lista de ID de cuenta. Todos los volúmenes de estas cuentas se eliminan del sistema.	matriz en números enteros	Ninguno	Consulte Nota.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
volúmenes	Información acerca del volumen recién eliminado.	volumen
curva	La curva es un conjunto de pares clave-valor. Las claves son los tamaños de I/o en bytes. Los valores representan el coste de ejecutar un IOP en un tamaño de I/o específico. La curva se calcula en relación con una operación de 4096 bytes establecida en 100 IOPS.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "DeleteVolumes",
   "params": {
      "accountIDs" : [1, 2, 3]
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
    } ]
  }
}
```


Nuevo desde la versión

9.6

GetBackupTarget

Puede utilizar el `GetBackupTarget` método para devolver información acerca de un destino de copia de seguridad específico que ha creado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
BackupTargetID	Identificador único asignado al destino de backup.	entero	Ninguno	Sí
nombre	El nombre del destino de backup.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
BackupTarget	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 1,
  "method": "GetBackupTarget",
  "params": {
      "backupTargetID": 1
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {
     "backupTarget": {
     "attributes" : {
        "size" : 100
     },
     "backupTargetID" : 1,
     "name" : "mytargetbackup"
    }
  }
}
```

Nuevo desde la versión

9.6

GetVolumeStats

Puede utilizar el `GetVolumeStats` método para obtener mediciones de actividad de alto nivel para un único volumen. Los valores se acumulan a partir de la creación del volumen.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	Especifica el volumen para el cual se recopilan estadísticas.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumeStats	Información de la actividad de volumen.	VolumeStats

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetVolumeStats",
   "params": {
      "volumeID": 32
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "volumeStats": {
      "accountID": 1,
      "actualIOPS": 0,
      "asyncDelay": null,
      "averageIOPSize": 0,
      "burstIOPSCredit": 0,
      "clientQueueDepth": 0,
      "desiredMetadataHosts": null,
      "latencyUSec": 0,
      "metadataHosts": {
        "deadSecondaries": [],
        "liveSecondaries": [
          32
        ],
        "primary": 60
      },
      "nonZeroBlocks": 0,
      "readBytes": 0,
      "readBytesLastSample": 0,
      "readLatencyUSec": 0,
      "readOps": 0,
      "readOpsLastSample": 0,
      "samplePeriodMSec": 0,
      "throttle": 0,
      "timestamp": "2016-04-01T21:01:39.130840Z",
      "unalignedReads": 0,
      "unalignedWrites": 0,
      "volumeAccessGroups": [],
      "volumeID": 1,
      "volumeSize": 5000658944,
      "volumeUtilization": 0,
      "writeBytes": 0,
      "writeBytesLastSample": 0,
      "writeLatencyUSec": 0,
      "writeOps": 0,
      "writeOpsLastSample": 0,
      "zeroBlocks": 1220864
    }
  }
}
```

Nuevo desde la versión

9.6

GetDefaultQoS

Puede utilizar el `GetDefaultQoS` Método para obtener los valores de calidad de servicio predeterminados para un volumen recién creado.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Calidad de servicio	Los valores predeterminados de calidad de servicio.	Calidad de servicio

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetDefaultQoS",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "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
   }
}
```

Nuevo desde la versión

9.6

GetQoSPolicy

Puede utilizar el `GetQoSPolicy` Método para obtener detalles sobre una política de calidad de servicio específica del sistema.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
QosPolicyID	El código de la directiva que se va a recuperar.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
QosPolicy	Detalles de la política de calidad de servicio solicitada.	QoSPolicy

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "GetQoSPolicy",
    "params": {
        "qosPolicyID": 2
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
      ]
    }
  }
}
```


Nuevo desde la versión

10.0

GetVolumeCount

Puede utilizar el `GetVolumeCount` método para obtener el número de volúmenes que actualmente están en el sistema.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
cuente	El número de volúmenes que actualmente están en el sistema.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetVolumeCount",
    "params": {
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "count": 7
  }
}
```

Nuevo desde la versión

9.6

GetVolumeEffect

Puede utilizar el `GetVolumeEfficiency` método para obtener información acerca de un volumen. Solo se utiliza el volumen que se da como parámetro en este método de API para calcular la capacidad.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	Especifica el volumen para el cual se calcula la capacidad.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
compresión	La cantidad de espacio que se ahorra al comprimir los datos en un único volumen. Se afirma como una relación, donde 1 significa que los datos se han almacenado sin comprimir.	flotante
deduplicación	La cantidad de espacio que se está guardando en un solo volumen al no duplicar datos. Se indica como una relación.	flotante
Volúmenes missingVolumes	Los volúmenes que no se pudieron consultar para los datos de eficiencia. Los volúmenes que faltan pueden ser causados por la recolección de basura (GC) con menos de una hora de antigüedad, pérdida temporal de red o servicios reiniciados desde el ciclo de GC.	matriz en números enteros
Thin Provisioning	La relación entre el espacio utilizado y la cantidad de espacio asignado para almacenar datos. Se indica como una relación.	flotante
fecha/hora	La última vez que se recopilaron datos de eficiencia después de GC.	Cadena de datos ISO 8601

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetVolumeEfficiency",
   "params": {
      "volumeID": 606
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {
       "compression": 2.001591240821456,
       "deduplication": 1,
       "missingVolumes": [],
       "thinProvisioning": 1.009861932938856,
       "timestamp": "2014-03-10T16:06:33Z"
   }
}
```

Nuevo desde la versión

9.6

ListActiveVolumes

Puede utilizar el `ListActiveVolumes` método para obtener la lista de volúmenes activos que actualmente están en el sistema. La lista de volúmenes se ordena en orden VolumeID y puede devolverse en varias partes (páginas).

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IncludeVirtualVolumes	Los volúmenes virtuales se incluyen en la respuesta de forma predeterminada. Para excluir volúmenes virtuales, se debe establecer en FALSE.	booleano	verdadero	No
StartVolumeID	Iniciando VolumeID para devolver. Si no existe ningún volumen con este ID de volumen, el siguiente volumen por orden VolumeID se utiliza como el inicio de la lista. Para desplazarse por la lista, pase el ID de volumen del último volumen en la respuesta anterior + 1.	entero	0	No
límite	Número máximo de objetos de información del volumen que se van a devolver. 0 (cero) devuelve todos los volúmenes (ilimitados).	entero	(ilimitada)	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
volúmenes	Lista de volúmenes activos.	volumen cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListActiveVolumes",
   "params": {
      "startVolumeID"  : 0,
      "limit" : 1000
   },
   "id" : 1
}
```

Ejemplo de respuesta

Debido a la longitud de este ejemplo de respuesta, se documenta en un tema complementario.

Nuevo desde la versión

9.6

ListBackupTargets

Puede utilizar el `ListBackupTargets` método para obtener información acerca de todos los destinos de copia de seguridad que se han creado.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
BackupTargets	Los objetos que se devuelven para cada destino de backup. Objetos incluidos: • Atributos: Lista de parejas nombre-valor en el formato de objetos JSON. (Objeto JSON) • BackupTargetID: Identificador único asignado al destino de copia de seguridad. (entero) • Name: Nombre del destino de backup. (cadena)	Objeto JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListBackupTargets",
   "params": {},
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {
     "backupTargets": [
       {
        "attributes" : {},
        "backupTargetID" : 1,
        "name" : "mytargetbackup"
       }
     ]
  }
}
```

Nuevo desde la versión

9.6

ListBulkVolumeJobs

Puede utilizar el `ListBulkVolumeJobs` método para obtener información sobre cada operación de lectura o escritura masiva de volúmenes que se produce en el sistema.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
BulkVolumeJobs	Una cabina de información para cada trabajo de volumen masivo.	BulkVolumeJob cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListBulkVolumeJobs",
   "params": {
      },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
        }
      ]
   }
}
```


Nuevo desde la versión

9.6

ListDeletedVolumes

Puede utilizar el `ListDeletedVolumes` método para recuperar la lista de volúmenes que se marcaron para su eliminación y purgaron del sistema.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IncludeVirtualVolumes	Los volúmenes virtuales se incluyen en la respuesta de forma predeterminada. Para excluir volúmenes virtuales, se debe establecer en FALSE.	booleano	verdadero	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
volúmenes	Lista de volúmenes eliminados.	volumen cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListDeletedVolumes",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Las respuestas para este método son similares al ejemplo siguiente:

```
{
    "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": []
            }
        ]
    }
}
```

Nuevo desde la versión

9.6

ListQoSPolicies

Puede utilizar el `ListQoSPolicies` Método para mostrar la configuración de todas las políticas de calidad de servicio del sistema.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
QosPolicies	Una lista de detalles acerca de cada política de calidad de servicio.	QoSPolicy cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 231,
  "method": "ListQoSPolicies",
  "params": {}
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
        ]
      }
    ]
  }
}
```

Nuevo desde la versión

10.0

ListSyncJobs

Puede utilizar el `ListSyncJobs` Método para obtener información sobre los trabajos de sincronización que se ejecutan en un clúster de almacenamiento de Element. Este método muestra información acerca de los trabajos de sincronización remota, de clonado y de segmentos.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
SyncJobs	Lista de objetos que describen los procesos de sincronización que se están ejecutando en el sistema.	SyncJob cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListSyncJobs",
   "params": { },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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"
        }
      ]
    }
}
```


Nuevo desde la versión

9.6

ListVolumeQoSHistogramas

Puede utilizar el `ListVolumeQoSHistograms` Método para generar un histograma del uso de calidad de servicio de un volumen o de varios volúmenes. Esto le permite comprender mejor cómo los volúmenes están usando la calidad de servicio.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	Una lista opcional de ID de volumen que especifica qué volúmenes deben tener generados histogramas de calidad de servicio.	matriz en números enteros	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
QosHistogramas	Una lista de objetos que describen el uso de volúmenes para uno o más volúmenes.	Cabina de objetos JSON

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
    "method": "ListVolumeQoSHistograms",
        "params": {
            "volumeIDs": [1]
        },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
```

```
    "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

Puede utilizar el `ListVolumes` método para obtener una lista de volúmenes que están en un clúster. Para especificar los volúmenes que desea volver en la lista, se pueden especificar los parámetros disponibles.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
cuentas	Solo se devuelven los volúmenes propiedad de las cuentas especificadas aquí. Se excluyen mutuamente con el parámetro volumeID.	matriz en números enteros	Ninguno	No
IncludeVirtualVolumes	De forma predeterminada, se incluyen los volúmenes virtuales en la respuesta. Para excluir volúmenes virtuales, se debe establecer en FALSE.	booleano	verdadero	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IsPaireado	Devuelve volúmenes emparejados o que no están emparejados. Los posibles valores son los siguientes: • True: Devuelve todos los volúmenes emparejados. • False: Devuelve todos los volúmenes que no están emparejados.	booleano	Ninguno	No
límite	Permite configurar el número máximo de resultados de volumen que se devuelven. Se excluyen mutuamente con el parámetro volumeID.	entero	10000	No
StartVolumeID	Solo se muestran los volúmenes con un ID mayor o igual que este valor. Se excluyen mutuamente con el parámetro volumeID.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	Una lista de ID de volumen. Si se especifica este parámetro, otros parámetros únicamente funcionan en este conjunto de volúmenes. Se excluyen mutuamente con los parámetros Accounts, startVolumeID y limit.	matriz en números enteros	No	No
Nombre de volumen	Solo se devuelve la información de objetos de volumen que coincide con el nombre del volumen.	cadena	No	No
Estado de volumen	Solo se devuelven los volúmenes con el estado igual que el valor status. Los posibles valores son los siguientes: • creando • copias snapshot • activo • eliminado	cadena	No	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
volúmenes	Lista de volúmenes.	volumen cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListVolumes",
    "params": {
        "volumeIDs": [1],
        "volumeStatus": "active",
        "isPaired": "false"
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "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": []
            }
        ]
    }
}
```

Nuevo desde la versión

9.6

ListVolumeStats

Puede utilizar el `ListVolumeStats` Método para obtener mediciones de actividad de alto nivel para un solo volumen, una lista de volúmenes o todos los volúmenes (si se omite el parámetro volumeIDs). Los valores de medición se acumulan a partir de la creación del volumen.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IncludeVirtualVolumes	De forma predeterminada, se incluyen los volúmenes virtuales en la respuesta. Para excluir volúmenes virtuales, se debe establecer en FALSE.	booleano	verdadero	No
ID de volumen	Una lista de los volúmenes de los cuales se puede recuperar la información de la actividad.	matriz en números enteros	No	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumeStats	Lista de información de actividad de volumen.	VolumeStats cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListVolumeStats",
    "params": {
        "volumeIDs": [1]
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

ListVolumesForAccount

Puede utilizar el `ListVolumesForAccount` método para enumerar los volúmenes activos y (pendientes) eliminados de una cuenta.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IncludeVirtualVolumes	De forma predeterminada, se incluyen los volúmenes virtuales en la respuesta. Para excluir volúmenes virtuales, se debe establecer en FALSE.	booleano	verdadero	No
ID de cuenta	Se devuelven todos los volúmenes que son propiedad de este ID de cuenta.	entero	No	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
volúmenes	Lista de información de volumen.	volumen cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListVolumesForAccount",
   "params": {
      "accountID"  : 1
   },
   "id" : 1
}
```

Ejemplo de respuesta

Las respuestas para este método son similares al ejemplo siguiente:

```
{
    "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": []
            }
        ]
    }
}
```

Nuevo desde la versión

9.6

ListVolumeStatsByAccount

Puede utilizar el `ListVolumeStatsByAccount` método para enumerar medidas de actividad de volumen de alto nivel en cada cuenta. Los valores se suman de todos los volúmenes que pertenecen a la cuenta.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IncludeVirtualVolumes	De forma predeterminada, se incluyen los volúmenes virtuales en la respuesta. Para excluir volúmenes virtuales, se debe establecer en FALSE.	booleano	verdadero	No
cuentas	Lista de ID de cuenta cuyos estadísticas de volumen desea devolver. Si se omite, se devuelven las estadísticas de todas las cuentas.	matriz en números enteros	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumeStats	Lista de información de actividad de volumen para cada cuenta.**Nota:** el miembro volumeID es 0 para cada entrada, ya que los valores representan la suma de todos los volúmenes propiedad de la cuenta.	VolumeStats cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method": "ListVolumeStatsByAccount",
  "params": {"accounts": [3]},
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}
```

Nuevo desde la versión

9.6

ListVolumeStatsByVirtualVolume

Puede utilizar el `ListVolumeStatsByVirtualVolume` método para mostrar estadísticas de volumen de cualquier volumen del sistema asociado con el volumen virtual. Las estadísticas se acumulan a partir de la creación del volumen.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volúmenes virtuales	Una lista de uno o más ID de volúmenes virtuales de los cuales se puede recuperar información. Si se especifica este parámetro, el método muestra información únicamente acerca de estos volúmenes virtuales.	Cabina de cadenas de UUID	No	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumeStats	Una lista de los objetos que contienen información de actividades para cada volumen virtual en el sistema.	VolumeStats cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListVolumeStatsByVirtualVolume",
  "params": {},
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```
{
  "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
```

```
        }
      ]
    }
  }
```

Nuevo desde la versión

9.6

ListVolumeStatsByVolume

Puede utilizar el `ListVolumeStatsByVolume` método para enumerar las mediciones de actividad de alto nivel para cada volumen, por volumen. Los valores se acumulan a partir de la creación del volumen.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IncludeVirtualVolumes	De forma predeterminada, se incluyen los volúmenes virtuales en la respuesta. Para excluir volúmenes virtuales, se debe establecer en FALSE.	booleano	verdadero	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumeStats	Lista de información de actividad de volumen.	VolumeStats cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListVolumeStatsByVolume",
   "params": {},
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "volumeStats": [
      {
        "accountID": 3,
        "actualIOPS": 0,
        "asyncDelay": null,
        "averageIOPSize": 4096,
        "burstIOPSCredit": 30000,
        "clientQueueDepth": 0,
        "desiredMetadataHosts": null,
        "latencyUSec": 0,
        "metadataHosts": {
          "deadSecondaries": [],
          "liveSecondaries": [
              16
          ],
          "primary": 12
        },
        "nonZeroBlocks": 7499205,
        "readBytes": 159012818944,
        "readBytesLastSample": 0,
        "readLatencyUSec": 0,
        "readOps": 38821489,
        "readOpsLastSample": 0,
        "samplePeriodMSec": 500,
        "throttle": 0,
        "timestamp": "2016-10-17T20:55:31.087537Z",
        "unalignedReads": 0,
        "unalignedWrites": 0,
        "volumeAccessGroups": [
          1
        ],
        "volumeID": 1,
```

```
        "volumeSize": 53687091200,
        "volumeUtilization": 0,
        "writeBytes": 52992585728,
        "writeBytesLastSample": 0,
        "writeLatencyUSec": 0,
        "writeOps": 12937643,
        "writeOpsLastSample": 0,
        "zeroBlocks": 5607995
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

ListVolumeStatsByVolumeAccessGroup

Puede utilizar el `ListVolumeStatsByVolumeAccessGroup` método para enumerar las mediciones de actividad total de todos los volúmenes que son miembros de los grupos de acceso de volúmenes especificados.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
IncludeVirtualVolumes	De forma predeterminada, se incluyen los volúmenes virtuales en la respuesta. Para excluir volúmenes virtuales, se debe establecer en FALSE.	booleano	verdadero	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VolumeAccessGroups	Una matriz de VolumeAccessGroupID para la que se devuelve la actividad del volumen. Si se omite, se devuelven las estadísticas de todos los grupos de acceso de volúmenes.	matriz en números enteros	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumeStats	Lista de información de actividad de volumen para todos los volúmenes del grupo de acceso de volumen especificado.**Nota:** el miembro volumeID es 0 para cada entrada, ya que los valores representan la suma de todos los volúmenes propiedad de la cuenta.	VolumeStats

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListVolumeStatsByVolumeAccessGroup",
    "params": {"volumeAccessGroups": [1]},
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

ModifyBackupTarget

Puede utilizar el `ModifyBackupTarget` método para cambiar los atributos de un destino de backup.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
BackupTargetID	ID de destino único que se va a modificar el destino.	entero	Ninguno	Sí
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
nombre	Nuevo nombre del destino del backup.	cadena	Ninguno	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ModifyBackupTarget",
   "params": {
      "backupTargetID" : 1,
      "name": "yourtargetS3"
      "attributes" : {
          "size" : 500,
      }
   },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {}
}
```

Nuevo desde la versión

9.6

ModifyQoSPolicy

Puede utilizar el `ModifyQoSPolicy` Método para modificar una política de calidad de servicio existente en el sistema.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
QosPolicyID	El ID de la política que se va a modificar.	entero	Ninguno	Sí
nombre	Si se proporciona, el nombre de la política QoS (p. ej., Gold, Platinum o Silver) se cambia a este valor.	cadena	Ninguno	No
calidad de servicio	Si se proporciona, la configuración de QoS para esta directiva se cambia a esta configuración. Puede proporcionar valores de calidad de servicio parciales y solo cambiar algunos de los ajustes de calidad de servicio.	Objeto QoS	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
QosPolicy	Detalles de la política de calidad de servicio recién modificada.	QoSPolicy

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 1950,
  "method": "ModifyQoSPolicy",
  "params": {
    "qosPolicyID": 2,
    "qos": {
      "minIOPS": 51,
      "maxIOPS": 15002,
      "burstIOPS": 15002
    }
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
      ]
    }
  }
}
```


Nuevo desde la versión

10.0

Volumen ModificíoVolume

Puede utilizar el `ModifyVolume` método para modificar la configuración en un volumen existente. Puede realizar modificaciones en un volumen a la vez y los cambios se producen de inmediato.

Si no especifica valores de calidad de servicio al modificar un volumen, seguirán siendo los mismos que antes de la modificación. Puede recuperar los valores de calidad de servicio predeterminados para un volumen recién creado mediante la ejecución de `GetDefaultQoS` método.

Cuando se necesita aumentar el tamaño de un volumen que se está replicando, hágalo en el siguiente orden para evitar errores de replicación:

1. Aumente el tamaño del volumen con replicationTarget Access.
2. Aumente el tamaño del origen o del volumen con el acceso READWRITE.

Asegúrese de que los volúmenes de destino y origen tengan el mismo tamaño.

Si cambia el estado de acceso a Locked o replicationTarget, se finalizan todas las conexiones iSCSI existentes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	El ID de volumen del volumen que se va a modificar.	entero	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
acceso	Acceso permitido para el volumen. Los posibles valores son los siguientes: • `readOnly`: Sólo se permiten operaciones de lectura. • `readWrite`: Se permiten lecturas y escrituras. • `locked`: No se permiten lecturas ni escrituras. Si no se especifica, el valor de acceso no cambia. • `replicationTarget`: Identifique un volumen como volumen de destino para un conjunto de volúmenes emparejados. Si el volumen no está emparejado, el estado de acceso se bloquea. Si no se especifica un valor, el valor de acceso no cambia. • `snapMirrorTarget`: Identifique un volumen como volumen de destino para la replicación de SnapMirror.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de cuenta	El ID de cuenta a la que se reasigna el volumen. Si no se especifica ninguno, se utiliza el nombre de cuenta anterior.	entero	Ninguno	No
AsociateWithQoSPolicy	Asocie el volumen con la política de calidad de servicio especificada. Los posibles valores son los siguientes: • `true`: Asocie el volumen con la directiva QoS especificada en el parámetro QoSPolicyID. • `false`: No asocie el volumen con la directiva QoS especificada en el parámetro QoSPolicyID. Cuando es false, se elimina cualquier asociación de directiva existente, independientemente de si se especifica una directiva QoS en el parámetro QoSPolicy.	booleano	Ninguno	No
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
CreateTime	Una cadena de fecha ISO 8601 que se establecerá como fecha de creación del nuevo volumen. Requerido si setCreateTime se establece en TRUE.	Cadena ISO 8601	Ninguno	No
EnableSnapMirrorReplication	Determina si el volumen se puede usar para la replicación con extremos de SnapMirror. Los posibles valores son los siguientes: • `true` • `false`	booleano	falso	No
Tamaño 50	Especifica el número máximo de instantáneas de primera entrada y salida (FIFO) admitidas por el volumen. Tenga en cuenta que las instantáneas FIFO y no FIFO utilizan el mismo pool de ranuras de instantánea disponibles en un volumen. Utilice esta opción para limitar el consumo de instantáneas FIFO de las ranuras de instantánea disponibles. Tenga en cuenta que no puede modificar este valor para que sea inferior al recuento de instantáneas FIFO actual.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
MinFioSize	Especifica el número de ranuras de instantánea reservadas sólo para las instantáneas primero en salir (FIFO). Puesto que las instantáneas FIFO y no FIFO comparten la misma agrupación, el parámetro minFifoSize reduce el número total de posibles instantáneas no FIFO en la misma cantidad. Tenga en cuenta que no puede modificar este valor para que entre en conflicto con el recuento de instantáneas no FIFO actual.	entero	Ninguno	No
modo	Modo de replicación del volumen. Los posibles valores son los siguientes: • `asynch`: Espera a que el sistema reconozca que los datos se almacenan en el origen antes de escribir en el destino. • `sync`: No espera a que el origen reconozca la transmisión de datos para comenzar a escribir datos en el destino.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
calidad de servicio	La nueva configuración de calidad de servicio para este volumen. Si no se especifica, la configuración de calidad de servicio no se modifica. Los posibles valores son los siguientes: • `minIOPS` • `maxIOPS` • `burstIOPS`	Calidad de servicio	Ninguno	No
QosPolicyID	El ID de la política cuya configuración de calidad de servicio debe aplicarse a los volúmenes especificados. Este parámetro es mutuamente exclusivo con qos.	entero	Ninguno	No
SetCreateTime	Establezca esta opción en true para cambiar la fecha registrada de creación del volumen.	booleano	Ninguno	No
Tamaño total	El nuevo tamaño en bytes del volumen. 1000000000 es igual a 1 GB. El tamaño se redondea hasta el megabyte más cercano. Este parámetro solo se puede usar para aumentar el tamaño de un volumen.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
volumen	Objeto que contiene información acerca del volumen recién modificado.	volumen

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ModifyVolume",
  "params": {
     "volumeID": 5,
     "attributes": {
        "name1": "value1",
        "name2": "value2",
        "name3": "value3"
     },
     "qos": {
        "minIOPS": 60,
        "maxIOPS": 100,
        "burstIOPS": 150,
        "burstTime": 60
     },
      "access" :"readWrite"
     },
      "totalSize": 20000000000,
     "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
      "volume": {
          "access": "readWrite",
          "accountID": 1,
          "attributes": {
```

```
            "name1": "value1",
            "name2": "value2",
            "name3": "value3"
        },
        "blockSize": 4096,
        "createTime": "2016-03-28T16:16:13Z",
        "deleteTime": "",
        "enable512e": true,
        "iqn": "iqn.2010-01.com.solidfire:jyay.1459181777648.5",
        "name": "1459181777648",
        "purgeTime": "",
        "qos": {
            "burstIOPS": 150,
            "burstTime": 60,
            "curve": {
                "4096": 100,
                "8192": 160,
                "16384": 270,
                "32768": 500,
                "65536": 1000,
                "131072": 1950,
                "262144": 3900,
                "524288": 7600,
                "1048576": 15000
            },
            "maxIOPS": 100,
            "minIOPS": 60
        },
        "scsiEUIDeviceID": "6a79617900000005f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000006a79617900000005",
        "sliceCount": 1,
        "status": "active",
        "totalSize": 1000341504,
        "virtualVolumeID": null,
        "volumeAccessGroups": [
            1
        ],
        "volumeID": 5,
        "volumePairs": []
    }
  }
}
```


Nuevo desde la versión

9.6

Obtenga más información

GetDefaultQoS

ModificyVolumes

Puede utilizar el `ModifyVolumes` método para configurar hasta 500 volúmenes existentes a la vez. Los cambios se realizan inmediatamente. Si `ModifyVolumes` no se puede modificar ninguno de los volúmenes especificados, no se modifica ninguno de los volúmenes especificados.

Si no se especifican los valores de calidad de servicio al modificar volúmenes, los valores de calidad de servicio de cada volumen permanecen sin cambios. Puede recuperar los valores de calidad de servicio predeterminados para un volumen recién creado mediante la ejecución de `GetDefaultQoS` método.

Cuando se necesitan aumentar los volúmenes de tamaño que se están replicando, hágalo en el siguiente orden para evitar errores de replicación:

1. Aumente el tamaño del volumen con replicationTarget Access.
2. Aumente el tamaño del origen o del volumen con el acceso READWRITE.

Asegúrese de que los volúmenes de destino y origen tengan el mismo tamaño.

Si cambia el estado de acceso a Locked o replicationTarget, se finalizan todas las conexiones iSCSI existentes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio

acceso	Acceso permitido para los volúmenes. Los posibles valores son los siguientes: • `readOnly`: Sólo se permiten operaciones de lectura. • `readWrite`: Se permiten lecturas y escrituras. • `locked`: No se permiten lecturas ni escrituras. Si no se especifica, el valor de acceso no cambia. • `replicationTarget`: Identifique un volumen como volumen de destino para un conjunto de volúmenes emparejados. Si el volumen no está emparejado, el estado de acceso se bloquea. Si no se especifica un valor, el valor de acceso no cambia.	cadena	Ninguno	No
ID de cuenta	El ID de cuenta a la que se reasignan los volúmenes. Si no se especifica ninguno, se utiliza el nombre de cuenta anterior.	entero	Ninguno	No

AsociateWithQoSPolicy	Asocie el volumen con la política de calidad de servicio especificada. Los posibles valores son los siguientes: • True: Asocie el volumen con la política QoS especificada en el parámetro QoSPolicyID. • False: No asocie el volumen con la política QoS especificada en el parámetro QoSPolicyID. Cuando es false, se elimina cualquier asociación de directiva existente, independientemente de si se especifica una directiva QoS en el parámetro QoSPolicy.	booleano	Ninguno	No
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
CreateTime	Una cadena de fecha ISO 8601 que se establecerá como fecha de creación del nuevo volumen. Requerido si setCreateTime se establece en TRUE.	Cadena ISO 8601	Ninguno	No

EnableSnapMirrorReplication	Determina si el volumen se puede usar para la replicación con extremos de SnapMirror. Los posibles valores son los siguientes: • `true` • `false`	booleano	falso	No
Tamaño 50	Especifica el número máximo de instantáneas de primera entrada y salida (FIFO) admitidas por el volumen. Tenga en cuenta que las instantáneas FIFO y no FIFO utilizan el mismo pool de ranuras de instantánea disponibles en un volumen. Utilice esta opción para limitar el consumo de instantáneas FIFO de las ranuras de instantánea disponibles. Tenga en cuenta que no puede modificar este valor para que sea inferior al recuento de instantáneas FIFO actual.	entero	Ninguno	No

MinFioSize	Especifica el número de ranuras de instantánea reservadas sólo para las instantáneas primero en salir (FIFO). Puesto que las instantáneas FIFO y no FIFO comparten la misma agrupación, el parámetro minFifoSize reduce el número total de posibles instantáneas no FIFO en la misma cantidad. Tenga en cuenta que no puede modificar este valor para que entre en conflicto con el recuento de instantáneas no FIFO actual.	entero	Ninguno	No
modo	Modo de replicación del volumen. Los posibles valores son los siguientes: • `asynch`: Espera a que el sistema reconozca que los datos se almacenan en el origen antes de escribir en el destino. • `sync`: No espera a que el origen reconozca la transmisión de datos para comenzar a escribir datos en el destino.	cadena	Ninguno	No

calidad de servicio	La nueva configuración de calidad de servicio de los volúmenes. Si no se especifica, la configuración de calidad de servicio no se modifica. Los posibles valores son los siguientes: • `minIOPS` • `maxIOPS` • `burstIOPS`	Calidad de servicio	Ninguno	No
QosPolicyID	El ID de la política cuya configuración de calidad de servicio debe aplicarse a los volúmenes especificados. Este parámetro es mutuamente exclusivo con qos.	entero	Ninguno	No
SetCreateTime	Establezca esta opción en true para cambiar la fecha registrada de creación del volumen.	booleano	Ninguno	No
Tamaño total	El tamaño nuevo de los volúmenes en bytes. 1000000000 es igual a 1 GB. El tamaño se redondea hasta el megabyte más cercano. Este parámetro solo se puede usar para aumentar el tamaño de un volumen.	entero	Ninguno	No
ID de volumen	Una lista de identificadores de volumen de los volúmenes que se van a modificar.	matriz en números enteros	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
volumen	Una cabina de objetos que contienen información sobre cada volumen recién modificado.	volumen cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ModifyVolumes",
  "params": {
    "volumeIDs": [2,3],
    "attributes": {
      "name1": "value1",
      "name2": "value2",
      "name3": "value3"
    },
    "qos": {
      "minIOPS": 50,
      "maxIOPS": 100,
      "burstIOPS": 150,
      "burstTime": 60
    },
    "access" : "replicationTarget"
  },
  "totalSize": 80000000000,
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "volumes": [
      {
        "access": "replicationTarget",
        "accountID": 1,
```

```
        "attributes": {
          "name1": "value1",
          "name2": "value2",
          "name3": "value3"
        },
        "blockSize": 4096,
        "createTime": "2016-04-06T17:25:13Z",
        "deleteTime": "",
        "enable512e": false,
        "iqn": "iqn.2010-01.com.solidfire:jo73.2",
        "name": "doctest1",
        "purgeTime": "",
        "qos": {
          "burstIOPS": 150,
          "burstTime": 60,
          "curve": {
            "4096": 100,
            "8192": 160,
            "16384": 270,
            "32768": 500,
            "65536": 1000,
            "131072": 1950,
            "262144": 3900,
            "524288": 7600,
            "1048576": 15000
          },
          "maxIOPS": 100,
          "minIOPS": 50
        },
        "scsiEUIDeviceID": "6a6f373300000002f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000006a6f373300000002",
        "sliceCount": 1,
        "status": "active",
        "totalSize": 1000341504,
        "virtualVolumeID": null,
        "volumeAccessGroups": [],
        "volumeID": 2,
        "volumePairs": []
      },
      {
        "access": "replicationTarget",
        "accountID": 1,
        "attributes": {
          "name1": "value1",
          "name2": "value2",
          "name3": "value3"
```

```
        },
        "blockSize": 4096,
        "createTime": "2016-04-06T17:26:31Z",
        "deleteTime": "",
        "enable512e": false,
        "iqn": "iqn.2010-01.com.solidfire:jo73.3",
        "name": "doctest2",
        "purgeTime": "",
        "qos": {
          "burstIOPS": 150,
          "burstTime": 60,
          "curve": {
            "4096": 100,
            "8192": 160,
            "16384": 270,
            "32768": 500,
            "65536": 1000,
            "131072": 1950,
            "262144": 3900,
            "524288": 7600,
            "1048576": 15000
          },
          "maxIOPS": 100,
          "minIOPS": 50
        },
        "scsiEUIDeviceID": "6a6f373300000003f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000006a6f373300000003",
        "sliceCount": 1,
        "status": "active",
        "totalSize": 1000341504,
        "virtualVolumeID": null,
        "volumeAccessGroups": [],
        "volumeID": 3,
        "volumePairs": []
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

Obtenga más información

GetDefaultQoS

PurgeDeletedVolume

Puede utilizar el `PurgeDeletedVolume` método para purgar de inmediato y de forma permanente un volumen que se ha eliminado. Debe eliminar un volumen mediante `DeleteVolume` antes de que se pueda purgar.

Los volúmenes se purgan automáticamente después de un período de tiempo, por lo que normalmente no se requiere el uso de este método.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	El ID de volumen del volumen que se va a purgar.	entero	No	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "PurgeDeletedVolume",
   "params": {
      "volumeID"  : 5
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result": {}
}
```

Nuevo desde la versión

9.6

Obtenga más información

DeleteVolume

PurgeDeletedVolumes

Puede utilizar el `PurgeDeletedVolumes` método para purgar volúmenes inmediatamente y de forma permanente que se hayan eliminado; puede usar este método para purgar hasta 500 volúmenes al mismo tiempo.

Debe eliminar volúmenes mediante `DeleteVolumes` antes de que se puedan purgar. Los volúmenes se purgan automáticamente después de un período de tiempo, por lo que normalmente no se requiere el uso de este método.

> Si purga un gran número de volúmenes a la vez, o si los volúmenes que purga cada uno tienen muchas instantáneas asociadas, el método puede fallar y devolver el error "xDBConnectionLoss". Si esto sucede, vuelva a intentar llamar al método con menos volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	Una lista de identificadores de volumen de los volúmenes que se van a purgar del sistema.	matriz en números enteros	No	No
ID de cuenta	Una lista de los ID de cuentas. Todos los volúmenes de todas las cuentas especificadas se purgan en el sistema.	matriz en números enteros	No	No
VolumeAccessGroupID	Una lista de volumeAccessGroupID. Todos los volúmenes de todos los grupos de acceso de volúmenes especificados se purgan del sistema.	matriz en números enteros	No	No

Nota: puede especificar sólo uno de los parámetros anteriores por llamada de método. Si se especifica más de uno o ninguno, se producirá un error.

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "PurgeDeletedVolumes",
   "params": {
      "accountIDs" : [1, 2, 3]
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result": {}
}
```

Nuevo desde la versión

9.6

Obtenga más información

DeleteVolumes

RemoveBackupTarget

Puede utilizar el `RemoveBackupTarget` método para eliminar destinos de copia de seguridad.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
BackupTargetID	ID de destino único del destino que se va a quitar.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "RemoveBackupTarget",
   "params": {
        "backupTargetID" : 1
   },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {}
}
```

Nuevo desde la versión

9.6

RestoreDeletedVolume

Puede utilizar el `RestoreDeletedVolume` método para marcar un volumen eliminado como activo de nuevo. Esta acción hace que el volumen esté disponible inmediatamente para la conexión iSCSI.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	El ID de volumen del volumen eliminado que se va a restaurar.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "RestoreDeletedVolume",
   "params": {
      "volumeID"  : 5
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result": {}
}
```

Nuevo desde la versión

9.6

SetDefaultQoS

Puede utilizar el `SetDefaultQoS` Método para configurar los valores predeterminados de calidad de servicio (QoS) (que se miden en entradas y salidas por segundo o IOPS) de un volumen.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
MinIOPS	El número mínimo de IOPS sostenidas que proporciona el clúster a un volumen.	entero	Ninguno	No
IOPS	El número máximo de IOPS sostenidas que proporciona el clúster a un volumen.	entero	Ninguno	No
BurstIOPS	El número máximo de IOPS permitidas en un escenario de ráfaga breve.	entero	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
MinIOPS	El número mínimo de IOPS sostenidas que proporciona el clúster a un volumen.	entero
IOPS	El número máximo de IOPS sostenidas que proporciona el clúster a un volumen.	entero
BurstIOPS	El número máximo de IOPS permitidas en un escenario de ráfaga breve.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "SetDefaultQoS",
    "params": {
        "burstIOPS":8000,
        "maxIOPS":1000,
        "minIOPS":200
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id":1,
    "result": {
        "burstIOPS":8000,
        "maxIOPS":1000,
        "minIOPS":200
    }
}
```

Nuevo desde la versión

9.6

StartBulkVolumeRead

Puede utilizar el `StartBulkVolumeRead` método para iniciar una sesión de lectura masiva de volúmenes en un volumen especificado.

Solo se pueden ejecutar simultáneamente dos procesos de volúmenes masivos en un volumen. Cuando se inicializa la sesión, se leen datos de un volumen de almacenamiento de SolidFire que se almacena en un origen de backup externo. Un servidor web que se ejecuta en un nodo de almacenamiento de Element, accede a los datos externos. La información de interacción del servidor para el acceso a datos externos es pasada por un script que se ejecuta en el sistema de almacenamiento.

Al inicio de una operación de lectura masiva de volúmenes, se realiza una copia de Snapshot del volumen y la copia de Snapshot se elimina cuando finaliza la lectura. También es posible leer una copia de Snapshot del volumen si se introduce el ID de la copia de Snapshot como un parámetro. Cuando se lee una snapshot anterior, el sistema no crea una snapshot nueva del volumen ni elimina la snapshot anterior cuando finaliza la lectura.

Este proceso crea una nueva snapshot si no se proporciona el ID de una snapshot existente. Se pueden crear copias de Snapshot si la ocupación del clúster se encuentra en la etapa 2 o 3. Las copias de Snapshot no se crean cuando la ocupación del clúster se encuentra en la etapa 4 o 5.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
formato	El formato de los datos del volumen. Puede ser: • `uncompressed`: Todos los bytes del volumen se devuelven sin compresión. • `native`: Los datos Opaque se devuelven que son más pequeños y eficientes almacenados y escritos en una escritura masiva posterior.	cadena	Ninguno	Sí
ID de volumen	El ID del volumen que se leerá.	entero	Ninguno	Sí
ID de copia Snapshot	El ID de una snapshot creada previamente para lecturas de volúmenes masivos. Si no se introduce ningún ID, se realiza una snapshot de la imagen de volumen activo actual.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
guión	El nombre de un script ejecutable. Si no se otorga ningún nombre de script, la clave y la URL son necesarias para acceder a los nodos de almacenamiento Element. La secuencia de comandos se ejecuta en el nodo primario, y la clave y la URL se devuelven al script para que se pueda contactar con el servidor web local.	cadena	Ninguno	No
ScriptParameters	Parámetros JSON para pasar al script.	Objeto JSON	Ninguno	No
atributos	Atributos JSON para el trabajo de volúmenes masivos.	Objeto JSON	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
Establish asyncHandle	El ID del proceso asíncrono que se comprobará para que finalice.	entero
clave	Clave opaca que identifica de forma exclusiva la sesión.	cadena
url	URL para acceder al servidor web del nodo.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "StartBulkVolumeRead",
   "params": {
      "volumeID" : 5,
      "format"  : "native",
      "snapshotID" : 2
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
      "id" : 1,
   "result" : {
      "asyncHandle" : 1,
      "key" : "11eed8f086539205beeaadd981aad130",
      "url" : "https://127.0.0.1:44000/"
   }
}
```

Nuevo desde la versión

9.6

StartBulkVolumeWrite

Puede utilizar el `StartBulkVolumeWrite` método para iniciar una sesión de escritura masiva de volúmenes en un volumen especificado.

Solo se pueden ejecutar simultáneamente dos procesos de volúmenes masivos en un volumen. Cuando se inicializa la sesión, los datos se escriben en un volumen de almacenamiento de Element desde un origen de backup externo. Un servidor web que se ejecuta en un nodo de almacenamiento de Element, accede a los datos externos. La información de interacción del servidor para el acceso a datos externos es pasada por un script que se ejecuta en el sistema de almacenamiento.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
formato	El formato de los datos del volumen. Puede ser: • `uncompressed`: Todos los bytes del volumen se devuelven sin compresión. • `native`: Los datos Opaque se devuelven que son más pequeños y eficientes almacenados y escritos en una escritura masiva posterior.	cadena	Ninguno	Sí
ID de volumen	El ID del volumen en el que se va a escribir.	entero	Ninguno	Sí
guión	El nombre de un script ejecutable. Si no se otorga ningún nombre de script, la clave y la URL son necesarias para acceder a los nodos de almacenamiento Element. La secuencia de comandos se ejecuta en el nodo primario, y la clave y la URL se devuelven al script para que se pueda contactar con el servidor web local.	cadena	Ninguno	No
ScriptParameters	Parámetros JSON para pasar al script.	Objeto JSON	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
atributos	Atributos JSON para el trabajo de volúmenes masivos.	Objeto JSON	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
Establish asyncHandle	El ID del proceso asíncrono que se comprobará para que finalice.	entero
clave	Clave opaca que identifica de forma exclusiva la sesión.	cadena
url	URL para acceder al servidor web del nodo.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "StartBulkVolumeWrite",
   "params": {
      "volumeID" : 5,
      "format"  : "native",
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id" : 1,
   "result" : {
      "asyncHandle" : 1,
      "key" : "11eed8f086539205beeaadd981aad130",
      "url" : "https://127.0.0.1:44000/"
   }
}
```

Nuevo desde la versión

9.6

UpdateBulkVolumeStatus

Puede utilizar el `UpdateBulkVolumeStatus` método para actualizar el estado de un trabajo de volumen masivo que se inició con el `StartBulkVolumeRead` o. `StartBulkVolumeWrite` métodos.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
clave	Clave asignada durante la inicialización de un StartBulkVolumeRead o. StartBulkVolumeWrite sesión.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
estado	El sistema establece el estado del trabajo de volumen masivo dado. Los posibles valores son los siguientes: • Running: Trabajos que aún están activos. • Completado: Trabajos que se han realizado. • Failed: Trabajos con errores.	cadena	Ninguno	Sí
Porcentaje completado	El progreso completado del trabajo de volumen masivo como porcentaje.	cadena	Ninguno	No
mensaje	Devuelve el estado del trabajo de volumen masivo una vez completado el trabajo.	cadena	Ninguno	No
atributos	Atributos JSON; actualiza lo que está en el trabajo de volumen masivo.	Objeto JSON	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo

estado	Estado de la sesión solicitada. Estado devuelto: • preparando • activo • listo • error	cadena
atributos	Devuelve los atributos especificados en la llamada al método. Los valores se devuelven tanto si han cambiado como si no.	cadena
url	La URL para acceder al servidor web del nodo; se proporciona solo si la sesión sigue activa.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "UpdateBulkVolumeStatus",
   "params": {
          "key": "0b2f532123225febda2625f55dcb0448",
          "status": "running"
      },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id" : 1,
   "result": {
      "status" : "running",
      "url" : "https://10.10.23.47:8443/"
    }
}
```

Nuevo desde la versión

9.6

Obtenga más información

- StartBulkVolumeRead
- StartBulkVolumeWrite

Métodos API de grupo de acceso de volúmenes

Los métodos de grupo de acceso de volúmenes permiten añadir, quitar, ver y modificar grupos de acceso de volúmenes, que son colecciones de volúmenes a los que los usuarios pueden acceder mediante iniciadores iSCSI o Fibre Channel.

- AddInitiatorsToVolumeAccessGroup
- AddVolumesToVolumeAccessGroup
- CreateVolumeAccessGroup
- DeleteVolumeAccessGroup
- ListVolumeAccessGroups
- RemoveVolumesFromVolumeAccessGroup
- RemoveInitiatorsFromVolumeAccessGroup
- ModifyVolumeAccessGroup
- GetVolumeAccessGroupEfficency

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

AddInitiatorsToVolumeAccessGroup

Puede utilizar el `AddInitiatorsToVolumeAccessGroup` método para añadir iniciadores a un grupo de acceso de volúmenes especificado.

El formato aceptado de un IQN de iniciador es IQN.yyyy-mm, donde y y m son dígitos, seguidos de texto que solo puede contener dígitos, caracteres alfabéticos en minúscula, un punto (.), dos puntos (:) o un guion (-). Consulte el siguiente ejemplo:

```
iqn.2010-01.com.solidfire:17oi.solidfire-0.1
```

El formato aceptado de WWPN de un iniciador Fibre Channel es AA:BB:CC:dd:11:22:33:44, o AabBCCdd11223344. Consulte el siguiente ejemplo:

```
21:00:00:0e:1e:11:f1:81
```

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
iniciadores	Lista de ID o nombres de iniciador (IQN y WWPN) que se van a incluir en el grupo de acceso de volúmenes. Si pasa una lista de nombres de iniciador, se crean los iniciadores si no existen todavía. Si pasa una lista de ID de iniciador, el método devuelve un error si alguno de los iniciadores aún no existe. Pasar los nombres de iniciadores está obsoleto; debe usar ID de iniciador cuando sea posible.	matriz de enteros o matriz de cadenas (obsoleto)		Sí
VolumeAccessGroupID	El ID del grupo de acceso de volúmenes para añadir el iniciador.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumeAccessGroup	Un objeto que contiene información acerca del grupo de acceso de volúmenes recién modificado.	VolumeAccessGroup

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 13171,
  "method": "AddInitiatorsToVolumeAccessGroup",
  "params": {
    "initiators": [116,117],
    "volumeAccessGroupID": 96
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
      ]
    }
  }
}
```

Nuevo desde la versión

9.6

AddVolumesToVolumeAccessGroup

Puede utilizar el `AddVolumesToVolumeAccessGroup` método para añadir volúmenes a un grupo de acceso de volúmenes especificado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
volúmenes	La lista de ID de volumen que se van a añadir al grupo de acceso de volúmenes.	matriz en números enteros	Ninguno	Sí
VolumeAccessGroupID	VolumeAccessGroupID del grupo de acceso de volúmenes al cual se añaden volúmenes.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumeAccessGroup	Un objeto que contiene información acerca del grupo de acceso de volúmenes recién modificado.	VolumeAccessGroup

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "AddVolumesToVolumeAccessGroup",
   "params": {
      "volumeAccessGroupID": 96,
      "volumes": [1,2]
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```
{
  "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
      ]
    }
  }
}
```


Nuevo desde la versión

9.6

CreateVolumeAccessGroup

Puede utilizar `CreateVolumeAccessGroup` para crear un nuevo grupo de acceso de volúmenes. Al crear el grupo de acceso de volúmenes, es necesario asignarle un nombre y de manera opcional se pueden introducir iniciadores y volúmenes.

Cualquier IQN de iniciador que se añade al grupo de acceso de volúmenes puede acceder a cualquier volumen del grupo sin autenticación CHAP.

> Los volúmenes clonados no heredan pertenencia al grupo de acceso de volúmenes en el volumen de origen.

Tenga en cuenta lo siguiente al crear grupos de acceso de volúmenes:

- Un grupo de acceso de volúmenes puede contener hasta 64 IQN de iniciador.
- Un iniciador solo puede pertenecer a un grupo de acceso de volúmenes.
- Un grupo de acceso de volúmenes puede contener hasta 2000 volúmenes.
- Cada grupo de acceso de volúmenes puede pertenecer a un máximo de cuatro grupos de acceso de volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
iniciadores	Lista de ID o nombres de iniciador (IQN y WWPN) que se van a incluir en el grupo de acceso de volúmenes. Si pasa una lista de nombres de iniciador, se crean los iniciadores si no existen todavía. Si pasa una lista de ID de iniciador, el método devuelve un error si alguno de los iniciadores aún no existe. Pasar los nombres de iniciadores está obsoleto; debe usar ID de iniciador cuando sea posible.	matriz de enteros o matriz de cadenas (obsoleto)		No
nombre	El nombre del grupo de acceso de volúmenes. No es necesario ser único, pero se recomienda. Debe tener entre 1 y 64 caracteres de longitud.	cadena	Ninguno	Sí
volúmenes	Lista de ID de volumen que se incluirán en el grupo de acceso de volúmenes.	matriz en números enteros		No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	{}	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
VolumeAccessGroup	Un objeto que contiene información acerca del grupo de acceso de volúmenes recién creado.	VolumeAccessGroup
VolumeAccessGroupID	El ID del grupo de acceso de volúmenes recién creado.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "CreateVolumeAccessGroup",
   "params": {
      "name": "myaccessgroup",
      "initiators": ["iqn.1993-08.org.debian: 01: a31b1d799d5c"],
      "volumes": [327],
      "attributes": {}
   }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": null,
  "result": {
    "volumeAccessGroup": {
      "attributes": {},
      "deletedVolumes": [],
      "initiatorIDs": [
        95
      ],
      "initiators": [
        "iqn.1993-08.org.debian: 01: a31b1d799d5c"
      ],
      "name": "myaccessgroup",
      "volumeAccessGroupID": 96,
      "volumes": [
        327
      ]
    },
    "volumeAccessGroupID": 96
  }
}
```


Nuevo desde la versión

9.6

Obtenga más información

- GetAsyncResult
- ListSyncJobs
- Volumen ModificíoVolume

DeleteVolumeAccessGroup

Puede utilizar `DeleteVolumeAccessGroup` para eliminar un grupo de acceso de volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VolumeAccessGroupID	El ID del grupo de acceso de volúmenes que se eliminará.	entero	Ninguno	Sí
DeleteOrphanInitiators	Especifica si se eliminarán objetos iniciadores o no. Los posibles valores son los siguientes: • True: Elimine los objetos iniciadores después de que se eliminen de un grupo de acceso de volúmenes. • False: No se eliminan los objetos del iniciador después de que se quitan de un grupo de acceso de volúmenes. Este es el valor predeterminado.	booleano	falso	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
fuerza	Al añadir esta Marca, se fuerza la eliminación del grupo de acceso de volúmenes aunque tenga un ID de red virtual o una etiqueta. Los posibles valores son los siguientes: • True: Se eliminará el grupo de acceso de volúmenes. • False: Valor predeterminado. No elimine el grupo de acceso de volúmenes si tiene una etiqueta o un ID de red virtual.	booleano	falso	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "DeleteVolumeAccessGroup",
   "params": {
          "force": true,
      "volumeAccessGroupID"  : 3
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id" : 1,
   "result": {}
}
```

Nuevo desde la versión

9.6

ListVolumeAccessGroups

Puede utilizar el `ListVolumeAccessGroups` método para obtener información sobre los grupos de acceso de volúmenes que están actualmente en el sistema.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
límite	Número máximo de objetos volumeAccessGroup que devolver. Se excluyen mutuamente con el parámetro volumeAccessGroups.	entero	Ilimitada	No
StartVolumeAccessGroupID	El ID de grupo de acceso de volúmenes con el que comenzar la lista. Se excluyen mutuamente con el parámetro volumeAccessGroups.	entero	0	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VolumeAccessGroups	Lista de valores volumeAccessGroupID que se van a recuperar. Se excluyen mutuamente con los parámetros startVolumeAccessGroupID y limit.	matriz en números enteros		No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
VolumeAccessGroups	Una lista de objetos que describen cada grupo de acceso de volúmenes.	VolumeAccessGroup cabina
VolumeAccessGroupsNotFound	El sistema no encuentra una lista de los grupos de acceso de volúmenes. Presente si se utilizó el parámetro volumeAccessGroups y el sistema no pudo encontrar uno o más grupos de acceso de volúmenes que se especificaron.	matriz en números enteros

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListVolumeAccessGroups",
   "params": {
      "startVolumeAccessGroupID": 3,
      "limit"   : 1
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "volumeAccessGroups": [
      {
        "attributes": {},
        "deletedVolumes": [],
        "initiatorIDs": [],
        "initiators": [],
        "name": "example1",
        "volumeAccessGroupID": 3,
        "volumes": []
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

RemoveVolumesFromVolumeAccessGroup

Puede utilizar el `RemoveVolumesFromVolumeAccessGroup` método para quitar volúmenes de un grupo de acceso de volúmenes especificado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VolumeAccessGroupID	VolumeAccessGroupID para quitar volúmenes de.	entero	Ninguno	Sí
volúmenes	Los ID de volumen de los volúmenes que se quitarán del grupo de acceso de volúmenes.	matriz en números enteros	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumeAccessGroup	Un objeto que contiene información acerca del grupo de acceso de volúmenes recién modificado.	VolumeAccessGroup

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "RemoveVolumesFromVolumeAccessGroup",
   "params": {
      "volumeAccessGroupID": 96,
      "volumes": [1,2]
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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": []
    }
  }
}
```

Nuevo desde la versión

9.6

RemoveInitiatorsFromVolumeAccessGroup

Puede utilizar el `RemoveInitiatorsFromVolumeAccessGroup` método para quitar iniciadores de un grupo de acceso de volúmenes especificado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VolumeAccessGroupID	El ID del grupo de acceso de volúmenes del que se quitan los iniciadores.	entero	Ninguno	Sí
iniciadores	Lista de ID o nombres de iniciador (IQN y WWPN) que se van a incluir en el grupo de acceso de volúmenes. Si pasa una lista de nombres de iniciador, se crean los iniciadores si no existen todavía. Si pasa una lista de ID de iniciador, el método devuelve un error si alguno de los iniciadores aún no existe. Pasar los nombres de iniciadores está obsoleto; debe usar ID de iniciador cuando sea posible.	matriz de enteros (recomendado) o matriz de cadenas (obsoleto)	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
DeleteOrphanInitiators	Especifica si se eliminarán los objetos iniciadores después de que se eliminen de un grupo de acceso de volúmenes o no. Los posibles valores son los siguientes: • True: Elimine los objetos iniciadores después de que se eliminen de un grupo de acceso de volúmenes. • False: No se eliminan los objetos del iniciador después de que se quitan de un grupo de acceso de volúmenes. Este es el valor predeterminado.	booleano	falso	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumeAccessGroup	Un objeto que contiene información acerca del grupo de acceso de volúmenes recién modificado.	VolumeAccessGroup

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 13171,
  "method": "RemoveInitiatorsFromVolumeAccessGroup",
  "params": {
    "initiators": [114,115],
    "volumeAccessGroupID": 96
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 13171,
  "result": {
    "volumeAccessGroup": {
      "attributes": {},
      "deletedVolumes": [
        327
      ],
      "initiatorIDs": [],
      "initiators": [],
      "name": "test",
      "volumeAccessGroupID": 96,
      "volumes": [
        346
      ]
    }
  }
}
```

Nuevo desde la versión

9.6

ModifyVolumeAccessGroup

Puede utilizar el `ModifyVolumeAccessGroup` método para actualizar los iniciadores y añadir o quitar volúmenes de un grupo de acceso de volúmenes.

Si un iniciador o volumen especificado es un duplicado de lo que existe actualmente, el grupo de acceso de volúmenes se deja como está. Si no especifica un valor para los volúmenes o los iniciadores, no se cambia la lista actual de iniciadores y volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VolumeAccessGroupID	El ID del grupo de acceso de volúmenes que se desea modificar.	entero	Ninguno	Sí
nombre	El nuevo nombre de este grupo de acceso de volúmenes.	cadena	Ninguno	No
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
iniciadores	Lista de ID o nombres de iniciador (IQN y WWPN) que se van a incluir en el grupo de acceso de volúmenes. Si pasa una lista de nombres de iniciador, se crean los iniciadores si no existen todavía. Si pasa una lista de ID de iniciador, el método devuelve un error si alguno de los iniciadores aún no existe. Pasar los nombres de iniciadores está obsoleto; debe usar ID de iniciador cuando sea posible.	matriz de enteros (recomendado) o matriz de cadenas (obsoleto)	Ninguno	No

DeleteOrphanInitiators	Especifica si se eliminarán los objetos iniciadores después de que se eliminen de un grupo de acceso de volúmenes o no. Los posibles valores son los siguientes: • True: Elimine los objetos iniciadores después de que se eliminen de un grupo de acceso de volúmenes. • False: No se eliminan los objetos del iniciador después de que se quitan de un grupo de acceso de volúmenes. Este es el valor predeterminado.	booleano	falso	No
volúmenes	Una lista de ID de volumen de los volúmenes que se van a modificar.	matriz en números enteros	Ninguno	VolumeAccessGroup

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
VolumeAccessGroup	Un objeto que contiene información acerca del grupo de acceso de volúmenes recién modificado.	VolumeAccessGroup

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ModifyVolumeAccessGroup",
   "params": {
      "volumeAccessGroupID": 96,
      "name": "accessgrouptest",
      "initiators": [115,114],
      "volumes": [
         346
    ],
      "attributes": {}
   }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
      ]
    }
  }
}
```

Nuevo desde la versión

9.6

Obtenga más información

- AddInitiatorsToVolumeAccessGroup
- AddVolumesToVolumeAccessGroup
- RemoveInitiatorsFromVolumeAccessGroup
- RemoveVolumesFromVolumeAccessGroup

GetVolumeAccessGroupEfficency

Puede utilizar el `GetVolumeAccessGroupEfficiency` método para obtener información de eficiencia sobre un grupo de acceso de volúmenes. Solo el grupo de acceso de volúmenes que se proporciona como parámetro en este método de API se utiliza para calcular la capacidad.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VolumeAccessGroupID	Especifica el grupo de acceso de volúmenes en el que se calcula la capacidad.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
compresión	La cantidad de espacio que ahorra la compresión de datos en todos los volúmenes del grupo de acceso de volúmenes. Se afirma como una relación en la que el valor 1 significa que los datos se han almacenado sin compresión.	flotante
deduplicación	La cantidad de espacio ahorrado no duplicando datos para todos los volúmenes del grupo de acceso de volúmenes. Se indica como una relación.	flotante

Thin Provisioning	La relación entre el espacio utilizado y la cantidad de espacio asignado para almacenar datos. Se indica como una relación.	flotante
fecha/hora	La última vez que se recopilaron datos de eficiencia después de la recolección de basura.	Cadena de datos ISO 8601
Volúmenes missingVolumes	Los volúmenes que no se pudieron consultar para los datos de eficiencia. Los volúmenes que faltan pueden deberse a una recopilación de datos basura reciente, a una pérdida temporal de red o a servicios reiniciados desde el ciclo de recopilación de datos basura.	matriz en números enteros

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "GetVolumeAccessGroupEfficiency",
   "params": {
      "volumeAccessGroupID": 1
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
   "id": 1,
   "result": {
       "compression": 2.006012925331075,
       "deduplication": 1,
       "missingVolumes": [],
       "thinProvisioning": 1.009861932938856,
       "timestamp": "2014-03-10T17:05:27Z"
   }
}
```

Nuevo desde la versión

9.6

Métodos de API de Snapshot de volumen

Los métodos de la API de Snapshot de volumen del software Element permiten gestionar copias de Snapshot de volumen. Es posible crear, modificar, clonar y eliminar copias de Snapshot de volumen con los métodos de API de snapshot de volumen.

- Información general de Snapshot
- CreateGroupSnapshot
- CreateSchedule
- CreateSnapshot
- DeleteGroupSnapshot
- DeleteSnapshot
- GetSchedule
- ListGroupSnapshots
- ListSchedules
- ListSnapshots
- ModifiyGroupSnapshot
- ModificySchedule
- ModificySnapshot
- RollbackToGroupSnapshot
- RollbackToSnapshot

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Información general de Snapshot

Una copia de Snapshot de volumen es una copia de un momento específico de un volumen. Las copias de Snapshot se pueden usar para revertir un volumen al estado que tenía en el momento de creación de las copias.

Puede agrupar copias de Snapshot de volumen para que los volúmenes relacionados puedan respaldarse o revertirse de forma coherente. Una snapshot de grupo captura una imagen puntual de todos los archivos de segmentos de volúmenes. A continuación, se puede usar la imagen para revertir un grupo de volúmenes a un estado de un momento específico y garantizar que todos los datos sean consistentes en todos los volúmenes del grupo.

Se pueden programar snapshots de volúmenes para que se produzcan de forma autónoma en intervalos definidos. Puede definir intervalos por tiempo, días de la semana o días del mes. También puede utilizar

copias Snapshot programadas para garantizar que se realice un backup de las copias Snapshot en un almacenamiento remoto con fines de archivado.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

CreateGroupSnapshot

Puede utilizar `CreateGroupSnapshot` para crear una copia de un momento específico de un grupo de volúmenes.

Es posible usar esta Snapshot más adelante como backup o reversión para garantizar que los datos en el grupo de volúmenes sean consistentes durante el momento específico que se creó la Snapshot.

CLUSTER_LLENY

Puede crear copias de Snapshot si la ocupación del clúster se encuentra en la etapa 1, 2 o 3. No se pueden crear copias de Snapshot cuando la ocupación del clúster llegue a la etapa 4 o 5.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`attributes`	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`enableRemoteReplication`	Especifica si la copia de Snapshot se replicará o no en el almacenamiento remoto. Los posibles valores son los siguientes: • `true`: La instantánea se replicará en el almacenamiento remoto. • `false`: La instantánea no se replicará en el almacenamiento remoto.	booleano	falso	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`ensureSerialCreation`	Especifica que no se debe crear la instantánea si hay una replicación de instantánea anterior en curso. Los valores posibles son: • `true`: Esto garantiza que sólo se replica una instantánea a la vez. Se producirá un error al crear una nueva snapshot si aún hay una replicación de snapshot anterior en curso. • `false`: Predeterminado. Esta creación de snapshot se permite si otra replicación de snapshot aún está en curso.	booleano	`false`	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`expirationTime`	Especifique la hora después de la cual puede eliminarse la snapshot. No se puede utilizar con `retention`. Si ninguno `expirationTime`, o. `retention` se especifican, la instantánea no caducará. El formato de hora es una cadena de fecha ISO 8601 para vencimiento basado en tiempo; de lo contrario, no caducará. Valor de `null` hace que la copia de snapshot se retenga de forma permanente. Valor de `fifo` Hace que la instantánea se conserve primero en entrar primero en salir (FIFO), en relación con otras instantáneas FIFO del volumen. La API fallará si no hay espacio FIFO disponible.	Cadena de fecha ISO 8601	Ninguno	No
`name`	El nombre de la copia de Snapshot de grupo. Si no se introduce ningún nombre, se utilizará la fecha y la hora en que se tomó la snapshot de grupo. La longitud máxima permitida para el nombre es de 255 caracteres.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`retention`	Este parámetro es el mismo que el `expirationTime` El parámetro, excepto el formato de hora es HH:mm:ss Si ninguno `expirationTime` tampoco `retention` se especifican, la instantánea no caducará.	cadena	Ninguno	No
`snapMirrorLabel`	La etiqueta que utiliza el software SnapMirror para especificar la política de retención de snapshots en un extremo de SnapMirror.	cadena	Ninguno	No
`volumes`	ID único de la imagen de volumen de la que se desea copiar.	Cabina volumeID	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo

miembros	Lista de suma de comprobación, volumeID y snapshotID para cada miembro del grupo. Valores válidos: • Suma de comprobación: Una pequeña representación de cadena de los datos de la instantánea almacenada. Esta suma de comprobación se puede utilizar más adelante para comparar otras instantáneas con el fin de detectar errores en los datos. (cadena) • SnapshotID: ID exclusivo de una copia de Snapshot desde la que se realiza la nueva copia de Snapshot. El ID de copia Snapshot debe ser de una copia Snapshot en un volumen determinado. (entero) • VolumeID: El ID del volumen de origen de la copia de Snapshot. (entero)	Cabina de objetos JSON
GroupSnapshotID	El ID único de la copia de Snapshot de grupo nueva.	ID de groupSnapshot
GroupSnapshot	Objeto que contiene información acerca de la snapshot de grupo recién creada.	GroupSnapshot

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "CreateGroupSnapshot",
   "params": {
      "volumes": [1,2]
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

CreateSchedule

Puede utilizar `CreateSchedule` para programar una snapshot automática de un volumen en un intervalo definido.

Es posible usar la snapshot creada más adelante como un backup o una reversión para garantizar que los datos de un volumen o un grupo de volúmenes sean consistentes en el momento específico en el que se creó la snapshot. Si se programa la ejecución de una copia de Snapshot en un período que no sea divisible entre 5 minutos, la copia de Snapshot se ejecutará en el siguiente período que lo sea 5. Por ejemplo, si se programa la ejecución de una copia de Snapshot a las 12:42:00 UTC, se realizará a las 12:45:00 UTC. No se podrá programar la ejecución de una copia de Snapshot en intervalos inferiores a 5 minutos.

Puede crear copias de Snapshot si la ocupación del clúster se encuentra en la etapa 1, 2 o 3. No se pueden crear copias de Snapshot cuando la ocupación del clúster llegue a la etapa 4 o 5.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`attributes`	Utilice la cadena "'frequency'" para indicar la frecuencia de la instantánea. Los posibles valores son los siguientes: • `Days of Week` • `Days of Month` • `Time Interval`	Objeto JSON	Ninguno	No
`hasError`	**Se necesita ayuda con descripción**	booleano	`false`	No
`hours`	Cantidad de horas entre instantáneas recurrentes o hora en la hora GMT que la snapshot se realizará en el modo días de la semana o días del mes. Los valores válidos abarcan de 0 a 23.	entero	Ninguno	No
`lastRunStatus`	El resultado o el estado de la última creación de snapshot programada.	cadena	Ninguno	No
`name`	El nombre de la copia de Snapshot. Si no se introduce ningún nombre, se utilizará la fecha y la hora en que se tomó la snapshot de grupo. La longitud máxima permitida para el nombre es de 244 caracteres.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`minutes`	Cantidad de minutos entre las snapshots que se repiten o el minuto en la hora GMT en que la snapshot se producirá en el modo días de la semana o días del mes. Los valores válidos son de 5 a 59.	entero	Ninguno	No
`paused`	Indica si la programación debe estar en pausa o no. Valores válidos: • `true` • `false`	booleano	Ninguno	No
`recurring`	Indica si la programación será periódica o no. Valores válidos: • `true` • `false`	booleano	Ninguno	No
`runNextInterval`	Especifica si se va a ejecutar la snapshot la próxima vez que esté activo el programador. Cuando se configura en true, la snapshot programada se ejecuta la próxima vez que el programador esté activo y se restablece en false. Valores válidos: • `true` • `false`	booleano	`false`	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`scheduleName`	Nombre único de la programación. La longitud máxima permitida para el nombre de programación es de 244 caracteres.	cadena	Ninguno	Sí
`scheduleType`	Indica el tipo de programación que se va a crear. El valor válido es snapshot.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`scheduleInfo`	El nombre único que se le asignó a la programación, el período de retención de la copia de Snapshot que se creó y el ID de volumen del volumen a partir del cual se creó la copia de Snapshot. Valores válidos: • `volumeID`: El ID del volumen que se incluirá en la instantánea. (entero) • `volumes`: Lista de ID de volumen que se incluirán en la instantánea de grupo. (matriz entera) • `name`: El nombre de la instantánea que se va a utilizar. (cadena) • `enableRemoteReplication`: Indica si la instantánea debe incluirse en la replicación remota. (booleano) • `retention`: La cantidad de tiempo que la instantánea se conservará en HH:mm:ss Si está vacío, la copia de Snapshot se conserva siempre. (cadena) `fifo`: La instantánea se	Objeto JSON	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`snapMirrorLabel`	La etiqueta que utiliza el software SnapMirror para especificar la política de retención de snapshots en un extremo de SnapMirror.	cadena	Ninguno	No
`startingDate`	Hora después de la cual se ejecutará la programación. Si no se define, la programación se inicia de inmediato. Con formato de hora UTC.	Cadena de fecha ISO 8601	Ninguno	No
`toBeDeleted`	Especifica que esta programación de snapshots se debe eliminar una vez que se completa la creación de la snapshot.	booleano	`false`	No
`monthdays`	Los días del mes en que se realizará una copia de Snapshot. Los valores válidos son de 1 a 31.	matriz en números enteros	Ninguno	Sí (si está programado para los días del mes)

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`weekdays`	Día de la semana en que se va a crear la snapshot. Valores requeridos (si se utiliza): • `Day`: 0 a 6 (de domingo a sábado) • `Offset`: Por cada semana posible en un mes, 1 a 6 (Si es mayor de 1, sólo igualado en el día Nth-1 de la semana. Por ejemplo, offset:3 para domingo significa el tercer domingo del mes, mientras que offset:4 para miércoles significa el cuarto miércoles del mes. Offset:0 significa que no se realiza ninguna acción. Offset:1 (predeterminado) significa que la snapshot se crea para este día de la semana, independientemente de dónde esté en el mes	Cabina de objetos JSON	Ninguno	Sí (si está programado para los días de la semana)

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
ID de intervalo	Se creó el ID de la programación.	entero

programación	Objeto que contiene información acerca de la programación recién creada.	programación

Ejemplo de solicitud 1

En el siguiente ejemplo de programación se tienen los parámetros siguientes:

- No se especifican horas ni minutos de inicio, por lo que el programa comienza lo más cerca posible a medianoche (00:00:00Z).
- No es recurrente (sólo se ejecutará una vez).
- Se ejecuta una vez en el primer domingo o miércoles después del 1 de junio de 2015, UTC 19:17:15Z (cualquier día que llegue primero).
- Solo incluye un volumen (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
}
}
}
```

Ejemplo de respuesta 1

La solicitud anterior devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
  }
}
```


Ejemplo de solicitud 2

En el siguiente ejemplo de programación se tienen los parámetros siguientes:

- Es recurrente (se ejecutará en cada intervalo programado del mes a la hora especificada).

- Funciona el 1, 10, 15 y 30 de cada mes siguiente a la fecha de inicio.
- Se ejecuta a las 12:15 PM cada día que está programado para ocurrir.
- Solo incluye un volumen (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
}
```

Ejemplo de respuesta 2

La solicitud anterior devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
  }
}
```


Ejemplo de solicitud 3

En el siguiente ejemplo de programación se tienen los parámetros siguientes:

- Comienza dentro de los 5 minutos del intervalo programado el 2 de abril de 2015.
- Es recurrente (se ejecutará en cada intervalo programado del mes a la hora especificada).
- Se ejecuta en el segundo, tercero y cuarto de cada mes después de la fecha de inicio.
- Se ejecuta a las 14:45 PM cada día que está programado para ocurrir.
- Incluye un grupo de volúmenes (volúmenes = 1 y 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
}
```

Ejemplo de respuesta 3

La solicitud anterior devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
  }
}
```


Nuevo desde la versión

9.6

CreateSnapshot

Puede utilizar `CreateSnapshot` para crear una copia de un momento específico de un volumen. Es posible crear una snapshot desde cualquier volumen o desde una snapshot

existente.

Si no se proporciona un identificador de copia Snapshot con este método de API, se crea una copia Snapshot a partir de la rama activa del volumen. Si el volumen a partir del que se crea la snapshot se está replicando en un clúster remoto, la snapshot también puede replicarse en el mismo destino. Use el parámetro enableRemoteReplication para habilitar la replicación Snapshot.

Puede crear copias de Snapshot si la ocupación del clúster se encuentra en la etapa 1, 2 o 3. No se pueden crear copias de Snapshot cuando la ocupación del clúster llegue a la etapa 4 o 5.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`attributes`	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
`enableRemoteReplication`	Especifica si la copia de Snapshot se replicará o no en el almacenamiento remoto. Los posibles valores son los siguientes: • `true`: La instantánea se replicará en el almacenamiento remoto. • `false`: La instantánea no se replicará en el almacenamiento remoto.	booleano	falso	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`ensureSerialCreation`	Especifica que no se debe crear la instantánea si hay una replicación de instantánea anterior en curso. Los valores posibles son: • `true`: Esto garantiza que sólo se replica una instantánea a la vez. Se producirá un error al crear una nueva snapshot si aún hay una replicación de snapshot anterior en curso. • `false`: Predeterminado. Esta creación de snapshot se permite si otra replicación de snapshot aún está en curso.	booleano	`false`	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Tiempo de caducidad	Especifique la hora después de la cual puede eliminarse la snapshot. No se puede utilizar con `retention`. Si no se especifica ni el tiempo de caducidad ni la retención, la snapshot no caducará. El formato de hora es una cadena de fecha ISO 8601 para vencimiento basado en tiempo; de lo contrario, no caducará. Valor de `null` hace que la copia de snapshot se retenga de forma permanente. Valor de `fifo` Hace que la instantánea se conserve primero en salir, con relación a otras instantáneas del FIFO del volumen. La API fallará si no hay espacio FIFO disponible.	cadena	Ninguno	No
`name`	El nombre de la copia de Snapshot. Si no se introduce ningún nombre, se utilizará la fecha y la hora en que se realizó la instantánea. La longitud máxima permitida para el nombre es de 255 caracteres.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`retention`	Este parámetro es el mismo que el `expirationTime` El parámetro, excepto el formato de hora es HH:mm:ss Si ninguno `expirationTime` tampoco `retention` se especifican, la instantánea no caducará.	cadena	Ninguno	No
`snapMirrorLabel`	La etiqueta que utiliza el software SnapMirror para especificar la política de retención de snapshots en un extremo de SnapMirror.	cadena	Ninguno	No
`snapshotID`	El ID exclusivo de una copia de Snapshot a partir de la cual se realiza la nueva copia de Snapshot. El ID de copia Snapshot aprobada debe ser una copia de Snapshot en un volumen determinado.	entero	Ninguno	No
`volumeID`	ID único de la imagen de volumen de la que se desea copiar.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo

suma de comprobación	Una cadena que representa los dígitos correctos de la instantánea almacenada. Esta suma de comprobación se puede utilizar más adelante para comparar otras instantáneas con el fin de detectar errores en los datos.	cadena
ID de copia Snapshot	El ID exclusivo de la snapshot nueva.	ID de snapshot
snapshot	Un objeto que contiene información acerca de la snapshot recién creada.	snapshot

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "CreateSnapshot",
   "params": {
      "volumeID": 1
   },
   "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
  }
}
```


Excepción

Una excepción xNotPrimary se muestra cuando la `CreateSnapshot` Se llama a la API y la snapshot no se puede crear. Este es el comportamiento esperado. Vuelva a intentar el `CreateSnapshot` Llamada a API.

Nuevo desde la versión

9.6

DeleteGroupSnapshot

Puede utilizar `DeleteGroupSnapshot` para eliminar una copia de snapshot de grupo.

Puede utilizar el parámetro saveMembers para conservar todas las instantáneas que se han realizado para los volúmenes del grupo, pero se eliminará la asociación de grupo.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
GroupSnapshotID	El ID único de la copia de Snapshot de grupo.	entero	Ninguno	Sí
Miembros de saveMembers	Especifica qué se debe eliminar al eliminar una copia de Snapshot de grupo. Valores válidos: • True: Se mantienen las instantáneas, pero se elimina la asociación de grupo. • False: Se eliminan el grupo y las instantáneas.	booleano	falso	No

Valor de retorno

Este método no tiene ningún valor devuelto.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "DeleteGroupSnapshot",
     "params": {
       "groupSnapshotID": 10,
       "saveMembers" : true
        },
     "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nuevo desde la versión

9.6

DeleteSnapshot

Puede utilizar el `DeleteSnapshot` método para eliminar una snapshot.

Una copia de Snapshot que actualmente es la copia de Snapshot activa no se puede eliminar. Debe revertir y hacer otra copia de Snapshot activa para poder eliminar la copia de Snapshot actual.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de copia Snapshot	El ID de la copia de Snapshot que se desea eliminar.	entero	Ninguno	Sí
OverrideSnapMirror Hold	Anule el bloqueo colocado en las snapshots durante la replicación. Puede usar este parámetro para eliminar copias de Snapshot obsoletas de SnapMirror después de haber eliminado la relación de SnapMirror asociada.	booleano	falso	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "DeleteSnapshot",
"params": {
"snapshotID": 8,
"overrideSnapMirrorHold": true
},
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nuevo desde la versión

9.6

Obtenga más información

RollbackToSnapshot

GetSchedule

Puede utilizar `GetSchedule` para obtener información acerca de una snapshot programada.

Puede ver información sobre una programación específica si hay muchas programaciones de snapshots en el sistema. También puede recuperar información sobre más de un programa con este método especificando ID adicionales en el parámetro ScheduleID.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de intervalo	ID exclusivo del programa o varias programaciones que se mostrarán.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
programación	Una cabina de atributos de programación.	programación cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
"method": "GetSchedule",
  "params": {
              "scheduleID" : 2
      },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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": []
      }
   }
}
```


Nuevo desde la versión

9.6

ListGroupSnapshots

Puede utilizar `ListGroupSnapshots` método para obtener información acerca de todas las instantáneas de grupo que se han creado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
GroupSnapshotID	Recuperar información de un ID de snapshot de grupo individual.	entero	Ninguno	No
volúmenes	Una cabina de ID de volumen únicos que se pueden consultar. Si no se especifica este parámetro, se incluyen todas las copias de Snapshot de grupo en el clúster.	Cabina volumeID	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
GroupSnapshots	Lista de los objetos que contienen información sobre cada snapshot de grupo.	GroupSnapshot cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListGroupSnapshots",
  "params": {
  "volumes": [
     31,
     49
    ]
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
```

```
  "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"
      }
```

```
    ]
}
```

Nuevo desde la versión

9.6

ListSchedules

Puede utilizar `ListSchedules` para obtener información acerca de todas las instantáneas programadas que se han creado.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
programaciones	Una lista de las programaciones que actualmente están en el clúster.	programación cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListSchedules",
    "params": {},
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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": []
        }
      ]
   }
}
```

Nuevo desde la versión

9.6

ListSnapshots

Puede utilizar `ListSnapshots` para devolver los atributos de cada snapshot que se toma en el volumen.

La información sobre las copias de Snapshot que residen en el clúster de destino se muestra en el clúster de origen cuando se llama a este método desde el clúster de origen.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	Recupera snapshots de un volumen. Si no se muestra volumeID, se devuelven todas las copias de Snapshot de todos los volúmenes.	entero	Ninguno	No
ID de copia Snapshot	Recupera información de un ID de snapshot individual.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
snapshot	Información sobre cada snapshot de cada volumen. Si no se muestra volumeID, se devuelven todas las copias de Snapshot de todos los volúmenes. Las copias de Snapshot que están en un grupo se devuelven con un ID de grupo.	snapshot cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListSnapshots",
   "params": {
             "volumeID": "1"
       },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
        }
      ]
    }
  }
```


Nuevo desde la versión

9.6

ModifiyGroupSnapshot

Puede utilizar `ModifyGroupSnapshot` para cambiar los atributos de un grupo de snapshots. Este método también se puede usar para habilitar copias de Snapshot creadas en el volumen de lectura/escritura (origen) y que se replican de forma remota a un sistema de almacenamiento de destino.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
EnableRemoteReplication	Utilice para habilitar la copia de Snapshot creada para replicarse en un clúster remoto. Los posibles valores son los siguientes: • `true`: La instantánea se replicará en el almacenamiento remoto. • `false`: La instantánea no se replicará en el almacenamiento remoto.	booleano	falso	No

Tiempo de caducidad	Especifique la hora después de la cual puede eliminarse la snapshot. No se puede utilizar con retención. Si no se especifica ni el tiempo de caducidad ni la retención en la snapshot original, la snapshot no caducará. El formato de hora es una cadena de fecha ISO 8601 para vencimiento basado en tiempo; de lo contrario, no caducará. Valor de `null` hace que la copia de snapshot se retenga de forma permanente. El valor de fifo hace que la instantánea se conserve primero en entrar primero en salir (FIFO), en relación con otras instantáneas del FIFO del volumen. La API fallará si no hay espacio FIFO disponible.	Cadena de fecha ISO 8601	Ninguno	No
nombre	El nombre de la copia de Snapshot de grupo. Si no se introduce ningún nombre, se utilizará la fecha y la hora en que se tomó la snapshot de grupo. La longitud máxima permitida para el nombre es de 255 caracteres.	cadena	Ninguno	No
GroupSnapshotID	El ID del grupo de copias de Snapshot.	cadena	Ninguno	Sí

SnapMirrorLabel	La etiqueta que utiliza el software SnapMirror para especificar la política de retención de snapshots en un extremo de SnapMirror.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
GroupSnapshot	Objeto que contiene información acerca de la snapshot de grupo recién modificada.	GroupSnapshot

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 695,
  "method": "ModifyGroupSnapshot",
  "params": {
    "groupSnapshotID": 3,
    "enableRemoteReplication": true,
    "expirationTime": "2016-04-08T22:46:25Z"
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
    }
  }
}
```


Nuevo desde la versión

9.6

ModificySchedule

Puede utilizar `ModifySchedule` cambiar los intervalos en los que se produce una snapshot programada. También puede eliminar o pausar una programación mediante este método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
atributos	Se utiliza para cambiar la frecuencia de la aparición de la snapshot. Los posibles valores son los siguientes: • `Days of Week` • `Days of Month` • `Time Interval`	Objeto JSON	Ninguno	No
horas	Cantidad de horas entre las instantáneas o la hora en que se realizará la copia de Snapshot en el modo días de la semana o días del mes. Los valores válidos abarcan de 0 a 24.	cadena	Ninguno	No
nombre	El nombre de la copia de Snapshot. Si no se introduce ningún nombre, se utilizará la fecha y la hora en que se tomó la snapshot de grupo. La longitud máxima permitida para el nombre es de 244 caracteres.	cadena	Ninguno	No

minutos	Cantidad de minutos entre las instantáneas o los minutos en los que se realizará la copia de Snapshot en el modo días de la semana o días del mes. Los valores válidos abarcan de 0 a 59.	entero	Ninguno	No
LastRunStatus	El resultado o el estado de la última creación de snapshot programada.	cadena	Ninguno	No
en pausa	Indica si la programación debe estar en pausa o no. Valores válidos: • `true` • `false`	booleano	Ninguno	No
recurrente	Indica si la programación será periódica o no. Valores válidos: • `true` • `false`	booleano	Ninguno	No

RunNextInterval	Utilice para elegir si desea ejecutar o no la snapshot la próxima vez que esté activo el programador. Valores válidos: • `true` • `false` Cuando se configura en true, la snapshot programada se ejecuta la próxima vez que el programador esté activo y, a continuación, se restablece en false.	booleano	falso	No
ID de intervalo	El ID único de la programación.	entero	Ninguno	Sí
Nombre de la pila	Nombre único de la programación. La longitud máxima permitida para el nombre de programación es de 244 caracteres.	cadena	Ninguno	No
Tipo de columna	Indica el tipo de programación que se va a crear. El único valor admitido es `snapshot`.	cadena	Ninguno	Sí

`scheduleInfo`	El nombre único que se le asignó a la programación, el período de retención de la copia de Snapshot que se creó y el ID de volumen del volumen a partir del cual se creó la copia de Snapshot. Valores válidos: • `enableRemoteReplication`: Indica si la instantánea debe incluirse en la replicación remota. (booleano) • `ensureSerialCreation`: Especifica si se debe permitir la creación de una nueva instantánea si se está realizando una replicación de instantánea anterior. (booleano) • `name`: El nombre de la instantánea que se va a utilizar. (cadena) • `retention`: La cantidad de tiempo que se retiene la instantánea. Dependiendo de la hora, se muestra en uno de los siguientes formatos: ◦ `fifo`: La instantánea se mantiene en base al primero en primero en salir (FIFO). Si está	"programación"	Ninguno	No

SnapMirrorLabel	La etiqueta que utiliza el software SnapMirror para especificar la política de retención de snapshots en un extremo de SnapMirror.	cadena	Ninguno	No
ToDeDeleted	Indica si la programación está marcada para eliminarse. Valores válidos: • `true` • `false`	booleano	Ninguno	No
Fecha de inicio	Indica la fecha la primera vez que se inició o empezará la programación.	Cadena de fecha ISO 8601	Ninguno	No
mesdays	Los días del mes en que se realizará una copia de Snapshot. Los valores válidos son de 1 a 31.	matriz en números enteros	Ninguno	Sí
días laborables	Día de la semana en que se va a crear la snapshot. El día de la semana comienza el domingo con el valor de 0 y un desplazamiento de 1.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
programación	Objeto que contiene los atributos de programación modificados.	programación

Ejemplo de solicitud

```
{
  "method": "ModifySchedule",
  "params": {
    "scheduleName" : "Chicago",
    "scheduleID" : 3
    },
  "id": 1
}
```

Ejemplo de respuesta

```
{
  "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
      }
      ]
    }
  }
}
```


Nuevo desde la versión

9.6

ModificySnapshot

Puede utilizar `ModifySnapshot` para cambiar los atributos actualmente asignados a una snapshot. También se puede usar este método para habilitar las copias de Snapshot creadas en el volumen de lectura/escritura (origen) y que se replican de forma remota a un clúster de almacenamiento de destino donde se ejecuta el software Element.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
EnableRemoteReplication	Utilice para habilitar la copia de Snapshot creada para replicarse en un clúster de almacenamiento remoto. Los posibles valores son los siguientes: • `true`: La instantánea se replicará en el almacenamiento remoto. • `false`: La instantánea no se replicará en el almacenamiento remoto.	booleano	falso	No

Tiempo de caducidad	Especifique la hora después de la cual puede eliminarse la snapshot. No se puede utilizar con retención. Si no se especifica ni el tiempo de caducidad ni la retención en la snapshot original, la snapshot no caducará. El formato de hora es una cadena de fecha ISO 8601 para vencimiento basado en tiempo; de lo contrario, no caducará. El valor null hace que la snapshot se retenga de forma permanente. El valor de fifo hace que la instantánea se conserve primero en entrar primero en salir (FIFO), en relación con otras instantáneas del FIFO del volumen. La API fallará si no hay espacio FIFO disponible.	Cadena de fecha ISO 8601	Ninguno	No
nombre	El nombre de la copia de Snapshot. Si no se introduce ningún nombre, se utilizará la fecha y la hora en que se realizó la instantánea. La longitud máxima permitida para el nombre es de 255 caracteres.	cadena	Ninguno	No

SnapMirrorLabel	La etiqueta que utiliza el software SnapMirror para especificar la política de retención de snapshots en un extremo de SnapMirror.	cadena	Ninguno	No
ID de copia Snapshot	Identificador de la copia de Snapshot.	cadena	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
snapshot	Un objeto que contiene información acerca de la snapshot recién modificada.	snapshot

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ModifySnapshot",
  "params": {
    "snapshotID": 3114,
    "enableRemoteReplication": "true",
    "name" : "Chicago"
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
    }
  }
}
```


Nuevo desde la versión

9.6

RollbackToGroupSnapshot

Puede utilizar `RollbackToGroupSnapshot` para revertir todos los volúmenes individuales de un grupo de snapshots a la snapshot individual de cada volumen.

Al revertir a una copia de Snapshot de grupo, se crea una copia de Snapshot temporal de cada volumen dentro de la copia de Snapshot de grupo.

- Se permite la creación de una copia de Snapshot si la ocupación del clúster se encuentra en la etapa 1, 2 o 3. Las copias de Snapshot no se crean cuando la ocupación del clúster se encuentra en la etapa 4 o 5.
- Es posible que se produzca un error en la reversión de volúmenes a una copia de Snapshot de grupo cuando la sincronización de segmentos está en curso. Vuelva a intentarlo `RollbackToGroupSnapshot` una vez finalizada la sincronización.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
`groupSnapshotID`	El ID único de la copia de Snapshot de grupo.	entero	Ninguno	Sí
`attributes`	La lista de pares nombre-valor en el formato de objetos JSON.	Objeto JSON	Ninguno	No
`name`	Nombre de la copia de Snapshot de grupo del estado actual del volumen que se crea si `saveCurrentState` se establece en true. Si no se otorga un nombre, el nombre de las copias de Snapshot (grupo y volumen individual) se establece en una Marca de hora en la que se produjo la reversión.	cadena	Ninguno	No
`saveCurrentState`	Especifica si se debe guardar o no la imagen de volumen activo anterior. Valores válidos: • `true`: Se mantiene la imagen de volumen activo anterior. • `false`: Se elimina la imagen de volumen activo anterior.	booleano	falso	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
miembros	Una cabina que contiene volumeID y snapshotID de miembros de la copia de Snapshot de grupo. Valores: • Suma de comprobación: Una pequeña representación de cadena de los datos de la instantánea almacenada. Esta suma de comprobación se puede utilizar más adelante para comparar otras instantáneas con el fin de detectar errores en los datos. (cadena) • SnapshotID: ID exclusivo de una copia de Snapshot desde la que se realiza la nueva copia de Snapshot. El ID de copia Snapshot debe ser una copia de Snapshot en un volumen determinado. (entero) • VolumeID: El ID del volumen de origen de la copia de Snapshot. (entero)	Cabina de objetos JSON
GroupSnapshotID	Si `saveCurrentState` se estableció en false, este valor es null. Si `saveCurrentState` Se estableció en TRUE, el ID único de la snapshot de grupo recién creada.	entero
GroupSnapshot	Si `saveCurrentState` se estableció en false, este valor es null. Si `saveCurrentState` se estableció en true, un objeto que contiene información sobre la snapshot de grupo que `RollbackToGroupSnapshot` sólo voló hacia atrás.	GroupSnapshot

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 438,
  "method": "RollbackToGroupSnapshot",
  "params": {
    "groupSnapshotID": 1,
    "name": "grpsnap1",
    "saveCurrentState": true
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

RollbackToSnapshot

Puede utilizar el `RollbackToSnapshot` método para realizar una snapshot existente de la imagen de volumen activa. Este método crea una snapshot nueva a partir de una snapshot existente.

La nueva snapshot estará activa y se conservará la snapshot existente hasta que se elimine manualmente. La instantánea anteriormente activa se elimina a menos que se establezca el parámetro saveCurrentState en TRUE.

CLUSTER_LLENY

- Puede crear copias de Snapshot si la ocupación del clúster se encuentra en la etapa 1, 2 o 3. No se pueden crear copias de Snapshot cuando la ocupación del clúster llegue a la etapa 4 o 5.
- Es posible que se produzca un error en la reversión de un volumen a una copia de Snapshot cuando la sincronización de segmentos está en curso. Vuelva a intentarlo `RollbackToSnapshot` una vez finalizada la sincronización.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de volumen	El ID de volumen del volumen.	entero	Ninguno	Sí
atributos	La lista de pares nombre-valor en el formato de objetos JSON.	Atributos JSON	Ninguno	No
nombre	Nombre de la copia de Snapshot. Si no se da ningún nombre, se utiliza el nombre de la instantánea a la que se va a revertir con "- copy" adjunto al final del nombre.	cadena	Ninguno	No
ID de copia Snapshot	El ID de una copia de Snapshot creada previamente en el volumen determinado.	entero	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
SaveCurrentState	Especifica si se debe guardar o no una imagen de volumen activo anterior. Valores válidos: • True: Se mantiene la imagen del volumen activo anterior. • False: Se elimina la imagen del volumen activo anterior.	booleano	falso	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
suma de comprobación	Una pequeña representación de cadena de los datos de la instantánea almacenada.	cadena
ID de copia Snapshot	Si saveCurrentState se estableció en FALSE, este valor es nulo. Si saveCurrentState se estableció en true, el identificador único de la instantánea recién creada.	entero
snapshot	Si saveCurrentState se estableció en FALSE, este valor es nulo. Si saveCurrentState se estableció en true, un objeto que contiene información acerca de la instantánea recién creada.	snapshot

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
 "method": "RollbackToSnapshot",
 "params": {
    "volumeID": 1,
    "snapshotID": 3114,
    "saveCurrentState": true
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
  }
}
```

Nuevo desde la versión

9.6

Métodos de API para volúmenes virtuales

Los métodos de API de volumen virtual del software Element permiten gestionar volúmenes virtuales (VVol). Los VVol existentes se pueden ver con estos métodos API, así como crear, modificar y eliminar contenedores de almacenamiento de volúmenes virtuales. Aunque no puede utilizar estos métodos para funcionar en volúmenes normales, puede utilizar los métodos de API de volumen normales para enumerar la información sobre VVol.

- CreateStorageContainer
- DeleteStorageContainers
- GetStorageContainerEfficiency
- GetVirtualVolumeCount
- ListProtocolEndpoints
- ListStorageContainers
- ListVirtualVolumeBindings
- ListVirtualVolumeHosts
- ListVirtualVolumes
- ListVirtualVolumeTasks
- ModificyStorageContainer

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

CreateStorageContainer

Puede utilizar el `CreateStorageContainer` Método para crear un contenedor de almacenamiento volumen virtual (VVol). Los contenedores de almacenamiento se pueden usar para crear informes y asignar recursos. Es necesario crear al menos un contenedor de almacenamiento para usar la función Virtual Volumes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
nombre	Nombre del contenedor de almacenamiento. Sigue las restricciones de nomenclatura de cuentas de software Element.	cadena	Ninguno	Sí
ID de cuenta	Cuenta que no es un contenedor de almacenamiento que se convertirá en un contenedor de almacenamiento.	entero	Ninguno	No
InitiatorSecret	El secreto de la autenticación CHAP del iniciador.	cadena	Ninguno	No
TargetSecret	El secreto de la autenticación CHAP del destino.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Contenedor de almacenamiento	Objeto que contiene información sobre el contenedor de almacenamiento recién creado.	Contenedor de almacenamiento

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "CreateStorageContainer",
    "params": {
        "name" : "example"
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
    }
  }
}
```

Nuevo desde la versión

9.6

DeleteStorageContainers

Puede utilizar el `DeleteStorageContainers` Método para eliminar hasta 2000 contenedores de almacenamiento Virtual Volume (VVol) del sistema a la vez. Los contenedores de almacenamiento que se quitan no deben contener ningún VVol.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ContenerID de almacenamiento	Una lista de ID de los contenedores de almacenamiento que se van a eliminar. Puede especificar hasta 2000 ID en la lista.	Cabina de UUID	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DeleteStorageContainers",
    "params": {
        "storageContainerIDs" : ["a9ec1138-e386-4a44-90d7-b9acbbc05176"]
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nuevo desde la versión

9.6

GetStorageContainerEfficiency

Puede utilizar el `GetStorageContainerEfficiency` método para recuperar información de eficiencia acerca de un contenedor de almacenamiento de volumen virtual.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de almacenamiento ContainerID	El ID del contenedor de almacenamiento del que se puede recuperar la información de eficiencia.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
compresión	La cantidad de espacio que ahorra la compresión de datos en todos los volúmenes virtuales del contenedor de almacenamiento. Se afirma como una relación en la que el valor 1 significa que los datos se han almacenado sin compresión.	flotante
deduplicación	La cantidad de espacio ahorrado no duplicando los datos de todos los volúmenes virtuales del contenedor de almacenamiento. Se indica como una relación.	flotante
Volúmenes missingVolumes	Los volúmenes virtuales que no se pudieron consultar para los datos de eficiencia. Los volúmenes que faltan pueden deberse a que el ciclo de recolección de elementos no utilizados (GC) tiene menos de una hora de antigüedad, a una pérdida temporal de conectividad de red o a servicios reiniciados desde el ciclo de GC.	matriz en números enteros
Thin Provisioning	La relación entre el espacio utilizado y la cantidad de espacio asignado para almacenar datos. Se indica como una relación.	flotante
fecha/hora	La última vez que se recopilaron datos de eficiencia después de GC.	Cadena de datos ISO 8601

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetStorageContainerEfficiency",
  "params": {
    "storageContainerID" : "6c95e24f-9f0b-4793-affb-5a4bc6c3d7e1"
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "compression": 1,
    "deduplication": 1,
    "missingVolumes": [],
    "thinProvisioning": 1,
    "timestamp": "2016-04-12T15:39:49Z"
  }
}
```

Nuevo desde la versión

9.6

GetVirtualVolumeCount

Puede utilizar el `GetVirtualVolumeCount` método para recuperar el número de volúmenes virtuales que actualmente están en el sistema.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
cuente	El número de volúmenes virtuales que actualmente están en el sistema.	entero

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetVirtualVolumeCount",
    "params": {
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "count": 5
  }
}
```

Nuevo desde la versión

9.6

ListProtocolEndpoints

Puede utilizar el `ListProtocolEndpoints` método para recuperar información sobre todos los extremos de protocolo en el clúster. Los extremos de protocolo rigen el acceso a sus contenedores de almacenamiento de volúmenes virtuales asociados.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ProtocolEndpointID	Una lista de ID de extremo de protocolo acerca de los cuales se puede recuperar información. Si omite este parámetro, el método muestra información acerca de todos los extremos de protocolo.	Matriz de UUID de protocolEndpointID	Ninguno	No

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
ProtocoloEndpoints	Lista de objetos que contienen información sobre cada extremo de protocolo del sistema.	ProtocolEndpoint cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "id": 1,
  "method": "ListProtocolEndpoints",
  "params": {}
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

ListStorageContainers

Puede utilizar el `ListStorageContainers` método para recuperar información sobre todos los contenedores de almacenamiento de volúmenes virtuales que conoce el sistema.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ContenerID de almacenamiento	Una lista de los ID de contenedor de almacenamiento de los que se puede recuperar información. Si omite este parámetro, el método muestra información acerca de todos los contenedores de almacenamiento del sistema.	Cabina de UUID	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Contenedores de almacenamiento	Lista de objetos que contienen información sobre todos los contenedores de almacenamiento del sistema.	Contenedor de almacenamiento cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
   "method": "ListStorageContainers",
   "params": {
      "storageContainerIDs": ["efda8307-b916-4424-979e-658a3f16894d"]
   },
   "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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": []
      }
    ]
  }
}
```

Nuevo desde la versión

9.6

ListVirtualVolumeBindings

Puede utilizar el `ListVirtualVolumeBindings` método para obtener una lista de todos los volúmenes virtuales en el clúster enlazados con extremos de protocolo.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VirtualVolumeBindingIDs	Una lista de ID de vinculación de volúmenes virtuales de los cuales se puede recuperar información. Si omite este parámetro, el método muestra información acerca de todas las vinculaciones de volúmenes virtuales.	matriz en números enteros	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
vinculaciones	Una lista de objetos que describen todos los volúmenes virtuales del clúster vinculados a los extremos de protocolo.	vinculación

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListVirtualVolumeBindings",
    "params": {
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

ListVirtualVolumeHosts

Puede utilizar el `ListVirtualVolumeHosts` método para obtener una lista de todos los hosts de volúmenes virtuales que se conocen en el clúster. Un host de volumen virtual es un host VMware ESX que inició una sesión con el proveedor de API VASA.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VirtualVolumeHostIDs	Una lista de los ID de host de los volúmenes virtuales de los cuales se puede recuperar información. Si omite este parámetro, el método muestra información acerca de todos los hosts de volúmenes virtuales.	Matriz de UUID de virtualVolumeHostID	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
hosts	Una lista de los objetos que describen los hosts de volúmenes virtuales del clúster.	host cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListVirtualVolumeHosts",
    "params": {
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
        ]
      }
    ]
  }
}
```

Nuevo desde la versión

9.6

ListVirtualVolumes

Puede utilizar el `ListVirtualVolumes` método para enumerar los volúmenes virtuales que actualmente están en el sistema. Se puede usar este método para enumerar todos los volúmenes virtuales, o bien para enumerar solo un subconjunto.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
detalles	El nivel de detalle en la respuesta. Los posibles valores son los siguientes: • True: Incluya más detalles sobre cada VVol en la respuesta. • False: Incluya el nivel estándar de detalle de cada VVol en la respuesta.	booleano	Falso	No
límite	El número máximo de volúmenes virtuales que se van a enumerar.	entero	10000	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
recursiva	Especifica si se debe incluir información sobre los hijos de cada VVol en la respuesta o no. Los posibles valores son los siguientes: • True: Incluya información sobre los hijos de cada VVol en la respuesta. • Falso: No incluya información sobre los hijos de cada VVol en la respuesta.	booleano	Falso	No
StartVirtualVolumeID	El ID del volumen virtual en el que se iniciará la lista en la respuesta.	UIDType	Ninguno	No
ID de volúmenes virtuales	Una lista de los ID de volúmenes virtuales de los cuales se puede recuperar información. Si omite este parámetro, el método devuelve información acerca de solo estos volúmenes virtuales.	Matriz de UUID de virtualVolumeID	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
NextVirtualVolumeID	El ID del siguiente volumen virtual de la lista.	UUID

VirtualVolumes	Una lista de los objetos que describen los volúmenes virtuales que actualmente están en el sistema.	Volumen virtual cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListVirtualVolumes",
    "params": {
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

ListVirtualVolumeTasks

Puede utilizar el `ListVirtualVolumeTasks` método para obtener una lista de tareas con volúmenes virtuales en el sistema.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
VirtualVolumeTaskID	Una lista de los ID de tarea de volúmenes virtuales de los cuales se puede recuperar información. Si omite este parámetro, el método muestra información acerca de todas las tareas de los volúmenes virtuales.	Cabina de UUID	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
tareas	Una lista de los objetos que describen las tareas de volúmenes virtuales en el clúster.	tarea cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ListVirtualVolumeTasks",
    "params": {
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```
{
  "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"
      }
    ]
  }
}
```


Nuevo desde la versión

9.6

ModificyStorageContainer

Puede utilizar el `ModifyStorageContainer` método para realizar cambios en un contenedor de almacenamiento de volumen virtual existente.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
ID de almacenamiento ContainerID	El ID único del contenedor de almacenamiento de volumen virtual que se desea modificar.	UUID	Ninguno	Sí
InitiatorSecret	El nuevo secreto para la autenticación CHAP del iniciador.	cadena	Ninguno	No
TargetSecret	El nuevo secreto para la autenticación CHAP del destino.	cadena	Ninguno	No

Valores devueltos

Este método tiene el siguiente valor devuelto:

Nombre	Descripción	Tipo
Contenedor de almacenamiento	Información acerca del contenedor de almacenamiento que se acaba de crear.	Contenedor de almacenamiento

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "ModifyStorageContainer",
    "params": {
      "storageContainerID": "6c95e24f-9f0b-4793-affb-5a4bc6c3d7e1",
      "targetSecret": "O,IM;tOQdn9$JJ*8"
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
    }
  }
}
```


Nuevo desde la versión

9.6

Control de acceso

Los métodos de API de Element disponibles varían según el tipo de acceso que se haya configurado.

cuentas

Los siguientes métodos están disponibles para el tipo de acceso de cuentas:

AddAccount
GetAccountByID
ModificyAccount
GetAccountByName
Cuentas de lista
GetAccountEfficiency
RemoveAccount

administrador

Todos los métodos están disponibles para el tipo de acceso de administrador.

ClusterAdmin

Los siguientes métodos están disponibles para el tipo de acceso de administrador del clúster:

AddClusterAdmin
ListBackupTargets
AddInitiatorsToVolumeAccessGroup
ListBulkVolumeJobs
AddLdapClusterAdmin
ListClusterAdmins
AddVirtualNetwork
ListClusterPairs
AddVirtualNetwork
ListNodeFiberChannelPortInfo
AddVolumesVolumeAccessGroup
ListBackupTargets
CloneMultipleVolumes
ListDrivehardware
CompleteClusterPairing
ListFiberChannelSessions
CompleteVolumePairing
ListFiberChannelPortInfo
CreateBackupTarget

ListGroupSnapshots
CreateSchedule
ListActivePairedVolumes
CreateSnapshot
ModifyBackupTarget
CreateSupportBundle
ModifyClusterAdmin
CreateClusterSupportBundle
ModifiyGroupSnapshot
CreateGroupSnapshot
ModifyClusterFullThreshold
CreateVolumeAccessGroup
ModifyVolumeAccessGroup
DeleteAllSupportBundles
ModifyVolumeAccessGroupLunAssignments
DeleteSnapshot
ModifyVolumePair
DeleteGroupSnapshot
ModificyVirtualNetwork
DeleteVolumeAccessGroup
RemoveClusterAdmin
DisableEncryptionAtest

RemoveVolumePair
Autenticación DisableLdapAuthentication
RemoveVirtualNetwork
DisableSnmp
RemoveVolumesFromVolumeAccessGroup
EnableEncryptionAtest
RemoveInitiatorsFromVolumeAccessGroup
EnableLdapAuthentication
RollbackToSnapshot
EnableSnmp
RollbackToGroupSnapshot
GetBackupTarget
SetLoginSessionInfo
GetClusterFullThreshold
SetNtpInfo
GetClusterMasterNodeID
SetSnmpACL
GetHardwarConfig
SetSnmpInfo
GetLdapConfiguration
SetSnmpTrapInfo
GetLoginSessionInfo

SetRemoteLoggingHosts
GetNtpInfo
Apagado
GetNvramInfo
StartBulkVolumeRead
GetRawStats
StartBulkVolumeWrite
GetSnmpACL
StartClusterPairing
GetVolumeAccessGroupEfficency
StartVolumePairing
GetVolumeAccessLunAssignments
TestLdapAuthentication
GetVirtualNetwork

unidades

Los siguientes métodos se encuentran disponibles para el tipo de acceso de las unidades:

ListDrives
RemoveDrives
AddDrives
SecureEraseDrives

nodos

Los siguientes métodos están disponibles para el tipo de acceso del nodo:

AddNodes
ListPendingNodes
ListActiveNodes
RemoveNodes

lea

Existen los siguientes métodos para el tipo de acceso de lectura:

GetAccountByID
ListCloneJobs
GetAccountByName
ListDeletedVolumes
GetAsyncResult
ListDrivehardware
GetClusterCapacity
ListDrives
GetDefaultQoS
ListEvents
GetDriveStats
ListISCSISessions
GetSoftwareUpgrade
ListPendingNodes
GetVolumeStats
ListSyncJobs

Cuentas de lista
ListVolumeAccessGroups
ListActiveNodes
ListVolumeStatsByAccount
ListActiveNodes
ListVolumeStatsByVolume
ListActiveVolumes
ListVolumeStatsByVolumeAccessGroup
ListAllNodes
ListVolumesForAccount
ListBackupTargets

creación de informes

Los siguientes métodos están disponibles para el tipo de acceso a la generación de informes:

ClearClusterFaults
GetVolumeEffect
GetAccountEfficiency
GetVolumeStats
GetClusterCapacity
ListCloneJobs
GetClusterHardwareInfo
ListClusterFaults
GetClusterInfo

ListClusterPairs
GetClusterMasterNodeID
ListDrivehardware
GetClusterStats
ListEvents
GetDriveHardwarwareInfo
ListISCSISessions
GetDriveStats
ListSchedules
GetNetworkConfig
Servicios de listas
GetNodeHardwareInfo
ListSyncJobs
GetNodeStats
ListVirtualNetworks
GetSnmpInfo
ListVolumeStatsByAccount
GetSnmpTrapInfo
ListVolumeStatsByVolume
GetVolumeAccessGroupEfficency
ListVolumeStatsByVolumeAccessGroup

repositorios

El método ListAllNodes está disponible para el tipo de acceso repositorios.

volúmenes

Los siguientes métodos están disponibles para el tipo de acceso de volúmenes:

CreateVolume
DeleteVolume
ModifyBackupTarget
CloneVolume
DeleteVolumePairing
ModificyVolumes
CloneMultipleVolumes
GetBackupTarget
ModifyVolumePair
CreateBackupTarget
GetDefaultQoS
PurgeDeletedVolume
CreateSnapshot
ListActiveVolumes
RemoveBackupTarget
CreateGroupSnapshot
ListBackupTarget
RemoveVolumePair
CompleteVolumePairing

ListGroupSnapshots
RestoreDeletedVolume
CloneMultipleVolumes
ListVolumesForAccount
RollbackToGroupSnapshot
DeleteGroupSnapshot
ListDeletedVolumes
RollbackToSnapshot
DeleteSnapshot
ListGroupSnapshots
StartBulkVolumeRead
StartBulkVolumeWrite
StartVolumePairing
UpdateBulkVolumeStatus

escritura

Los siguientes métodos están disponibles para el tipo de acceso de escritura:

AddDrives
RemoveNodes
AddNodes
RemoveAccount
AddAccount
RemoveVolumesFromVolumeAccessGroup

AddVolumeToVolumeAccessGroup
RemoveInitiatorsFromVolumeAccessGroup
AddInitiatorsToVolumeAccessGroup
DeleteVolumeAccessGroup
CreateVolumeAccessGroup
DeleteVolume
ModifyVolumeAccessGroup
RestoreDeletedVolume
ModificyAccount
PurgeDeletedVolume
CreateVolume
Volumen ModificíoVolume
CloneVolume
GetAsyncResult
RemoveDrives

Ejemplos de respuestas

Aquí se ofrecen ejemplos completos de respuestas.

- Getconfig
- GetClusterHardwareInfo
- GetLldpInfo
- GetNetworkConfig
- GetNodeHardwareInfo (salida para iSCSI)
- GetNodeHardwareInfo (salida para nodos Fibre Channel)
- GetNvramInfo
- ListActiveNodes
- ListActiveVolumes

- TestHardwarConfig

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Getconfig

La `GetConfig` método devuelve una respuesta similar al ejemplo siguiente. Debido a la longitud, la respuesta contiene información solo para un nodo del clúster.


```
{
    "id": 1,
    "result": {
        "config": {
            "cluster": {
                "cipi": "Bond10G",
                "cluster": "AutoTest2-Fjqt",
                "encryptionCapable": true,
                "ensemble": [
                    "1:10.1.1.0",
                    "3:10.1.1.0",
                    "4:10.1.1.0"
                ],
                "mipi": "Bond1G",
                "name": "NLABP2605",
                "nodeID": 1,
                "pendingNodeID": 0,
                "role": "Storage",
                "sipi": "Bond10G",
                "state": "Active",
                "version": "11.0"
            },
            "network": {
            "Bond10G": {
                "#default": false,
                "address": "10.1.1.0",
                "auto": true,
                "bond-downdelay": "0",
                "bond-fail_over_mac": "None",
                "bond-miimon": "100",
                "bond-mode": "ActivePassive",
                "bond-primary_reselect": "Failure",
                "bond-slaves": "eth0 eth1",
                "bond-updelay": "200",
```

```
                "dns-nameservers": "10.1.1.0, 10.1.1.0",
                "dns-search": "ten.test.company.net., company.net.",
                "family": "inet",
                "gateway": "10.1.1.0",
                "linkSpeed": 10000,
                "macAddress": "c8:1f:66:ee:59:b9",
                "macAddressPermanent": "00:00:00:00:00:00",
                "method": "static",
                "mtu": "9000",
                "netmask": "255.255.240.0",
                "network": "10.1.1.0",
                "physical": {
                    "address": "10.1.1.0",
                    "macAddress": "c8:1f:66:ee:59:b9",
                    "macAddressPermanent": "00:00:00:00:00:00",
                    "mtu": "9000",
                    "netmask": "255.255.240.0",
                    "network": "10.1.1.0",
                    "upAndRunning": true
                },
                "routes": [],
                "status": "UpAndRunning",
                "symmetricRouteRules": [
                    "ip route add 10.1.1.1/20 dev Bond1G src 10.1.2.2
table Bond1G",
                    "ip rule add from 10.1.1.1 table Bond1G",
                    "ip route add default via 10.1.1.254"
                ],
                "upAndRunning": true,
                "virtualNetworkTag": "0"
            },
            "eth0": {
                "auto": true,
                "bond-master": "Bond10G",
                "family": "inet",
                "linkSpeed": 10000,
                "macAddress": "c8:1f:66:ee:59:b9",
                "macAddressPermanent": "c8:1f:66:ee:59:b9",
                "method": "bond",
                "physical": {
                    "address": "0.0.0.0",
                    "macAddress": "c8:1f:66:ee:59:b9",
                    "macAddressPermanent": "c8:1f:66:ee:59:b9",
                    "netmask": "N/A",
                    "network": "N/A",
                    "upAndRunning": true
```

```
                },
                "status": "UpAndRunning",
                "upAndRunning": true
            },
            "lo": {
                "auto": true,
                "family": "inet",
                "linkSpeed": 0,
                "macAddress": "00:00:00:00:00:00",
                "macAddressPermanent": "00:00:00:00:00:00",
                "method": "loopback",
                "physical": {
                    "address": "0.0.0.0",
                    "macAddress": "00:00:00:00:00:00",
                    "macAddressPermanent": "00:00:00:00:00:00",
                    "netmask": "N/A",
                    "network": "N/A",
                    "upAndRunning": true
                },
                "status": "UpAndRunning",
                "upAndRunning": true
            }
        }
        }
    }
}
```

GetClusterHardwareInfo

La `GetClusterHardwareInfo` método devuelve una respuesta similar al ejemplo siguiente.

```
{
 "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

La `GetLldpInfo` método devuelve una respuesta similar al ejemplo siguiente.

```
{
  "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

La `GetNetworkConfig` método devuelve una respuesta similar al ejemplo siguiente.

```
{
    "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 (salida para iSCSI)

La `GetNodeHardwareInfo` El método de iSCSI devuelve una respuesta similar al ejemplo siguiente.

```
{
    "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 (salida para nodos Fibre Channel)

La `GetNodeHardwareInfo` El método de nodos Fibre Channel devuelve una respuesta similar al ejemplo siguiente.


```
{
"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

La `GetNvramInfo` método devuelve una respuesta similar al ejemplo siguiente.

```
{
  id: 1,
  result: {
    nvramInfo: {
      details: {
         errors: {
           numOfErrorLogEntries: "0"
         },
         extended: {
            dialogVersion: "4",
            event: [
               {
                    name: "flushToFlash",
                    time: "2014-02-24 20:30:28",
                    value: "0"
         },
         {
                    name: "flushToFlash",
                    time: "1946-02-06 17:16:42",
                    value: "0"
         },
         {
                    name: "flushToFlash",
                    time: "2014-02-25 00:48:06",
                    value: "0"
         },
         {
                    name: "flushToFlash",
                    time: "2014-02-25 15:44:07",
```

```
                value: "0"
        },
        {
                name: "flushToFlash",
                time: "2014-03-17 17:21:46",
                value: "0"
        },
        {
                name: "flushToFlash",
                time: "2014-03-17 17:59:30",
                value: "0"
        },
        {
                name: "flushToFlash",
                time: "2014-03-17 18:06:27",
                value: "0"
        },
        {
                name: "flushToFlash",
                time: "2014-03-17 21:43:17",
                value: "0"
        },
        {
                name: "excessiveCurrent",
                time: "2014-02-25 00:00:29",
                value: "39"
        },
         {
                name: "excessiveCurrent",
                time: "2014-03-01 00:00:24",
                value: "23"
         }
      ],
           eventOccurrences: [
        {
                count: "15",
                name: "flushToFlash"
        },
        {
                count: "2",
                name: "excessiveCurrent"
        }
                initialCapacitance: "6.653 F",
                initialEsr: "0.097 Ohm",
           measurement: [
        {
```

```
                level_0: " 0",
                level_1: " 112",
                level_2: " 670919",
                level_3: " 455356",
                level_4: " 90215",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "enterpriseFlashControllerTemperature",
                recent: "64 C"
        },
        {
                level_0: " 0",
                level_1: " 27",
                level_2: " 456896",
                level_3: " 717565",
                level_4: " 39422",
                level_5: " 2692",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "capacitor1And2Temperature",
                recent: "28.64 C"
        },
        {
                level_0: " 0",
                level_1: " 2080",
                level_2: " 907196",
                level_3: " 280178",
                level_4: " 26539",
                level_5: " 609",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "capacitor3And4Temperature",
                recent: "28.60 C"
        },
        {
                errorPeriod: {
                    duration: "24",
                    startTime: "2014-02-06 00:23:54",
                    worst: "8"
```

```
                },
                level_0: " 0",
                level_1: " 839",
                level_2: " 272794",
                level_3: " 404758",
                level_4: " 35216",
                level_5: " 377818",
                level_6: " 103891",
                level_7: " 21274",
                level_8: " 12",
                level_9: " 0",
                name: "rearVentAmbientTemperature",
                recent: "46.82 C"
        },
        {
                level_0: " 0",
                level_1: " 742749",
                level_2: " 460016",
                level_3: " 13837",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "rms200BoardTemperature",
                recent: "50.62 C"
        },
        {
                name: "voltageOfCapacitor1",
                recent: "2.308 V"
        },
        {
                name: "voltageOfCapacitor2",
                recent: "2.305 V"},
        {
                name: "voltageOfCapacitor3",
                recent: "2.314 V"
        },
        {
                name: "voltageOfCapacitor4",
                recent: "2.307 V"
        },
        {
               level_0: " 175052",
               level_1: " 51173",
```

```
                level_2: " 435788",
                level_3: " 12766",
                level_4: " 4",
                level_5: " 6",
                level_6: " 541813",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "capacitorPackVoltage",
                recent: "9.233 V"
        },
        {
                level_0: " 0",
                level_1: " 0",
                level_2: " 0",
                level_3: " 0",
                level_4: " 0",
                level_5: " 0",
                level_6: " 4",
                level_7: " 1",
                level_8: " 4",
                level_9: " 6",
                name: "capacitorPackVoltageAtEndOfFlushToFlash",
                recent: "5.605 V"
        },
        {
                name: "currentDerivedFromV3V4",
                recent: "0.000 A"
        },
        {
                level_0: " 7",
                level_1: " 4",
                level_2: " 3",
                level_3: " 1",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "derivedEnergy",
                recent: "175 Joules"
        },
        {
                level_0: " 0",
                level_1: " 0",
```

```
                level_2: " 0",
                level_3: " 0",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 17",
                level_8: " 19",
                level_9: " 7",
                name: "derivedCapacitanceOfThePack",
                recent: "5.959 F"
        },
        {
                level_0: " 0",
                level_1: " 43",
                level_2: " 0",
                level_3: " 0",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "derivedEsrOfCapacitorPack",
                recent: "0.104 Ohm"
        },
        {
                level_0: " 0",
                level_1: " 0",
                level_2: " 0",
                level_3: " 0",
                level_4: " 15",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "timeToRunFlushToFlash",
                recent: "22.40 Seconds"
        },
        {
                level_0: " 0",
                level_1: " 0",
                level_2: " 7",
                level_3: " 0",
                level_4: " 0",
                level_5: " 0",
```

```
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "timeToRunRestore",
                recent: "20.44 Seconds"
        },
        {
                level_0: " 0",
                level_1: " 1",
                level_2: " 3",
                level_3: " 2",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 1",
                name: "timeToChargeCapacitors",
                recent: "48 Seconds"
        },
        {
                level_0: " 448586",
                level_1: " 2998",
                level_2: " 0",
                level_3: " 0",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "correctableBitsInErrorOnReadingAPage"
        },
        {
                level_0: " 2998",
                level_1: " 0",
                level_2: " 0",
                level_3: " 0",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name:
```

```
"correctableBitsInErrorOnReadingTheWorstBchRegionOfAPage"
        },
        {
                level_0: " 0",
                level_1: " 37",
                level_2: " 280274",
                level_3: " 422999",
                level_4: " 245814",
                level_5: " 242470",
                level_6: " 24447",
                level_7: " 561",
                level_8: " 0",
                level_9: " 0",
                name: "fanInletAmbientTemperature",
                recent: "41.74 C"
        }
        ],
                predictedCapacitanceDepletion: "504328 uF",
                smartCounters: [
        {
                name: "numberOf512ByteBlocksReadFromDdr",
                value: "218284648"
        },
        {
                name: "numberOf512ByteBlocksWrittenToDdr",
                value: "12031567354"
        },
        {
                name: "numberOfHostReadCommands",
                value: "5366315"
        },
        {
                name: "numberOfHostWriteCommands",
                value: "1266099334"
        },
        {
                name: "controllerBusyTimeMinutes",
                value: "0"
        },
        {
                name: "numberOfPowerCycles",
                value: "13"
        },
        {
                name: "powerOnHours",
                value: "1009"
```

```
        },
        {
                name: "unsafeShutdowns",
                value: "5"
        },
        {
                name: "mediaErrors",
                value: "0"
        },
        {
                name: "numberOfErrorLogs",
                value: "2"
        }
        ],
         snapshotTime: "2014-03-20 16:43:49"
    },
    firmware: {
         activeSlotNumber: "2",
         slot1Version: "1e5817bc",
         slot2Version: "1e0d70ac",
         slot3Version: "1e5817bc",
         slot4Version: "1e5817bc"
   },
    smart: {
        availableSpace: "0%",
        availableSpaceThreshold: "0%",
        controllerBusyTimeMinutes: "0",
        criticalErrorVector: "0x0",
        mediaErrors: "0",
        numberOf512ByteBlocksRead: "218284648",
        numberOf512ByteBlocksWritten: "12031567354",
        numberOfErrorInfoLogs: "2",
        numberOfHostReadCommands: "5366315",
        numberOfHostWriteCommands: "1266099334",
        numberOfPowerCycles: "13",
        powerOnHours: "1009",
        temperature: "323 Kelvin",
        unsafeShutdowns: "5"
     }
    },
    status: "Warning",
    statusInfo: {
    warning: [
        "excessiveCurrent (2x)"
      ]
    },
```

```
      type: "RMS-200"
     }
   }
}
```

ListActiveNodes

La `ListActiveNodes` método devuelve una respuesta similar al ejemplo siguiente.

```
 {
    "id": 1,
    "result": {
        "nodes": [
            {
                "associatedFServiceID": 0,
                "associatedMasterServiceID": 1,
                "attributes": {},
                "cip": "172.27.21.23",
                "cipi": "Bond10G",
                "fibreChannelTargetPortGroup": null,
                "mip": "172.27.1.23",
                "mipi": "Bond1G",
                "name": "PSN-1-23",
                "nodeID": 1,
                "platformInfo": {
                    "chassisType": "R620",
                    "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @
2.50GHz",
                    "nodeMemoryGB": 72,
                    "nodeType": "SF3010"
                },
                "sip": "172.27.21.23",
                "sipi": "Bond10G",
                "softwareVersion": "9.0.0.1298",
                "uuid": "4C4C4544-0056-3810-804E-B5C04F4C5631",
                "virtualNetworks": [
                    {
                        "address": "10.1.2.4",
                        "virtualNetworkID": 1
                    },
                    {
                        "address": "10.2.2.10",
                        "virtualNetworkID": 2
                    }
                ]
```

```
            },
            {
                "associatedFServiceID": 0,
                "associatedMasterServiceID": 4,
                "attributes": {},
                "cip": "172.27.21.24",
                "cipi": "Bond10G",
                "fibreChannelTargetPortGroup": null,
                "mip": "172.27.1.24",
                "mipi": "Bond1G",
                "name": "PSN-1-24",
                "nodeID": 2,
                "platformInfo": {
                    "chassisType": "R620",
                    "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @
2.50GHz",
                    "nodeMemoryGB": 72,
                    "nodeType": "SF3010"
                },
                "sip": "172.27.21.24",
                "sipi": "Bond10G",
                "softwareVersion": "9.0.0.1298",
                "uuid": "4C4C4544-0042-4210-804E-C3C04F4C5631",
                "virtualNetworks": [
                    {
                        "address": "10.1.2.5",
                        "virtualNetworkID": 1
                    },
                    {
                        "address": "10.2.2.11",
                        "virtualNetworkID": 2
                    }
                ]
            },
            {
                "associatedFServiceID": 0,
                "associatedMasterServiceID": 2,
                "attributes": {},
                "cip": "172.27.21.25",
                "cipi": "Bond10G",
                "fibreChannelTargetPortGroup": null,
                "mip": "172.27.1.25",
                "mipi": "Bond1G",
                "name": "PSN-1-25",
                "nodeID": 3,
                "platformInfo": {
```

```
                    "chassisType": "R620",
                    "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @
2.50GHz",
                    "nodeMemoryGB": 72,
                    "nodeType": "SF3010"
                },
                "sip": "172.27.21.25",
                "sipi": "Bond10G",
                "softwareVersion": "9.0.0.1298",
                "uuid": "4C4C4544-0053-4210-8051-C6C04F515631",
                "virtualNetworks": [
                    {
                        "address": "10.1.2.6",
                        "virtualNetworkID": 1
                    },
                    {
                        "address": "10.2.2.12",
                        "virtualNetworkID": 2
                    }
                ]
            },
            {
                "associatedFServiceID": 0,
                "associatedMasterServiceID": 3,
                "attributes": {},
                "cip": "172.27.21.26",
                "cipi": "Bond10G",
                "fibreChannelTargetPortGroup": null,
                "mip": "172.27.1.26",
                "mipi": "Bond1G",
                "name": "PSN-1-26",
                "nodeID": 4,
                "platformInfo": {
                    "chassisType": "R620",
                    "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @
2.50GHz",
                    "nodeMemoryGB": 72,
                    "nodeType": "SF3010"
                },
                "sip": "172.27.21.26",
                "sipi": "Bond10G",
                "softwareVersion": "9.0.0.1298",
                "uuid": "4C4C4544-0056-3810-804E-B4C04F4C5631",
                "virtualNetworks": [
                    {
                        "address": "10.1.2.7",
```

```
                        "virtualNetworkID": 1
                    },
                    {
                        "address": "10.2.2.13",
                        "virtualNetworkID": 2
                    }
                ]
            }
        ]
    }
 }
```

ListActiveVolumes

La `ListActiveVolumes` método devuelve una respuesta similar al ejemplo siguiente.

```
{
    "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"
                    }
                ]
            }
        ]
    }
}
```

TestHardwarConfig

La `TestHardwareConfig` método devuelve una respuesta similar al ejemplo siguiente.

```
{
"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"
            }
        }
    ]
}
}
```

Plugin de NetApp Element para vCenter Server

El plugin de NetApp Element para vCenter Server proporciona un plugin para la interfaz de VMware vSphere para que se puedan gestionar y supervisar los clústeres de almacenamiento que ejecutan el software NetApp Element.

Para obtener más información sobre el plugin de Element para vCenter Server, consulte "Documentación del plugin de NetApp Element para vCenter Server".

Si quiere más información

- "Documentación de SolidFire y el software Element"

Supervise el almacenamiento con SolidFire Active IQ

"SolidFire Active IQ" es una herramienta web que proporciona vistas históricas actualizadas continuamente de los datos de todo el clúster. Es posible configurar alertas para eventos, umbrales o métricas específicos. SolidFire Active IQ le permite supervisar la capacidad y el rendimiento del sistema, así como mantenerse informado sobre el estado del clúster.

Puede encontrar la siguiente información sobre su sistema en SolidFire Active IQ:

- Número de nodos y estado de los nodos: En buen estado, sin conexión o fallo
- Representación gráfica de la CPU, el uso de memoria y la limitación de nodos
- Los detalles sobre el nodo, como el número de serie, la ubicación de la ranura en el chasis, el modelo y la versión del software NetApp Element que se ejecuta en el nodo de almacenamiento
- Información relacionada con la CPU y el almacenamiento sobre los equipos virtuales

Para obtener más información sobre SolidFire Active IQ, consulte "Documentación de SolidFire Active IQ".

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"
- "Herramientas del del sitio de soporte de NetApp para Active IQ"

Trabaje con el nodo de gestión

Información general sobre los nodos de gestión

Es posible usar el nodo de gestión (mNode) para usar los servicios del sistema, gestionar los activos y las configuraciones del clúster, ejecutar pruebas y utilidades del sistema, configurar Active IQ para la supervisión del sistema y habilitar el acceso al soporte de NetApp para la solución de problemas.

> Como práctica recomendada, solo asocie un nodo de gestión a una instancia de VMware vCenter y evite definir los mismos recursos de almacenamiento y computación o instancias de vCenter en varios nodos de gestión.

En los clústeres que ejecutan el software Element versión 11.3 o posterior, se puede trabajar con el nodo de gestión mediante una de las dos interfaces:

- Con la interfaz de usuario del nodo de gestión (`https://[mNode IP]:442`), puede realizar cambios en la configuración de la red y del clúster, ejecutar pruebas del sistema o utilizar utilidades del sistema.
- Con la interfaz de usuario de API de REST integrada (`https://[mNode IP]/mnode`), puede ejecutar o comprender las API relacionadas con los servicios del nodo de administración, incluida la configuración del servidor proxy, las actualizaciones de nivel de servicio o la administración de activos.

Instale o recupere un nodo de gestión:

- "Instale un nodo de gestión"
- "Configurar una controladora de interfaz de red (NIC) de almacenamiento"
- "Recupere un nodo de gestión"

Acceda al nodo de gestión:

- "Acceder al nodo de gestión (interfaz de usuario o API de REST)"

Cambie el certificado SSL predeterminado:

- "Cambie el certificado SSL predeterminado del nodo de gestión"

Realice tareas con la interfaz de usuario del nodo de gestión:

- "Información general de la interfaz de usuario del nodo de gestión"

Realice tareas con las API DE REST del nodo de gestión:

- "Información general de la interfaz de usuario de la API DE REST del nodo de"

Deshabilite o habilite la funcionalidad SSH remota o inicie una sesión de túnel de soporte remoto con el soporte de NetApp para ayudarle a resolver problemas:

- "Habilite las conexiones remotas de soporte de NetApp"
- "Gestione la funcionalidad SSH en el nodo de gestión"

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Instale o recupere un nodo de gestión

Instale un nodo de gestión

Puede instalar manualmente el nodo de gestión para el clúster que ejecuta el software NetApp Element con la imagen adecuada de su configuración.

Este proceso manual está dirigido a administradores de almacenamiento all-flash de SolidFire que no utilizan el motor de puesta en marcha de NetApp para la instalación de nodos de gestión.

Lo que necesitará

- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- En la instalación utiliza IPv4. El nodo de gestión 11.3 no admite IPv6.

  Si necesita compatibilidad con IPv6, se puede usar el nodo de gestión 11.1.

- Tiene permiso para descargar software del sitio de soporte de NetApp.
- Identificó el tipo de imagen del nodo de gestión correcto para su plataforma:

Plataforma	Tipo de imagen de instalación
Microsoft Hyper-V	.iso
KVM	.iso
VSphere de VMware	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

- (Nodo de gestión 12.0 y posterior con servidor proxy) ha actualizado el control de cloud híbrido de NetApp a los servicios de gestión versión 2.16 antes de configurar un servidor proxy.

Acerca de esta tarea

El nodo de gestión Element 12.2 es una actualización opcional. No es necesario para las puestas en marcha existentes.

Antes de seguir este procedimiento, debe tener conocimientos de "Volúmenes persistentes" y si desea usarlos o no. Los volúmenes persistentes son opcionales, pero se recomienda para la recuperación de datos de configuración del nodo de gestión en caso de pérdida de una máquina virtual (VM).

Pasos

1. Descargue ISO o OVA e implemente la VM
2. Cree el administrador del nodo de gestión y configure la red
3. Configurar la sincronización de hora

4. Configure el nodo de gestión
5. Configurar activos de controladora

Descargue ISO o OVA e implemente la VM

1. Descargue el OVA o ISO para su instalación desde "Software Element" En el sitio de soporte de NetApp.
   a. Seleccione **Descargar la versión más reciente** y acepte el EULA.
   b. Seleccione la imagen del nodo de gestión que desea descargar.
2. Si ha descargado el OVA, siga estos pasos:
   a. Implemente el OVA.
   b. Si el clúster de almacenamiento se encuentra en una subred separada de su nodo de gestión (eth0) y desea utilizar volúmenes persistentes, añada una segunda controladora de interfaz de red (NIC) a la máquina virtual en la subred de almacenamiento (por ejemplo, eth1) o asegúrese de que la red de gestión pueda enrutar a la red de almacenamiento.
3. Si ha descargado la ISO, siga estos pasos:
   a. Cree una nueva máquina virtual de 64 bits desde el hipervisor con la siguiente configuración:
      - Seis CPU virtuales
      - 24 GB DE MEMORIA RAM
      - Tipo de adaptador de almacenamiento definido en LSI Logic Parallel

        El valor predeterminado para el nodo de gestión puede ser LSI Logic SAS. En la ventana **Nueva máquina virtual**, compruebe la configuración del adaptador de almacenamiento seleccionando **Personalizar hardware** > **hardware virtual**. Si es necesario, cambie LSI Logic SAS a **LSI Logic Parallel**.

      - Disco virtual de 400 GB, thin provisioning
      - Una interfaz de red virtual con acceso a Internet y acceso a la MVIP de almacenamiento.
      - (Opcional) una interfaz de red virtual con acceso de la red de gestión al clúster de almacenamiento de. Si el clúster de almacenamiento se encuentra en una subred separada de su nodo de gestión (eth0) y desea utilizar volúmenes persistentes, añada una segunda controladora de interfaz de red (NIC) a la máquina virtual en la subred de almacenamiento (eth1) o asegúrese de que la red de gestión pueda enrutar a la red de almacenamiento.

        No encienda la VM antes del paso que indique hacerlo más adelante en este procedimiento.

   b. Adjunte ISO a la máquina virtual y arranque en la imagen de instalación .iso.

      La instalación de un nodo de gestión con la imagen puede provocar un retraso de 30 segundos antes de que aparezca la pantalla de inicio.

4. Active la máquina virtual del nodo de gestión cuando se complete la instalación.

Cree el administrador del nodo de gestión y configure la red

1. Con la interfaz de usuario de terminal (TUI), cree un usuario administrador del nodo de gestión.

Para desplazarse por las opciones del menú, pulse las teclas de flecha hacia arriba o hacia abajo. Para desplazarse por los botones, pulse TAB. Para pasar de los botones a los campos, pulse TAB. Para desplazarse por los campos, pulse las teclas de flecha hacia arriba o hacia abajo.

2. Si hay un servidor de protocolo de configuración dinámica de hosts (DHCP) en la red que asigna direcciones IP con una unidad de transmisión máxima (MTU) inferior a 1500 bytes, debe realizar los siguientes pasos:

   a. Coloque temporalmente el nodo de gestión en una red vSphere sin DHCP, como iSCSI.
   b. Reinicie la máquina virtual o reinicie la red de la máquina virtual.
   c. Con la TUI, configure la IP correcta en la red de gestión con un MTU mayor o igual a 1500 bytes.
   d. Vuelva a asignar la red de máquina virtual correcta a la máquina virtual.

   Un DHCP que asigna IP con una MTU de menos de 1500 bytes puede impedir que configure la red del nodo de gestión o utilice la interfaz de usuario del nodo de gestión.

3. Configure la red del nodo de gestión (eth0).

   Si necesita una NIC adicional para aislar el tráfico de almacenamiento, consulte las instrucciones para configurar otra NIC: "Configurar una controladora de interfaz de red (NIC) de almacenamiento".

Configurar la sincronización de hora

1. Asegúrese de que la hora se haya sincronizado entre el nodo de gestión y el clúster de almacenamiento mediante NTP:

   A partir del elemento 12.3.1, los subpasos (a) a (e) se realizan automáticamente. Para el nodo de gestión 12.3.1, vaya a. subpaso (f) para completar la configuración de sincronización de tiempo.

1. Inicie sesión en el nodo de gestión mediante SSH o la consola proporcionada por su hipervisor.
2. Stop NTPD:

```
sudo service ntpd stop
```

3. Edite el archivo de configuración NTP `/etc/ntp.conf`:

   a. Comente los servidores predeterminados (`server 0.gentoo.pool.ntp.org`) agregando una `#` delante de cada uno.
   b. Agregue una nueva línea para cada servidor de tiempo predeterminado que desee agregar. Los servidores de hora predeterminados deben ser los mismos servidores NTP que se utilicen en el clúster de almacenamiento que se utilizará en un "paso posterior".

```
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. Guarde el archivo de configuración cuando finalice.

4. Fuerce una sincronización NTP con el servidor que se acaba de añadir.

```
sudo ntpd -gq
```

5. Reinicie NTPD.

```
sudo service ntpd start
```

6. Deshabilitar la sincronización de hora con el host a través del hipervisor (el siguiente es un ejemplo de VMware):

> Si implementa el mNode en un entorno de hipervisor distinto a VMware, por ejemplo, desde la imagen .iso en un entorno de OpenStack, consulte la documentación del hipervisor para obtener los comandos equivalentes.

a. Desactivar la sincronización periódica:

```
vmware-toolbox-cmd timesync disable
```

b. Mostrar y confirmar el estado actual del servicio:

```
vmware-toolbox-cmd timesync status
```

c. En vSphere, compruebe que el `Synchronize guest time with host` La casilla no está activada en las opciones de la máquina virtual.

> No habilite esta opción si realiza cambios futuros en la máquina virtual.

> No edite el NTP después de completar la configuración de sincronización de hora porque afecta al NTP cuando ejecuta el "comando setup" en el nodo de gestión.

Configure el nodo de gestión

1. Configure y ejecute el comando de configuración del nodo de gestión:

   Se le pedirá que introduzca contraseñas en un mensaje seguro. Si su clúster de está situado detrás de un servidor proxy, debe configurar el proxy de manera que pueda llegar a una red pública.

   ```
   sudo /sf/packages/mnode/setup-mnode --mnode_admin_user [username]
   --storage_mvip [mvip] --storage_username [username] --telemetry_active
   [true]
   ```

   a. Sustituya el valor entre corchetes [ ] (incluidos los corchetes) para cada uno de los siguientes parámetros necesarios:

      La forma abreviada del nombre del comando está entre paréntesis ( ) y se puede sustituir por el nombre completo.

      - **--mnode_admin_user (-mu) [username]**: El nombre de usuario de la cuenta de administrador del nodo de gestión. Probablemente este sea el nombre de usuario de la cuenta de usuario que utilizó para iniciar sesión en el nodo de gestión.
      - **--Storage_mvip (-sm) [dirección MVIP]**: La dirección IP virtual de gestión (MVIP) del clúster de almacenamiento que ejecuta el software Element. Configure el nodo de gestión con el mismo clúster de almacenamiento que utilizó durante "Configuración de servidores NTP".
      - **--Storage_username (-su) [nombre de usuario]**: El nombre de usuario administrador del clúster de almacenamiento para el clúster especificado por `--storage_mvip` parámetro.
      - **--Telemetry_active (-t) [true]**: Conserve el valor true que permite la recopilación de datos para análisis por Active IQ.

   b. (Opcional): Añada los parámetros de extremo de Active IQ al comando:

      - **--remote_host (-rh) [AIQ_endpoint]**: El punto final donde se envían los datos de telemetría Active IQ para ser procesados. Si no se incluye el parámetro, se utiliza el extremo predeterminado.

   c. (Recomendado): Añada los siguientes parámetros de volumen persistente. No modifique ni elimine la cuenta y los volúmenes creados para la funcionalidad de volúmenes persistentes o se producirá una pérdida en la funcionalidad de gestión.

      - **--use_persistent_Volumes (-pv) [true/false, default: False]**: Enable o disable volúmenes persistentes. Introduzca el valor en true para habilitar la funcionalidad de volúmenes persistentes.
      - **--persistent_Volumes_account (-pva) [account_name]**: If `--use_persistent_volumes` está configurado en true, use este parámetro e introduzca el nombre de la cuenta de almacenamiento que se usará para los volúmenes persistentes.

        Utilice un nombre de cuenta único para volúmenes persistentes que sean diferentes del nombre de cuenta existente en el clúster. Es de vital importancia mantener la cuenta de los volúmenes persistentes separados del resto del entorno.

      - **--persistent_Volumes_mvip (-pvm) [mvip]**: Introduzca la dirección IP virtual de gestión (MVIP) del clúster de almacenamiento que ejecuta el software Element que se usará con volúmenes persistentes. Esto solo es necesario si el nodo de gestión gestiona varios clústeres de

almacenamiento. Si no se gestionan varios clústeres, se utiliza la dirección MVIP del clúster predeterminada.

d. Configure un servidor proxy:

- **--use_proxy (-up) [true/false, default: False]**: Activa o desactiva el uso del proxy. Este parámetro es necesario para configurar un servidor proxy.
- **--proxy_hostname_or_ip (-pi) [host]**: El nombre de host del proxy o IP. Esto es necesario si desea utilizar un proxy. Si lo especifica, se le solicitará que introduzca `--proxy_port`.
- **--proxy_username (-pu) [nombre de usuario]**: El nombre de usuario del proxy. Este parámetro es opcional.
- **--proxy_password (-pp) [password]**: La contraseña del proxy. Este parámetro es opcional.
- **--proxy_Port (-pq) [puerto, por defecto: 0]**: El puerto proxy. Si especifica esto, se le pedirá que introduzca el nombre de host del proxy o la dirección IP (`--proxy_hostname_or_ip`).
- **--proxy_ssh_Port (-ps) [puerto, por defecto: 443]**: El puerto proxy SSH. De forma predeterminada, se establece el puerto 443.

e. (Opcional) Use Parameter help si necesita información adicional acerca de cada parámetro:

- **--help (-h)**: Devuelve información acerca de cada parámetro. Los parámetros se definen como obligatorios u opcionales según la puesta en marcha inicial. Los requisitos de los parámetros de actualización y nueva puesta en marcha pueden variar.

f. Ejecute el `setup-mnode` comando.

Configurar activos de controladora

1. Busque el ID de instalación:
   a. Desde un explorador, inicie sesión en la API DE REST del nodo de gestión:
   b. Vaya a la MVIP de almacenamiento e inicie sesión. Esta acción hace que se acepte el certificado para el siguiente paso.
   c. Abra la interfaz de usuario de la API DE REST del servicio de inventario en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

   d. Seleccione **autorizar** y complete lo siguiente:
      i. Introduzca el nombre de usuario y la contraseña del clúster.
      ii. Introduzca el ID de cliente as `mnode-client`.
      iii. Seleccione **autorizar** para iniciar una sesión.
   e. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.
   f. Seleccione **probar**.
   g. Seleccione **Ejecutar**.
   h. Desde el cuerpo de respuesta del código 200, copie y guarde `id` para la instalación para utilizar en un paso posterior.

      Su instalación tiene una configuración de activos base que se creó durante la instalación o la actualización.

2. Añada un activo de controladora de vCenter para el control del cloud híbrido de NetApp a los activos conocidos del nodo de gestión:
   a. Acceda a la interfaz de usuario de API de servicio mnode en el nodo de gestión introduciendo la dirección IP del nodo de gestión seguida de `/mnode`:

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

   b. Seleccione **autorizar** o cualquier icono de bloqueo y complete lo siguiente:
      i. Introduzca el nombre de usuario y la contraseña del clúster.
      ii. Introduzca el ID de cliente as `mnode-client`.
      iii. Seleccione **autorizar** para iniciar una sesión.
      iv. Cierre la ventana.
   c. Seleccione **POST /assets/{Asset_id}/controllers** para agregar un subactivo de controlador.

      > Debe crear un nuevo rol HCC de NetApp en vCenter para añadir un subsistema de controladora. Este nuevo rol de HCC de NetApp limitará la visión de los servicios de los nodos de gestión a activos de NetApp. Consulte "Cree una función HCC de NetApp en vCenter".

   d. Seleccione **probar**.
   e. Introduzca el ID de activo base principal que copió en el portapapeles en el campo **Asset_id**.
   f. Introduzca los valores de carga útil necesarios con el tipo `vCenter` De aplicaciones y vCenter.
   g. Seleccione **Ejecutar**.

Obtenga más información

- "Volúmenes persistentes"
- "Añada un activo de controladora al nodo de gestión"
- "Configurar un NIC de almacenamiento"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Configurar una controladora de interfaz de red (NIC) de almacenamiento

Si utiliza una NIC adicional para almacenamiento, puede conectarse SSH al nodo de gestión o usar la consola de vCenter y ejecutar un comando curl para configurar una interfaz de red etiquetada o sin etiqueta.

Antes de empezar

- Conoce la dirección IP eth0.
- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Implementó un nodo de gestión 11.3 o posterior.

Opciones de configuración

Elija la opción relevante para su entorno:

- Configure un controlador de interfaz de red (NIC) de almacenamiento para una interfaz de red sin etiquetas
- Configure un controlador de interfaz de red (NIC) de almacenamiento para una interfaz de red etiquetada

Configure un controlador de interfaz de red (NIC) de almacenamiento para una interfaz de red sin etiquetas

Pasos

1. Abra una consola SSH o vCenter.
2. Sustituya los valores de la siguiente plantilla de comandos y ejecute el comando:

> Los valores se representan mediante `$` para cada uno de los parámetros necesarios para la nueva interfaz de red de almacenamiento. La `cluster` es necesario y se puede utilizar para cambiar el nombre del host del nodo de gestión en la siguiente plantilla. `--insecure` o. `-k` las opciones no se deben utilizar en entornos de producción.

```
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"
}
'
```

Configure un controlador de interfaz de red (NIC) de almacenamiento para una interfaz de red etiquetada

Pasos

1. Abra una consola SSH o vCenter.
2. Sustituya los valores de la siguiente plantilla de comandos y ejecute el comando:

> Los valores se representan mediante `$` para cada uno de los parámetros necesarios para la nueva interfaz de red de almacenamiento. La `cluster` es necesario y se puede utilizar para cambiar el nombre del host del nodo de gestión en la siguiente plantilla. `--insecure` o. `-k` las opciones no se deben utilizar en entornos de producción.

```
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"
}
'
```

Obtenga más información

- "Añada un activo de controladora al nodo de gestión"
- "Plugin de NetApp Element para vCenter Server"

- "Documentación de SolidFire y el software Element"

Recupere un nodo de gestión

Puede recuperar y volver a poner en marcha manualmente el nodo de gestión para el clúster que ejecuta el software NetApp Element si el nodo de gestión anterior usaba volúmenes persistentes.

Es posible implementar un nuevo OVA y ejecutar un script de nueva puesta en marcha para extraer datos de configuración de un nodo de gestión previamente instalado que ejecuta la versión 11.3 y posteriores.

Lo que necesitará

- El nodo de gestión anterior ejecutaba la versión 11.3 o posterior del software NetApp Element con "Volúmenes persistentes" funcionalidad activada.
- Conoce la dirección MVIP y la SVIP del clúster que contiene los volúmenes persistentes.
- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- En la instalación utiliza IPv4. El nodo de gestión 11.3 no admite IPv6.
- Tiene permiso para descargar software del sitio de soporte de NetApp.
- Identificó el tipo de imagen del nodo de gestión correcto para su plataforma:

Plataforma	Tipo de imagen de instalación
Microsoft Hyper-V	.iso
KVM	.iso
VSphere de VMware	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

Pasos

1. Descargue ISO o OVA e implemente la VM
2. Configure la red
3. Configurar la sincronización de hora
4. Configure el nodo de gestión

Descargue ISO o OVA e implemente la VM

1. Descargue el OVA o ISO para su instalación desde "Software Element" En el sitio de soporte de NetApp.
   a. Seleccione **Descargar la versión más reciente** y acepte el EULA.
   b. Seleccione la imagen del nodo de gestión que desea descargar.
2. Si ha descargado el OVA, siga estos pasos:
   a. Implemente el OVA.
   b. Si el clúster de almacenamiento se encuentra en una subred separada de su nodo de gestión (eth0) y desea utilizar volúmenes persistentes, añada una segunda controladora de interfaz de red (NIC) a la máquina virtual en la subred de almacenamiento (por ejemplo, eth1) o asegúrese de que la red de

gestión pueda enrutar a la red de almacenamiento.

3. Si ha descargado la ISO, siga estos pasos:
   a. Cree una nueva máquina virtual de 64 bits desde el hipervisor con la siguiente configuración:
      - Seis CPU virtuales
      - 24 GB DE MEMORIA RAM
      - Disco virtual de 400 GB, thin provisioning
      - Una interfaz de red virtual con acceso a Internet y acceso a la MVIP de almacenamiento.
      - (Opcional para el almacenamiento all-flash SolidFire) una interfaz de red virtual con acceso de red de gestión al clúster de almacenamiento. Si el clúster de almacenamiento se encuentra en una subred separada de su nodo de gestión (eth0) y desea utilizar volúmenes persistentes, añada una segunda controladora de interfaz de red (NIC) a la máquina virtual en la subred de almacenamiento (eth1) o asegúrese de que la red de gestión pueda enrutar a la red de almacenamiento.

      No encienda la máquina virtual antes del paso que indique hacerlo más adelante en este procedimiento.

   b. Adjunte ISO a la máquina virtual y arranque en la imagen de instalación .iso.

      La instalación de un nodo de gestión con la imagen puede provocar un retraso de 30 segundos antes de que aparezca la pantalla de inicio.

4. Encienda la máquina virtual del nodo de gestión cuando se complete la instalación.

Configure la red

1. Con la interfaz de usuario de terminal (TUI), cree un usuario administrador del nodo de gestión.

   Para desplazarse por las opciones del menú, pulse las teclas de flecha hacia arriba o hacia abajo. Para desplazarse por los botones, pulse TAB. Para pasar de los botones a los campos, pulse TAB. Para desplazarse por los campos, pulse las teclas de flecha hacia arriba o hacia abajo.

2. Configure la red del nodo de gestión (eth0).

   Si necesita una NIC adicional para aislar el tráfico de almacenamiento, consulte las instrucciones para configurar otra NIC: "Configurar una controladora de interfaz de red (NIC) de almacenamiento".

Configurar la sincronización de hora

1. Asegúrese de que la hora se haya sincronizado entre el nodo de gestión y el clúster de almacenamiento mediante NTP:

   A partir del elemento 12.3.1, los subpasos (a) a (e) se realizan automáticamente. Para el nodo de gestión 12.3.1, vaya a. subpaso (f) para completar la configuración de sincronización de tiempo.

1. Inicie sesión en el nodo de gestión mediante SSH o la consola proporcionada por su hipervisor.
2. Stop NTPD:

```
sudo service ntpd stop
```

3. Edite el archivo de configuración NTP `/etc/ntp.conf`:
   a. Comente los servidores predeterminados (`server 0.gentoo.pool.ntp.org`) agregando una `#` delante de cada uno.
   b. Agregue una nueva línea para cada servidor de tiempo predeterminado que desee agregar. Los servidores de hora predeterminados deben ser los mismos servidores NTP que se utilicen en el clúster de almacenamiento que se utilizará en un "paso posterior".

```
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. Guarde el archivo de configuración cuando finalice.
4. Fuerce una sincronización NTP con el servidor que se acaba de añadir.

```
sudo ntpd -gq
```

5. Reinicie NTPD.

```
sudo service ntpd start
```

6. Deshabilitar la sincronización de hora con el host a través del hipervisor (el siguiente es un ejemplo de VMware):

> Si implementa el mNode en un entorno de hipervisor distinto a VMware, por ejemplo, desde la imagen .iso en un entorno de OpenStack, consulte la documentación del hipervisor para obtener los comandos equivalentes.

   a. Desactivar la sincronización periódica:

```
vmware-toolbox-cmd timesync disable
```

   b. Mostrar y confirmar el estado actual del servicio:

```
vmware-toolbox-cmd timesync status
```

c. En vSphere, compruebe que el `Synchronize guest time with host` La casilla no está activada en las opciones de la máquina virtual.

> No habilite esta opción si realiza cambios futuros en la máquina virtual.

> No edite el NTP después de completar la configuración de sincronización de hora porque afecta al NTP cuando ejecuta el comando re-deploy en el nodo de gestión.

Configure el nodo de gestión

1. Cree un directorio de destino temporal para el contenido del paquete de servicios de gestión:

```
mkdir -p /sf/etc/mnode/mnode-archive
```

2. Descargue el paquete de servicios de gestión (versión 2.15.28 o posterior) que se instaló anteriormente en el nodo de gestión existente y guárdelo en el `/sf/etc/mnode/` directorio.
3. Extraiga el paquete descargado con el siguiente comando, reemplazando el valor entre corchetes [ ] (incluidos los paréntesis) por el nombre del archivo de paquete:

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle
file]
```

4. Extraiga el archivo resultante en la `/sf/etc/mnode-archive` directorio:

```
tar -C /sf/etc/mnode/mnode-archive -xvf
/sf/etc/mnode/services_deploy_bundle.tar.gz
```

5. Crear un archivo de configuración para cuentas y volúmenes:

```
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. Sustituya el valor entre corchetes [ ] (incluidos los corchetes) para cada uno de los siguientes parámetros necesarios:

- **[mvip IP address]**: La dirección IP virtual de administración del clúster de almacenamiento. Configure el nodo de gestión con el mismo clúster de almacenamiento que utilizó durante "Configuración de servidores NTP".
- **[nombre de cuenta de volumen persistente]**: Nombre de la cuenta asociada a todos los volúmenes persistentes en este clúster de almacenamiento.

6. Configure y ejecute el comando de nueva puesta en marcha del nodo de gestión para conectarse a los volúmenes persistentes alojados en el clúster e inicie servicios con datos de configuración de nodos de gestión anteriores:

   Se le pedirá que introduzca contraseñas en un mensaje seguro. Si su clúster de está situado detrás de un servidor proxy, debe configurar el proxy de manera que pueda llegar a una red pública.

   ```
   sudo /sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
   ```

   a. Sustituya el valor entre corchetes [ ] (incluidos los corchetes) por el nombre de usuario de la cuenta de administrador del nodo de gestión. Probablemente este sea el nombre de usuario de la cuenta de usuario que utilizó para iniciar sesión en el nodo de gestión.

      Puede agregar el nombre de usuario o permitir que la secuencia de comandos le solicite la información.

   b. Ejecute el `redeploy-mnode` comando. El script muestra un mensaje de éxito una vez que se ha completado la reimplantación.

   c. Si accede a las interfaces web de Element (como el nodo de gestión o Hybrid Cloud Control de NetApp) mediante el nombre de dominio completo (FQDN) del sistema, "volver a configurar la autenticación del nodo de gestión".

Funcionalidad SSH que proporciona "Acceso a la sesión del túnel de soporte remoto (RST) de NetApp Support" está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 y posteriores. Si ya había habilitado la funcionalidad SSH en el nodo de gestión, es posible que deba hacerlo "Vuelva a deshabilitar SSH" en el nodo de gestión recuperado.

Obtenga más información

- "Volúmenes persistentes"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Acceda al nodo de gestión

A partir de la versión 11.3 del software NetApp Element, el nodo de gestión contiene dos interfaces de usuario: Una interfaz de usuario para gestionar los servicios basados en REST y una interfaz de usuario por nodo para gestionar la configuración de red y de clúster, así como las pruebas y utilidades del sistema operativo.

Para los clústeres que ejecutan el software Element de la versión 11.3 o posterior, es posible usar una de dos interfaces:

- Con la interfaz de usuario del nodo de gestión (`https:// [mNode IP]:442`), puede realizar cambios en la configuración de la red y del clúster, ejecutar pruebas del sistema o utilizar utilidades del sistema.

- Mediante el uso de la interfaz de usuario de API de REST integrada (`https://[mNode IP}/mnode`), puede ejecutar o comprender las API relacionadas con los servicios del nodo de administración, incluida la configuración del servidor proxy, las actualizaciones de nivel de servicio o la administración de activos.

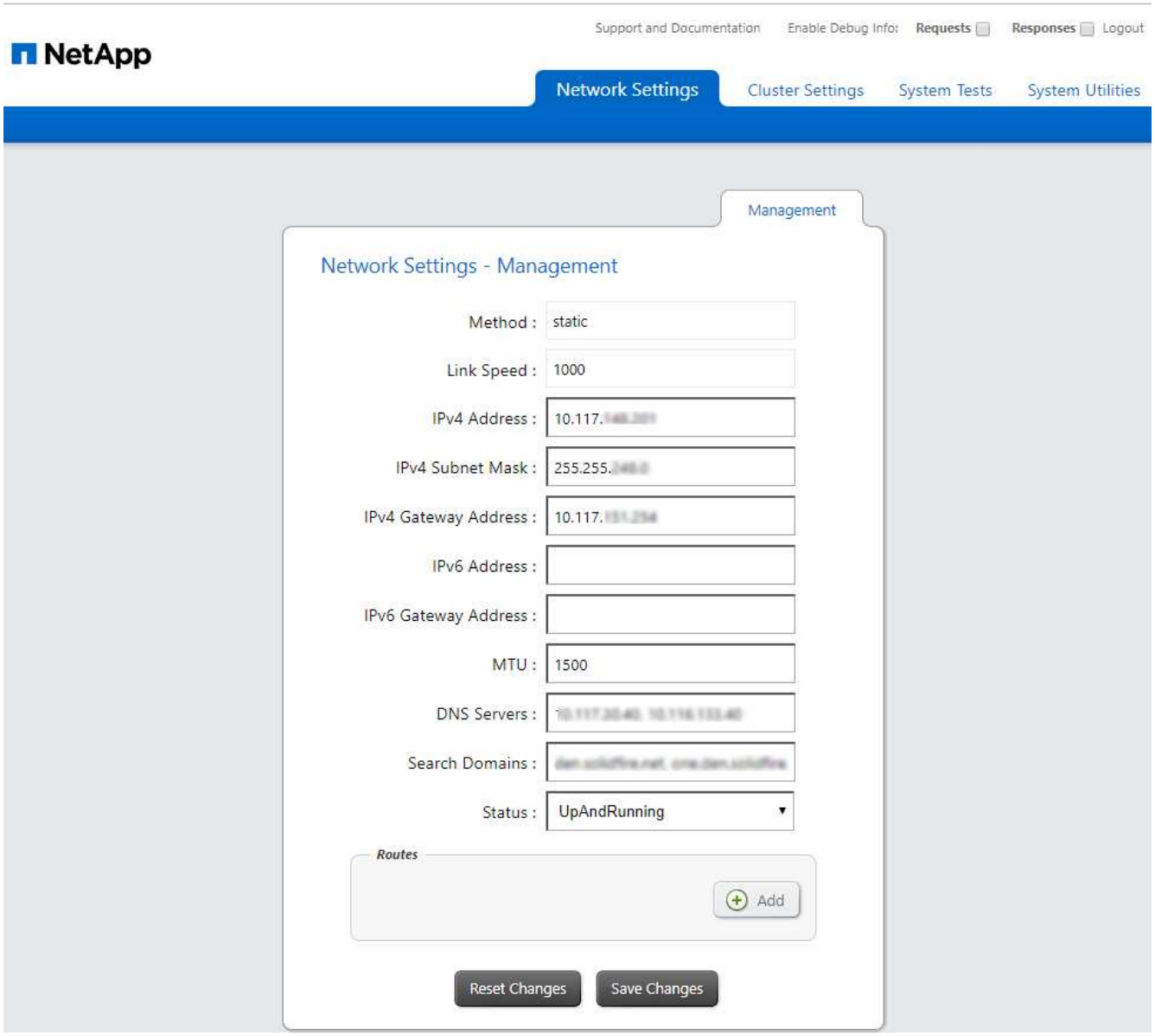
Acceda a la interfaz de usuario de cada nodo de gestión

Desde la interfaz de usuario por nodo, puede acceder a la configuración de red y clúster y utilizar las pruebas y las utilidades del sistema.

Pasos

1. Para acceder a la interfaz de usuario por nodo de gestión, introduzca la dirección IP del nodo de gestión seguida de :442

```
https://[IP address]:442
```



2. Introduzca el nombre de usuario y la contraseña del nodo de gestión cuando se le solicite.

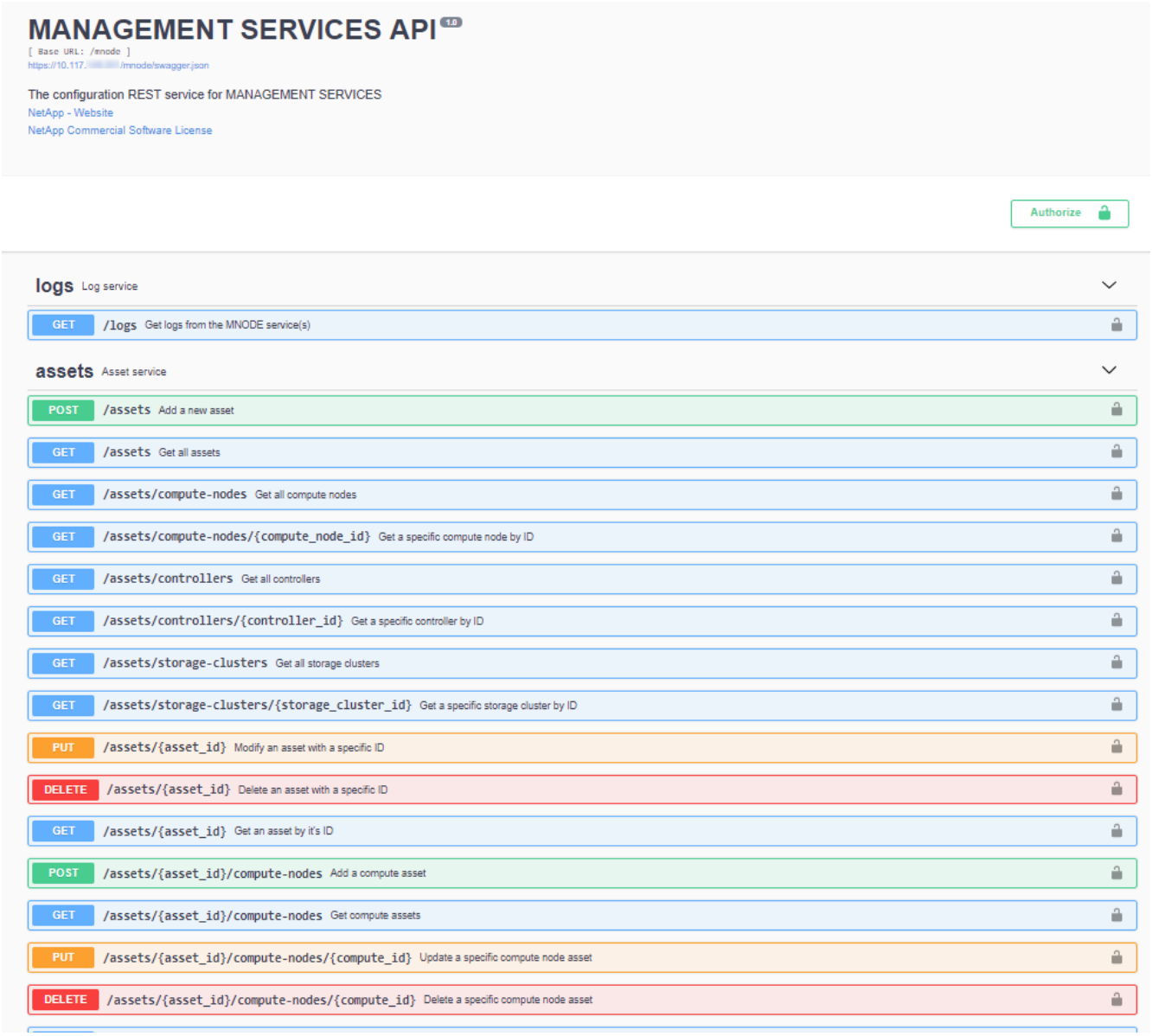
Acceda a la interfaz de usuario de API DE REST del nodo de gestión

Desde la interfaz de usuario de la API DE REST, puede acceder a un menú de API relacionadas con el servicio que controlan los servicios de gestión en el nodo de gestión.

Pasos

1. Para acceder a la interfaz de usuario de la API DE REST para los servicios de gestión, introduzca la dirección IP del nodo de gestión seguida de `/mnode`:

```
https://[IP address]/mnode
```



2. Seleccione **autorizar** o cualquier icono de bloqueo e introduzca las credenciales de administración del clúster para los permisos de uso de las API.

Obtenga más información

- "Habilite la supervisión de Active IQ y NetApp"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Trabaje con la interfaz de usuario del nodo de gestión

Información general de la interfaz de usuario del nodo de gestión

Con la interfaz de usuario del nodo de gestión (`https://<ManagementNodeIP>:442`), puede realizar cambios en la configuración de la red y del clúster, ejecutar pruebas del sistema o utilizar utilidades del sistema.

Tareas que se pueden realizar con la interfaz de usuario del nodo de gestión:

- "Configure la supervisión de alertas"
- "Modifique y pruebe la red, el clúster y la configuración del sistema de los nodos de gestión"
- "Ejecute las utilidades del sistema desde el nodo de gestión"

Obtenga más información

- "Acceda al nodo de gestión"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Configure la supervisión de alertas

Las herramientas de supervisión de alertas están configuradas para la supervisión de alertas NetApp HCI. Estas herramientas no están configuradas ni se utilizan para el almacenamiento all-flash de SolidFire. Si ejecuta las herramientas de estos clústeres, se genera el siguiente error 405, el cual se espera para la configuración: `webUIParseError : Invalid response from server. 405`

Para obtener más información sobre la configuración de la supervisión de alertas para NetApp HCI, consulte "Configure la supervisión de alertas"

Modifique y pruebe la red, el clúster y la configuración del sistema de los nodos de gestión

Puede modificar y probar la red de los nodos de gestión, el clúster y la configuración del sistema.

- Actualice la configuración de red del nodo de gestión
- Actualice la configuración del clúster del nodo de gestión
- Pruebe los ajustes del nodo de gestión

Actualice la configuración de red del nodo de gestión

En la pestaña Network Settings de la interfaz de usuario de nodo de gestión por nodo, puede modificar los campos de la interfaz de red de los nodos de gestión.

1. Abra la interfaz de usuario de cada nodo de gestión.
2. Seleccione la ficha **Configuración de red**.
3. Vea o introduzca la siguiente información:
   a. **Método**: Elija uno de los siguientes métodos para configurar la interfaz:
      - `loopback`: Utilice para definir la interfaz de bucle invertido de IPv4.
      - `manual`: Se utiliza para definir interfaces para las que no se realiza ninguna configuración de forma predeterminada.
      - `dhop`: Se utiliza para obtener una dirección IP a través de DHCP.
      - `static`: Se utiliza para definir interfaces Ethernet con direcciones IPv4 asignadas estáticamente.
   b. **Velocidad de enlace**: La velocidad negociada por la NIC virtual.
   c. **Dirección IPv4**: La dirección IPv4 de la red eth0.
   d. **Máscara de subred IPv4**: Subdivisiones de dirección de la red IPv4.
   e. **Dirección de puerta de enlace IPv4**: Dirección de red del router para enviar paquetes fuera de la red local.
   f. **Dirección IPv6**: La dirección IPv6 de la red eth0.
   g. **Dirección de puerta de enlace IPv6**: Dirección de red del enrutador para enviar paquetes fuera de la red local.

      Las opciones IPv6 no son compatibles con las versiones 11.3 o posteriores del nodo de gestión.

   h. **MTU**: Tamaño de paquete más grande que un protocolo de red puede transmitir. Debe ser mayor o igual que 1500. Si se añade un segundo NIC de almacenamiento, el valor debería ser 9000.
   i. **Servidores DNS**: Interfaz de red utilizada para la comunicación de clústeres.
   j. **Buscar dominios**: Busque direcciones MAC adicionales disponibles para el sistema.
   k. **Estado**: Valores posibles:
      - `UpAndRunning`
      - `Down`
      - `Up`
   l. **Rutas**: Rutas estáticas a hosts o redes específicos a través de la interfaz asociada que las rutas están configuradas para utilizar.

Actualice la configuración del clúster del nodo de gestión

En la pestaña Cluster Settings de la interfaz de usuario por nodo para la gestión de los nodos, los campos de la interfaz de clúster se pueden modificar cuando un nodo está en el estado Available, Pending, PendingActive y Active.

1. Abra la interfaz de usuario de cada nodo de gestión.

2. Seleccione la ficha **Configuración del clúster**.
3. Vea o introduzca la siguiente información:
   - **Rol**: Función que tiene el nodo de administración en el clúster. El posible valor es: `Management`.
   - **Versión**: Versión del software Element que se ejecuta en el cluster.
   - **Interfaz predeterminada**: Interfaz de red predeterminada utilizada para la comunicación del nodo de administración con el clúster que ejecuta el software Element.

Pruebe los ajustes del nodo de gestión

Después de cambiar la configuración de red y de gestión del nodo de gestión y confirmar los cambios, puede ejecutar pruebas para validar los cambios realizados.

1. Abra la interfaz de usuario de cada nodo de gestión.
2. En la interfaz de usuario del nodo de gestión, seleccione **pruebas del sistema**.
3. Realice alguna de las siguientes acciones:
   a. Para comprobar que los ajustes de red configurados son válidos para el sistema, seleccione **probar configuración de red**.
   b. Para probar la conectividad de red a todos los nodos del clúster en las interfaces 1G y 10G mediante paquetes ICMP, seleccione **probar ping**.
4. Vea o introduzca lo siguiente:
   - **Hosts**: Especifique una lista separada por comas de direcciones o nombres de host de los dispositivos que se van a hacer ping.
   - **Intentos**: Especifique el número de veces que el sistema debe repetir la prueba ping. El valor predeterminado es 5.
   - **Tamaño de paquete**: Especifique el número de bytes que se enviarán en el paquete ICMP que se envía a cada IP. El número de bytes debe ser inferior al MTU máximo especificado en la configuración de red.
   - **Tiempo de espera msec**: Especifique el número de milisegundos que se deben esperar para cada respuesta de ping individual. Valor predeterminado: 500 ms.
   - **Tiempo de espera total Sec**: Especifique el tiempo en segundos que el ping debe esperar a una respuesta del sistema antes de emitir el siguiente intento de ping o de terminar el proceso. El valor predeterminado es 5.
   - **Prohibir fragmentación**: Activar el indicador DF (no fragmentar) para los paquetes ICMP.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Ejecute las utilidades del sistema desde el nodo de gestión

Se puede usar la interfaz de usuario por nodo para el nodo de gestión a fin de crear o eliminar paquetes de soporte de clústeres, restablecer la configuración de nodos o reiniciar las redes.

Pasos

1. Abra la interfaz de usuario de cada nodo de gestión con las credenciales de administrador del nodo de gestión.
2. Seleccione **Utilidades del sistema**.
3. Seleccione el botón de la utilidad que desea ejecutar:
   a. **Potencia de control**: Reinicia, enciende o apaga el nodo. Especifique cualquiera de las siguientes opciones.

      Esta operación provoca la pérdida temporal de conectividad de red.

      - **Acción**: Las opciones incluyen `Restart` y.. `Halt` (apagado).
      - **Retardo de activación**: Cualquier tiempo adicional antes de que el nodo vuelva a estar en línea.

   b. **Crear paquete de soporte de clúster**: Crea el paquete de soporte de clúster para ayudar a las evaluaciones de diagnóstico del soporte de NetApp de uno o más nodos de un clúster. Especifique las siguientes opciones:
      - **Nombre del paquete**: Nombre único para cada paquete de soporte creado. Si no se proporciona ningún nombre, "supportBundle" y el nombre de nodo se utilizan como nombre de archivo.
      - **Mvip**: La MVIP del cluster. Los paquetes se agrupan en todos los nodos del clúster. Este parámetro es obligatorio si no se especifica el parámetro Nodes.
      - **Nodes**: Las direcciones IP de los nodos de los que se van a recopilar paquetes. Use nodos o Mvip, pero no ambos, para especificar los nodos a partir de los cuales se van a formar paquetes. Este parámetro es obligatorio si no se especifica Mvip.
      - **Nombre de usuario**: El nombre de usuario administrador del clúster.
      - **Contraseña**: La contraseña de administrador del clúster.
      - **Permitir incompleto**: Permite que la secuencia de comandos continúe ejecutándose si los paquetes no se pueden recopilar de uno o más de los nodos.
      - **Extra args**: Este parámetro se carga al `sf_make_support_bundle` guión. Este parámetro solo se debe usar si lo solicita el soporte de NetApp.

   c. **Eliminar todos los paquetes de soporte**: Elimina los paquetes de soporte actuales del nodo de administración.
   d. **Restablecer nodo**: Restablece el nodo de administración a una nueva imagen de instalación. Esto cambia todas las opciones, excepto la configuración de red al estado predeterminado. Especifique las siguientes opciones:
      - **Build**: La dirección URL de una imagen de software de elemento remoto a la que se restablecerá el nodo.
      - **Opciones**: Especificaciones para ejecutar las operaciones de restablecimiento. El soporte de NetApp puede proporcionar detalles si es necesario.

        Esta operación provoca la pérdida temporal de conectividad de red.

   e. **Reiniciar red**: Reinicia todos los servicios de red en el nodo de gestión.

      Esta operación provoca la pérdida temporal de conectividad de red.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Trabaje con la API DE REST del nodo de gestión

Información general de la interfaz de usuario de la API DE REST del nodo de

Mediante el uso de la interfaz de usuario de API de REST integrada (`https://<ManagementNodeIP>/mnode`), puede ejecutar o comprender las API relacionadas con los servicios del nodo de administración, incluida la configuración del servidor proxy, las actualizaciones de nivel de servicio o la administración de activos.

Tareas que se pueden realizar con API de REST:

Autorización

- "Obtenga autorización para utilizar las API de REST"

Configuración de activos

- "Habilite la supervisión de Active IQ y NetApp"
- "Configure un servidor proxy para el nodo de gestión"
- "Configure Cloud Control de NetApp híbrido para varias instancias de vCenter"
- "Añada un activo de controladora al nodo de gestión"
- "Crear y gestionar activos de clúster de almacenamiento"

Gestión de activos

- "Ver o editar activos de controladora existentes"
- "Crear y gestionar activos de clúster de almacenamiento"
- "Use la API DE REST para recoger registros del sistema Element"
- "Verifique el sistema operativo del nodo de gestión y las versiones de servicios"
- "Obtener registros de los servicios de gestión"

Obtenga más información

- "Acceda al nodo de gestión"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Obtenga autorización para utilizar las API de REST

Se debe autorizar para poder usar las API de para los servicios de gestión en la interfaz de usuario de la API de REST. Para ello, obtenga un token de acceso.

Para obtener un token, debe proporcionar credenciales de administrador del clúster y un ID de cliente. Cada ficha dura aproximadamente diez minutos. Después de que caduque un token, puede volver a autorizarse

para un nuevo token de acceso.

La funcionalidad de autorización se configura durante la instalación y la puesta en marcha del nodo de gestión. El servicio de token se basa en el clúster de almacenamiento que haya definido durante la configuración.

Antes de empezar

- La versión del clúster debe ejecutar el software NetApp Element 11.3 o una versión posterior.
- Debe haber implementado un nodo de gestión que ejecute la versión 11.3 o posterior.

Comando API

```
TOKEN=`curl -k -X POST https://MVIP/auth/connect/token -F client_id=mnode-
client -F grant_type=password -F username=CLUSTER_ADMIN -F
password=CLUSTER_PASSWORD|awk -F':' '{print $2}'|awk -F',' '{print
$1}'|sed s/\"//g`
```

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Para acceder a la interfaz de usuario de API DE REST del servicio, introduzca la dirección IP del nodo de gestión seguida del nombre de servicio, por ejemplo `/mnode/`:

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

2. Seleccione **autorizar**.

   Como alternativa, puede seleccionar un icono de bloqueo junto a cualquier API de servicio.

3. Complete lo siguiente:
   a. Introduzca el nombre de usuario y la contraseña del clúster.
   b. Introduzca el ID de cliente as `mnode-client`.
   c. No introduzca un valor para el secreto de cliente.
   d. Seleccione **autorizar** para iniciar una sesión.
4. Cierre el cuadro de diálogo **autorizaciones disponibles**.

   Si intenta ejecutar un comando después de que caduque el token, a. `401 Error: UNAUTHORIZED` aparece el mensaje. Si ve esto, vuelva a autorizar.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Habilite la supervisión de Active IQ y NetApp

Puede habilitar la supervisión del almacenamiento de Active IQ si todavía no lo hizo

durante la instalación o la actualización. Puede que tenga que utilizar este procedimiento si no configuró SolidFire Active IQ durante la instalación de para un sistema de almacenamiento all-flash de SolidFire.

El servicio del recopilador Active IQ reenvía los datos de configuración y los indicadores de rendimiento del clúster basados en software Element a SolidFire Active IQ para realizar informes históricos y supervisar el rendimiento prácticamente en tiempo real. El servicio de supervisión de NetApp permite el reenvío de errores del clúster de almacenamiento a vCenter para notificaciones de alerta.

Antes de empezar

- Algunas funciones de Active IQ, por ejemplo, Quality of Service (QoS), requieren Element 11.3 o posterior para funcionar correctamente. Para confirmar que tiene la capacidad de utilizar todas las funciones de Active IQ, NetApp recomienda lo siguiente:
  - El clúster de almacenamiento ejecuta el software NetApp Element 11.3 o una versión posterior.
  - Un nodo de gestión se implementó con la versión 11.3 o posterior.
- Tienes acceso a Internet. El servicio de recopilador Active IQ no se puede utilizar de sitios oscuros que no tienen conectividad externa.

Pasos

1. Obtenga el ID de activo base para la instalación:
   a. Abra la interfaz de usuario de la API DE REST del servicio de inventario en el nodo de gestión:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Seleccione **autorizar** y complete lo siguiente:
      i. Introduzca el nombre de usuario y la contraseña del clúster.
      ii. Introduzca el ID de cliente as `mnode-client`.
      iii. Seleccione **autorizar** para iniciar una sesión.
      iv. Cierre la ventana.
   c. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.
   d. Seleccione **probar**.
   e. Seleccione **Ejecutar**.
   f. Del cuerpo de respuesta del código 200, copie el `id` para la instalación.

```
{
  "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",
```

Su instalación tiene una configuración de activos base que se creó durante la instalación o la actualización.

2. Activar telemetría:
   a. Acceda a la interfaz de usuario de API de servicio mnode en el nodo de gestión introduciendo la dirección IP del nodo de gestión seguida de `/mnode`:

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

   b. Seleccione **autorizar** o cualquier icono de bloqueo y complete lo siguiente:
      i. Introduzca el nombre de usuario y la contraseña del clúster.
      ii. Introduzca el ID de cliente as `mnode-client`.
      iii. Seleccione **autorizar** para iniciar una sesión.
      iv. Cierre la ventana.
   c. Configure el activo base:
      i. Seleccione **PUT /assets/{asset_id}**.
      ii. Seleccione **probar**.
      iii. Introduzca lo siguiente en la carga útil de JSON:

```
{
"telemetry_active": true
"config": {}
}
```

      iv. Introduzca el ID base del paso anterior en **Asset_ID**.
      v. Seleccione **Ejecutar**.

      El servicio Active IQ se reinicia automáticamente cada vez que cambian los activos. La modificación de activos produce un breve retraso antes de aplicar la configuración.

3. Si todavía no lo ha hecho, añada un activo de controladora de vCenter para el control del cloud híbrido de NetApp a los activos conocidos del nodo de gestión:

   Se requiere un activo de controlador para los servicios de supervisión de NetApp.

   a. Seleccione **POST /assets/{Asset_id}/controllers** para agregar un subactivo de controlador.
   b. Seleccione **probar**.
   c. Introduzca el ID de activo base principal que copió en el portapapeles en el campo **Asset_id**.
   d. Introduzca los valores de carga útil requeridos con `type` como `vCenter` De aplicaciones y vCenter.

```
{
"username": "string",
"password": "string",
"ip": "string",
"type": "vCenter",
"host_name": "string",
"config": {}
}
```

   `ip` Es la dirección IP de vCenter.

   e. Seleccione **Ejecutar**.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Configure Cloud Control de NetApp híbrido para varias instancias de vCenter

Es posible configurar NetApp Hybrid Cloud Control para gestionar activos desde dos o más vCenter que no utilicen Linked Mode.

Debe utilizar este proceso después de la instalación inicial cuando necesite añadir activos para una instalación a escala reciente o cuando no se agreguen automáticamente activos nuevos a la configuración. Utilice estas API para añadir activos que se han añadido recientemente a su instalación.

Lo que necesitará

- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Un nodo de gestión se implementó con la versión 11.3 o posterior.

Pasos

1. "Añada nuevas instancias de vCenter como activos de la controladora" a la configuración del nodo de gestión.
2. Actualice la API del servicio de inventario en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

Como alternativa, puede esperar 2 minutos para que el inventario se actualice en la interfaz de usuario de control del cloud híbrido de NetApp.

a. Seleccione **autorizar** y complete lo siguiente:
   i. Introduzca el nombre de usuario y la contraseña del clúster.
   ii. Introduzca el ID de cliente as `mnode-client`.
   iii. Seleccione **autorizar** para iniciar una sesión.
   iv. Cierre la ventana.
b. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.
c. Seleccione **probar**.
d. Seleccione **Ejecutar**.
e. Desde la respuesta, copie el ID del activo de instalación (`"id"`).
f. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations/{id}**.
g. Seleccione **probar**.
h. Establezca Refresh a. `True`.
i. Pegue el ID de activo de instalación en el campo **id**.
j. Seleccione **Ejecutar**.

3. Actualice el explorador de NetApp Hybrid Cloud Control para ver los cambios.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Añada un activo de controladora al nodo de gestión

Es posible añadir un activo de controladora a la configuración del nodo de gestión mediante la interfaz de usuario de API DE REST.

Es posible que tenga que agregar un activo si ha escalado recientemente su instalación y no se han añadido automáticamente nuevos activos a la configuración. Utilice estas API para añadir activos que se han añadido recientemente a su instalación.

Lo que necesitará

- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Un nodo de gestión se implementó con la versión 11.3 o posterior.
- Se creó un nuevo rol HCC de NetApp en vCenter para limitar la vista de servicios de nodos de gestión a activos de solo NetApp. Consulte "Cree una función HCC de NetApp en vCenter"

Pasos

1. Obtenga el ID de activo base para la instalación:
   a. Abra la interfaz de usuario de la API DE REST del servicio de inventario en el nodo de gestión:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Seleccione **autorizar** y complete lo siguiente:
      i. Introduzca el nombre de usuario y la contraseña del clúster.
      ii. Introduzca el ID de cliente as `mnode-client`.
      iii. Seleccione **autorizar** para iniciar una sesión.
      iv. Cierre la ventana.
   c. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.
   d. Seleccione **probar**.
   e. Seleccione **Ejecutar**.
   f. Del cuerpo de respuesta del código 200, copie el `id` para la instalación.

      ```
      {
        "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",
      ```

      Su instalación tiene una configuración de activos base que se creó durante la instalación o la actualización.

   g. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations/{id}**.
   h. Seleccione **probar**.
   i. Pegue el ID de activo de instalación en el campo **id**.
   j. Seleccione **Ejecutar**.
   k. En la respuesta, copie y guarde el ID de controladora del clúster (`"controllerId"`) para usar en un paso posterior.
2. Para añadir un subactivo de controladora a un activo base existente, seleccione:

   ```
   POST /assets/{asset_id}/controllers
   ```

a. Abra la interfaz de usuario de API DE REST de mNode Service en el nodo de gestión:

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

b. Seleccione **autorizar** y complete lo siguiente:
   i. Introduzca el nombre de usuario y la contraseña del clúster.
   ii. Introduzca el ID de cliente as `mnode-client`.
   iii. Seleccione **autorizar** para iniciar una sesión.
   iv. Cierre la ventana.

c. Seleccione **POST /Asset/{Asset_id}/controllers**.

d. Seleccione **probar**.

e. Introduzca el ID de activo base principal en el campo **Asset_id**.

f. Añada los valores necesarios a la carga útil.

g. Seleccione **Ejecutar**.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Crear y gestionar activos de clúster de almacenamiento

Es posible añadir activos de clúster de almacenamiento nuevos al nodo de gestión, editar las credenciales almacenadas para activos de clúster de almacenamiento conocidos y eliminar activos de clúster de almacenamiento del nodo de gestión mediante la API REST.

Lo que necesitará

- Asegúrese de que la versión del clúster de almacenamiento ejecute la versión 11.3 o posterior del software NetApp Element.
- Asegúrese de haber implementado un nodo de gestión que ejecuta la versión 11.3 o una versión posterior.

Opciones de gestión de los activos del clúster de almacenamiento

Seleccione una de las siguientes opciones:

- Recuperar el ID de instalación y el ID de clúster de un activo de clúster de almacenamiento
- Añada un nuevo activo de clúster de almacenamiento
- Editar las credenciales almacenadas de un activo de clúster de almacenamiento
- Eliminar un activo de clúster de almacenamiento

Recuperar el ID de instalación y el ID de clúster de un activo de clúster de almacenamiento

Puede usar la API REST para obtener el ID de instalación y el ID de clúster de almacenamiento. Es necesario que el ID de instalación añada un nuevo activo de clúster de almacenamiento y el ID de clúster para modificar

o eliminar un activo de clúster de almacenamiento específico.

Pasos

1. Acceda a la interfaz de usuario de LA API DE REST para el servicio de inventario introduciendo la dirección IP del nodo de gestión seguida de `/inventory/1/`:

   ```
   https://<ManagementNodeIP>/inventory/1/
   ```

2. Seleccione **autorizar** o cualquier icono de bloqueo y complete lo siguiente:
   a. Introduzca el nombre de usuario y la contraseña del clúster.
   b. Introduzca el ID de cliente as `mnode-client`.
   c. Seleccione **autorizar** para iniciar una sesión.
   d. Cierre la ventana.
3. Seleccione **GET /Installations**.
4. Seleccione **probar**.
5. Seleccione **Ejecutar**.

   La API muestra una lista de todas las instalaciones conocidas.

6. Desde el cuerpo de respuesta de código 200, guarde el valor en `id` en la lista de instalaciones encontrará. Este es el ID de instalación. Por ejemplo:

   ```
   "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. Acceda a la interfaz de usuario de API DE REST del servicio de almacenamiento introduciendo la dirección IP del nodo de gestión seguida de `/storage/1/`:

   ```
   https://<ManagementNodeIP>/storage/1/
   ```

8. Seleccione **autorizar** o cualquier icono de bloqueo y complete lo siguiente:
   a. Introduzca el nombre de usuario y la contraseña del clúster.
   b. Introduzca el ID de cliente as `mnode-client`.

c. Seleccione **autorizar** para iniciar una sesión.

d. Cierre la ventana.

9. Seleccione **GET /Clusters**.
10. Seleccione **probar**.
11. Introduzca el ID de instalación que guardó anteriormente en la `installationId` parámetro.
12. Seleccione **Ejecutar**.

    La API muestra una lista de todos los clústeres de almacenamiento conocidos en esta instalación.

13. En el cuerpo de respuesta del código 200, busque el clúster de almacenamiento correcto y guarde el valor en el clúster `storageId` campo. Este es el ID del clúster de almacenamiento.

Añada un nuevo activo de clúster de almacenamiento

Es posible usar la API DE REST para añadir uno o varios activos nuevos del clúster de almacenamiento al inventario de nodos de gestión. Cuando se añade un nuevo activo de clúster de almacenamiento, se registra automáticamente con el nodo de gestión.

Lo que necesitará

- Ha copiado la El ID del clúster de almacenamiento y el ID de instalación para los clústeres de almacenamiento que desea añadir.
- Si va a añadir más de un nodo de almacenamiento, ha leído y comprendido las limitaciones de "Cluster de autoridad" compatibilidad con varios clústeres de almacenamiento.

> Todos los usuarios definidos en el clúster autorizado se definen como usuarios en todos los demás clústeres ligados a la instancia de Hybrid Cloud Control de NetApp.

Pasos

1. Acceda a la interfaz de usuario de API DE REST del servicio de almacenamiento introduciendo la dirección IP del nodo de gestión seguida de `/storage/1/`:

   ```
   https://<ManagementNodeIP>/storage/1/
   ```

2. Seleccione **autorizar** o cualquier icono de bloqueo y complete lo siguiente:

   a. Introduzca el nombre de usuario y la contraseña del clúster.

   b. Introduzca el ID de cliente as `mnode-client`.

   c. Seleccione **autorizar** para iniciar una sesión.

   d. Cierre la ventana.

3. Seleccione **POST /cluster**.
4. Seleccione **probar**.
5. Introduzca la información del nuevo clúster de almacenamiento en los siguientes parámetros en el campo **cuerpo de la solicitud**:

```
{
  "installationId": "a1b2c34d-e56f-1a2b-c123-1ab2cd345d6e",
  "mvip": "10.0.0.1",
  "password": "admin",
  "userId": "admin"
}
```

Parámetro	Tipo	Descripción
`installationId`	cadena	La instalación en la que añadir el nuevo clúster de almacenamiento. Introduzca el ID de instalación que guardó anteriormente en este parámetro.
`mvip`	cadena	La dirección IP virtual de gestión de IPv4 (MVIP) del clúster de almacenamiento.
`password`	cadena	La contraseña que se utiliza para comunicarse con el clúster de almacenamiento de.
`userId`	cadena	El ID de usuario que se utiliza para comunicarse con el clúster de almacenamiento (el usuario debe tener privilegios de administrador).

6. Seleccione **Ejecutar**.

   La API muestra un objeto que contiene información acerca del activo del clúster de almacenamiento recién añadido, como información del nombre, la versión y la dirección IP.

Editar las credenciales almacenadas de un activo de clúster de almacenamiento

Puede editar las credenciales almacenadas que utiliza el nodo de gestión para iniciar sesión en un clúster de almacenamiento. El usuario que seleccione debe tener acceso de administrador del clúster.

Asegúrese de haber seguido los pasos de Recuperar el ID de instalación y el ID de clúster de un activo de clúster de almacenamiento antes de continuar.

Pasos

1. Acceda a la interfaz de usuario de API DE REST del servicio de almacenamiento introduciendo la dirección IP del nodo de gestión seguida de `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Seleccione **autorizar** o cualquier icono de bloqueo y complete lo siguiente:

a. Introduzca el nombre de usuario y la contraseña del clúster.
b. Introduzca el ID de cliente as `mnode-client`.
c. Seleccione **autorizar** para iniciar una sesión.
d. Cierre la ventana.

3. Seleccione **PUT /Clusters/{storageId}**.
4. Seleccione **probar**.
5. Pegue el ID del clúster de almacenamiento que ha copiado anteriormente en el `storageId` parámetro.
6. Cambie uno o ambos de los siguientes parámetros en el campo **cuerpo de solicitud**:

```
{
  "password": "adminadmin",
  "userId": "admin"
}
```

Parámetro	Tipo	Descripción
`password`	cadena	La contraseña que se utiliza para comunicarse con el clúster de almacenamiento de.
`userId`	cadena	El ID de usuario que se utiliza para comunicarse con el clúster de almacenamiento (el usuario debe tener privilegios de administrador).

7. Seleccione **Ejecutar**.

Eliminar un activo de clúster de almacenamiento

Es posible eliminar un activo de clúster de almacenamiento si el clúster de almacenamiento ya no está en servicio. Cuando se quita un activo de clúster de almacenamiento, este se cancela automáticamente del nodo de gestión.

Asegúrese de haber seguido los pasos de Recuperar el ID de instalación y el ID de clúster de un activo de clúster de almacenamiento antes de continuar.

Pasos

1. Acceda a la interfaz de usuario de API DE REST del servicio de almacenamiento introduciendo la dirección IP del nodo de gestión seguida de `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Seleccione **autorizar** o cualquier icono de bloqueo y complete lo siguiente:
a. Introduzca el nombre de usuario y la contraseña del clúster.

b. Introduzca el ID de cliente as `mnode-client`.
c. Seleccione **autorizar** para iniciar una sesión.
d. Cierre la ventana.

3. Seleccione **DELETE /Clusters/{storageId}**.
4. Seleccione **probar**.
5. Introduzca el ID del clúster de almacenamiento que copió anteriormente en el `storageId` parámetro.
6. Seleccione **Ejecutar**.

   Una vez realizado correctamente, la API devuelve una respuesta vacía.

Obtenga más información

- "Cluster de autoridad"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Ver o editar activos de controladora existentes

Es posible ver información y editar las controladoras VMware vCenter existentes en la configuración del nodo de gestión mediante la API DE REST. Las controladoras son instancias de VMware vCenter registradas en el nodo de gestión para su instalación de SolidFire de NetApp.

Antes de empezar

- Asegúrese de que la versión de su clúster ejecute la versión 11.3 o posterior del software NetApp Element.
- Asegúrese de haber implementado un nodo de gestión que ejecuta la versión 11.3 o una versión posterior.

Acceda a la API DE REST de servicios de gestión

Pasos

1. Acceda a la interfaz de usuario de la API DE REST para servicios de gestión. Para ello, introduzca la dirección IP del nodo de gestión seguida de `/vcenter/1/`:

   ```
   https://<ManagementNodeIP>/vcenter/1/
   ```

2. Seleccione **autorizar** o cualquier icono de bloqueo y complete lo siguiente:
   a. Introduzca el nombre de usuario y la contraseña del clúster.
   b. Introduzca el ID de cliente as `mnode-client`.
   c. Seleccione **autorizar** para iniciar una sesión.
   d. Cierre la ventana.

Ver la información almacenada sobre las controladoras existentes

Es posible ver una lista de las controladoras de vCenter existentes que están registradas con el nodo de gestión y ver información almacenada sobre ellas mediante la API DE REST.

Pasos

1. Seleccione **GET /compute/controllers**.
2. Seleccione **probar**.
3. Seleccione **Ejecutar**.

   La API muestra una lista de todas las controladoras de vCenter conocidas, junto con la dirección IP, el ID de controladora, el nombre de host y el ID de usuario que se utilizan para comunicarse con cada controladora.

4. Si desea el estado de conexión de una controladora determinada, copie el ID de controladora del `id` de esa controladora en el portapapeles y consulte Ver el estado de una controladora existente.

Ver el estado de una controladora existente

Es posible ver el estado de cualquiera de las controladoras existentes de vCenter que estén registradas en el nodo de gestión. La API muestra un estado que indica si el control de cloud híbrido de NetApp puede conectarse con la controladora de vCenter, así como el motivo de dicho estado.

Pasos

1. Seleccione **GET /Compute/controllers/{Controller_id}/status**.
2. Seleccione **probar**.
3. Introduzca el ID de controladora que copió anteriormente en la `controller_id` parámetro.
4. Seleccione **Ejecutar**.

   La API muestra el estado de esta controladora de vCenter en particular, junto con un motivo por el cual ese estado.

Edite las propiedades almacenadas de un controlador

Es posible editar el nombre de usuario o la contraseña almacenados de cualquiera de las controladoras existentes de vCenter registradas en el nodo de gestión. No se puede editar la dirección IP almacenada de una controladora de vCenter existente.

Pasos

1. Seleccione **PUT /compute/controllers/{Controller_id}**.
2. Introduzca el ID de la controladora de una controladora de vCenter en el `controller_id` parámetro.
3. Seleccione **probar**.
4. Cambie uno de los siguientes parámetros en el campo **cuerpo de solicitud**:

Parámetro	Tipo	Descripción
`userId`	cadena	Cambie el ID de usuario usado para comunicarse con la controladora de vCenter (el usuario debe tener privilegios de administrador).
`password`	cadena	Cambie la contraseña usada para comunicarse con la controladora de vCenter.

5. Seleccione **Ejecutar**.

   La API muestra información actualizada de la controladora.

Obtenga más información

- "Añada un activo de controladora al nodo de gestión"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Configure un servidor proxy

Si su clúster de está situado detrás de un servidor proxy, debe configurar el proxy de manera que pueda llegar a una red pública.

Un servidor proxy se utiliza para recopiladores de telemetría y conexiones de túnel inverso. Puede habilitar y configurar un servidor proxy con la interfaz de usuario de la API de REST si aún no configuró un servidor proxy durante la instalación o la actualización. También puede modificar la configuración existente del servidor proxy o deshabilitar un servidor proxy.

El comando para configurar un servidor proxy se actualiza y, a continuación, devuelve la configuración del proxy actual del nodo de gestión. Active IQ, el servicio de supervisión de NetApp y otras utilidades del software Element que se instalan en el nodo de gestión, incluido el túnel de soporte inverso para el soporte de NetApp.

Antes de empezar

- Debe conocer información sobre el host y las credenciales del servidor proxy que desea configurar.
- Asegúrese de que la versión de su clúster ejecute la versión 11.3 o posterior del software NetApp Element.
- Asegúrese de haber implementado un nodo de gestión que ejecuta la versión 11.3 o una versión posterior.
- (Nodo de gestión 12.0 y posterior) ha actualizado NetApp Hybrid Cloud Control a los servicios de gestión versión 2.16 antes de configurar un servidor proxy.

Pasos

1. Acceda a la interfaz de usuario de API DE REST en el nodo de gestión. Para ello, introduzca la dirección IP del nodo de gestión seguida de `/mnode`:

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

2. Seleccione **autorizar** o cualquier icono de bloqueo y complete lo siguiente:
   a. Introduzca el nombre de usuario y la contraseña del clúster.
   b. Introduzca el ID de cliente as `mnode-client`.
   c. Seleccione **autorizar** para iniciar una sesión.
   d. Cierre la ventana.
3. Seleccione **COLOCAR /settings**.
4. Seleccione **probar**.
5. Para habilitar un servidor proxy, debe definir `use_proxy` a verdadero. Introduzca el nombre de host o la IP y los destinos de puerto proxy.

   El nombre de usuario del proxy, la contraseña del proxy y el puerto SSH son opcionales y deben omitirse si no se usan.

   ```
   {
   "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. Seleccione **Ejecutar**.

Es posible que deba reiniciar su nodo de gestión según su entorno.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Verifique el sistema operativo del nodo de gestión y las versiones de servicios

Puede verificar los números de versión del sistema operativo del nodo de gestión, del paquete de servicios de gestión y de los servicios individuales que se ejecutan en el nodo de gestión mediante la API DE REST en el nodo de gestión.

Lo que necesitará

- El clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Un nodo de gestión se implementó con la versión 11.3 o posterior.

Opciones

- Comandos API
- PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

Comandos API

- Obtenga información de la versión acerca del sistema operativo del nodo de gestión, el paquete de servicios de gestión y el servicio API del nodo de gestión (mnode-api) que se ejecutan en el nodo de gestión:

```
curl -X GET "https://<ManagementNodeIP>/mnode/about" -H  "accept:
application/json"
```

- Obtenga información de versión sobre los servicios individuales que se ejecutan en el nodo de gestión:

```
curl -X GET "https://<ManagementNodeIP>/mnode/services?status=running"
-H  "accept: */*" -H  "Authorization: ${TOKEN}"
```

Usted puede encontrar al portador `${TOKEN}` Lo utiliza el comando API cuando lo utiliza "autorizar". El portador `${TOKEN}` está en la respuesta curl.

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Acceda a la interfaz de usuario de la API DE REST del servicio introduciendo la dirección IP del nodo de gestión seguida de `/mnode/`:

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

2. Debe realizar una de las siguientes acciones:
   - Obtenga información de la versión acerca del sistema operativo del nodo de gestión, el paquete de servicios de gestión y el servicio API del nodo de gestión (mnode-api) que se ejecutan en el nodo de gestión:
     i. Seleccione **GET /about**.
     ii. Seleccione **probar**.
     iii. Seleccione **Ejecutar**.

     La versión del paquete de servicios de gestión (`"mnode_bundle_version"`), versión del sistema operativo del nodo de gestión (`"os_version"`) Y la versión de la API del nodo de gestión (`"version"`) se indican en el cuerpo de respuesta.
   - Obtenga información de versión sobre los servicios individuales que se ejecutan en el nodo de gestión:
     i. Seleccione **GET /Services**.
     ii. Seleccione **probar**.
     iii. Seleccione el estado como **en ejecución**.
     iv. Seleccione **Ejecutar**.

     Los servicios que se ejecutan en el nodo de gestión se indican en el cuerpo de respuesta.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Obtener registros de los servicios de gestión

Es posible recuperar registros de los servicios que se ejecutan en el nodo de gestión mediante la API DE REST. Puede extraer registros de todos los servicios públicos o especificar servicios específicos y utilizar parámetros de consulta para definir mejor los resultados devueltos.

Lo que necesitará

- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Un nodo de gestión se implementó con la versión 11.3 o posterior.

Pasos

1. Abra la interfaz de usuario de API de REST en el nodo de gestión.
   - A partir de los servicios de administración 2.21.61:

     ```
     https://<ManagementNodeIP>/mnode/4/
     ```

   - Para los servicios de gestión 2.20.69 o anteriores:

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

2. Seleccione **autorizar** o cualquier icono de bloqueo y complete lo siguiente:
   a. Introduzca el nombre de usuario y la contraseña del clúster.
   b. Introduzca el ID de cliente como mnode-client si el valor no está ya rellenado.
   c. Seleccione **autorizar** para iniciar una sesión.
   d. Cierre la ventana.
3. Seleccione **GET /logs**.
4. Seleccione **probar**.
5. Especifique los siguientes parámetros:
   - `Lines`: Introduzca el número de líneas que desea que devuelva el registro. Este parámetro es un entero que se establece de manera predeterminada en 1000.

     Evite solicitar el historial completo del contenido de registro estableciendo líneas en 0.

   - `since`: Agrega una Marca de tiempo ISO-8601 para el punto de inicio de los registros de servicio.

     Usar un razonable `since` parámetro cuando se recogen registros de timespans más amplios.

- `service-name`: Introduzca un nombre de servicio.

  Utilice la `GET /services` comando para mostrar los servicios del nodo de gestión.

- `stopped`: Establecer en `true` para recuperar registros de servicios detenidos.

6. Seleccione **Ejecutar**.
7. En el cuerpo de la respuesta, seleccione **Descargar** para guardar la salida del registro.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Gestión de conexiones de soporte

Inicie una sesión de soporte remota de NetApp

Si necesita soporte técnico para su sistema de almacenamiento all-flash SolidFire, el soporte de NetApp puede conectarse de forma remota con su sistema. Para iniciar una sesión y tener acceso remoto, el soporte de NetApp puede abrir una conexión de Secure Shell (SSH) inversa a su entorno.

Puede abrir un puerto TCP para una conexión de túnel SSH inverso con el soporte de NetApp. Gracias a esta conexión, el soporte de NetApp puede iniciar sesión en su nodo de gestión.

Antes de empezar

- Para los servicios de gestión 2.18 y posteriores, la funcionalidad para el acceso remoto se deshabilita en el nodo de gestión de manera predeterminada. Para activar la función de acceso remoto, consulte "Gestione la funcionalidad SSH en el nodo de gestión".
- Si el nodo de gestión está detrás de un servidor proxy, se necesitan los siguientes puertos TCP en el archivo sshd.config:

Puerto TCP	Descripción	Dirección de conexión
443	Llamadas API/HTTPS para un reenvío de puertos inverso a través de un túnel de soporte abierto a la interfaz de usuario web	Del nodo de gestión a los nodos de almacenamiento
22	Acceso de inicio de sesión SSH	Del nodo de gestión a los nodos de almacenamiento o desde los nodos de almacenamiento al nodo de gestión

Pasos

- Inicie sesión en su nodo de almacenamiento y abra una sesión de terminal.
- En un símbolo del sistema, introduzca lo siguiente:

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

- Para cerrar el túnel de soporte remoto, introduzca lo siguiente:

```
rst --killall
```

- (Opcional) Deshabilitar "función de acceso remoto" de nuevo.

> SSH sigue estando habilitado en el nodo de gestión si no se la deshabilita. La configuración habilitada para SSH continúa en el nodo de gestión a través de actualizaciones y renovaciones hasta que se deshabilita manualmente.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Gestione la funcionalidad SSH en el nodo de gestión

Es posible deshabilitar, volver a habilitar o determinar el estado de la funcionalidad SSH en el nodo de gestión (mNode) mediante la API DE REST. Funcionalidad SSH que proporciona "Acceso a la sesión del túnel de soporte remoto (RST) de NetApp Support" está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 o posterior.

A partir de los servicios de gestión 2.20.69, puede habilitar y deshabilitar la funcionalidad SSH en el nodo de gestión mediante la interfaz de usuario de control de cloud híbrido de NetApp.

Lo que necesitará

- **Permisos de control del cloud híbrido de NetApp**: Tiene permisos como administrador.
- **Permisos de administrador de clúster**: Tiene permisos como administrador en el clúster de almacenamiento.
- **Software Element**: El clúster ejecuta el software NetApp Element 11.3 o posterior.
- **Nodo de gestión**: Ha implementado un nodo de gestión que ejecuta la versión 11.3 o posterior.
- **Actualizaciones de servicios de administración**:
  - Para utilizar la interfaz de usuario de control del cloud híbrido de NetApp, ha actualizado el "paquete de servicios de gestión" a la versión 2.20.69 o posterior.
  - Para usar la interfaz de usuario de la API DE REST, se ha actualizado el "paquete de servicios de gestión" a la versión 2.17.

Opciones

- Deshabilite o habilite la funcionalidad SSH en el nodo de gestión mediante la IU de control de cloud híbrido de NetApp

Puede realizar cualquiera de las siguientes tareas después de realizar "autenticar":

- Deshabilite o habilite la funcionalidad SSH en el nodo de gestión mediante las API de
- Determine el estado de la capacidad SSH en el nodo de gestión mediante las API de

Deshabilite o habilite la funcionalidad SSH en el nodo de gestión mediante la IU de control de cloud híbrido de NetApp

Es posible deshabilitar o volver a habilitar la funcionalidad SSH en el nodo de gestión. Funcionalidad SSH que proporciona "Acceso a la sesión del túnel de soporte remoto (RST) de NetApp Support" está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 o posterior. Al deshabilitar SSH, no se finalizan ni desconectan las sesiones de cliente SSH existentes en el nodo de gestión. Si deshabilita SSH y opta por volver a habilitarla más adelante, puede hacerlo mediante la interfaz de usuario de control de cloud híbrido de NetApp.

Para habilitar o deshabilitar el acceso de soporte con SSH para un clúster de almacenamiento, debe usar el "Página de configuración del clúster de la interfaz de usuario de Element".

Pasos

1. En el panel de control, seleccione el menú de opciones de la parte superior derecha y seleccione **Configurar**.
2. En la pantalla **Support Access for Management Node**, cambie el conmutador para activar el SSH del nodo de administración.
3. Después de completar la solución de problemas, en la pantalla **Support Access for Management Node**, cambie el conmutador para desactivar el SSH del nodo de gestión.

Deshabilite o habilite la funcionalidad SSH en el nodo de gestión mediante las API de

Es posible deshabilitar o volver a habilitar la funcionalidad SSH en el nodo de gestión. Funcionalidad SSH que proporciona "Acceso a la sesión del túnel de soporte remoto (RST) de NetApp Support" está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 o posterior. Al deshabilitar SSH, no se finalizan ni desconectan las sesiones de cliente SSH existentes en el nodo de gestión. Si deshabilita SSH y opta por volver a habilitarla más adelante, puede hacerlo mediante la misma API.

Comando API

Para los servicios de gestión 2.18 o posterior:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Para los servicios de gestión 2.17 o anteriores:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Usted puede encontrar al portador `${TOKEN}` Lo utiliza el comando API cuando lo utiliza "autorizar". El portador `${TOKEN}` está en la respuesta curl.

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Acceda a la interfaz de usuario de API DE REST para el servicio API del nodo de gestión. Para ello, introduzca la dirección IP del nodo de gestión seguida de `/mnode/`:

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

2. Seleccione **autorizar** y complete lo siguiente:
   a. Introduzca el nombre de usuario y la contraseña del clúster.
   b. Introduzca el ID de cliente as `mnode-client`.
   c. Seleccione **autorizar** para iniciar una sesión.
   d. Cierre la ventana.
3. En la interfaz de usuario DE LA API DE REST, seleccione **PUT /settings/ssh**.
   a. Seleccione **probar**.
   b. Establezca el parámetro **Enabled** en `false` Para deshabilitar SSH o. `true` Para volver a habilitar la funcionalidad SSH que estaba deshabilitada anteriormente.
   c. Seleccione **Ejecutar**.

Determine el estado de la capacidad SSH en el nodo de gestión mediante las API de

Puede determinar si la capacidad SSH está habilitada o no en el nodo de gestión mediante una API de servicio de nodo de gestión. SSH está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 o posteriores.

Comando API

Para los servicios de gestión 2.18 o posterior:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Para los servicios de gestión 2.17 o anteriores:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Usted puede encontrar al portador `${TOKEN}` Lo utiliza el comando API cuando lo utiliza "autorizar". El portador `${TOKEN}` está en la respuesta curl..

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Acceda a la interfaz de usuario de API DE REST para el servicio API del nodo de gestión. Para ello, introduzca la dirección IP del nodo de gestión seguida de `/mnode/`:

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

2. Seleccione **autorizar** y complete lo siguiente:
    a. Introduzca el nombre de usuario y la contraseña del clúster.
    b. Introduzca el ID de cliente as `mnode-client`.
    c. Seleccione **autorizar** para iniciar una sesión.
    d. Cierre la ventana.
3. En la interfaz de usuario DE LA API DE REST, seleccione **GET /settings/ssh**.
    a. Seleccione **probar**.
    b. Seleccione **Ejecutar**.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Actualice la versión Element 12,3.x de su sistema de almacenamiento all-flash NetApp SolidFire

Información general sobre la secuencia de actualización

Es posible mantener actualizado el sistema de almacenamiento de SolidFire Element después de la puesta en marcha. Para ello, se deben actualizar secuencialmente todos los componentes de almacenamiento de NetApp.

Estos componentes incluyen servicios de gestión, HealthTools, NetApp Hybrid Cloud Control, software Element, nodo de gestión y (según la instalación) el plugin Element para vCenter Server.

> A partir del 2023 de noviembre, no puede iniciar una actualización de componente con control de nube híbrida de NetApp o API de REST porque los certificados de clave de firma (privados y públicos) caducaron el 5 de noviembre de 2023. Puede resolver este problema siguiendo la solución que se explica en el artículo de la base de conocimientos "No se pueden iniciar las actualizaciones de SolidFire y HCI debido a un error de carga del paquete de actualización".

La secuencia de actualización del sistema Contenido describe las tareas necesarias para completar una actualización del sistema de almacenamiento all-flash de SolidFire. Lo ideal es que estos procedimientos se realicen como parte de la secuencia de actualización más grande y no de forma aislada. Si es necesaria una actualización o actualización basada en componentes, consulte los requisitos previos del procedimiento para garantizar que se aborden complejidades adicionales.

La "Secuencia de actualización de vSphere" Incluir el contenido del plugin de Element para vCenter Server describe los pasos adicionales previos y posteriores a la actualización necesarios para volver a instalar el plugin de Element para vCenter Server.

Lo que necesitará

- Ejecuta el nodo de gestión 11.3 o una versión posterior. Las versiones más recientes del nodo de gestión tienen una arquitectura modular que proporciona servicios individuales.

  > Para comprobar la versión, inicie sesión en el nodo de gestión y vea el número de versión de Element en el banner de inicio de sesión. Si no tiene 11.3, consulte "Actualice su nodo de gestión".

- Ha actualizado sus servicios de administración a al menos la versión 2.1.326.

  Las actualizaciones con Hybrid Cloud Control de NetApp no están disponibles en versiones anteriores del paquete de servicio.

- Debe asegurarse de que la hora del sistema en todos los nodos esté sincronizada y que NTP esté correctamente configurado para el clúster de almacenamiento y los nodos. Cada nodo debe configurarse con un servidor de nombres DNS en la interfaz de usuario web por nodo (`https://[IP address]:442`) sin fallos de clúster sin resolver relacionados con la desviación de tiempo.

secuencia de actualización del sistema

Es posible usar la siguiente secuencia para actualizar el sistema de almacenamiento all-flash SolidFire de NetApp para Element 12.3.x.

Pasos

1. "Actualice los servicios de gestión de Hybrid Cloud Control".

   Si actualiza los servicios de gestión a la versión 2.16 o posterior y ejecuta un nodo de gestión de 11.3 a 11.8, deberá aumentar la RAM de la máquina virtual del nodo de gestión antes de actualizar los servicios de gestión.

   Debe actualizar al paquete de servicios de gestión más reciente antes de actualizar el software Element.

2. "(Opcional) Actualice a la versión más reciente de HealthTools".

   Actualizar HealthTools solo es necesario si el nodo de gestión y el software Element que está ejecutando es 11.1 o anterior. HealthTools no es necesario para realizar actualizaciones de elementos mediante el control de cloud híbrido de NetApp.

3. "Ejecute comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento".
4. "Actualice el software Element y el firmware de almacenamiento".
5. "(Opcional) Actualice solo el firmware de almacenamiento de Element".

   Puede realizar esta tarea cuando haya una nueva actualización del firmware de almacenamiento disponible fuera de una versión principal.

6. "(Opcional) Actualice el nodo de gestión".

   Ya no se necesita actualizar el sistema operativo del nodo de gestión para actualizar el software Element en el clúster de almacenamiento. Si el nodo de gestión es la versión 11.3 o posterior, solo tiene que actualizar los servicios de gestión a la versión más reciente para realizar actualizaciones de Element mediante el control de cloud híbrido de NetApp. Siga el procedimiento de actualización del nodo de gestión para su escenario si desea actualizar el sistema operativo del nodo de gestión por otros motivos, como la corrección de seguridad.

7. "Actualice el plugin de Element para vCenter Server".

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Procedimientos de actualización del sistema

Actualice los servicios de gestión

Es posible actualizar los servicios de gestión a la versión de paquete más reciente después de haber instalado el nodo de gestión 11.3 o una versión posterior.

A partir del lanzamiento del nodo de gestión Element 11.3, el diseño del nodo de gestión se ha modificado en función de una nueva arquitectura modular que proporciona servicios individuales. Estos servicios modulares ofrecen funcionalidad de gestión centralizada y ampliada para un sistema de almacenamiento all-flash SolidFire. Los servicios de gestión incluyen servicios de telemetría, de registro y de actualización, el servicio QoSSIOC para el plugin de Element para vCenter Server, Cloud Control de NetApp, etc.

Acerca de esta tarea

- Debe actualizar al paquete de servicios de gestión más reciente antes de actualizar el software Element.

> - Los servicios de gestión 2.22.7 incluyen el plugin de Element para vCenter Server 5.0, que contiene el plugin remoto. Si usa el plugin de Element, debe actualizar a los servicios de gestión 2.22.7 o una versión posterior para cumplir con la directiva de VMware que elimina la compatibilidad con los plugins locales. "Leer más".
> - Para obtener las notas de la versión de los servicios de gestión más recientes, en las que se describen servicios principales, funciones nuevas, correcciones de errores y soluciones alternativas para cada paquete de servicio, consulte "las notas de la versión de los servicios de gestión"

Lo que necesitará

A partir de los servicios de gestión 2.20.69, debe aceptar y guardar el contrato de licencia de usuario final (CLUF) antes de utilizar la API o la interfaz de usuario de control de cloud híbrido de NetApp para actualizar los servicios de gestión:

1. Abra la dirección IP del nodo de gestión en un navegador web:

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

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto para actualizaciones actuales y futuras** y seleccione **Guardar**.

Opciones de actualización

Los servicios de gestión se pueden actualizar con la interfaz de usuario de Hybrid Cloud Control de NetApp o la API DE REST del nodo de gestión:

- Actualice los servicios de gestión con Hybrid Cloud Control (Método recomendado)
- Actualice los servicios de gestión mediante la API del nodo de gestión

Actualice los servicios de gestión con Hybrid Cloud Control

Puede actualizar los servicios de gestión de NetApp mediante Hybrid Cloud Control de NetApp.

Los paquetes de servicios de gestión ofrecen funcionalidades y correcciones mejoradas para la instalación

fuera de las versiones principales.

Antes de empezar

- Ejecuta el nodo de gestión 11.3 o una versión posterior.
- Si actualiza los servicios de gestión a la versión 2.16 o posterior y ejecuta un nodo de gestión de 11.3 a 11.8, deberá aumentar la RAM de la máquina virtual del nodo de gestión antes de actualizar los servicios de gestión:
  a. Apague la máquina virtual del nodo de gestión.
  b. Cambie la RAM de la máquina virtual del nodo de gestión de 12 GB a 24 GB de RAM.
  c. Encienda la máquina virtual del nodo de gestión.
- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Ha actualizado sus servicios de administración a al menos la versión 2.1.326. Las actualizaciones de control del cloud híbrido de NetApp no están disponibles en paquetes de servicio anteriores.

Para obtener una lista de los servicios disponibles para cada versión del paquete de servicio, consulte "Notas de la versión de los servicios de gestión".

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

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

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. En la página actualizaciones, seleccione la ficha **Servicios de administración**.
5. Siga las instrucciones de la página para descargar y guardar un paquete de actualización de servicios de administración en su equipo.
6. Seleccione **examinar** para localizar el paquete que guardó y cargarlo.

   Después de cargar el paquete, la actualización se inicia automáticamente.

   Después de comenzar la actualización, puede ver el estado de la actualización en esta página. Durante la actualización, es posible que pierda la conexión con NetApp Hybrid Cloud Control y tenga que volver a iniciar sesión para ver los resultados de la actualización.

Actualice los servicios de gestión mediante la API del nodo de gestión

Los usuarios deberían llevar a cabo, idealmente, actualizaciones de los servicios de gestión desde el control del cloud híbrido de NetApp. Sin embargo, puede cargar, extraer y poner en marcha manualmente una actualización de paquete de servicio para los servicios de gestión en el nodo de gestión mediante la API DE REST. Puede ejecutar cada comando desde la interfaz de usuario de la API de REST para el nodo de gestión.

Antes de empezar

- Implementó un nodo de gestión de software de NetApp Element 11.3 o posterior.
- Si actualiza los servicios de gestión a la versión 2.16 o posterior y ejecuta un nodo de gestión de 11.3 a

11.8, deberá aumentar la RAM de la máquina virtual del nodo de gestión antes de actualizar los servicios de gestión:

a. Apague la máquina virtual del nodo de gestión.

b. Cambie la RAM de la máquina virtual del nodo de gestión de 12 GB a 24 GB de RAM.

c. Encienda la máquina virtual del nodo de gestión.

- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Ha actualizado sus servicios de administración a al menos la versión 2.1.326. Las actualizaciones de control del cloud híbrido de NetApp no están disponibles en paquetes de servicio anteriores.

> Para obtener una lista de los servicios disponibles para cada versión del paquete de servicio, consulte "Notas de la versión de los servicios de gestión".

Pasos

1. Abra la interfaz de usuario de API DE REST en el nodo de gestión: `https://<ManagementNodeIP>/mnode`
2. Seleccione **autorizar** y complete lo siguiente:
   a. Introduzca el nombre de usuario y la contraseña del clúster.
   b. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.
   c. Seleccione **autorizar** para iniciar una sesión.
   d. Cierre la ventana.
3. Cargue y extraiga el paquete de servicio en el nodo de gestión mediante este comando: `PUT /services/upload`
4. Ponga en marcha los servicios de gestión en el nodo de gestión: `PUT /services/deploy`
5. Supervise el estado de la actualización: `GET /services/update/status`

   Una actualización correcta devuelve un resultado similar al siguiente ejemplo:

```
{
"current_version": "2.10.29",
"details": "Updated to version 2.17.52",
"status": "success"
}
```

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Actualice a la versión más reciente de HealthTools

Antes de iniciar una actualización del almacenamiento de Element desde 11.1 o una versión anterior, debe actualizar el paquete HealthTools. Actualizar HealthTools solo es

necesario si el nodo de gestión y el software Element que está ejecutando es 11.1 o anterior. HealthTools no es necesaria para "Realizar actualizaciones de Element mediante el control de cloud híbrido de NetApp".

> El software Element 12.3.2 es la versión final que se puede actualizar a mediante NetApp HealthTools. Si ejecuta el software Element 11.3 o posterior, debe usar NetApp Hybrid Cloud Control para actualizar el software Element. Es posible actualizar las versiones de Element 11.1 o anteriores mediante NetApp HealthTools.

Lo que necesitará

- Este sistema ejecuta el nodo de gestión 11.0, 11.1 o posterior.
- Ha actualizado sus servicios de administración a al menos la versión 2.1.326.

  Las actualizaciones de control de cloud híbrido de NetApp no están disponibles en versiones anteriores del paquete de servicio.

- Ha descargado la última versión de "HealthTools" y copió el archivo de instalación en el nodo de gestión.

  > Puede comprobar la versión instalada localmente de HealthTools ejecutando el `sfupdate-healthtools -v` comando.

- Para usar HealthTools con sitios oscuros, debe realizar estos pasos adicionales:
  - Descargar una "Archivo JSON" En el sitio de soporte de NetApp de un equipo que no es el nodo de gestión y cambie su nombre `metadata.json`.
  - Deje que el nodo de gestión esté activo y en funcionamiento en el sitio oscuro.

Acerca de esta tarea

Los comandos del conjunto HealthTools requieren privilegios escalados para ejecutarse. Cualquiera de los comandos de prefacio con `sudo` o bien, remita al usuario a privilegios de usuario raíz.

> La versión de HealthTools que utilice podría estar más actualizada que la entrada de muestra y la respuesta que se muestra a continuación.

Pasos

1. Ejecute el `sfupdate-healthtools <path to install file>` Comando para instalar el nuevo software HealthTools.

   Entrada de muestra:

   ```
   sfupdate-healthtools /tmp/solidfire-healthtools-2020.03.01.09.tgz
   ```

   Respuesta de ejemplo:

```
Checking key signature for file /tmp/solidfirehealthtools-
2020.03.01.09/components.tgz
installing command sfupdate-healthtools
Restarting on version 2020.03.01.09
sfupdate-healthtools /sf/bin/sfupdate-healthtools -r 2020.03.01.09
installing command sfupgradecheck
installing command sfinstall
installing command sfresetupgrade
```

2. Ejecute el `sfupdate-healthtools -v` comando para comprobar que la versión instalada se ha actualizado.

   Respuesta de ejemplo:

```
Currently installed version of HealthTools:
2020.03.01.09
```

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Ejecute comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento

Debe ejecutar comprobaciones del estado antes de actualizar el almacenamiento Element para garantizar que todos los nodos de almacenamiento del clúster estén listos para la siguiente actualización de almacenamiento de Element.

Lo que necesitará

- **Servicios de administración**: Ha actualizado el último paquete de servicios de administración (2.10.27 o posterior).

  > Debe actualizar al paquete de servicios de gestión más reciente antes de actualizar el software Element.

- **Nodo de gestión**:está ejecutando el nodo de administración 11.3 o posterior.
- **Software Element**: La versión del clúster ejecuta el software NetApp Element 11.3 o posterior.
- **Contrato de licencia para el usuario final (CLUF)**: A partir de los servicios de gestión 2.20.69, debe aceptar y guardar el CLUF antes de utilizar la IU o API de control de cloud híbrido de NetApp para ejecutar comprobaciones del estado del almacenamiento de Element:
  a. Abra la dirección IP del nodo de gestión en un navegador web:

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

b. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.

c. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.

d. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto para actualizaciones actuales y futuras** y seleccione **Guardar**.

Opciones de comprobación del estado

Puede realizar comprobaciones del estado con la interfaz de usuario de control de cloud híbrido de NetApp, la API de control de cloud híbrido de NetApp o la suite HealthTools:

- Utilice Cloud Control de NetApp híbrido para ejecutar comprobaciones del estado del almacenamiento Element antes de actualizar el almacenamiento (Método preferido)
- Utilice API para ejecutar comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento
- Utilice HealthTools para ejecutar comprobaciones del estado del almacenamiento Element antes de actualizar el almacenamiento

También puede obtener más información sobre las comprobaciones del estado del almacenamiento que realiza el servicio:

- Comprobaciones del estado del almacenamiento realizadas por el servicio

Utilice Cloud Control de NetApp híbrido para ejecutar comprobaciones del estado del almacenamiento Element antes de actualizar el almacenamiento

Con Hybrid Cloud Control de NetApp, puede comprobar que un clúster de almacenamiento está listo para actualizarse.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

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

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. En la página **actualizaciones**, seleccione la ficha **almacenamiento**.
5. Seleccione la comprobación del estado para el clúster que desea comprobar si está listo para la actualización.
6. En la página **Comprobación del estado del almacenamiento**, seleccione **Ejecutar comprobación del estado**.
7. Si hay problemas, haga lo siguiente:

   a. Vaya al artículo de la base de conocimientos específico indicado para cada problema o realice la

solución especificada.

b. Si se especifica un KB, complete el proceso descrito en el artículo de la base de conocimientos correspondiente.

c. Después de resolver los problemas del clúster, seleccione **Volver a ejecutar comprobación del estado**.

Una vez que la comprobación del estado se completa sin errores, el clúster de almacenamiento está listo para actualizar. Consulte actualización del nodo de almacenamiento "instrucciones" para continuar.

Utilice API para ejecutar comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento

Es posible utilizar API DE REST para verificar que un clúster de almacenamiento esté listo para actualizarse. La comprobación del estado verifica que no hay obstáculos para la actualización, como los nodos pendientes, los problemas de espacio en disco y los fallos del clúster.

Pasos

1. Busque el ID del clúster de almacenamiento:

   a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

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

   b. Seleccione **autorizar** y complete lo siguiente:

      i. Introduzca el nombre de usuario y la contraseña del clúster.

      ii. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.

      iii. Seleccione **autorizar** para iniciar una sesión.

      iv. Cierre la ventana de autorización.

   c. En la interfaz de usuario de API de REST, seleccione `GET /assets`.

   d. Seleccione **probar**.

   e. Seleccione **Ejecutar**.

   f. De la respuesta, copie la `"id"` desde la `"storage"` sección del clúster que pretende comprobar si está listo para la actualización.

   > No utilice la `"parent"` Valor de esta sección porque éste es el ID del nodo de administración, no el ID del clúster de almacenamiento.

```
"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. Ejecute las comprobaciones del estado en el clúster de almacenamiento:

   a. Abra la interfaz de usuario de API DE REST de almacenamiento en el nodo de gestión:

      ```
      https://<ManagementNodeIP>/storage/1/
      ```

   b. Seleccione **autorizar** y complete lo siguiente:

      i. Introduzca el nombre de usuario y la contraseña del clúster.

      ii. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.

      iii. Seleccione **autorizar** para iniciar una sesión.

      iv. Cierre la ventana de autorización.

   c. Seleccione **POST /Health-checks**.

   d. Seleccione **probar**.

   e. En el campo Parameter, introduzca el ID del clúster de almacenamiento obtenido en el paso 1.

      ```
      {
        "config": {},
        "storageId": "123a45b6-1a2b-12a3-1234-1a2b34c567d8"
      }
      ```

   f. Seleccione **Ejecutar** para ejecutar una comprobación del estado en el clúster de almacenamiento especificado.

      La respuesta debe indicar el estado como `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. Copie el `healthCheckID` eso es parte de la respuesta.

3. Compruebe los resultados de las comprobaciones de estado:

   a. Seleccione **GET /Health-checks/{healthCheckId}**.
   b. Seleccione **probar**.
   c. Introduzca el ID de comprobación del estado en el campo parámetro.
   d. Seleccione **Ejecutar**.
   e. Desplácese hasta la parte inferior del cuerpo de respuesta.

      Si todas las comprobaciones del estado se realizan correctamente, la devolución es similar al ejemplo siguiente:

```
"message": "All checks completed successfully.",
"percent": 100,
"timestamp": "2020-03-06T00:03:16.321621Z"
```

4. Si la `message` return indica que se han producido problemas con el estado del clúster, haga lo siguiente:

   a. Seleccione **GET /Health-checks/{healthCheckId}/log**
   b. Seleccione **probar**.
   c. Introduzca el ID de comprobación del estado en el campo parámetro.
   d. Seleccione **Ejecutar**.
   e. Revise cualquier error específico y obtenga los enlaces asociados del artículo de la base de conocimientos.
   f. Vaya al artículo de la base de conocimientos específico indicado para cada problema o realice la

solución especificada.

g. Si se especifica un KB, complete el proceso descrito en el artículo de la base de conocimientos correspondiente.

h. Después de resolver los problemas del clúster, ejecute **GET /health-checks/{healthCheckId}/log** de nuevo.

Utilice HealthTools para ejecutar comprobaciones del estado del almacenamiento Element antes de actualizar el almacenamiento

Puede verificar que el clúster de almacenamiento esté listo para actualizar mediante el `sfupgradecheck` comando. Este comando verifica información como nodos pendientes, espacio de disco y fallos de clúster.

Si el nodo de gestión se encuentra en un sitio oscuro sin conectividad externa, la comprobación de preparación para la actualización necesita el `metadata.json` archivo descargado durante "Actualizaciones de HealthTools" para funcionar correctamente.

Acerca de esta tarea

Este procedimiento describe cómo tratar las comprobaciones de actualización que generan uno de los siguientes resultados:

- Ejecutando el `sfupgradecheck` el comando se ejecuta correctamente. Su clúster está listo para la actualización.
- Comprobaciones dentro de `sfupgradecheck` la herramienta falla con un mensaje de error. Su clúster no está listo para la actualización y se requieren pasos adicionales.
- Se produce un error en la comprobación de actualización porque HealthTools no está actualizado.
- Se produce un error en la comprobación de la actualización porque el nodo de gestión está en un sitio oscuro.

Pasos

1. Ejecute el `sfupgradecheck` comando:

```
sfupgradecheck -u <cluster-user-name> MVIP
```

> Para las contraseñas que contienen caracteres especiales, añada una barra diagonal inversa (`\`) antes de cada carácter especial. Por ejemplo: `mypass!@1` debe introducirse como `mypass\!\@`.

Comando de entrada de muestra con salida de muestra en la que no aparecen errores y está listo para la actualización:

```
sfupgradecheck -u admin 10.117.78.244
```

```
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltOQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/
SolidFire-Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management
node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltYQAQ/mNodeconnecti
vity
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and
the
management node
Node ID: 1 Upload speed: 90063.90 KBs/sec
Node ID: 3 Upload speed: 106511.44 KBs/sec
Node ID: 2 Upload speed: 85038.75 KBs/sec
```

2. Si hay errores, se requieren acciones adicionales. Consulte las siguientes subsecciones para obtener detalles.

Su clúster no está listo para la actualización

Si ve un mensaje de error relacionado con una de las comprobaciones del estado, siga estos pasos:

1. Revise la `sfupgradecheck` mensaje de error.

   Respuesta de ejemplo:

```
The following tests failed:
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Severity: ERROR
Failed node IDs: 2
Remedy: Remove unneeded files from root drive
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/SolidFire-
Disk-space-error
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltOQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Passed node IDs: 1, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/SolidFire-
Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management
node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltYQAQ/mNodeconnectivi
ty
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and
the management node
Node ID: 1 Upload speed: 86518.82 KBs/sec
Node ID: 3 Upload speed: 84112.79 KBs/sec
Node ID: 2 Upload speed: 93498.94 KBs/sec
```

En este ejemplo, el nodo 1 tiene poco espacio en disco. Puede encontrar más información en la "base de conocimientos" (KB) artículo incluido en el mensaje de error.

HealthTools está desfasada

Si aparece un mensaje de error que indica que HealthTools no es la última versión, siga estas instrucciones:

1. Revise el mensaje de error y tenga en cuenta que la comprobación de actualización falla.

   Respuesta de ejemplo:

   ```
   sfupgradecheck failed: HealthTools is out of date:
   installed version: 2018.02.01.200
   latest version: 2020.03.01.09.
   The latest version of the HealthTools can be downloaded from:
   https://mysupport.netapp.com/NOW/cgi-bin/software/
   Or rerun with the -n option
   ```

2. Siga las instrucciones descritas en la respuesta.

Su nodo de gestión está en un sitio oscuro

1. Revise el mensaje y tenga en cuenta que la comprobación de actualización falla:

   Respuesta de ejemplo:

   ```
   sfupgradecheck failed: Unable to verify latest available version of
   healthtools.
   ```

2. Descargar una "Archivo JSON" En el sitio de soporte de NetApp de un equipo que no es el nodo de gestión y cambie su nombre `metadata.json`.
3. Ejecute el siguiente comando:

   ```
   sfupgradecheck -l --metadata=<path-to-metadata-json>
   ```

4. Para obtener información detallada, consulte adicional "Actualizaciones de HealthTools" información para sitios oscuros.
5. Compruebe que el conjunto HealthTools está actualizado ejecutando el siguiente comando:

   ```
   sfupgradecheck -u <cluster-user-name> -p <cluster-password> MVIP
   ```

Comprobaciones del estado del almacenamiento realizadas por el servicio

Las comprobaciones del estado del almacenamiento realizan las siguientes comprobaciones por clúster.

Nombre de comprobación	Nodo/clúster	Descripción
check_asinc_results	Clúster	Verifica que el número de resultados asincrónicos en la base de datos está por debajo de un número de umbral.
check_cluster_errantes	Clúster	Comprueba que no hay errores del clúster de bloqueo de actualizaciones (tal y como se define en el origen de elementos).
compruebe_upload_speed	Nodo	Mide la velocidad de carga entre el nodo de almacenamiento y el nodo de gestión.
comprobación_velocidad_conexión	Nodo	Verifica que los nodos tienen conectividad con el nodo de gestión que sirve paquetes de actualización y realiza una estimación de la velocidad de conexión.
comprobar_núcleos	Nodo	Comprueba si hay volcado de bloqueo del kernel y archivos principales en el nodo. Se produce un error en la comprobación de cualquier bloqueo en un período de tiempo reciente (umbral de 7 días).
check_root_disk_space	Nodo	Verifica que el sistema de archivos raíz tiene suficiente espacio libre para realizar una actualización.
check_var_log_disk_space	Nodo	Lo verifica `/var/log` el espacio libre cumple con algún umbral de porcentaje libre. Si no lo hace, la comprobación girará y purgará los registros más antiguos para caer por debajo del umbral. La comprobación falla si no se puede crear suficiente espacio libre.
check_pending_nodes	Clúster	Verifica que no hay nodos pendientes en el clúster.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Actualice el software Element

Para actualizar el software NetApp Element, puede usar la interfaz de usuario de control de cloud híbrido de NetApp, la API DE REST o la suite de herramientas HealthTools. Ciertas operaciones se eliminan durante una actualización del software Element, como

añadir y quitar nodos, añadir y quitar unidades, y comandos asociados con iniciadores, grupos de acceso de volúmenes y redes virtuales, entre otros.

Lo que necesitará

- **Privilegios de administrador**: Dispone de permisos de administrador del clúster de almacenamiento para realizar la actualización.
- **Ruta de actualización válida**: Ha comprobado la información de ruta de actualización para la versión de elemento a la que está actualizando y ha comprobado que la ruta de actualización es válida.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["Base de conocimientos de NetApp: Matriz de actualización para clústeres de almacenamiento que ejecutan software NetApp Element"^]
- **Sincronización de hora del sistema**: Se ha asegurado de que la hora del sistema en todos los nodos está sincronizada y que NTP está correctamente configurado para el clúster de almacenamiento y los nodos. Cada nodo debe configurarse con un servidor de nombres DNS en la interfaz de usuario web por nodo (`https://[IP address]:442`) sin fallos de clúster sin resolver relacionados con la desviación de tiempo.
- **Puertos del sistema**: Si utiliza NetApp Hybrid Cloud Control para actualizaciones, se ha asegurado de que los puertos necesarios están abiertos. Consulte "Puertos de red" si quiere más información.
- **Nodo de gestión**: Para la API e IU de control de cloud híbrido de NetApp, el nodo de gestión de su entorno ejecuta la versión 11.3.
- **Servicios de administración**: Ha actualizado su paquete de servicios de administración a la última versión.

> Debe actualizar al paquete de servicios de gestión más reciente antes de actualizar el software Element a la versión 12.3.x. Si actualiza el software Element a la versión 12.3.x, necesita servicios de gestión 2.14.60 o posterior para continuar.

- **Estado del clúster**: Ha comprobado que el clúster está listo para actualizarse. Consulte "Ejecute comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento".
- **BMC actualizado para nodos H610S**: Ha actualizado la versión de BMC para los nodos H610S. Consulte "notas de la versión e instrucciones de actualización".
- **Contrato de licencia para el usuario final (CLUF)**: A partir de los servicios de gestión 2.20.69, debe aceptar y guardar el CLUF antes de utilizar la IU o la API de control de cloud híbrido de NetApp para actualizar el software Element:
  a. Abra la dirección IP del nodo de gestión en un navegador web:

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

  b. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
  c. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
  d. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto para actualizaciones actuales y futuras** y seleccione **Guardar**.

Opciones de actualización

Elija una de las siguientes opciones de actualización del software Element:

- Utilice la IU de control de cloud híbrido de NetApp para actualizar el almacenamiento de Element
- Utilice la API de control de cloud híbrido de NetApp para actualizar el almacenamiento de Element
- Actualice el software Element en sitios conectados mediante HealthTools
- Actualice el software Element en sitios oscuros mediante HealthTools

Si va a actualizar un nodo serie H610S a Element 12.3.x y el nodo ejecuta una versión de Element anterior a 11.8, deberá realizar pasos de actualización adicionales (fase 2) para cada nodo de almacenamiento. Si ejecuta Element 11.8 o una versión posterior, no será necesario realizar los pasos de actualización adicionales (fase 2).

Utilice la IU de control de cloud híbrido de NetApp para actualizar el almacenamiento de Element

Con la interfaz de usuario de Cloud Control de NetApp, puede actualizar un clúster de almacenamiento.

Para obtener problemas potenciales al actualizar los clústeres de almacenamiento con NetApp Hybrid Cloud Control y sus soluciones alternativas, consulte "Artículo de base de conocimientos".

En el caso de las plataformas que no H610S, el proceso de actualización tarda aproximadamente 30 minutos por nodo.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

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

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. En la página **actualizaciones**, seleccione **almacenamiento**.

   La ficha **almacenamiento** muestra los clústeres de almacenamiento que forman parte de la instalación. Si el control de cloud híbrido de NetApp no permite acceder a un clúster, no se mostrará en la página **actualizaciones**.

5. Elija una de las siguientes opciones y realice el conjunto de pasos que se aplican a su clúster:

Opción	Pasos
Todos los clústeres que ejecutan Element 11.8 y versiones posteriores	a. Seleccione **examinar** para cargar el paquete de actualización que ha descargado. b. Espere a que finalice la carga. Una barra de progreso muestra el estado de la carga. La carga del archivo se perderá si se desplaza fuera de la ventana del explorador. Se muestra un mensaje en pantalla después de que el archivo se haya cargado y validado correctamente. La validación puede tardar varios minutos. Si se aleja de la ventana del explorador en este momento, se conserva la carga del archivo. c. Seleccione **Iniciar actualización**. **Estado de actualización** cambia durante la actualización para reflejar el estado del proceso. También cambia en respuesta a las acciones que realice, como la pausa de la actualización o si la actualización devuelve un error. Consulte Cambios de estado de actualización. Mientras la actualización está en curso, puede salir de la página y volver a ella más tarde para continuar supervisando el progreso. La página no actualiza el estado ni la versión actual de forma dinámica si la fila del clúster está contraída. La fila del clúster debe estar ampliada para actualizar la tabla, o bien se puede actualizar la página. Es posible descargar registros una vez completada la actualización.

Opción	Pasos
Actualice un clúster de H610S que ejecuta la versión de Element anterior a 11.8.	a. Seleccione la flecha desplegable junto al clúster que desea actualizar y seleccione una de las versiones de actualización disponibles. b. Seleccione **Iniciar actualización**. Una vez finalizada la actualización, la interfaz de usuario le solicita que realice la fase 2 del proceso. c. Complete los pasos adicionales necesarios (fase 2) en la "Artículo de base de conocimientos", Y reconocer en la interfaz de usuario que ha completado la fase 2. Es posible descargar registros una vez completada la actualización. Para obtener más información sobre los distintos cambios de estado de actualización, consulte Cambios de estado de actualización.

Cambios de estado de actualización

Estos son los diferentes estados que muestra la columna **Estado de actualización** de la interfaz de usuario antes, durante y después del proceso de actualización:

Estado de actualización	Descripción
Actualizado	El clúster se actualizó a la versión de Element más reciente disponible.
Versiones disponibles	Hay disponibles versiones más recientes del firmware de almacenamiento o Element para su actualización.
En curso	La actualización está en curso. Una barra de progreso muestra el estado de la actualización. Los mensajes en pantalla también muestran los errores a nivel de nodo y muestran el ID de nodo de cada nodo del clúster a medida que avanza la actualización. Es posible supervisar el estado de cada nodo mediante la interfaz de usuario de Element o el plugin de NetApp Element para la interfaz de usuario de vCenter Server.
Actualice la pausa	Puede optar por poner en pausa la actualización. En función del estado del proceso de actualización, la operación de pausa puede realizarse correctamente o fallará. Verá un aviso de la interfaz de usuario que le solicita que confirme la operación de pausa. Para garantizar que el clúster esté en un lugar seguro antes de pausar una actualización, la operación de actualización puede tardar hasta dos horas en detenerse por completo. Para reanudar la actualización, seleccione **Reanudar**.

Estado de actualización	Descripción
En pausa	Colocó en pausa la actualización. Seleccione **Reanudar** para reanudar el proceso.
Error	Se produjo un error durante la actualización. Puede descargar el registro de errores y enviarlo al soporte de NetApp. Después de resolver el error, puede volver a la página y seleccionar **Reanudar**. Al reanudar la actualización, la barra de progreso se retrocede durante unos minutos mientras el sistema ejecuta la comprobación del estado y comprueba el estado actual de la actualización.
Completo con seguimiento	Solo para actualizar los nodos H610S desde una versión de Element anterior a 11.8. Una vez completada la fase 1 del proceso de actualización, este estado le pedirá que realice la fase 2 de la actualización (consulte la "Artículo de base de conocimientos"). Después de completar la fase 2 y confirmar que la ha completado, el estado cambia a **hasta la fecha**.

Utilice la API de control de cloud híbrido de NetApp para actualizar el almacenamiento de Element

Puede utilizar las API para actualizar los nodos de almacenamiento de un clúster a la versión más reciente del software Element. Puede utilizar una herramienta de automatización que prefiera para ejecutar las API. El flujo de trabajo de API que se documenta aquí, utiliza la interfaz de usuario de API DE REST disponible en el nodo de gestión como ejemplo.

Pasos

1. Descargue el paquete de actualización de almacenamiento en un dispositivo al que el nodo de gestión puede acceder.

   Vaya al software Element "descargas" y descargue la imagen del nodo de almacenamiento más reciente.

2. Cargue el paquete de actualización de almacenamiento en el nodo de gestión:
   a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

      ```
      https://<ManagementNodeIP>/package-repository/1/
      ```

   b. Seleccione **autorizar** y complete lo siguiente:
      i. Introduzca el nombre de usuario y la contraseña del clúster.
      ii. Introduzca el ID de cliente as `mnode-client`.
      iii. Seleccione **autorizar** para iniciar una sesión.
      iv. Cierre la ventana de autorización.
   c. En la interfaz de usuario DE LA API DE REST, seleccione **POST /packages**.
   d. Seleccione **probar**.
   e. Seleccione **Browse** y seleccione el paquete de actualización.

f. Seleccione **Ejecutar** para iniciar la carga.

g. Desde la respuesta, copie y guarde el ID del paquete (`"id"`) para usar en un paso posterior.

3. Compruebe el estado de la carga.

a. En la interfaz de usuario de la API DE REST, seleccione **GET /packages/{id}/status**.

b. Seleccione **probar**.

c. Introduzca el ID de paquete que ha copiado en el paso anterior en **id**.

d. Seleccione **Ejecutar** para iniciar la solicitud de estado.

La respuesta indica `state` como `SUCCESS` cuando finalice.

4. Busque el ID del clúster de almacenamiento:

a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

b. Seleccione **autorizar** y complete lo siguiente:

i. Introduzca el nombre de usuario y la contraseña del clúster.

ii. Introduzca el ID de cliente as `mnode-client`.

iii. Seleccione **autorizar** para iniciar una sesión.

iv. Cierre la ventana de autorización.

c. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.

d. Seleccione **probar**.

e. Seleccione **Ejecutar**.

f. Desde la respuesta, copie el ID del activo de instalación (`"id"`).

g. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations/{id}**.

h. Seleccione **probar**.

i. Pegue el ID de activo de instalación en el campo **id**.

j. Seleccione **Ejecutar**.

k. En la respuesta, copie y guarde el ID del clúster de almacenamiento (`"id"`) del clúster que desee actualizar para usarlo en un paso posterior.

5. Ejecute la actualización del almacenamiento:

a. Abra la interfaz de usuario de API DE REST de almacenamiento en el nodo de gestión:

```
https://<ManagementNodeIP>/storage/1/
```

b. Seleccione **autorizar** y complete lo siguiente:

i. Introduzca el nombre de usuario y la contraseña del clúster.

ii. Introduzca el ID de cliente as `mnode-client`.

iii. Seleccione **autorizar** para iniciar una sesión.

iv. Cierre la ventana de autorización.

c. Seleccione **POST /upgrades**.

d. Seleccione **probar**.

e. Introduzca el ID del paquete de actualización en el campo parámetro.

f. Introduzca el ID del clúster de almacenamiento en el campo parámetro.

La carga útil debe tener un aspecto similar al siguiente ejemplo:

```
{
  "config": {},
  "packageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4",
  "storageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4"
}
```

g. Seleccione **Ejecutar** para iniciar la actualización.

La respuesta debe indicar el estado como `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. Copie el ID de actualización (`"upgradeId"`) eso es parte de la respuesta.

6. Verifique el progreso y los resultados de la actualización:

   a. Seleccione **GET /upgrades/{actualizeId}**.

   b. Seleccione **probar**.

   c. Introduzca el ID de actualización desde el paso anterior en **Actualizar Id**.

   d. Seleccione **Ejecutar**.

   e. Realice una de las siguientes acciones si existen problemas o requisitos especiales durante la actualización:

Opción	Pasos
Debe corregir los problemas de estado del clúster debido a `failedHealthChecks` mensaje en el cuerpo de respuesta.	i. Vaya al artículo de la base de conocimientos específico indicado para cada problema o realice la solución especificada. ii. Si se especifica un KB, complete el proceso descrito en el artículo de la base de conocimientos correspondiente. iii. Después de resolver los problemas del clúster, vuelva a autenticarse si es necesario y seleccione **PONER /actualizaciones/{actualizable Id}**. iv. Seleccione **probar**. v. Introduzca el ID de actualización desde el paso anterior en **Actualizar Id**. vi. Introduzca `"action":"resume"` en el cuerpo de la solicitud. `{ "action": "resume" }` vii. Seleccione **Ejecutar**.
Debe pausar la actualización porque la ventana de mantenimiento se está cerrando o por otro motivo.	i. Vuelva a autenticarse si es necesario y seleccione **PONER /actualizaciones/{actualizeId}**. ii. Seleccione **probar**. iii. Introduzca el ID de actualización desde el paso anterior en **Actualizar Id**. iv. Introduzca `"action":"pause"` en el cuerpo de la solicitud. `{ "action": "pause" }` v. Seleccione **Ejecutar**.

Opción	Pasos
Si va a actualizar un clúster de H610S que ejecuta una versión de Element anterior a 11.8, consulte el estado `finishedNeedsAck` en el cuerpo de respuesta. Debe realizar pasos de actualización adicionales (fase 2) para cada nodo de almacenamiento H610S.	i. Consulte Actualizar los nodos de almacenamiento H610S a Element 12.3.x (fase 2) y complete el proceso de cada nodo. ii. Vuelva a autenticarse si es necesario y seleccione **PONER /actualizaciones/{actualizeId}**. iii. Seleccione **probar**. iv. Introduzca el ID de actualización desde el paso anterior en **Actualizar Id**. v. Introduzca `"action":"acknowledge"` en el cuerpo de la solicitud. `{ "action": "acknowledge" }` vi. Seleccione **Ejecutar**.

f. Ejecute la API **GET /upgrades/{actualizable Id}** varias veces, según sea necesario, hasta que el proceso se complete.

   Durante la actualización, el `status` lo que indica `running` si no se encuentra ningún error. Cuando cada nodo se actualiza, el `step` el valor cambia a. `NodeFinished`.

La actualización se completó correctamente cuando el `percent` el valor es `100` y la `state` lo que indica `finished`.

¿Qué ocurre si se produce un error en una actualización mediante el control del cloud híbrido de NetApp

Si se produce un error en una unidad o un nodo durante una actualización, la interfaz de usuario de Element mostrará errores en el clúster. El proceso de actualización no pasa al siguiente nodo y espera a que se resuelvan los errores del clúster. La barra de progreso de la interfaz de usuario de muestra que la actualización está esperando a que se resuelvan los errores del clúster. En esta fase, la selección de **Pausa** en la interfaz de usuario no funcionará, ya que la actualización espera a que el clúster esté en buen estado. Deberá ponerse en contacto con el servicio de soporte de NetApp para que le ayude con la investigación de un fallo.

El control del cloud híbrido de NetApp tiene un periodo de espera predefinido de tres horas, durante el cual puede suceder una de las siguientes situaciones:

- Los fallos del clúster se resuelven en el plazo de tres horas y se reanuda la actualización. No es necesario realizar ninguna acción en este escenario.
- El problema persiste después de tres horas y el estado de actualización muestra **error** con un banner rojo. Puede reanudar la actualización seleccionando **Reanudar** después de resolver el problema.
- El soporte de NetApp ha determinado que se debe cancelar temporalmente el proceso de actualización

para que pueda tomar medidas correctivas antes del plazo de tres horas. El equipo de soporte utilizará la API para cancelar la actualización.

> Si se cancela la actualización del clúster mientras se actualiza un nodo, es posible que las unidades se eliminen sin dignidad del nodo. Si las unidades se quitan sin gracia, el soporte de NetApp deberá volver a añadir las unidades durante la actualización. Es posible que el nodo tarde más en realizar actualizaciones de firmware o actividades de sincronización posteriores a la actualización. Si el progreso de la actualización parece estancado, póngase en contacto con el soporte de NetApp para obtener ayuda.

Actualice el software Element en sitios conectados mediante HealthTools

Pasos

1. Descargue el paquete de actualización de almacenamiento; vaya al software Element "descargas" y descargue la imagen del nodo de almacenamiento más reciente en un dispositivo que no sea el nodo de gestión.

   > Es necesario contar con la versión más reciente de HealthTools para actualizar el software de almacenamiento Element.

2. Copie el archivo ISO en el nodo de gestión en una ubicación accesible como /tmp.

   Cuando cargue el archivo ISO, asegúrese de que el nombre del archivo no cambia; de lo contrario, se producirá un error en los pasos posteriores.

3. **Opcional**: Descargue el ISO del nodo de gestión a los nodos del clúster antes de la actualización.

   Con este paso se reduce el tiempo de actualización, ya que se preconfigurando la ISO en los nodos de almacenamiento y se ejecutan comprobaciones internas adicionales para garantizar que el clúster tenga un estado adecuado que actualizar. Si realiza esta operación, el clúster no pondrá en modo "actualización" ni restringirá ninguna de las operaciones del clúster.

   ```
   sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO> --stage
   ```

   > Omita la contraseña de la línea de comandos para permitir `sfinstall` para solicitar la información. Para las contraseñas que contienen caracteres especiales, añada una barra diagonal inversa (`\`) antes de cada carácter especial. Por ejemplo: `mypass!@1` debe introducirse como `mypass\!\@`.

   Ejemplo Consulte la siguiente entrada de ejemplo:

   ```
   sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfisodium-11.0.0.345.iso
   --stage
   ```

   El resultado de la muestra que `sfinstall` intenta verificar si una versión más reciente de `sfinstall` está disponible:

```
sfinstall 10.117.0.244 -u admin
/tmp/solidfire-rtfisodium-11.0.0.345.iso 2018-10-01 16:52:15:
Newer version of sfinstall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https:// mysupport.netapp.com/NOW/cgi-bin/software/
or rerun with --skip-version-check
```

Consulte el siguiente extracto de muestra de una operación previa a la etapa correcta:

Cuando finalice la estadificación, se mostrará el mensaje `Storage Node Upgrade Staging Successful` tras el evento de actualización.

```
flabv0004 ~ # sfinstall -u admin
10.117.0.87 solidfire-rtfi-sodium-patch3-11.3.0.14171.iso --stage
2019-04-03 13:19:58: sfinstall Release Version: 2019.01.01.49 Management
Node Platform:
Ember Revision: 26b042c3e15a Build date: 2019-03-12 18:45
2019-04-03 13:19:58: Checking connectivity to MVIP 10.117.0.87
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.86
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.87
...
2019-04-03 13:19:58: Successfully connected to cluster and all nodes
...
2019-04-03 13:20:00: Do you want to continue? ['Yes', 'No']: Yes
...
2019-04-03 13:20:55: Staging install pack on cluster nodes
2019-04-03 13:20:55: newVersion: 11.3.0.14171
2019-04-03 13:21:01: nodeToStage: nlabp2814, nlabp2815, nlabp2816,
nlabp2813
2019-04-03 13:21:02: Staging Node nlabp2815 mip=[10.117.0.87] nodeID=[2]
(1 of 4 nodes)
2019-04-03 13:21:02: Node Upgrade serving image at
http://10.117.0.204/rtfi/solidfire-rtfisodium-
patch3-11.3.0.14171/filesystem.squashfs
...
2019-04-03 13:25:40: Staging finished. Repeat the upgrade command
without the --stage option to start the upgrade.
```

Los ISO preconfigurados se eliminarán automáticamente una vez que finalice la actualización. Sin embargo, si la actualización no se ha iniciado y necesita ser reprogramada, los ISOs pueden ser despreconfigurados manualmente usando el comando:

```
sfinstall <MVIP> -u <cluster_username> --destage
```

Una vez iniciada la actualización, la opción de dejar de estar disponible.

4. Inicie la actualización con el `sfinstall` Comando y la ruta al archivo ISO:

   ```
   sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO>
   ```

   ejemplo

   Consulte el siguiente comando de entrada de ejemplo:

   ```
   sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-
   11.0.0.345.iso
   ```

   El resultado de la muestra que `sfinstall` intenta verificar si una versión más reciente de `sfinstall` está disponible:

   ```
   sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-
   11.0.0.345.iso
   2018-10-01 16:52:15: Newer version of sfinstall available.
   This version: 2018.09.01.130, latest version: 2018.06.05.901.
   The latest version of the HealthTools can be downloaded from:
   https://mysupport.netapp.com/NOW/cgi-bin/software/ or rerun with --skip
   -version-check
   ```

   Consulte el siguiente extracto de ejemplo de una actualización correcta. Los eventos de actualización pueden utilizarse para supervisar el progreso de la actualización.

   ```
   # sfinstall 10.117.0.161 -u admin solidfire-rtfi-sodium-11.0.0.761.iso
   2018-10-11 18:28
   Checking connectivity to MVIP 10.117.0.161
   Checking connectivity to node 10.117.0.23
   Checking connectivity to node 10.117.0.24
   ...
   Successfully connected to cluster and all nodes
   ################################################################
   You are about to start a new upgrade
   10.117.0.161
   10.3.0.161
   solidfire-rtfi-sodium-11.0.0.761.iso
   Nodes:
   10.117.0.23 nlabp1023 SF3010 10.3.0.161
   10.117.0.24 nlabp1025 SF3010 10.3.0.161
   10.117.0.26 nlabp1027 SF3010 10.3.0.161
   10.117.0.28 nlabp1028 SF3010 10.3.0.161
   ################################################################
   Do you want to continue? ['Yes', 'No']: yes
   ```

```
...
Watching for new network faults. Existing fault IDs are set([]).
Checking for legacy network interface names that need renaming
Upgrading from 10.3.0.161 to 11.0.0.761 upgrade method=rtfi
Waiting 300 seconds for cluster faults to clear
Waiting for caches to fall below threshold
...
Installing mip=[10.117.0.23] nodeID=[1] (1 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[7] away from mip[10.117.0.23] nodeID[1] ssid[11]
to new ssid[15]
Moving primary slice=[12] away from mip[10.117.0.23] nodeID[1] ssid[11]
to new ssid[15]
...
Installing mip=[10.117.114.24] nodeID=[2] (2 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[5] away from mip[10.117.114.24] nodeID[2] ssid[7]
to new ssid[11]
...
Install of solidfire-rtfi-sodium-11.0.0.761 complete.
Removing old software
No staged builds present on nodeID=[1]
No staged builds present on nodeID=[2]
...
Starting light cluster block service check
```

Si va a actualizar un nodo serie H610S a Element 12.3.x y el nodo ejecuta una versión de Element anterior a 11.8, deberá realizar pasos de actualización adicionales (fase 2) para cada nodo de almacenamiento. Si ejecuta Element 11.8 o una versión posterior, no será necesario realizar los pasos de actualización adicionales (fase 2).

Actualice el software Element en sitios oscuros mediante HealthTools

Puede utilizar el conjunto de herramientas HealthTools para actualizar el software NetApp Element en un sitio oscuro que no tiene conectividad externa.

Lo que necesitará

1. Vaya al software Element "descargas".
2. Seleccione la versión de software correcta y descargue la imagen del nodo de almacenamiento más reciente en un equipo que no es el nodo de gestión.

Es necesario contar con la versión más reciente de HealthTools para actualizar el software de almacenamiento Element.

3. Descargue esto "Archivo JSON" En el sitio de soporte de NetApp de un equipo que no es el nodo de gestión y cambie su nombre `metadata.json`.
4. Copie el archivo ISO en el nodo de gestión en una ubicación accesible, como `/tmp`.

Puede hacerlo utilizando, por ejemplo, SCP. Cuando cargue el archivo ISO, asegúrese de que el nombre del archivo no cambia; de lo contrario, se producirá un error en los pasos posteriores.

Pasos

1. Ejecute el `sfupdate-healthtools` comando:

```
sfupdate-healthtools <path-to-healthtools-package>
```

2. Compruebe la versión instalada:

```
sfupdate-healthtools -v
```

3. Compruebe la versión más reciente con respecto al archivo JSON de metadatos:

```
sfupdate-healthtools -l --metadata=<path-to-metadata-json>
```

4. Asegúrese de que el clúster esté listo:

```
sudo sfupgradecheck -u <cluster_username> -p <cluster_password> MVIP
--metadata=<path-to-metadata-json>
```

5. Ejecute el `sfinstall` Comando con la ruta al archivo ISO y al archivo JSON de metadatos:

```
sfinstall -u <cluster_username> <MVIP> <path-toinstall-file-ISO>
--metadata=<path-to-metadata-json-file>
```

Consulte el siguiente comando de entrada de ejemplo:

```
sfinstall -u admin 10.117.78.244 /tmp/solidfire-rtfi-11.3.0.345.iso
--metadata=/tmp/metadata.json
```

Opcional puede añadir el `--stage` marcar con la `sfinstall` comando para preconfigurar la actualización por adelantado.

Si va a actualizar un nodo serie H610S a Element 12.3.x y el nodo ejecuta una versión de Element anterior a 11.8, deberá realizar pasos de actualización adicionales (fase 2) para cada nodo de almacenamiento. Si ejecuta Element 11.8 o una versión posterior, no será necesario realizar los pasos de actualización adicionales (fase 2).

Qué ocurre si se produce un error en una actualización mediante HealthTools

Si la actualización del software falla, puede pausar la actualización.

Solo debe pausar una actualización con Ctrl-C. Esto permite que el sistema se limpie a sí mismo.

Cuando `sfinstall` espera a que se borren los fallos del clúster y si algún fallo provoca que se mantengan, `sfinstall` no continuará al siguiente nodo.

Pasos

1. Debe parar `sfinstall` Con Ctrl+C.
2. Póngase en contacto con el soporte de NetApp para recibir ayuda con la investigación de fallo.
3. Reanude la actualización con el mismo `sfinstall` comando.
4. Cuando una actualización se detiene con Ctrl+C, si la actualización se encuentra actualizando un nodo, elija una de las siguientes opciones:
   - **Wait**: Permita que el nodo que está actualizando finalice antes de restablecer las constantes del clúster.
   - **Continuar**: Continuar la actualización, que cancela la pausa.
   - **Anular**: Restablece las constantes del clúster y anula la actualización inmediatamente.

     Si se cancela la actualización del clúster mientras se actualiza un nodo, es posible que las unidades se eliminen sin dignidad del nodo. Si las unidades se quitan sin gracia, el soporte de NetApp deberá volver a añadir las unidades durante la actualización. Es posible que el nodo tarde más en realizar actualizaciones de firmware o actividades de sincronización posteriores a la actualización. Si el progreso de la actualización parece estancado, póngase en contacto con el soporte de NetApp para obtener ayuda.

Actualizar los nodos de almacenamiento H610S a Element 12.3.x (fase 2)

Si va a actualizar un nodo serie H610S a Element 12.3.x y el nodo ejecuta una versión de Element anterior a 11.8, el proceso de actualización implica dos fases.

La fase 1, que se realiza primero, sigue los mismos pasos que la actualización estándar al proceso de Element 12.3.x. Instala el software Element y todas las actualizaciones de firmware de la versión 5 de forma gradual a través del clúster, nodo por nodo. Debido a la carga útil del firmware, se estima que el proceso tardará aproximadamente de 1.5 a 2 horas por nodo H610S, incluido un único ciclo de arranque en frío al final de la actualización de cada nodo.

La fase 2 implica completar los pasos para realizar un apagado completo de un nodo y una desconexión de alimentación para cada nodo H610S que se describe en un requerido "KB". Se calcula que esta fase tarda aproximadamente una hora por nodo H610S.

Después de completar la fase 1, cuatro de las cinco actualizaciones de firmware se activan durante el arranque en frío en cada nodo H610S; sin embargo, el firmware del dispositivo lógico programable complejo (CPLD) requiere una desconexión de alimentación completa y reconexión para su instalación completa. La actualización de firmware de CPLD protege contra errores NVDIMM y eliminación de unidades de metadatos durante los reinicios o ciclos de apagado y encendido futuros. Se calcula que este restablecimiento de alimentación tarda aproximadamente una hora por nodo H610S. Requiere apagar el nodo, quitar los cables de alimentación o desconectar la alimentación a través de una PDU inteligente, esperar aproximadamente 3 minutos, y volver a conectar la alimentación.

Antes de empezar

- Completó la fase 1 del proceso de actualización de H610S y actualizó los nodos de almacenamiento mediante uno de los procedimientos de actualización de almacenamiento estándar de Element.

La fase 2 requiere personal in situ.

Pasos

1. (Fase 2) complete el proceso de restablecimiento de alimentación necesario para cada nodo H610S del clúster:

Si el clúster también tiene nodos que no son H610S, estos nodos que no son H610S están exentos de la fase 2 y no necesita que se apague o que tenga desconectada la alimentación.

1. Comuníquese con el soporte de NetApp para obtener ayuda y programar esta actualización.
2. Siga el procedimiento de actualización de fase 2 de este procedimiento "KB" Esto es necesario para completar una actualización para cada nodo H610S.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Actualizar el firmware de almacenamiento

A partir de Element 12.0 y la versión 2.14 de los servicios de gestión, puede realizar actualizaciones solo de firmware en los nodos de almacenamiento mediante la interfaz de usuario de Cloud Control de NetApp híbrido y la API DE REST. Este procedimiento no actualiza el software Element y permite actualizar el firmware de almacenamiento fuera de una versión de Element principal.

Lo que necesitará

- **Privilegios de administrador**: Dispone de permisos de administrador del clúster de almacenamiento para realizar la actualización.
- **Sincronización de hora del sistema**: Se ha asegurado de que la hora del sistema en todos los nodos está sincronizada y que NTP está correctamente configurado para el clúster de almacenamiento y los nodos. Cada nodo debe configurarse con un servidor de nombres DNS en la interfaz de usuario web por nodo (`https://[IP address]:442`) sin fallos de clúster sin resolver relacionados con la desviación de tiempo.
- **Puertos del sistema**: Si utiliza NetApp Hybrid Cloud Control para actualizaciones, se ha asegurado de

que los puertos necesarios están abiertos. Consulte "Puertos de red" si quiere más información.

- **Nodo de gestión**: Para la API e IU de control de cloud híbrido de NetApp, el nodo de gestión de su entorno ejecuta la versión 11.3.
- **Servicios de administración**: Ha actualizado su paquete de servicios de administración a la última versión.

> Para los nodos de almacenamiento H610S que ejecutan la versión 12.0 del software Element, debe aplicar D-patch SUST-909 antes de actualizar al paquete de firmware de almacenamiento 2.27. Póngase en contacto con el soporte de NetApp para obtener el parche en D antes de la actualización. Consulte "Notas de la versión del paquete de firmware de almacenamiento 2.27".

> Debe actualizar al paquete de servicios de gestión más reciente antes de actualizar el firmware en los nodos de almacenamiento. Si actualiza el software Element a la versión 12.2 o posterior, debe utilizar los servicios de gestión 2.14.60 o posterior para continuar.

- **Cluster Health**: Ha ejecutado comprobaciones de estado. Consulte "Ejecute comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento".
- **Contrato de licencia para el usuario final (CLUF)**: A partir de los servicios de administración 2.20.69, debe aceptar y guardar el CLUF antes de utilizar la UI o API de control de cloud híbrido de NetApp para actualizar el firmware de almacenamiento:
  a. Abra la dirección IP del nodo de gestión en un navegador web:

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

  b. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
  c. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
  d. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto para actualizaciones actuales y futuras** y seleccione **Guardar**.
- **BMC actualizado para nodos H610S**: Ha actualizado la versión de BMC para los nodos H610S. Consulte "notas de la versión e instrucciones de actualización".

> Para obtener una matriz completa de firmware y firmware de controlador para su hardware, consulte "Versiones de firmware de almacenamiento compatibles para los nodos de almacenamiento de SolidFire"

Opciones de actualización

Elija una de las siguientes opciones de actualización del firmware de almacenamiento:

- Utilice la interfaz de usuario de control del cloud híbrido de NetApp para actualizar el firmware de almacenamiento
- Utilice la API de control del cloud híbrido de NetApp para actualizar el firmware del almacenamiento

Utilice la interfaz de usuario de control del cloud híbrido de NetApp para actualizar el firmware de almacenamiento

Puede usar la interfaz de usuario de control de cloud híbrido de NetApp para actualizar el firmware de los

nodos de almacenamiento del clúster.

Lo que necesitará

- Si el nodo de gestión no está conectado a Internet, lo tiene "se ha descargado el bundle de firmware de almacenamiento".

Para obtener problemas potenciales al actualizar los clústeres de almacenamiento con NetApp Hybrid Cloud Control y sus soluciones alternativas, consulte "Artículo de base de conocimientos".

El proceso de actualización tarda aproximadamente 30 minutos por nodo de almacenamiento. Si actualiza un clúster de almacenamiento de Element a un firmware de almacenamiento posterior a la versión 2.76, los nodos de almacenamiento individuales solo se reiniciarán durante la actualización si se escribió el nuevo firmware en el nodo.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

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

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. En la página **actualizaciones**, seleccione **almacenamiento**.

La ficha **almacenamiento** muestra los clústeres de almacenamiento que forman parte de la instalación. Si el control de cloud híbrido de NetApp no permite acceder a un clúster, no se mostrará en la página **actualizaciones**. Si los clústeres ejecutan Element 12.0 o una versión posterior, se mostrará la versión actual del paquete de firmware indicado para estos clústeres. Si los nodos de un solo clúster tienen diferentes versiones de firmware en ellos o mientras la actualización progresa, verá **multiple** en la columna **Versión del paquete de firmware actual**. Puede seleccionar **Multiple** para desplazarse a la página **Nodes** para comparar las versiones de firmware. Si todos los clústeres ejecutan versiones de Element anteriores a 12.0, no se mostrará ninguna información sobre los números de versión del bundle de firmware.

Si el clúster está actualizado y/o no hay paquetes de actualización disponibles, no se muestran las pestañas **Element** y **sólo firmware**. Estas pestañas también no se muestran cuando hay una actualización en curso. Si se muestra la ficha **elemento**, pero no la ficha **sólo firmware**, no hay paquetes de firmware disponibles.

5. Seleccione la flecha desplegable junto al clúster que va a actualizar.
6. Seleccione **examinar** para cargar el paquete de actualización que ha descargado.
7. Espere a que finalice la carga. Una barra de progreso muestra el estado de la carga.

La carga del archivo se perderá si se desplaza fuera de la ventana del explorador.

Se muestra un mensaje en pantalla después de que el archivo se haya cargado y validado correctamente. La validación puede tardar varios minutos. Si se aleja de la ventana del explorador en este momento, se

conserva la carga del archivo.

8. Seleccione **sólo firmware** y seleccione una de las versiones de actualización disponibles.
9. Seleccione **Iniciar actualización**.

Estado de actualización cambia durante la actualización para reflejar el estado del proceso. También cambia en respuesta a las acciones que realice, como la pausa de la actualización o si la actualización devuelve un error. Consulte Cambios de estado de actualización.

Mientras la actualización está en curso, puede salir de la página y volver a ella más tarde para continuar supervisando el progreso. La página no actualiza el estado ni la versión actual de forma dinámica si la fila del clúster está contraída. La fila del clúster debe estar ampliada para actualizar la tabla, o bien se puede actualizar la página.

Es posible descargar registros una vez completada la actualización.

Cambios de estado de actualización

Estos son los diferentes estados que muestra la columna **Estado de actualización** de la interfaz de usuario antes, durante y después del proceso de actualización:

Estado de actualización	Descripción
Actualizado	El clúster se actualizó a la versión más reciente disponible de Element o el firmware se actualizó a la versión más reciente.
No se puede detectar	Este estado se muestra cuando la API del servicio de almacenamiento devuelve un estado de actualización que no está en la lista enumerada de posibles Estados de actualización.
Versiones disponibles	Hay disponibles versiones más recientes del firmware de almacenamiento o Element para su actualización.
En curso	La actualización está en curso. Una barra de progreso muestra el estado de la actualización. Los mensajes en pantalla también muestran los errores a nivel de nodo y muestran el ID de nodo de cada nodo del clúster a medida que avanza la actualización. Es posible supervisar el estado de cada nodo mediante la interfaz de usuario de Element o el plugin de NetApp Element para la interfaz de usuario de vCenter Server.

Estado de actualización	Descripción
Actualice la pausa	Puede optar por poner en pausa la actualización. En función del estado del proceso de actualización, la operación de pausa puede realizarse correctamente o fallará. Verá un aviso de la interfaz de usuario que le solicita que confirme la operación de pausa. Para garantizar que el clúster esté en un lugar seguro antes de pausar una actualización, la operación de actualización puede tardar hasta dos horas en detenerse por completo. Para reanudar la actualización, seleccione **Reanudar**.
En pausa	Colocó en pausa la actualización. Seleccione **Reanudar** para reanudar el proceso.
Error	Se produjo un error durante la actualización. Puede descargar el registro de errores y enviarlo al soporte de NetApp. Después de resolver el error, puede volver a la página y seleccionar **Reanudar**. Al reanudar la actualización, la barra de progreso se retrocede durante unos minutos mientras el sistema ejecuta la comprobación del estado y comprueba el estado actual de la actualización.

¿Qué ocurre si se produce un error en una actualización mediante el control del cloud híbrido de NetApp

Si se produce un error en una unidad o un nodo durante una actualización, la interfaz de usuario de Element mostrará errores en el clúster. El proceso de actualización no pasa al siguiente nodo y espera a que se resuelvan los errores del clúster. La barra de progreso de la interfaz de usuario de muestra que la actualización está esperando a que se resuelvan los errores del clúster. En esta fase, la selección de **Pausa** en la interfaz de usuario no funcionará, ya que la actualización espera a que el clúster esté en buen estado. Deberá ponerse en contacto con el servicio de soporte de NetApp para que le ayude con la investigación de un fallo.

El control del cloud híbrido de NetApp tiene un periodo de espera predefinido de tres horas, durante el cual puede suceder una de las siguientes situaciones:

- Los fallos del clúster se resuelven en el plazo de tres horas y se reanuda la actualización. No es necesario realizar ninguna acción en este escenario.
- El problema persiste después de tres horas y el estado de actualización muestra **error** con un banner rojo. Puede reanudar la actualización seleccionando **Reanudar** después de resolver el problema.
- El soporte de NetApp ha determinado que se debe cancelar temporalmente el proceso de actualización para que pueda tomar medidas correctivas antes del plazo de tres horas. El equipo de soporte utilizará la API para cancelar la actualización.

Si se cancela la actualización del clúster mientras se actualiza un nodo, es posible que las unidades se eliminen sin dignidad del nodo. Si las unidades se quitan sin gracia, el soporte de NetApp deberá volver a añadir las unidades durante la actualización. Es posible que el nodo tarde más en realizar actualizaciones de firmware o actividades de sincronización posteriores a la actualización. Si el progreso de la actualización parece estancado, póngase en contacto con el soporte de NetApp para obtener ayuda.

Utilice la API de control del cloud híbrido de NetApp para actualizar el firmware del almacenamiento

Puede utilizar las API para actualizar los nodos de almacenamiento de un clúster a la versión más reciente del software Element. Puede utilizar una herramienta de automatización que prefiera para ejecutar las API. El flujo de trabajo de API que se documenta aquí, utiliza la interfaz de usuario de API DE REST disponible en el nodo de gestión como ejemplo.

Pasos

1. Descargue el paquete de actualización de firmware de almacenamiento en un dispositivo al que se pueda acceder el nodo de gestión; vaya al software Element "descargas" y descargue la imagen del firmware de almacenamiento más reciente.
2. Cargue el paquete de actualización del firmware de almacenamiento en el nodo de gestión:
   a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

      ```
      https://<ManagementNodeIP>/package-repository/1/
      ```

   b. Seleccione **autorizar** y complete lo siguiente:
      i. Introduzca el nombre de usuario y la contraseña del clúster.
      ii. Introduzca el ID de cliente as `mnode-client`.
      iii. Seleccione **autorizar** para iniciar una sesión.
      iv. Cierre la ventana de autorización.
   c. En la interfaz de usuario DE LA API DE REST, seleccione **POST /packages**.
   d. Seleccione **probar**.
   e. Seleccione **Browse** y seleccione el paquete de actualización.
   f. Seleccione **Ejecutar** para iniciar la carga.
   g. Desde la respuesta, copie y guarde el ID del paquete (`"id"`) para usar en un paso posterior.
3. Compruebe el estado de la carga.
   a. En la interfaz de usuario de la API DE REST, seleccione **GET /packages/{id}/status**.
   b. Seleccione **probar**.
   c. Introduzca el ID del paquete de firmware que ha copiado en el paso anterior en **id**.
   d. Seleccione **Ejecutar** para iniciar la solicitud de estado.

      La respuesta indica `state` como `SUCCESS` cuando finalice.
4. Busque el ID de activo de instalación:
   a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Seleccione **autorizar** y complete lo siguiente:
      i. Introduzca el nombre de usuario y la contraseña del clúster.
      ii. Introduzca el ID de cliente as `mnode-client`.

iii. Seleccione **autorizar** para iniciar una sesión.

iv. Cierre la ventana de autorización.

c. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.

d. Seleccione **probar**.

e. Seleccione **Ejecutar**.

f. Desde la respuesta, copie el ID del activo de instalación (`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. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations/{id}**.

h. Seleccione **probar**.

i. Pegue el ID de activo de instalación en el campo **id**.

j. Seleccione **Ejecutar**.

k. En la respuesta, copie y guarde el ID del clúster de almacenamiento (`"id"`) del clúster que desee actualizar para usarlo en un paso posterior.

```
"storage": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterUuid": "a1bd1111-4f1e-46zz-ab6f-0a1111b1111x",
        "id": "a1bd1111-4f1e-46zz-ab6f-a1a1a111b012",
```

5. Ejecute la actualización del firmware de almacenamiento:

a. Abra la interfaz de usuario de API DE REST de almacenamiento en el nodo de gestión:

```
https://<ManagementNodeIP>/storage/1/
```

b. Seleccione **autorizar** y complete lo siguiente:

i. Introduzca el nombre de usuario y la contraseña del clúster.

ii. Introduzca el ID de cliente as `mnode-client`.

iii. Seleccione **autorizar** para iniciar una sesión.

iv. Cierre la ventana.

c. Seleccione **POST /upgrades**.

d. Seleccione **probar**.

e. Introduzca el ID del paquete de actualización en el campo parámetro.

f. Introduzca el ID del clúster de almacenamiento en el campo parámetro.

g. Seleccione **Ejecutar** para iniciar la actualización.

La respuesta debe indicar el estado como `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. Copie el ID de actualización (`"upgradeId"`) eso es parte de la respuesta.

6. Verifique el progreso y los resultados de la actualización:

   a. Seleccione **GET /upgrades/{actualizeId}**.

   b. Seleccione **probar**.

   c. Introduzca el ID de actualización desde el paso anterior en **Actualizar Id**.

   d. Seleccione **Ejecutar**.

   e. Realice una de las siguientes acciones si existen problemas o requisitos especiales durante la actualización:

Opción	Pasos
Debe corregir los problemas de estado del clúster debido a `failedHealthChecks` mensaje en el cuerpo de respuesta.	i. Vaya al artículo de la base de conocimientos específico indicado para cada problema o realice la solución especificada. ii. Si se especifica un KB, complete el proceso descrito en el artículo de la base de conocimientos correspondiente. iii. Después de resolver los problemas del clúster, vuelva a autenticarse si es necesario y seleccione **PONER /actualizaciones/{actualizable Id}**. iv. Seleccione **probar**. v. Introduzca el ID de actualización desde el paso anterior en **Actualizar Id**. vi. Introduzca `"action":"resume"` en el cuerpo de la solicitud. `{ "action": "resume" }` vii. Seleccione **Ejecutar**.
Debe pausar la actualización porque la ventana de mantenimiento se está cerrando o por otro motivo.	i. Vuelva a autenticarse si es necesario y seleccione **PONER /actualizaciones/{actualizeId}**. ii. Seleccione **probar**. iii. Introduzca el ID de actualización desde el paso anterior en **Actualizar Id**. iv. Introduzca `"action":"pause"` en el cuerpo de la solicitud. `{ "action": "pause" }` v. Seleccione **Ejecutar**.

f. Ejecute la API **GET /upgrades/{actualizable Id}** varias veces, según sea necesario, hasta que el proceso se complete.

   Durante la actualización, el `status` lo que indica `running` si no se encuentra ningún error. Cuando cada nodo se actualiza, el `step` el valor cambia a. `NodeFinished`.

La actualización se completó correctamente cuando el `percent` el valor es `100` y la `state` lo que indica `finished`.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Actualice un nodo de gestión

Puede actualizar el nodo de gestión a la versión 12.3.x del nodo de gestión desde la versión 11.0 o posterior.

Ya no se necesita actualizar el sistema operativo del nodo de gestión para actualizar el software Element en el clúster de almacenamiento. Si el nodo de gestión es la versión 11.3 o posterior, solo tiene que actualizar los servicios de gestión a la versión más reciente para realizar actualizaciones de Element mediante el control de cloud híbrido de NetApp. Siga el procedimiento de actualización del nodo de gestión para su escenario si desea actualizar el sistema operativo del nodo de gestión por otros motivos, como la corrección de seguridad.

El plugin de vCenter versión 4.4 o posterior requiere un nodo de gestión 11.3 o posterior que se cree con una arquitectura modular y proporcione servicios individuales.

Opciones de actualización

Elija una de las siguientes opciones de actualización del nodo de gestión:

- El nodo de gestión 12.3.2 contiene una mitigación de seguridad para los clústeres de almacenamiento con la función Virtual Volumes (VVol) habilitada. Si el clúster de almacenamiento ya está en Element 12.3 y la función VVol está habilitada, debe actualizarse a 12.3.2.
- No hay cambios de funcionalidad adicionales ni correcciones de errores en el nodo de gestión 12.3.1. Si ya ejecuta el nodo de gestión 12.3, no es necesario actualizarlo a 12.3.1.

- Si va a actualizar desde el nodo de gestión 12.2:Actualice un nodo de gestión a la versión 12.3.x desde 12.2
- Si va a actualizar desde el nodo de gestión 12.0:Actualice un nodo de gestión a la versión 12.3.x desde 12.0
- Si va a actualizar desde el nodo de gestión 11.3, 11.5, 11.7 o 11.8:Actualice un nodo de gestión a la versión 12.3.x de 11.3 a 11.8
- Si va a actualizar desde el nodo de gestión 11.0 o 11.1:Actualice un nodo de gestión a la versión 12.3.x desde 11.1 o 11.0
- Si va a actualizar desde un nodo de gestión versión 10.x:Migrar desde el nodo de gestión versión 10.x a 11.x.

Elija la siguiente opción si ha * actualizado secuencialmente* (1) la versión de los servicios de administración y (2) la versión de almacenamiento de Element y desea **mantener** su nodo de gestión existente:

Si no actualiza secuencialmente los servicios de gestión seguidos por el almacenamiento de Element, no se puede volver a configurar la autenticación mediante este procedimiento. Siga en su lugar el procedimiento de actualización adecuado.

- Si va a mantener el nodo de gestión existente:Volver a configurar la autenticación mediante la API DE REST del nodo de gestión

Actualice un nodo de gestión a la versión 12.3.x desde 12.2

Puede realizar una actualización in situ del nodo de gestión de la versión 12.2 a la versión 12.3.x sin necesidad de aprovisionar una nueva máquina virtual del nodo de gestión.

> El nodo de gestión Element 12.3.x es una actualización opcional. No es necesario para las puestas en marcha existentes.

Lo que necesitará

- La RAM de la máquina virtual del nodo de gestión es 24 GB.
- El nodo de gestión que pretende actualizar es la versión 12.0 y utiliza redes IPv4. La versión 12.3.x del nodo de gestión no es compatible con IPv6.

> Para comprobar la versión del nodo de gestión, inicie sesión en su nodo de gestión y vea el número de versión de Element en el banner de inicio de sesión.

- Ha actualizado el paquete de servicios de gestión a la versión más reciente con Hybrid Cloud Control de NetApp. Puede acceder a NetApp Hybrid Cloud Control desde la siguiente IP: `https://<ManagementNodeIP>`
- Si actualiza el nodo de gestión a la versión 12.3.x, necesita servicios de gestión 2.14.60 o una versión posterior para continuar.
- Ha configurado un adaptador de red adicional (si es necesario) utilizando las instrucciones para "Configuración de una NIC de almacenamiento adicional".

> Es posible que los volúmenes persistentes requieran un adaptador de red adicional si eth0 no se puede enrutar a la SVIP. Configure un nuevo adaptador de red en la red de almacenamiento iSCSI para permitir la configuración de volúmenes persistentes.

- Los nodos de almacenamiento ejecutan Element 11.3 o una versión posterior.

Pasos

1. Inicie sesión en la máquina virtual del nodo de gestión mediante SSH o el acceso de consola.
2. Descargue el "Nodo de gestión ISO" Para el software Element, desde el sitio de soporte de NetApp hasta la máquina virtual del nodo de gestión.

   > El nombre de la ISO es similar a. `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Compruebe la integridad de la descarga. Para ello, ejecute md5sum en el archivo descargado y compare el resultado con lo que está disponible en el sitio de soporte de NetApp para el software Element, como en el siguiente ejemplo:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

4. Monte la imagen ISO del nodo de gestión y copie el contenido en el sistema de archivos mediante los siguientes comandos:

```
sudo mkdir -p /upgrade
```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso>
/mnt
```

```
sudo cp -r /mnt/* /upgrade
```

5. Cambie al directorio inicial y desmonte el archivo ISO de `/mnt`:

```
sudo umount /mnt
```

6. Elimine el ISO para conservar espacio en el nodo de gestión:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

7. En el nodo de gestión que desea actualizar, ejecute el siguiente comando para actualizar la versión del sistema operativo del nodo de gestión. El script conserva todos los archivos de configuración necesarios después de la actualización, como el recopilador Active IQ y la configuración de proxy.

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

   El nodo de gestión se reinicia con un sistema operativo nuevo una vez que finaliza el proceso de actualización.

   > Después de ejecutar el comando sudo descrito en este paso, se mata la sesión SSH. Se requiere acceso a la consola para una supervisión continua. Si no tiene acceso a la consola al realizar la actualización, vuelva a intentar el inicio de sesión SSH y verifique la conectividad después de 15 a 30 minutos. Una vez que inicia sesión, puede confirmar la nueva versión del sistema operativo en el banner SSH que indica que la actualización se ha realizado correctamente.

8. En el nodo de gestión, ejecute el `redeploy-mnode` secuencia de comandos para mantener los valores de configuración anteriores de los servicios de administración:

   > El script conserva la configuración anterior de servicios de gestión, incluida la configuración del servicio de recopilador Active IQ, controladoras (vCenter) o proxy, en función de la configuración.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

Si había deshabilitado anteriormente la funcionalidad SSH en el nodo de gestión, debe hacerlo "Vuelva a deshabilitar SSH" en el nodo de gestión recuperado. Funcionalidad SSH que proporciona "Acceso a la sesión del túnel de soporte remoto (RST) de NetApp Support" está habilitado en el nodo de gestión de manera predeterminada.

Actualice un nodo de gestión a la versión 12.3.x desde 12.0

Puede realizar una actualización in situ del nodo de gestión de la versión 12.0 a la versión 12.3.x sin necesidad de aprovisionar una nueva máquina virtual del nodo de gestión.

El nodo de gestión Element 12.3.x es una actualización opcional. No es necesario para las puestas en marcha existentes.

Lo que necesitará

- El nodo de gestión que pretende actualizar es la versión 12.0 y utiliza redes IPv4. La versión 12.3.x del nodo de gestión no es compatible con IPv6.

  Para comprobar la versión del nodo de gestión, inicie sesión en su nodo de gestión y vea el número de versión de Element en el banner de inicio de sesión.

- Ha actualizado el paquete de servicios de gestión a la versión más reciente con Hybrid Cloud Control de NetApp. Puede acceder a NetApp Hybrid Cloud Control desde la siguiente IP: `https://<ManagementNodeIP>`
- Si actualiza el nodo de gestión a la versión 12.3.x, necesita servicios de gestión 2.14.60 o una versión posterior para continuar.
- Ha configurado un adaptador de red adicional (si es necesario) utilizando las instrucciones para "Configuración de una NIC de almacenamiento adicional".

  Es posible que los volúmenes persistentes requieran un adaptador de red adicional si eth0 no se puede enrutar a la SVIP. Configure un nuevo adaptador de red en la red de almacenamiento iSCSI para permitir la configuración de volúmenes persistentes.

- Los nodos de almacenamiento ejecutan Element 11.3 o una versión posterior.

Pasos

1. Configure la RAM de la máquina virtual del nodo de gestión:
   a. Apague la máquina virtual del nodo de gestión.
   b. Cambie la RAM de la máquina virtual del nodo de gestión de 12 GB a 24 GB de RAM.
   c. Encienda la máquina virtual del nodo de gestión.
2. Inicie sesión en la máquina virtual del nodo de gestión mediante SSH o el acceso de consola.
3. Descargue el "Nodo de gestión ISO" Para el software Element, desde el sitio de soporte de NetApp hasta la máquina virtual del nodo de gestión.

El nombre de la ISO es similar a. `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Compruebe la integridad de la descarga. Para ello, ejecute md5sum en el archivo descargado y compare el resultado con lo que está disponible en el sitio de soporte de NetApp para el software Element, como en el siguiente ejemplo:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

5. Monte la imagen ISO del nodo de gestión y copie el contenido en el sistema de archivos mediante los siguientes comandos:

   ```
   sudo mkdir -p /upgrade
   ```

   ```
   sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso> /mnt
   ```

   ```
   sudo cp -r /mnt/* /upgrade
   ```

6. Cambie al directorio inicial y desmonte el archivo ISO de `/mnt`:

   ```
   sudo umount /mnt
   ```

7. Elimine el ISO para conservar espacio en el nodo de gestión:

   ```
   sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

8. En el nodo de gestión que desea actualizar, ejecute el siguiente comando para actualizar la versión del sistema operativo del nodo de gestión. El script conserva todos los archivos de configuración necesarios después de la actualización, como el recopilador Active IQ y la configuración de proxy.

   ```
   sudo /sf/rtfi/bin/sfrtfi_inplace file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
   ```

   El nodo de gestión se reinicia con un sistema operativo nuevo una vez que finaliza el proceso de actualización.

Después de ejecutar el comando sudo descrito en este paso, se mata la sesión SSH. Se requiere acceso a la consola para una supervisión continua. Si no tiene acceso a la consola al realizar la actualización, vuelva a intentar el inicio de sesión SSH y verifique la conectividad después de 15 a 30 minutos. Una vez que inicia sesión, puede confirmar la nueva versión del sistema operativo en el banner SSH que indica que la actualización se ha realizado correctamente.

9. En el nodo de gestión, ejecute el `redeploy-mnode` secuencia de comandos para mantener los valores de configuración anteriores de los servicios de administración:

   El script conserva la configuración anterior de servicios de gestión, incluida la configuración del servicio de recopilador Active IQ, controladoras (vCenter) o proxy, en función de la configuración.

   ```
   sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
   ```

   Funcionalidad SSH que proporciona "Acceso a la sesión del túnel de soporte remoto (RST) de NetApp Support" está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 y posteriores. Si ya había habilitado la funcionalidad SSH en el nodo de gestión, es posible que deba hacerlo "Vuelva a deshabilitar SSH" en el nodo de gestión actualizado.

Actualice un nodo de gestión a la versión 12.3.x de 11.3 a 11.8

Puede realizar una actualización in situ del nodo de gestión desde la versión 11.3, 11.5, 11.7 o 11.8 a la versión 12.3.x sin necesidad de aprovisionar una nueva máquina virtual del nodo de gestión.

El nodo de gestión Element 12.3.x es una actualización opcional. No es necesario para las puestas en marcha existentes.

Lo que necesitará

- El nodo de gestión que pretende actualizar es la versión 11.3, 11.5, 11.7 o 11.8 y utiliza redes IPv4. La versión 12.3.x del nodo de gestión no es compatible con IPv6.

  Para comprobar la versión del nodo de gestión, inicie sesión en su nodo de gestión y vea el número de versión de Element en el banner de inicio de sesión.

- Ha actualizado el paquete de servicios de gestión a la versión más reciente con Hybrid Cloud Control de NetApp. Puede acceder a NetApp Hybrid Cloud Control desde la siguiente IP: `https://<ManagementNodeIP>`
- Si actualiza el nodo de gestión a la versión 12.3.x, necesita servicios de gestión 2.14.60 o una versión posterior para continuar.
- Ha configurado un adaptador de red adicional (si es necesario) utilizando las instrucciones para "Configuración de una NIC de almacenamiento adicional".

Es posible que los volúmenes persistentes requieran un adaptador de red adicional si eth0 no se puede enrutar a la SVIP. Configure un nuevo adaptador de red en la red de almacenamiento iSCSI para permitir la configuración de volúmenes persistentes.

- Los nodos de almacenamiento ejecutan Element 11.3 o una versión posterior.

Pasos

1. Configure la RAM de la máquina virtual del nodo de gestión:
   a. Apague la máquina virtual del nodo de gestión.
   b. Cambie la RAM de la máquina virtual del nodo de gestión de 12 GB a 24 GB de RAM.
   c. Encienda la máquina virtual del nodo de gestión.
2. Inicie sesión en la máquina virtual del nodo de gestión mediante SSH o el acceso de consola.
3. Descargue el "Nodo de gestión ISO" Para el software Element, desde el sitio de soporte de NetApp hasta la máquina virtual del nodo de gestión.

   El nombre de la ISO es similar a. `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Compruebe la integridad de la descarga. Para ello, ejecute md5sum en el archivo descargado y compare el resultado con lo que está disponible en el sitio de soporte de NetApp para el software Element, como en el siguiente ejemplo:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

5. Monte la imagen ISO del nodo de gestión y copie el contenido en el sistema de archivos mediante los siguientes comandos:

   ```
   sudo mkdir -p /upgrade
   ```

   ```
   sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso> /mnt
   ```

   ```
   sudo cp -r /mnt/* /upgrade
   ```

6. Cambie al directorio inicial y desmonte el archivo ISO de `/mnt`:

   ```
   sudo umount /mnt
   ```

7. Elimine el ISO para conservar espacio en el nodo de gestión:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. En el nodo de gestión 11.3, 11.5, 11.7 o 11.8, ejecute el siguiente comando para actualizar la versión del sistema operativo del nodo de gestión. El script conserva todos los archivos de configuración necesarios después de la actualización, como el recopilador Active IQ y la configuración de proxy.

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

El nodo de gestión se reinicia con un sistema operativo nuevo una vez que finaliza el proceso de actualización.

> Después de ejecutar el comando sudo descrito en este paso, se mata la sesión SSH. Se requiere acceso a la consola para una supervisión continua. Si no tiene acceso a la consola al realizar la actualización, vuelva a intentar el inicio de sesión SSH y verifique la conectividad después de 15 a 30 minutos. Una vez que inicia sesión, puede confirmar la nueva versión del sistema operativo en el banner SSH que indica que la actualización se ha realizado correctamente.

9. En el nodo de gestión, ejecute el `redeploy-mnode` secuencia de comandos para mantener los valores de configuración anteriores de los servicios de administración:

> El script conserva la configuración anterior de servicios de gestión, incluida la configuración del servicio de recopilador Active IQ, controladoras (vCenter) o proxy, en función de la configuración.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

> Funcionalidad SSH que proporciona "Acceso a la sesión del túnel de soporte remoto (RST) de NetApp Support" está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 y posteriores. Si ya había habilitado la funcionalidad SSH en el nodo de gestión, es posible que deba hacerlo "Vuelva a deshabilitar SSH" en el nodo de gestión actualizado.

Actualice un nodo de gestión a la versión 12.3.x desde 11.1 o 11.0

Puede realizar una actualización in situ del nodo de gestión desde 11.0 o 11.1 a la versión 12.3.x sin necesidad de aprovisionar una nueva máquina virtual del nodo de gestión.

Lo que necesitará

- Los nodos de almacenamiento ejecutan Element 11.3 o una versión posterior.

> Utilice las últimas HealthTools para actualizar el software Element.

- El nodo de gestión que pretende actualizar es la versión 11.0 o 11.1 y utiliza redes IPv4. La versión 12.3.x

del nodo de gestión no es compatible con IPv6.

> Para comprobar la versión del nodo de gestión, inicie sesión en su nodo de gestión y vea el número de versión de Element en el banner de inicio de sesión.

- Para el nodo de gestión 11.0, la memoria de la máquina virtual se debe aumentar manualmente a 12 GB.
- Se configuró un adaptador de red adicional (si es necesario) mediante las instrucciones para configurar un NIC de almacenamiento (eth1) en la guía del usuario del nodo de gestión del producto.

> Es posible que los volúmenes persistentes requieran un adaptador de red adicional si eth0 no se puede enrutar a la SVIP. Configure un nuevo adaptador de red en la red de almacenamiento iSCSI para permitir la configuración de volúmenes persistentes.

Pasos

1. Configure la RAM de la máquina virtual del nodo de gestión:
   a. Apague la máquina virtual del nodo de gestión.
   b. Cambie la RAM de la máquina virtual del nodo de gestión de 12 GB a 24 GB de RAM.
   c. Encienda la máquina virtual del nodo de gestión.
2. Inicie sesión en la máquina virtual del nodo de gestión mediante SSH o el acceso de consola.
3. Descargue el "Nodo de gestión ISO" Para el software Element, desde el sitio de soporte de NetApp hasta la máquina virtual del nodo de gestión.

   > El nombre de la ISO es similar a. `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Compruebe la integridad de la descarga. Para ello, ejecute md5sum en el archivo descargado y compare el resultado con lo que está disponible en el sitio de soporte de NetApp para el software Element, como en el siguiente ejemplo:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

5. Monte la imagen ISO del nodo de gestión y copie el contenido en el sistema de archivos mediante los siguientes comandos:

   ```
   sudo mkdir -p /upgrade
   ```

   ```
   sudo mount solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso /mnt
   ```

   ```
   sudo cp -r /mnt/* /upgrade
   ```

6. Cambie al directorio principal y desmonte el archivo ISO de /mnt:

```
sudo umount /mnt
```

7. Elimine el ISO para conservar espacio en el nodo de gestión:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. Ejecute uno de los siguientes scripts con opciones para actualizar la versión de sistema operativo del nodo de gestión. Ejecute sólo el script que sea apropiado para su versión. Cada script conserva todos los archivos de configuración necesarios después de la actualización, como el recopilador Active IQ y la configuración de proxy.

   a. En un nodo de gestión de 11.1 (11.1.0.73), ejecute el siguiente comando:

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.3.2288
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc
/sf/packages/nma"
```

   b. En un nodo de gestión de 11.1 (11.1.0.72), ejecute el siguiente comando:

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.1.2281
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc
/sf/packages/nma"
```

   c. En un nodo de gestión de 11.0 (11.0.0.781), ejecute el siguiente comando:

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.0.2253
/sf/packages/solidfire-nma-1.4.8/conf /sf/packages/sioc
/sf/packages/nma"
```

   El nodo de gestión se reinicia con un sistema operativo nuevo una vez que finaliza el proceso de actualización.

Después de ejecutar el comando sudo descrito en este paso, se mata la sesión SSH. Se requiere acceso a la consola para una supervisión continua. Si no tiene acceso a la consola al realizar la actualización, vuelva a intentar el inicio de sesión SSH y verifique la conectividad después de 15 a 30 minutos. Una vez que inicia sesión, puede confirmar la nueva versión del sistema operativo en el banner SSH que indica que la actualización se ha realizado correctamente.

9. En el nodo de gestión 12.3.x, ejecute el `upgrade-mnode` script para conservar los valores de configuración anteriores.

   Si va a migrar desde un nodo de gestión 11.0 o 11.1, el script copia el recopilador Active IQ al nuevo formato de configuración.

   a. Para un único clúster de almacenamiento gestionado por un nodo de gestión existente 11.0 o 11.1 con volúmenes persistentes:

   ```
   sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true -
   persistent volume> -pva <persistent volume account name - storage
   volume account>
   ```

   b. Para un único clúster de almacenamiento gestionado por un nodo de gestión existente 11.0 o 11.1 sin volúmenes persistentes:

   ```
   sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user>
   ```

   c. Para varios clústeres de almacenamiento gestionados por un nodo de gestión existente 11.0 o 11.1 con volúmenes persistentes:

   ```
   sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true -
   persistent volume> -pva <persistent volume account name - storage
   volume account> -pvm <persistent volumes mvip>
   ```

   d. En el caso de varios clústeres de almacenamiento gestionados por un nodo de gestión existente 11.0 o 11.1 sin volúmenes persistentes (el `-pvm` Indicador es proporcionar una de las direcciones MVIP del clúster):

   ```
   sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pvm <mvip for
   persistent volumes>
   ```

10. (Para todas las instalaciones de almacenamiento all-flash SolidFire de NetApp con el plugin de NetApp Element para vCenter Server) Actualice el plugin de vCenter en el nodo de gestión 12.3.x siguiendo los pasos del "Actualice el plugin de Element para vCenter Server" tema.
11. Busque el ID de activo para su instalación con la API del nodo de gestión:
    a. Desde un explorador, inicie sesión en la API DE REST del nodo de gestión:

i. Vaya a la MVIP de almacenamiento e inicie sesión. Esta acción hace que se acepte el certificado para el siguiente paso.

b. Abra la interfaz de usuario de la API DE REST del servicio de inventario en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

c. Seleccione **autorizar** y complete lo siguiente:

i. Introduzca el nombre de usuario y la contraseña del clúster.

ii. Introduzca el ID de cliente as `mnode-client`.

iii. Seleccione **autorizar** para iniciar una sesión.

iv. Cierre la ventana.

d. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.

e. Seleccione **probar**.

f. Seleccione **Ejecutar**.

g. Del cuerpo de respuesta del código 200, copie el `id` para la instalación.

Su instalación tiene una configuración de activos base que se creó durante la instalación o la actualización.

Migrar desde el nodo de gestión versión 10.x a 11.x.

Si tiene un nodo de gestión en la versión 10.x, no puede actualizar de 10.x a 11.x. En su lugar, se puede utilizar este procedimiento de migración para copiar mediante la configuración desde 10.x a un nodo de gestión 11.1 recién implementado. Si el nodo de gestión está actualmente en 11.0 o una versión superior, debe omitir este procedimiento. Necesita el nodo de gestión 11.0 o 11.1 y el "Últimas HealthTools" Para actualizar el software Element de 10.3 + a 11.x.

Pasos

1. Desde la interfaz de VMware vSphere, implemente el OVA del nodo de gestión 11.1 y encirelo.
2. Abra la consola de máquina virtual del nodo de gestión, que aparece la interfaz de usuario de terminal (TUI).
3. Use la TUI para crear un nuevo ID de administrador y asignar una contraseña.
4. En la TUI del nodo de gestión, inicie sesión en el nodo de gestión con el ID y la contraseña nuevos y valide que funciona.
5. En la TUI de nodos de gestión o vCenter, obtenga la dirección IP 11.1 del nodo de gestión y busque la dirección IP en el puerto 9443 para abrir la interfaz de usuario del nodo de gestión.

```
https://<mNode 11.1 IP address>:9443
```

6. En vSphere, seleccione **Configuración de NetApp Element** > **Configuración de mNode**. (En versiones anteriores, el menú de nivel superior es **Configuración de SolidFire de NetApp**).
7. Seleccione **acciones** > **Borrar**.
8. Para confirmar, seleccione **Sí**. El campo mNode Status debe informar de no configurado.

Cuando vaya a la ficha **mNode Settings** por primera vez, el campo mNode Status puede aparecer como **no configurado** en lugar del **UP** esperado; es posible que no pueda elegir **acciones** > **Clear**. Actualice el explorador. El campo mNode Status finalmente mostrará **UP**.

9. Cierre la sesión de vSphere.
10. En un explorador web, abra la utilidad de registro del nodo de gestión y seleccione **Administración de servicios QoSSIOC**:

```
https://<mNode 11.1 IP address>:9443
```

11. Establezca la nueva contraseña de QoSSIOC.

La contraseña predeterminada es `solidfire`. Se requiere esta contraseña para establecer la nueva contraseña.

12. Seleccione la pestaña **vCenter Plug-in Registration**.
13. Seleccione **Actualizar Plug-in**.
14. Introduzca los valores necesarios. Cuando haya terminado, seleccione **ACTUALIZAR**.
15. Inicie sesión en vSphere y seleccione **Configuración de NetApp Element** > **Configuración de mNode**.
16. Seleccione **acciones** > **Configurar**.
17. Proporcione la dirección IP del nodo de gestión y el ID de usuario del nodo de gestión (el nombre de usuario es `admin`), la contraseña que ha establecido en la ficha **QoSSIOC Service Management** de la utilidad de registro y el ID de usuario y la contraseña de vCenter.

    En vSphere, la pestaña **mNode Settings** debe mostrar el estado de mNode como **UP**, que indica que el nodo de gestión 11.1 está registrado en vCenter.

18. Desde la utilidad de registro del nodo de gestión (`https://<mNode 11.1 IP address>:9443`), reinicie el servicio SIOC desde **QoSSIOC Service Management**.
19. Espere un minuto y compruebe la ficha **Configuración de NetApp Element** > **Configuración de mNode**. Esto debería mostrar el estado de mNode como **UP**.

    Si el estado es **DOWN**, compruebe los permisos para `/sf/packages/sioc/app.properties`. El archivo debe tener permisos de lectura, escritura y ejecución para el propietario del archivo. Los permisos correctos deben aparecer de la siguiente manera:

```
-rwx------
```

20. Después de que se inicia el proceso SIOC y vCenter muestra el estado mNode como **UP**, compruebe los registros de la `sf-hci-nma` servicio en el nodo de gestión. No debe haber mensajes de error.
21. (Solo para el nodo de gestión 11.1) SSH en la versión 11.1 del nodo de gestión con privilegios raíz e inicie el servicio NMA con los siguientes comandos:

```
# systemctl enable /sf/packages/nma/systemd/sf-hci-nma.service
```

```
# systemctl start sf-hci-nma21
```

22. Ejecute acciones desde vCenter para quitar una unidad, añadir una unidad o reiniciar nodos. Esto activa las alertas de almacenamiento que se deben notificar en vCenter. Si esto funciona, las alertas del sistema NMA funcionan según lo esperado.
23. Si ONTAP Select se configura en vCenter, configure las alertas de ONTAP Select en NMA copiando el `.ots.properties` archivo del nodo de gestión anterior al nodo de gestión, versión 11.1 `/sf/packages/nma/conf/.ots.properties` File, y reinicie el servicio NMA mediante el siguiente comando:

```
systemctl restart sf-hci-nma
```

24. Compruebe que ONTAP Select esté funcionando. Para ello, consulte los registros con el siguiente comando:

```
journalctl -f | grep -i ots
```

25. Siga estos pasos para configurar Active IQ:
    a. SSH en la versión 11.1 del nodo de gestión y vaya al `/sf/packages/collector` directorio.
    b. Ejecute el siguiente comando:

```
sudo ./manage-collector.py --set-username netapp --set-password --set
-mvip <MVIP>
```

    c. Introduzca la contraseña de interfaz de usuario del nodo de gestión cuando se lo solicite.
    d. Ejecute los siguientes comandos:

```
./manage-collector.py --get-all
```

```
sudo systemctl restart sfcollector
```

    e. Verificación `sfcollector` registra para confirmar que funciona.
26. En vSphere, la pestaña **Configuración de NetApp Element** > **Configuración de mNode** debe mostrar el estado de mNode como **UP**.
27. Comprobar que NMA notifica alertas del sistema y alertas ONTAP Select.
28. Si todo funciona según lo esperado, apague y elimine el nodo de gestión 10.x.

Volver a configurar la autenticación mediante la API DE REST del nodo de gestión

Se puede conservar el nodo de gestión existente si se actualizaron secuencialmente (1) y (2) el almacenamiento de Element. Si ha seguido un orden de actualización diferente, consulte los procedimientos para actualizar nodos de gestión sin movimiento.

Antes de empezar

- Ha actualizado sus servicios de administración a 2.10.29 o posterior.
- El clúster de almacenamiento ejecuta Element 12.0 o una versión posterior.
- El nodo de gestión es 11.3 o posterior.
- Actualizó secuencialmente los servicios de gestión a continuación, actualizando el almacenamiento de Element. No puede volver a configurar la autenticación con este procedimiento a menos que haya completado las actualizaciones en la secuencia descrita.

Pasos

1. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

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

2. Seleccione **autorizar** y complete lo siguiente:
   a. Introduzca el nombre de usuario y la contraseña del clúster.
   b. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.
   c. Seleccione **autorizar** para iniciar una sesión.
3. En la interfaz DE usuario DE LA API DE REST, seleccione **POST /Services/reconfigure-auth**.
4. Seleccione **probar**.
5. Para el parámetro **LOAD_images**, seleccione `true`.
6. Seleccione **Ejecutar**.

   El cuerpo de respuesta indica que la reconfiguración se ha realizado correctamente.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Actualice el plugin de Element para vCenter Server

Para los entornos de vSphere existentes con un plugin de NetApp Element registrado para VMware vCenter Server, es posible actualizar el registro del plugin después de actualizar por primera vez el paquete de servicios de gestión que contiene el servicio del plugin.

Es posible actualizar el registro del plugin en vCenter Server Virtual Appliance (vcsa) o Windows desde la utilidad de registro. Debe cambiar el registro del plugin de vCenter en cada instancia de vCenter Server donde necesite usar el plugin.

Los servicios de gestión 2.22.7 incluyen el plugin de Element para vCenter Server 5.0, que contiene el plugin remoto. Si usa el plugin de Element, debe actualizar a los servicios de gestión 2.22.7 o una versión posterior para cumplir con la directiva de VMware que elimina la compatibilidad con los plugins locales. "Leer más".

Plugin de Element vCenter versión 5.0 o posterior

Este procedimiento de actualización cubre los siguientes escenarios de actualización:

- Va a actualizar al plugin de Element para vCenter Server 5,3, 5,2, 5,1 o 5,0.
- Actualice a un HTML5 8.0 o 7.0 vSphere Web Client.

El plugin de Element para vCenter 5,0 o posterior no es compatible con vCenter Server 6,7 y 6,5.

Cuando se actualiza desde el plugin de Element para vCenter Server 4.x a 5.x, los clústeres ya configurados con el plugin se pierden porque no se pueden copiar los datos de una instancia de vCenter en un plugin remoto. Debe volver a añadir los clústeres al plugin remoto. Esta es una actividad que solo debe hacer una vez al actualizar desde un plugin local a un plugin remoto.

Plugin de Element vCenter versión 4.10 o anterior

Este procedimiento de actualización cubre los siguientes escenarios de actualización:

- Actualice al plugin de Element para vCenter Server 4.10, 4.9, 4.8, 4.7, 4.6, 4.5, o 4.4.
- Va a actualizar a un HTML5 7.0, 6.7 o 6.5 vSphere Web Client.

- El plugin no es compatible con VMware vCenter Server 8.0 para el plugin de Element para VMware vCenter Server 4.x.
- El plugin no es compatible con VMware vCenter Server 6.5 para el plugin de Element para VMware vCenter Server 4.6, 4.7 y 4.8.

- Actualice a una instancia de Flash vSphere Web Client en 6.7.

El plugin es compatible con vSphere Web Client versión 6.7 U2 para Flash, 6.7 U3 (Flash y HTML5) y 7.0 U1. El plugin no es compatible con la versión 6.7 U2 compilación 13007421 del HTML5 vSphere Web Client y otras versiones de 6.7 U2 publicadas antes de la actualización 2a (compilación 13643870). Para obtener más información sobre las versiones de vSphere compatibles, consulte las notas de la versión de "la versión del plugin".

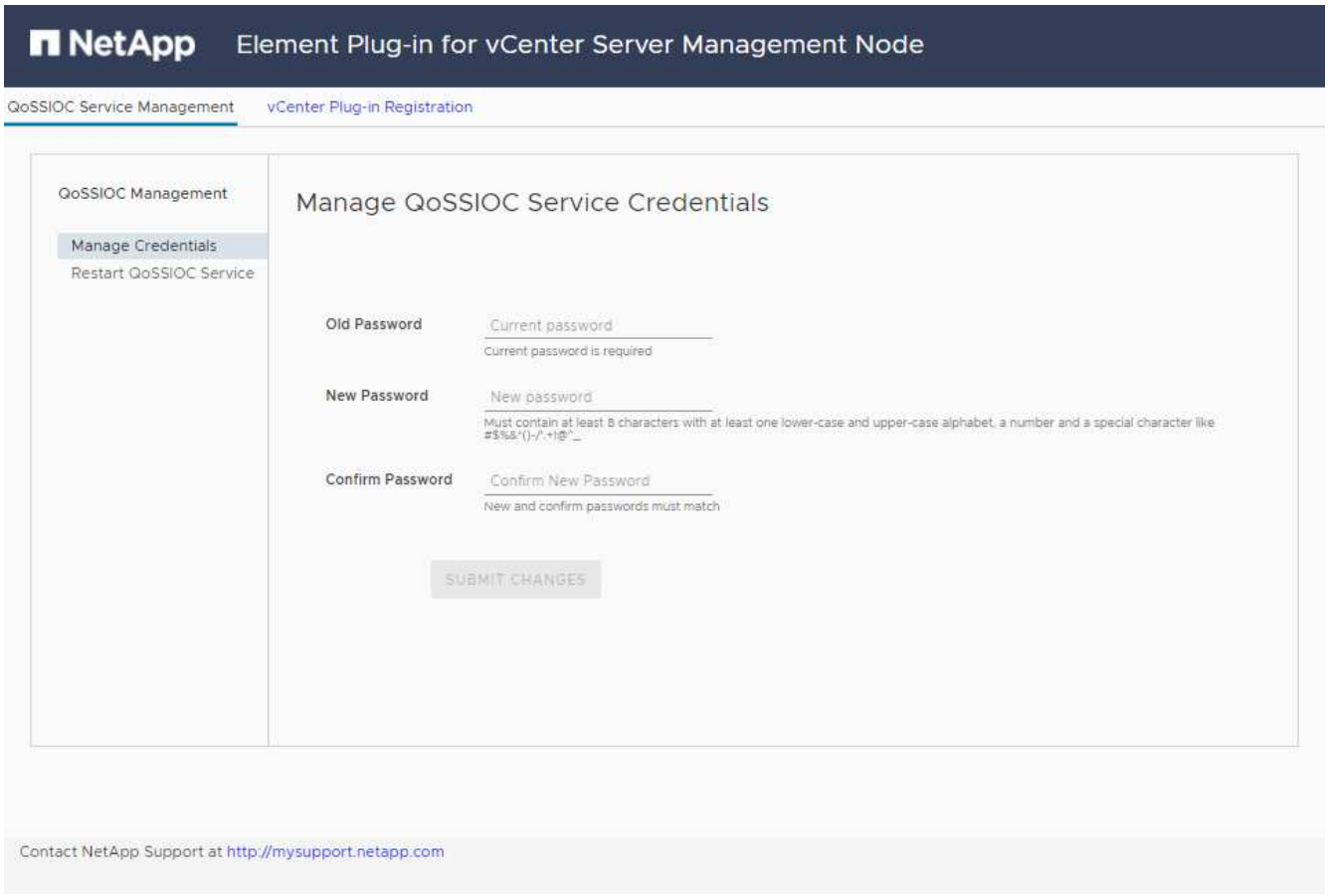
Lo que necesitará

- **Privilegios de administrador**: Tiene privilegios de la función de administrador de vCenter para instalar un complemento.
- **Actualizaciones de vSphere**: Ha realizado cualquier actualización de vCenter necesaria antes de actualizar el plugin de NetApp Element para vCenter Server. Este procedimiento da por sentado que ya se completaron las actualizaciones de vCenter.

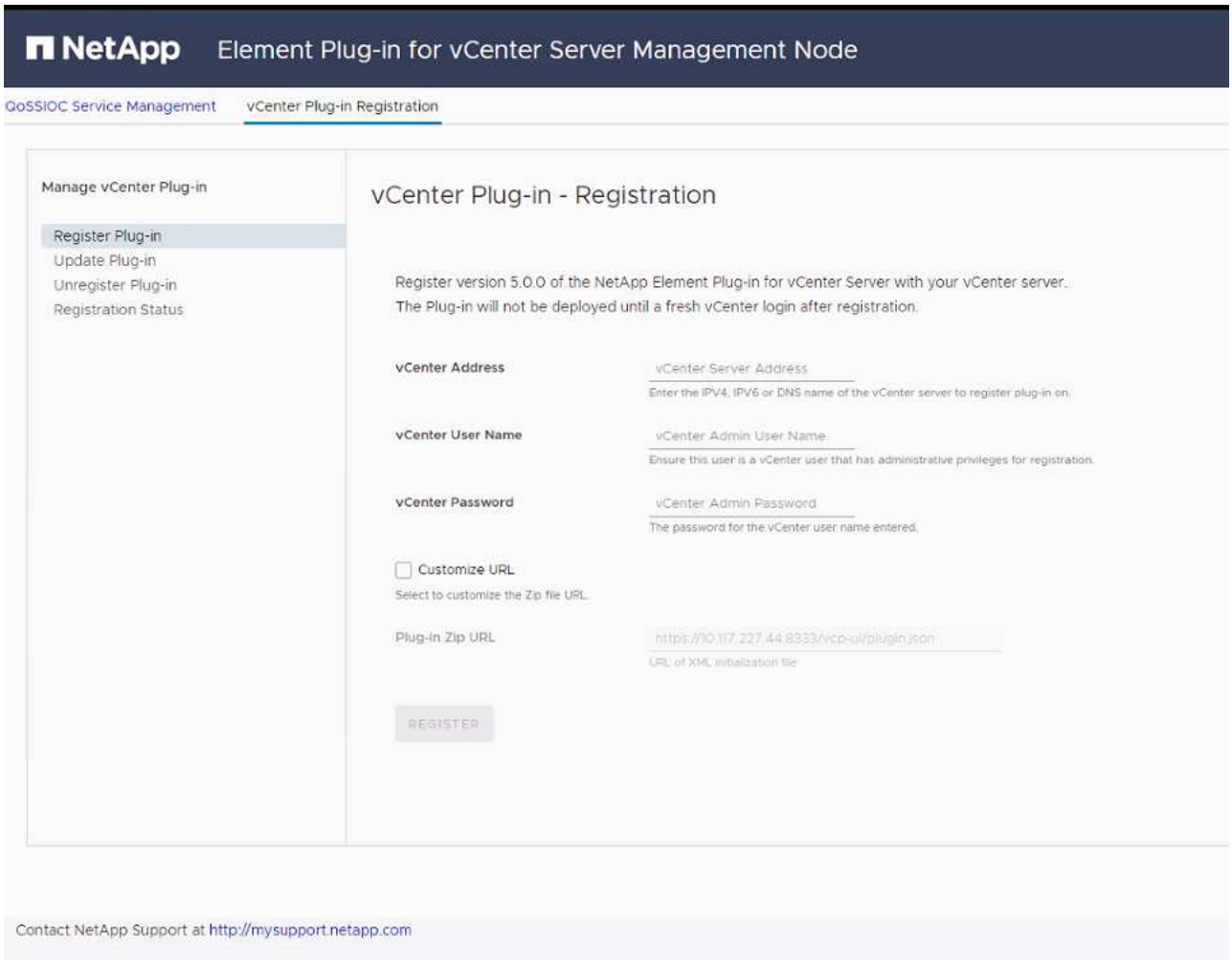
- **VCenter Server**: El plugin de vCenter versión 4.x o 5.x está registrado en vCenter Server. Desde la utilidad de registro (`https://<ManagementNodeIP>:9443`), seleccione **Registration Status**, complete los campos necesarios y seleccione **Check Status** para comprobar que el complemento de vCenter ya está registrado y que el número de versión de la instalación actual.
- **Actualizaciones de servicios de administración**: Ha actualizado el "paquete de servicios de gestión" a la última versión. Las actualizaciones en el complemento de vCenter se distribuyen mediante actualizaciones de servicios de gestión que se publican fuera de los principales lanzamientos de productos para el almacenamiento all-flash SolidFire de NetApp.
- **Actualizaciones del nodo de administración**:
  - A partir del plugin de Element vCenter versión 5.0, se ejecuta un nodo de gestión que haya estado "actualizado" a la versión 12.3.x o posterior.
  - Para el plugin de Element vCenter 4.4 a 4.10, ejecuta un nodo de gestión que haya sido "actualizado" a la versión 11.3 o posterior. El complemento de vCenter versión 4.4 o posterior requiere un nodo de gestión de 11.3 o posterior con una arquitectura modular que proporciona servicios individuales. El nodo de gestión debe estar encendido y tener configurada su dirección IP o dirección DHCP.
- **Actualizaciones de almacenamiento de elementos**:
  - A partir del plugin de Element vCenter versión 5.0, tiene un clúster que ejecuta el software NetApp Element 12.3.x o una versión posterior.
  - Para el plugin de Element vCenter versión 4.10 o una versión anterior, tiene un clúster que ejecuta el software NetApp Element 11.3 o una versión posterior.
- **VSphere Web Client**: Cerró la sesión en vSphere Web Client antes de iniciar cualquier actualización de plugin. Si no cierra sesión, el cliente web no reconocerá las actualizaciones realizadas durante este proceso al plug-in.

Pasos

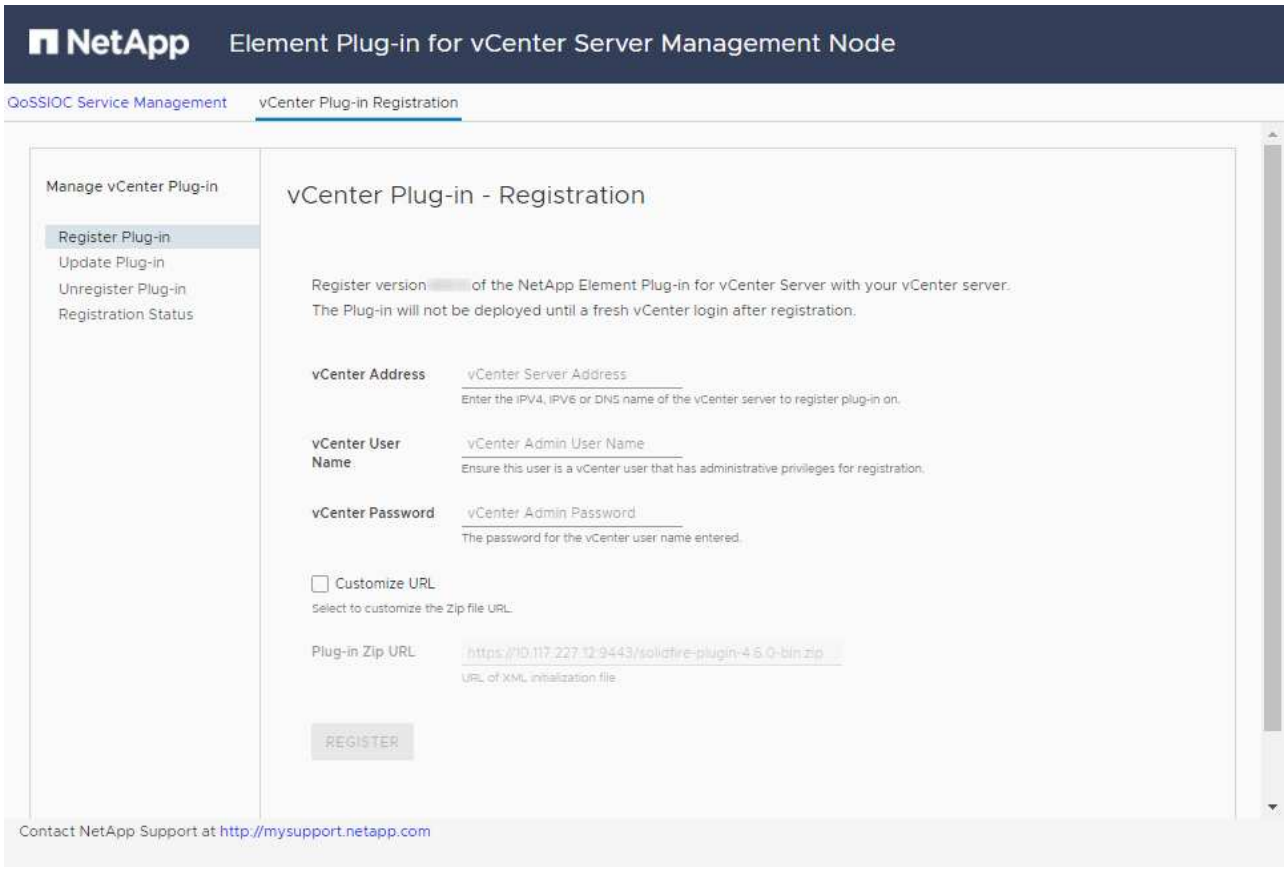
1. Introduzca la dirección IP para el nodo de gestión en un navegador, incluido el puerto TCP para el registro: `https://<ManagementNodeIP>:9443`La interfaz de usuario de la utilidad de registro se abre en la página **Manage QoSSIOC Service Credentials** del plugin.



2. Seleccione **vCenter Plug-in Registration**.
   - La página de registro del plugin de vCenter para el plugin de Element para vCenter Server 5.x:



- La página de registro del plugin de vCenter para el plugin de Element para vCenter Server 4.10 o una versión anterior:



3. En **Manage vCenter Plug-in**, seleccione **Update Plug-in**.
4. Confirme o actualice la siguiente información:
   a. La dirección IPv4 o el nombre de dominio completo del servicio vCenter en el que planea registrar el plugin.
   b. El nombre de usuario administrador de vCenter.

      Las credenciales de nombre de usuario y contraseña introducidas deben corresponder a un usuario con privilegios de la función de administrador de vCenter.

   c. La contraseña de administrador de vCenter.
   d. (Para servidores internos/sitios oscuros) dependiendo de la versión de Element para vCenter, una URL personalizada para el archivo JSON del plugin o el ZIP del plugin:
      i. A partir del plugin de Element para vCenter Server 5.0, una URL personalizada para el archivo JSON del plugin.

         Puede seleccionar **URL personalizada** para personalizar la URL si utiliza un servidor HTTP o HTTPS (sitio oscuro) o si ha modificado el nombre del archivo JSON o la configuración de red. Para obtener pasos de configuración adicionales si planea personalizar una URL, consulte la documentación del plugin de Element para vCenter Server sobre la modificación de las propiedades de vCenter para un servidor HTTP interno (sitio oscuro).

      ii. Para el plugin de Element para vCenter Server 4.10 o versiones anteriores, una URL personalizada para el ZIP del plugin.

Puede seleccionar **URL personalizada** para personalizar la URL si utiliza un servidor HTTP o HTTPS (sitio oscuro) o si ha modificado el nombre del archivo ZIP o la configuración de red. Para obtener pasos de configuración adicionales si planea personalizar una URL, consulte la documentación del plugin de Element para vCenter Server sobre la modificación de las propiedades de vCenter para un servidor HTTP interno (sitio oscuro).

5. Seleccione **Actualizar**.

   Aparece un banner en la interfaz de usuario de la utilidad de registro cuando el registro se realiza correctamente.

6. Inicie sesión en vSphere Web Client como administrador de vCenter. Si ya ha iniciado sesión en vSphere Web Client, primero debe cerrar la sesión, esperar dos o tres minutos y, a continuación, iniciar sesión de nuevo.

   Esta acción crea una base de datos nueva y completa la instalación en vSphere Web Client.

7. En vSphere Web Client, busque las siguientes tareas completadas en el monitor de tareas para garantizar que se haya completado la instalación: `Download plug-in` y.. `Deploy plug-in`.
8. Verifique que los puntos de extensión del plugin aparezcan en la pestaña **Shortcuts** de vSphere Web Client y en el panel lateral.
   - A partir del plugin de Element para vCenter Server 5.0, se muestra el punto de extensión NetApp Element Remote Plugin:

   - En el caso del plugin de Element para vCenter Server 4.10 o una versión anterior, los puntos de extensión NetApp Element Configuration y Management aparecen:

   Si los iconos del plugin de vCenter no se ven, consulte "Plugin de Element para vCenter Server" documentación sobre solución de problemas del plugin.

   Después de actualizar al plugin de NetApp Element para vCenter Server 4.8 o una versión posterior con VMware vCenter Server 6.7U1, si los clústeres de almacenamiento no se muestran en la lista o se muestra un error de servidor en las secciones **Clusters** y **Configuración de QoSSIOC** de la configuración de NetApp Element, consulte "Plugin de Element para vCenter Server" documentación sobre la solución de problemas de estos errores.

9. Verifique el cambio de versión en la ficha **Acerca de** del punto de extensión **Configuración NetApp Element** del plugin.

   Debería ver los detalles o detalles de la siguiente versión de una versión más reciente:

```
NetApp Element Plug-in Version: 5.3
NetApp Element Plug-in Build Number: 9
```

El plugin de vCenter incluye contenido de ayuda en línea. Para garantizar que la ayuda en línea incluya el contenido más reciente, borre la memoria caché del navegador después de actualizar el plugin.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Actualice los componentes de vSphere para un sistema de almacenamiento SolidFire de NetApp con el plugin de Element para vCenter Server

Al actualizar los componentes de VMware vSphere de la instalación de almacenamiento de SolidFire Element, tendrá que realizar algunos pasos adicionales a fin de aplicar a los sistemas con el plugin de Element para vCenter Server.

Pasos

1. Para actualizaciones de vcsa, "claro" Configuración de QoSSIOC en el plugin (**Configuración de NetApp Element > Configuración de QoSSIOC**). Aparece el campo **Estado de QoSSIOC** `Not Configured` una vez completado el proceso.
2. Para actualizaciones de vcsa y Windows, "cancele el registro" El plugin desde la instancia de vCenter Server a la que se asocia mediante la utilidad de registro.
3. "Actualice vSphere, incluidos vCenter Server, ESXi, VMs y otros componentes de VMware".

   Debe actualizar al plugin de NetApp Element para vCenter Server 5.0 o una versión posterior para otorgar la capacidad de implementar el plugin con VMware vCenter 7.0 Update 3 sin tener que aplicar una solución alternativa.

   Con el plugin de Element para vCenter Server 4.x, cuando se actualiza a VMware vCenter Server 7.0 Update 3, el plugin no puede ponerse en marcha. Para resolver este problema con Spring Framework 4, consulte "Este artículo de la base de conocimientos".

4. "Regístrese" El plugin de Element para vCenter Server nuevamente con vCenter.
5. "Añadir clústeres" con el plugin.
6. "Configure los ajustes de QoSSIOC" con el plugin.
7. "Habilite QoSSIOC" para todos los almacenes de datos controlados por el plugin.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Versiones anteriores de la documentación sobre el software SolidFire y NetApp Element

La documentación de las versiones anteriores está disponible en el sitio de soporte de NetApp.

- "Documentación de Element 12.2.1"
- "Documentación de Element 12.2"
- "Documentación de Element 12.0.1"
- "Documentación de Element 12.0"
- "Documentación de Element 11.8.2"
- "Documentación de Element 11.8.1"
- "Documentación de Element 11.8"
- "Documentación de Element 11.7"
- "Documentación de Element 11.5.1"
- "Documentación de Element 11.5"
- "Documentación del elemento 11.3P1"
- "Documentación de Element 11.3.2"
- "Documentación de Element 11.1 y versiones anteriores"

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

- "Aviso para Ember OS 12.3"
- "Aviso para HealthTools"
- "Aviso para el nodo de gestión 12.3"
- "Aviso para servicios de gestión 2.25.42 (complemento NetApp Element para VMware vCenter Server 5,3.9)"
- "Aviso para servicios de gestión 2.24.40 (complemento NetApp Element para VMware vCenter Server 5,2.12)"
- "Aviso relativo a los servicios de gestión 2.23.64 (complemento NetApp Element para VMware vCenter Server 5.1.12)"
- "Aviso relativo a los servicios de gestión 2.22.7 (complemento NetApp Element para VMware vCenter Server 5.0.37)"
- "Aviso relativo a los servicios de gestión 2.21.61 (complemento NetApp Element para VMware vCenter Server 4.10.12)"
- "Aviso para servicios de gestión 2.20.69 (plugin de NetApp Element para vCenter Server 4.9.14)"

- "Aviso para servicios de gestión 2.19.48 (plugin de NetApp Element para vCenter Server 4.8.34)"
- "Aviso para servicios de gestión 2.18.91 (plugin de NetApp Element para vCenter Server 4.7.10)"
- "Aviso para servicios de gestión 2.17.56 (plugin de NetApp Element para vCenter Server 4.6.32)"
- "Aviso para servicios de gestión 2.17.52 (plugin de NetApp Element para vCenter Server 4.6.29)"
- "Aviso para servicios de gestión 2.16 (plugin de NetApp Element para vCenter Server 4.6.29)"
- "Aviso para servicios de gestión 2.14 (plugin de NetApp Element para vCenter Server 4.5.42)"
- "Aviso para servicios de gestión 2.13 (plugin de NetApp Element para vCenter Server 4.5.42)"
- "Aviso para el paquete de firmware de almacenamiento 2.146"
- "Aviso para el paquete de firmware de almacenamiento 2.99.2"
- "Aviso para el paquete de firmware de almacenamiento 2.76"
- "Aviso para el paquete de firmware de almacenamiento 2.27"

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.