



Documentación del software SolidFire y Element

Element Software

NetApp
November 18, 2025

Tabla de contenidos

Documentación del software SolidFire y Element	1
Notas de la versión	2
Información sobre versiones actuales y anteriores	2
Software NetApp Element	2
Servicios de administración	2
Plugin de NetApp Element para vCenter Server	2
Firmware de almacenamiento	3
Encuentra más información	3
¿Qué novedades hay en el software Element?	3
Elemento 12.8	3
Elemento 12.7	4
Elemento 12.5	6
Encuentra más información	7
Conceptos	8
Descripción general del producto	8
Características de SolidFire	8
Despliegue de SolidFire	8
Encuentra más información	9
Arquitectura y componentes	9
Conozca la arquitectura de SolidFire	9
interfaces de software SolidFire	11
SolidFire Active IQ	13
Nodo de gestión para el software Element	13
Servicios de gestión para almacenamiento all-flash SolidFire	14
Nodos	14
Nodo de gestión	14
Nodo de almacenamiento	15
Nodo de canal de fibra	15
Estados de operación de los nodos	15
Encuentra más información	16
Clústeres	16
clústeres de almacenamiento autorizados	17
Regla de los tercios	17
capacidad varada	17
Eficiencia de 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 multifactor	19
FIPS 140-2 para HTTPS y cifrado de datos en reposo	19
Para más información	20

Cuentas y permisos	20
cuentas de administrador de clúster de almacenamiento	20
Cuentas de usuario	20
cuentas de usuario de clúster autorizadas	21
Cuentas de volumen	21
Almacenamiento	22
Volúmenes	22
Volúmenes virtuales (vVols)	22
Grupos de acceso por volumen	24
Iniciadores	24
Protección de datos	25
Tipos de replicación remota	25
Instantáneas de volumen para la protección de datos	27
clones de volumen	27
Descripción general del proceso de copia de seguridad y restauración para el almacenamiento de Element	28
Dominios de protección	28
Dominios de protección personalizados	28
Alta disponibilidad de Double Helix	29
Rendimiento y calidad del servicio	29
Parámetros de calidad del servicio	29
Límites de valor de QoS	30
Rendimiento de QoS	31
Políticas de QoS	31
Encuentra más información	32
Requisitos	33
Redes	33
Para más información	33
Configuración de conmutadores para clústeres que ejecutan el software Element	33
Para más información	34
Requisitos del puerto de red	34
Para más información	39
Pruébalo	40
Pruebe las funciones de almacenamiento utilizando el nodo de demostración de Element	40
Funcionalidad admitida:	40
Requisitos de VM	41
Requisitos del anfitrión	41
Descargar nodo de demostración de Element	41
Instalar el nodo de demostración de Element en VMware ESXi	41
Cómo obtener ayuda	42
Encuentra más información	43
Instalar y mantener el hardware	44
Información de hardware H410S y H610S	44
Instalar nodos de almacenamiento de la serie H	44
Reemplazar un nodo H410S	53

Reemplazar un nodo H610S	57
Reemplazar unidades	59
Reemplace una unidad de fuente de alimentación	63
Información sobre el hardware de la serie SF	66
Reemplazar un chasis	66
Reemplazar las unidades de los nodos de almacenamiento de la serie SF	68
Reemplace una unidad de fuente de alimentación	72
Volver a la información de la imagen de fábrica	73
Configurar la imagen de retorno a fábrica	73
Opciones de instalación y despliegue de RTFI	74
El proceso RTFI	75
Menú de opciones RTFI	77
nodos de almacenamiento	79
H610S	80
H410S	104
SF38410, SF19210, SF9605 y SF4805	108
Configurar almacenamiento	115
Aprenda cómo configurar el almacenamiento	115
Encuentra más información	115
Configurar un clúster con nodos de almacenamiento	116
Configurar un nodo de almacenamiento	116
Cree un clúster de almacenamiento.	118
Acceda a la interfaz de usuario del software Element	119
Agregar unidades a un clúster	120
Configurar un clúster con nodos Fibre Channel.	121
Configurar un nodo Fibre Channel.	121
Cree un nuevo clúster con nodos Fibre Channel.	121
Agregar nodos Fibre Channel a un clúster	122
Configurar zonas para nodos Fibre Channel	123
Cree un grupo de acceso por volumen para clientes Fibre Channel.	124
Determina qué componentes de SolidFire debes instalar.	124
Para más información	125
Configurar un nodo de administración	125
Encuentra más información	125
Configurar el acceso a la interfaz web del nombre de dominio completo	125
Configure el acceso a la interfaz web de FQDN mediante NetApp Hybrid Cloud Control.	126
Configure el acceso a la interfaz web mediante FQDN utilizando la API REST.	127
Eliminar el acceso a la interfaz web de FQDN mediante NetApp Hybrid Cloud Control	128
Eliminar el acceso a la interfaz web de FQDN mediante la API REST	128
Solución de problemas.	129
Encuentra más información	130
¿Qué sigue?	130
Encuentra más información	130
Gestiona el almacenamiento con el software Element.	131
Gestiona el almacenamiento con el software Element.	131

Encuentra más información	131
Acceda a la interfaz de usuario del software Element	131
Encuentra más información	132
Configure las opciones del sistema SolidFire después de la implementación.	132
Configure las opciones del sistema SolidFire después de la implementación.	132
Cambiar credenciales en NetApp HCI y NetApp SolidFire	132
Cambiar el certificado SSL predeterminado del software Element	137
Cambiar la contraseña IPMI predeterminada para los nodos	138
Utilice las opciones básicas de la interfaz de usuario del software Element.	139
Utilice las opciones básicas de la interfaz de usuario del software Element.	139
actividad de la API	139
Iconos en la interfaz de Elemento	140
Enviar comentarios	141
Gestionar cuentas	142
Gestionar cuentas	142
Trabajar con cuentas que utilizan CHAP	142
Administrar cuentas de usuario de administrador de clúster	145
Administrar LDAP	148
Administra tu sistema	156
Administra tu sistema	157
Habilitar la autenticación multifactor	157
Configurar los ajustes del clúster	158
Cree un clúster que admita unidades FIPS.	175
Establecer una comunicación segura	178
Comience con la administración de claves externas	180
Gestionar volúmenes y volúmenes virtuales	185
Aprenda sobre la gestión de volúmenes y volúmenes virtuales.	185
Trabajar con volúmenes	187
Trabajar con volúmenes virtuales	196
Trabajar con grupos de acceso por volumen e iniciadores	204
Proteja sus datos	212
Proteja sus datos	212
Utilice instantáneas de volumen para la protección de datos.	213
Realizar replicación remota entre clústeres que ejecutan el software NetApp Element	227
Utilice la replicación SnapMirror entre los clústeres Element y ONTAP (interfaz de usuario de Element).	241
Replicación entre el software NetApp Element y ONTAP (CLI de ONTAP)	253
Copia de seguridad y restauración de volúmenes	273
Configurar dominios de protección personalizados	277
Soluciona los problemas de tu sistema	279
Eventos del sistema	279
Ver el estado de las tareas en ejecución	283
Alertas del sistema	283
Ver actividad de rendimiento del nodo	301
Rendimiento de volumen	302

Sesiones iSCSI	304
Sesiones de Fibre Channel	305
Solucionar problemas de las unidades	306
Solucionar problemas de nodos	309
Trabajar con utilidades por nodo para nodos de almacenamiento	311
Comprender los niveles de plenitud del clúster	318
Administre y supervise el almacenamiento con NetApp Hybrid Cloud Control.....	320
Agregue y administre clústeres de almacenamiento mediante NetApp Hybrid Cloud Control.....	320
Agregar un clúster de almacenamiento	320
Confirmar el estado del clúster de almacenamiento	321
Editar credenciales del clúster de almacenamiento.....	321
Eliminar un clúster de almacenamiento	322
Activar y desactivar el modo de mantenimiento	322
Configurar el acceso a la interfaz web del nombre de dominio completo	324
Configure el acceso a la interfaz web de FQDN mediante NetApp Hybrid Cloud Control.....	325
Configure el acceso a la interfaz web mediante FQDN utilizando la API REST.....	325
Eliminar el acceso a la interfaz web de FQDN mediante NetApp Hybrid Cloud Control	326
Eliminar el acceso a la interfaz web de FQDN mediante la API REST	327
Solución de problemas.....	328
Encuentra más información	328
Cree y gestione cuentas de usuario mediante NetApp Hybrid Cloud Control.....	328
Habilitar LDAP	329
Gestionar cuentas de clúster autorizadas	329
Gestionar cuentas de volumen	331
Cree y gestione volúmenes mediante NetApp Hybrid Cloud Control.....	333
Crear un volumen.....	333
Aplicar una política de QoS a un volumen	334
Editar un volumen	335
Volúmenes de clonación	336
Agregar volúmenes a un grupo de acceso a volúmenes.....	337
Eliminar un volumen.....	338
Restaurar un volumen eliminado	338
Eliminar un volumen borrado	339
Crear y administrar grupos de acceso por volumen	339
Agregar un grupo de acceso por volumen.....	340
Editar un grupo de acceso a volumen	340
Eliminar un grupo de acceso a volumen	341
Crear y gestionar iniciadores	341
Crear un iniciador.....	342
Agregar iniciadores a un grupo de acceso por volumen	343
Cambiar un alias de iniciador.....	343
Eliminar iniciadores	344
Crear y gestionar políticas de QoS de volumen.....	344
Crea una política de QoS	345
Aplicar una política de QoS a un volumen.....	345

Cambiar la asignación de política QoS de un volumen	346
Editar una política de QoS	346
Eliminar una política de QoS	347
Supervise su sistema SolidFire con NetApp Hybrid Cloud Control.	347
Supervise los recursos de almacenamiento en el panel de control de la nube híbrida.	347
Consulta tu inventario en la página de Nodos.	352
Supervise los volúmenes en su clúster de almacenamiento.	354
Recopilar registros para la resolución de problemas.	356
Gestiona el almacenamiento con la API de Element	360
Software Element API	360
Aprenda a administrar el almacenamiento con la API de Element.	360
miembros del objeto de solicitud	364
miembros del objeto de respuesta	365
puntos de conexión de solicitud	365
Autenticación API	366
Métodos asíncronos	366
Atributos	367
objetos comunes	368
cuenta	368
información de sesión de autenticación	369
Trabajo de gran volumen	371
enlace (volúmenes virtuales)	372
Detalles del certificado	373
clúster	374
administrador del clúster	376
capacidad del clúster	377
configuración del clúster	379
Información del clúster	380
clusterPair	383
estadísticas del clúster	384
Estructura del clúster	387
conducir	387
Estadísticas de la unidad	390
error	392
evento	392
falla	395
Puerto de canal de fibra	398
Informe de nodo de error de fips	399
Informe de nodo fips	400
Informe fips	400
Instantánea de grupo	401
Información de hardware	402
host (volúmenes virtuales)	404
idpConfigInfo	405
iniciador	406

Autenticación ISCSIA	407
proveedor de clavesKmpip	408
servidor de clavesKmpip	409
Configuración LDAP	410
servidor de registro	411
red (interfaces enlazadas)	412
red (todas las interfaces)	417
red (interfaces Ethernet)	417
red (interfaces locales)	419
red (SNMP)	421
Interfaz de red	422
Estadísticas de interfaz de red	423
nodo	424
Dominios de protección de nodos	426
estadísticas del nodo	427
ontapVersionInfo	429
nodo activo pendiente	429
nodo pendiente	431
dominio de protección	433
Nivel de dominio de protección	433
Resiliencia del dominio de protección	434
protecciónDominioTolerancia	435
Resiliencia del esquema de protección	436
Tolerancia del esquema de protección	436
punto final del protocolo	437
Calidad de servicio	438
Política de QoS	439
Estado de instantánea del clúster remoto	440
cronograma	441
sesión (Canal de fibra)	444
sesión (iSCSI)	445
snapMirrorAggregate	448
snapMirrorClusterIdentity	448
snapMirrorEndpoint	449
snapMirrorJobScheduleCronInfo	450
snapMirrorLunInfo	450
snapMirrorInterfazDeRed	451
snapMirrorNode	452
snapMirrorPolicy	453
Regla de política de espejo snap	454
snapMirrorRelationship	455
snapMirrorVolume	458
snapMirrorVolumeInfo	459
snapMirrorVserver	460
snapMirrorVserverAggregateInfo	461

instantánea	462
Destinatario de trampa SNMP	465
contenedor de almacenamiento	465
trabajo de sincronización	467
tarea (volúmenes virtuales)	469
usmUser	471
red virtual	472
volumen virtual	473
volume	475
volumeAccessGroup	479
volumenPar	480
estadísticas de volumen	482
Métodos comunes	486
Obtener API	486
ObtenerResultadoAsíncrono	494
Obtener estadísticas completas	498
Obtener límites	498
Obtener origen	501
GetRawStats	502
ListAsyncResults	502
Métodos de la API de cuentas	506
Agregar cuenta	506
ObtenerCuentaPorID	509
ObtenerCuentaPorNombre	510
Obtén la eficiencia de la cuenta	512
Lista de cuentas	514
Modificar cuenta	516
Eliminar cuenta	519
Métodos de la API de administrador	520
Agregar administrador de clúster	520
ObtenerAdministradorDeClústerActual	523
Obtener banner de inicio de sesión	524
Lista de administradores de clúster	525
Modificar administrador de clúster	528
Eliminar administrador del clúster	529
Establecer banner de inicio de sesión	530
Métodos de la API de clúster	532
Agregar nodos	532
Borrar fallos de clúster	535
CrearPreferenciaDeInterfazDeClúster	537
EliminarPreferenciaDeInterfazDeClúster	538
Deshabilitar función	539
Habilitar función	540
Obtener capacidad del clúster	542
Umbral completo del clúster	544

Obtener información de hardware del clúster	550
Obtener información del clúster	552
GetClusterInterfacePreference	554
Obtener ID de nodo maestro del clúster	555
Obtener estadísticas del clúster	556
ObtenerInformación de versión del clúster	557
Obtener estado de la función	561
Obtener información de sesión de inicio de sesión	563
Información del hardware del nodo	565
Obtener estadísticas del nodo	566
Lista de nodos activos	569
Lista todos los nodos	569
ListClusterFaults	571
Preferencias de interfaz de clúster de lista	575
Lista de eventos	576
Estadísticas de nodo de lista	579
Lista de sesiones ISCSI	582
Servicios de listas	584
Lista de nodos pendientes	586
Lista de nodos activos pendientes	588
Modificar UmbralCompletoDeClúster	590
ModificarPreferenciaDeInterfazDeClúster	598
Eliminar nodos	599
SetLoginSessionInfo	601
Cerrar	603
Métodos de la API de creación de clústeres	604
VerificarClústerPropuesto	604
CrearClúster	606
Obtener configuración de Bootstrap	609
Métodos de la API de Drive	613
Agregar unidades	613
Información sobre el hardware de la unidad	615
GetDriveStats	617
ListDrives	620
ListDriveStats	622
Eliminar unidades	624
Unidades de borrado seguro	626
Métodos de la API de Fibre Channel	628
Obtener asignaciones de LUN de acceso al volumen	628
Información del puerto del canal de fibra	629
Lista de sesiones de FibreChannel	633
Información del puerto del canal de fibra del nodo de lista	634
Modificar asignaciones de Lun de grupo de acceso a volumen	636
Métodos de la API del iniciador	638
CrearIniciadores	639

EliminarIniciadores	643
Iniciadores de listas	645
ModificarIniciadores	646
Métodos de la API LDAP	650
Agregar administrador de clúster Ldap	650
Habilitar autenticación LDAP	652
Deshabilitar la autenticación LDAP	657
Obtener configuración LDAP	658
Prueba de autenticación LDAP	660
Métodos de la API de autenticación multifactor	662
Agregar administrador de clúster de IDIP	662
Crear configuración de Idp	664
Eliminar sesión de autenticación	666
Eliminar sesiones de autenticación por administrador de clúster	668
EliminarSesionesDeAutenticaciónPorNombreDeUsuario	669
Eliminar configuración de IDp	672
Deshabilitar la autenticación Idp	673
Habilitar autenticación Idp	674
Obtener estado de autenticación Idp	675
ListarSesionesDeAutenticaciónActivas	676
Configuraciones de ListIdp	677
Actualizar configuración de IDp	679
Métodos de la API de autenticación de sesión	682
ListaAuthSessionsByClusterAdmin	682
Listar sesiones de autenticación por nombre de usuario	684
Métodos de la API de Node	686
ComprobarPingEnVlan	687
Verificar adiciones de nodos propuestas	690
Crear paquete de soporte de clúster	693
Crear paquete de soporte	696
Eliminar todos los paquetes de soporte	699
Desactivar el modo de mantenimiento	699
Deshabilitar SSH	702
Habilitar modo de mantenimiento	703
Habilitar SSH	706
Obtener configuración de clúster	707
Obtener estado del clúster	709
Obtener configuración	710
Obtener configuración de la unidad	711
Obtener configuración de hardware	714
Obtener información de hardware	716
GetIpmiConfig	718
GetIpmiInfo	723
Obtener configuración de red	726
ObtenerInterfazDeRed	727

ObtenerCifrasTlsActivasDeNodo	731
Informe de unidades GetNodeFips	732
Obtener certificado SSL del nodo	733
ObtenerCifradosTLSCompatiblesConNodo	735
Obtener información del parche	737
ObtenerOperaciónPendiente	739
Obtener información Ssh	740
Hardware de la unidad de lista	741
Lista de interfaces de red	744
Listar estadísticas de interfaz de red	746
Pruebas de lista	748
Utilidades de lista	749
Eliminar certificado SSL del nodo	750
Restablecer unidades	751
Restablecer nodo	753
Restablecer nodoCifradosTlssuplementarios	756
Reiniciar la red	757
Reiniciar servicios	758
ConfigurarClúster	759
Configurar	761
Configurar configuración de red	763
SetNodeSSLCertificate	765
SetNodeSupplementalTlsCiphers	768
Cerrar	770
TestConnectEnsemble	771
TestConnectMvip	773
TestConnectSvip	777
Pruebas de manejo	782
Configuración de hardware de prueba	783
PruebaLocateCluster	785
Prueba de conectividad local	786
Configuración de red de prueba	789
Prueba de ping	792
Prueba de conectividad remota	795
Métodos de la API de replicación	798
orden de operaciones de emparejamiento de clústeres	798
Orden de operaciones de emparejamiento de volúmenes	799
Modos de replicación compatibles para clústeres emparejados	799
Emparejamiento de clústeres completo	800
Emparejamiento de volumen completo	801
ListClusterPairs	803
Lista de volúmenes emparejados activos	804
Modificar par de volúmenes	807
Eliminar par de clústeres	809
Eliminar par de volúmenes	810

Iniciar emparejamiento de clústeres	811
Emparejamiento de volumen inicial	813
Métodos de la API de seguridad	816
Agregar servidor de claves al proveedor Kmip	816
CrearKeyProviderKmip	817
CrearKeyServerKmip	819
Crear par de claves públicas y privadas	822
EliminarKeyProviderKmip	824
EliminarKeyServerKmip	825
Deshabilitar el cifrado en reposo	826
Habilitar cifrado en reposo	827
Solicitud de firma de certificado de cliente	830
ObtenerProveedorDeClavesKmip	831
ObtenerKeyServerKmip	832
Obtener información de cifrado de software en reposo	834
Proveedores de claves de lista Kmip	836
Lista de servidores clave Kmip	839
ModificarKeyServerKmip	843
Clave maestra de cifrado de software en reposo	846
Eliminar servidor de claves del proveedor Kmip	849
Firmar claves Ssh	850
TestKeyProviderKmip	854
Servidor de claves de prueba Kmip	855
Métodos de la API de SnapMirror	856
Abortar SnapMirrorRelationship	856
Relación BreakSnapMirror	857
BreakSnapMirrorVolume	858
Crear punto final de SnapMirror	860
CrearPuntoFinalDeSnapMirrorNoAdministrado	861
CrearRelaciónSnapMirror	862
CrearVolumenSnapMirror	864
Eliminar puntos finales de SnapMirror	865
EliminarRelacionesDeSnapMirror	866
Información de la versión de GetOntap	867
ObtenerIdentidadDeClústerDeSnapMirror	867
InicializarRelaciónSnapMirror	868
Agregados de ListSnapMirror	869
ListSnapMirrorEndpoints	870
ListSnapMirrorLuns	871
ListSnapMirrorNetworkInterfaces	872
Nodos de espejo de ListSnap	873
Políticas de espejo de ListSnap	874
Lista de horarios de reflejo de ajuste	875
Relaciones de espejo de ajuste de lista	875
ListSnapMirrorVolumes	877

Lista de servidores virtuales de SnapMirror	878
Modificar el punto final de SnapMirror	880
ModificarSnapMirrorEndpoint (no administrado)	880
Modificar relación de SnapMirror	881
ActualizarRelaciónSnapMirror	883
Relación de espejo de QuiesceSnap	884
Relación de ResumeSnapMirror	885
ResincronizarSnapMirrorRelationship	886
Métodos de la API de configuración del sistema	888
DeshabilitarBmcColdReset	888
Deshabilitar ClusterSsh	889
Deshabilitar SNMP	890
Habilitar reinicio en frío de Bmc	891
Habilitar ClusterSsh	892
Habilitar SNMP	894
ObtenerPropiedadesDeAsignaciónDeContenedor	895
Obtener información SSH del clúster	898
ObtenerEstructuraDeClúster	899
Informe GetFips	900
Obtener configuración de Lldp	902
Obtener información de Lldp	903
Informe de unidades GetNodeFips	904
Obtener información NTP	905
Obtener información de NVRAM	907
ObtenerDiseñoDeDominioDeProtección	908
Obtener hosts de registro remoto	910
Obtener ACL SNMP	911
Obtener información SNMP	912
Obtener estado SNMP	914
Obtener información de trampa SNMP	916
Obtener certificado SSL	917
Niveles de dominio de protección de listas	919
Eliminar certificado SSL	921
Restablecer configuración de red	922
Restablecer cifrados TLS suplementarios	923
Establecer estructura de clúster	924
ConfigurarLldp	925
SetNtpInfo	926
Establecer diseño de dominio de protección	928
Configurar hosts de registro remoto	931
SetSnmpACL	932
SetSnmpInfo	934
SetSnmpTrapInfo	937
Establecer certificado SSL	939
SnmpSendTestTraps	941

Disponibilidad de direcciones de prueba	942
Métodos de API de redes multiinquilino	944
Convenciones de nomenclatura de redes virtuales	944
Agregar red virtual	944
Modificar red virtual	947
Lista de redes virtuales	951
Eliminar red virtual	954
Métodos de la API de volumen	955
CancelarClon	955
CancelarClonDeGrupo	956
Clonar múltiples volúmenes	957
Clonar volumen	961
Volumen de copia	966
Crear política de QoS	968
Crear volumen	970
Crear destino de copia de seguridad	979
Eliminar política de QoS	980
Eliminar volumen	981
Eliminar volúmenes	984
ObtenerObjetivoDeCopiaDeSeguridad	987
Obtener estadísticas de volumen	989
Obtener QoS predeterminado	991
Obtener política de QoS	993
Obtener recuento de volumen	995
ObtenerEficiencia de Volumen	996
Listar volúmenes activos	998
ListBackupTargets	1000
Lista de trabajos de volumen masivo	1001
Lista de volúmenes eliminados	1003
Lista de políticas de QoS	1006
ListSyncJobs	1008
ListVolumeQoSHistogramas	1010
Lista de volúmenes	1012
Estadísticas de volumen de lista	1017
Listar volúmenes para la cuenta	1019
ListVolumeStatsByAccount	1022
Lista de estadísticas de volumen por volumen virtual	1024
Listar estadísticas de volumen por volumen	1026
Lista de estadísticas de volumen por grupo de acceso de volumen	1028
Modificar destino de copia de seguridad	1030
Modificar la política de QoS	1032
Modificar volumen	1034
Modificar volúmenes	1043
Purga de volumen eliminado	1052
Eliminar volúmenes eliminados	1053

Eliminar destino de copia de seguridad	1055
Restaurar volumen eliminado	1056
Establecer QoS predeterminado	1057
Iniciar lectura de volumen masivo	1059
Iniciar escritura masiva de volumen	1062
Actualizar estado del volumen masivo	1065
Métodos de la API de grupos de acceso por volumen	1068
AgregarIniciadoresAlGrupoDeAccesoPorVolumen	1068
Agregar volúmenes al grupo de acceso a volúmenes	1070
Crear grupo de acceso a volumen	1072
Eliminar grupo de acceso al volumen	1075
Listar grupos de acceso de volumen	1077
Eliminar volúmenes del grupo de acceso a volúmenes	1079
EliminarIniciadoresDelGrupoDeAccesoPorVolumen	1081
Modificar grupo de acceso al volumen	1084
ObtenerEficienciaDeGrupoDeAccesoDeVolumen	1088
Métodos de la API de instantáneas de volumen	1090
Resumen de instantáneas	1090
CrearInstantáneaDeGrupo	1090
Crear horario	1097
Crear instantánea	1110
Eliminar instantánea de grupo	1116
Eliminar instantánea	1118
Obtener horario	1119
Lista de instantáneas de grupo	1121
Listas de horarios	1124
Instantáneas de la lista	1126
Modificar instantánea de grupo	1128
Modificar horario	1132
Modificar instantánea	1139
Revertir a instantánea de grupo	1143
Revertir a instantánea	1148
Métodos de la API de volumen virtual	1151
CrearContenedorDeAlmacenamiento	1151
Eliminar contenedores de almacenamiento	1152
Obtener la eficiencia del contenedor de almacenamiento	1154
Obtener recuento de volúmenes virtuales	1155
ListProtocolEndpoints	1156
Listar contenedores de almacenamiento	1159
ListVirtualVolumeBindings	1160
Listar hosts de volumen virtual	1162
Listar volúmenes virtuales	1164
Listar tareas de volumen virtual	1168
ModificarContenedorDeAlmacenamiento	1169
Control de acceso	1171

cuentas	1171
administrador	1172
administrador del clúster	1172
unidades	1175
nodos	1175
leer	1176
informes	1177
repositorios	1179
volúmenes	1179
escribir	1180
Ejemplos de respuesta	1181
Obtener configuración	1181
Obtener información de hardware del clúster	1184
Obtener información de Lldp	1198
Obtener configuración de red	1227
GetNodeHardwareInfo (salida para iSCSI)	1231
GetNodeHardwareInfo (salida para nodos Fibre Channel)	1233
Obtener información de NVRAM	1241
Lista de nodos activos	1249
Listar volúmenes activos	1253
Configuración de hardware de prueba	1262
Plugin de NetApp Element para vCenter Server	1268
Para más información	1268
Monitorea el almacenamiento con SolidFire Active IQ	1269
Para más información	1269
Trabajar con el nodo de gestión	1270
Descripción general del nodo de gestión	1270
Instalar o recuperar un nodo de administración	1271
Instalar un nodo de administración	1271
Cree un rol de NetApp HCC en vCenter	1278
Configurar un controlador de interfaz de red (NIC) de almacenamiento	1283
Recuperar un nodo de administración	1285
Acceda al nodo de administración	1290
Acceda a la interfaz de usuario de administración por nodo	1290
Acceda a la interfaz de usuario de la API REST del nodo de administración	1291
Cambiar el certificado SSL predeterminado del nodo de administración	1292
Encuentra más información	1293
Trabajar con la interfaz de usuario del nodo de administración	1293
Descripción general de la interfaz de usuario del nodo de administración	1293
Configurar la monitorización de alertas	1294
Modifique y pruebe la configuración de la red, el clúster y el sistema del nodo de administración	1294
Ejecutar utilidades del sistema desde el nodo de administración	1296
Trabajar con la API REST del nodo de administración	1297
Descripción general de la interfaz de usuario de la API REST del nodo de administración	1297
Obtén autorización para usar las API REST	1298

Habilitar Active IQ y la monitorización de NetApp	1299
Configurar NetApp Hybrid Cloud Control para varios vCenters	1302
Agregar un activo de controlador al nodo de administración	1303
Crear y administrar activos de clúster de almacenamiento	1304
Ver o editar los recursos del controlador existentes	1310
Configurar un servidor proxy	1311
Verifique las versiones del sistema operativo y los servicios del nodo de administración	1313
Obtención de registros de los servicios de administración	1314
Gestionar conexiones de soporte	1315
Acceso a nodos de almacenamiento mediante SSH para la resolución de problemas básicos	1315
Inicie una sesión de soporte remoto de NetApp	1320
Gestionar la funcionalidad SSH en el nodo de administración	1321
Actualice su sistema de almacenamiento totalmente flash NetApp SolidFire	1325
Descripción general de la secuencia de actualización	1325
Secuencia de actualización del sistema	1326
Procedimientos de actualización del sistema	1327
Ejecute las comprobaciones de estado del almacenamiento de Element antes de actualizar el almacenamiento	1327
Actualizar un nodo de administración	1332
Servicios de gestión de actualizaciones	1336
Actualizar el software Element	1339
Actualizar el firmware de almacenamiento	1351
Actualizar el complemento Element para vCenter Server	1361
Actualice sus componentes de vSphere para un sistema de almacenamiento NetApp SolidFire con el complemento Element para vCenter Server	1368
Encuentra más información	1369
Documentación de versiones anteriores del software SolidFire y NetApp Element	1370
Para más información	1370
Avisos legales	1371
Copyright	1371
Marcas comerciales	1371
Patentes	1371
Política de privacidad	1371
Código abierto	1371

Documentación del software SolidFire y Element

Notas de la versión

Información sobre versiones actuales y anteriores

Aquí encontrará enlaces a las notas de la versión más reciente y anteriores de varios componentes del entorno de almacenamiento Element.



Se le solicitará que inicie sesión utilizando sus credenciales de soporte de NetApp .

Software NetApp Element

- ["Notas de la versión 12.8 del software NetApp Element"](#)
- ["Notas de la versión 12.7 del software NetApp Element"](#)
- ["Notas de la versión 12.5 del software NetApp Element"](#)
- ["Notas de la versión 12.3.2 del software NetApp Element"](#)
- ["Notas de la versión 12.3.1 del software NetApp Element"](#)
- ["Notas de la versión 12.3 del software NetApp Element"](#)
- ["Notas de la versión 12.2.1 del software NetApp Element"](#)
- ["Notas de la versión 12.2 del software NetApp Element"](#)
- ["Notas de la versión 12.0.1 del software NetApp Element"](#)
- ["Notas de la versión 12.0 del software NetApp Element"](#)
- ["Notas de la versión 11.8.2 del software NetApp Element"](#)
- ["Notas de la versión 11.8.1 del software NetApp Element"](#)
- ["Notas de la versión 11.8 del software NetApp Element"](#)
- ["Notas de la versión 11.7 del software NetApp Element"](#)
- ["Notas de la versión 11.5.1 del software NetApp Element"](#)
- ["Notas de la versión 11.3P1 del software NetApp Element"](#)

Servicios de administración

- ["Notas de la versión de los servicios de gestión"](#)

Plugin de NetApp Element para vCenter Server

- ["Notas de la versión del complemento vCenter 5.5"](#)*Nuevo*
- ["Notas de la versión del complemento vCenter 5.4"](#)
- ["Notas de la versión del complemento vCenter 5.3"](#)
- ["Notas de la versión del complemento vCenter 5.2"](#)
- ["Notas de la versión del complemento vCenter 5.1"](#)
- ["Notas de la versión del complemento vCenter 5.0"](#)
- ["Notas de la versión del complemento vCenter 4.10"](#)

- ["Notas de la versión del complemento vCenter 4.9"](#)
- ["Notas de la versión del complemento vCenter 4.8"](#)
- ["Notas de la versión del complemento vCenter 4.7"](#)
- ["Notas de la versión del complemento vCenter 4.6"](#)
- ["Notas de la versión del complemento vCenter 4.5"](#)
- ["Notas de la versión del complemento vCenter 4.4"](#)
- ["Notas de la versión del complemento vCenter 4.3"](#)

Firmware de almacenamiento

- ["Notas de la versión 2.182.0 del paquete de firmware de almacenamiento"](#)**NUEVO**
- ["Notas de la versión 2.175.0 del paquete de firmware de almacenamiento"](#)
- ["Notas de la versión 2.164.0 del paquete de firmware de almacenamiento"](#)
- ["Notas de la versión 2.150 del paquete de firmware de almacenamiento"](#)
- ["Notas de la versión 2.146 del paquete de firmware de almacenamiento"](#)
- ["Notas de la versión 2.99.2 del paquete de firmware de almacenamiento"](#)
- ["Notas de la versión 2.76 del paquete de firmware de almacenamiento"](#)
- ["Notas de la versión 2.27 del paquete de firmware de almacenamiento"](#)
- ["Notas de la versión 3.84.07 de H610S BMC"](#)
- ["Versiones de firmware y controladores ESXi compatibles"](#)**NUEVO**

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

¿Qué novedades hay en el software Element?

NetApp actualiza periódicamente el software SolidFire y Element para ofrecerle nuevas funciones, mejoras y correcciones de errores. Element 12.8 es la última versión e incluye actualizaciones de seguridad y componentes del sistema, mejoras operativas y problemas resueltos.



Las actualizaciones acumulativas de software y firmware se instalan como parte de una actualización de Element 12.8 basada en la versión actual de Element que se ejecuta en un clúster de almacenamiento. Por ejemplo, si un clúster actualmente ejecuta Element 12.5, puede actualizar directamente a Element 12.8 para obtener las actualizaciones acumulativas tanto de Element 12.7 como de 12.8. Para conocer las rutas de actualización compatibles, consulte el artículo de la base de conocimientos. "[¿Cuál es la matriz de actualización para clústeres de almacenamiento que ejecutan el software NetApp Element?](#)" .

Elemento 12.8

Obtén más información sobre las novedades de Element 12.8.

Balanceo de carga de volumen

El elemento 12.8 introduce la función de balanceo de carga de volumen. Puede utilizar esta función para equilibrar los volúmenes entre los nodos en función del nivel de IOPS real de cada volumen en lugar de las IOPS mínimas configuradas en la política de QoS. Solo puede utilizar la función de balanceo de carga de volumen para equilibrar volúmenes. No se puede utilizar para equilibrar volúmenes virtuales. La función de balanceo de carga de volumen está desactivada por defecto. Puedes activarlo y desactivarlo usando el `VolumeLoadBalanceOnActualIOPS` parámetro de API con el ["Habilitar función"](#) y ["Deshabilitar función"](#) métodos de la API o utilizando el ["Balanceo de carga de volumen"](#) opción en la interfaz de usuario de Element.

Información sobre la utilización del nodo de visualización

Con Element 12.8, puede ver la información de utilización de nodos como `nodeHeat` usando el `GetNodeStats` y `ListNodeStats` Métodos de la API. El `nodeHeat` El objeto es un miembro de la `nodeStats` Este objeto muestra información sobre la utilización del nodo en función de la relación entre las IOPS totales primarias o las IOPS totales y las IOPS configuradas promediadas en el tiempo.

Además, puede ver la utilización del nodo como un porcentaje de `recentPrimaryTotalHeat` en la pantalla Ver detalles de un nodo en la interfaz de usuario de Element.

Consulta las estadísticas de E/S de un volumen.

Con Element 12.8, puede ver las estadísticas de uso de E/S de un volumen como `sliceIopsStats` usando el `GetVolumeStats` y `ListVolumeStatsByVolume` Métodos de la API. Las estadísticas de E/S se calculan utilizando la información de IOPS de lectura y escritura para el volumen y se miden durante dos períodos de tiempo: las últimas 24 horas y la última hora. ["Más información"](#).

Algoritmo CHAP para sesión iSCSI

Un iniciador iSCSI host solicita una lista de algoritmos del protocolo de autenticación Challenge-Handshake (CHAP) para usar cuando crea una sesión iSCSI con un destino iSCSI Element. A partir de Element 12.8, puede ver el algoritmo CHAP compatible que el destino iSCSI de Element elige usar para una sesión iSCSI.

Actualizar la versión del hardware de la máquina virtual

Si va a realizar una actualización in situ de un nodo de administración existente a Element 12.8, antes de actualizar, debe asegurarse de que la versión del hardware de la máquina virtual en el nodo de administración sea compatible con ESXi 6.7 (versión de hardware de la máquina virtual 14) o posterior, según su entorno. ["Más información"](#).

Elemento 12.7

Obtén más información sobre las novedades de Element 12.7.

Algoritmos CHAP seguros

El elemento 12.7 incluye soporte para los algoritmos de protocolo de autenticación de desafío-comunicación (CHAP) seguros compatibles con FIPS SHA1, SHA-256 y SHA3-256. ["Más información"](#).

Tasa de sincronización de bloques dinámicos (bin)

Las operaciones del clúster, como adiciones, actualizaciones o mantenimiento de nodos, o adición de unidades, etc., activan la sincronización de bloques (bin) para distribuir los datos de bloques a los nodos nuevos o actualizados en una disposición del clúster. Utilizar una única velocidad lenta como tasa de

sincronización predeterminada provoca que estas operaciones tarden mucho tiempo y no aprovecha la mayor potencia de procesamiento de los nodos más grandes. A partir de Element 12.7, la velocidad de sincronización se ajusta dinámicamente en función del número de núcleos del nodo de almacenamiento, lo que permite que estas operaciones se realicen de forma significativamente más rápida.

Por ejemplo, cuando se agregan nodos de almacenamiento grandes de 28 núcleos (H610S, SF19210 y SF38410) que ejecutan Element 12.7 a un clúster existente, la velocidad de sincronización de entrada de datos se ajusta automáticamente a 110 Mbps en lugar de 60 Mbps. Además, cuando se sacan estos grandes nodos de almacenamiento del modo de mantenimiento de nodos, por ejemplo, durante una actualización de Element 12.3.x o posterior a Element 12.7 mediante NetApp Hybrid Cloud Control, la velocidad de sincronización para la velocidad de datos de bloques modificada se ajusta automáticamente a 110 Mbps en lugar de 20 Mbps.

Cuando se agregan nodos de almacenamiento medianos de 16 núcleos (H410S) y nodos de almacenamiento pequeños de 12 núcleos (SF4805) a un clúster Element 12.7, la velocidad de sincronización de datos se mantiene en 60 Mbps; sin embargo, para sincronizar los bloques modificados cuando se sacan del modo de mantenimiento de nodos durante las actualizaciones de Element 12.3.x a Element 12.7, la velocidad de sincronización se ajusta automáticamente de 20 Mbps a 60 Mbps para los nodos de almacenamiento medianos y a 40 Mbps para los nodos de almacenamiento más pequeños.

Al eliminar nodos de almacenamiento, no se produce ningún impacto en la tasa de sincronización de bloques, lo que evita repercusiones en el rendimiento de las operaciones de E/S del cliente.

Mejora de la recolección de basura

Para clústeres con nodos de almacenamiento más grandes, por ejemplo, un H610S-4, que tienen 1 PB de espacio utilizado, ejecutan cargas de trabajo muy altas con sobrescrituras y tienen una alta deduplicación y compresión, la operación de recolección de basura ahora puede mantenerse al día ya que el tamaño del filtro Bloom predeterminado se ha incrementado para los nodos más grandes de 700 GB o más de memoria a 1048576 bits. Este cambio se aplica automáticamente después de actualizar sus nodos de almacenamiento a Element 12.7 y no tiene ningún impacto en los nodos más pequeños.

Mejora de escala

Con Element 12.7, ya no es necesario seguir una secuencia específica al agregar varios nodos de almacenamiento de unidades de bloques y metadatos a un clúster existente. Utilizando la interfaz de usuario o la API de Element, puede seleccionar fácilmente todas las unidades disponibles y agregarlas en bloque simultáneamente. Element 12.7 gestiona automáticamente la sincronización de datos para que todos los servicios de bloques se sincronicen simultáneamente. Una vez que los servicios de bloques de cada nodo completan la sincronización, la unidad de metadatos de ese nodo se puede asignar a los volúmenes del host. Esta mejora de escala reduce significativamente la latencia de respuesta de lectura y evita la degradación del rendimiento mientras se sincronizan los datos en los nodos de almacenamiento recién añadidos.

Actualizaciones de firmware de nodos de almacenamiento

Element 12.7 incluye el paquete de firmware de almacenamiento versión 2.164.0, que incluye soporte para nuevos componentes del sistema. ["Más información"](#).



No hay nuevas actualizaciones de firmware en la versión Element 12.7. Sin embargo, según el paquete de firmware actual que se ejecuta en los nodos de almacenamiento, las actualizaciones acumulativas se instalan cuando actualiza a Element 12.7.

Documentación de SolidFire Active IQ

En la interfaz de usuario de SolidFire Active IQ, ahora puede navegar a la página de administración de QoS para ver las recomendaciones y la información de limitación de nodos para su clúster. Además, el panel de control del clúster ahora muestra el recuento total de instantáneas. Otras mejoras recientes incluyen la adición de información de nodos primarios y secundarios para volúmenes activos y el rendimiento promedio, IOPS y latencia promedio de los últimos 30 minutos en los volúmenes primarios de un nodo.

Ahora puede acceder a la documentación de SolidFire Active IQ desde la documentación del software Element. ["Más información"](#).

NetApp Bugs Online contiene información sobre problemas conocidos y resueltos.

Los problemas resueltos y conocidos se enumeran en la herramienta NetApp Bugs Online. Puedes consultar estos temas para el software Element y otros productos en ["Errores de NetApp en línea"](#).

Elemento 12.5

Obtén más información sobre las novedades de Element 12.5.

Acceso mejorado al nodo de almacenamiento

Element 12.5 introduce un acceso remoto mejorado a nodos individuales mediante certificados SSH firmados. Para proporcionar acceso remoto seguro a los nodos de almacenamiento, se ha creado una nueva cuenta de usuario local con privilegios limitados llamada `sfreadonly`. Ahora se crea durante RTFI de un nodo de almacenamiento. El `sfreadonly` La cuenta permite el acceso al backend del nodo de almacenamiento para tareas básicas de mantenimiento o solución de problemas. Ahora puedes configurar el `supportAdmin` Tipo de acceso para un usuario administrador de clúster que permita al soporte de NetApp acceder al clúster según sea necesario.

Gestión mejorada de dominios de protección personalizados

Element 12.5 presenta una nueva interfaz de usuario que le permite ver de forma rápida y sencilla los dominios de protección personalizados existentes y configurar nuevos dominios de protección personalizados.

Nuevas y mejoradas funciones de detección de fallos, eventos y alertas en clústeres

Element 12.5 mejora la resolución de problemas del sistema con la introducción de los nuevos códigos de error del clúster. `BmcSelfTestFailed` y `CpuThermalEventThreshold`. El elemento 12.5 también incluye mejoras de robustez para los eventos y alertas de clúster existentes, tales como: `nodeOffline`, `volumeOffline`, `driveHealthFault`, `networkEvent`, y `cSumEvent`.

Habilite el cifrado de software en reposo desde la interfaz de usuario de creación de clúster.

Con la incorporación de una nueva casilla de verificación en la interfaz de usuario Crear clúster, Element 12.5 le ofrece la opción de habilitar el cifrado de software en reposo para clústeres de almacenamiento all-flash SolidFire durante la creación del clúster.

Actualizaciones de firmware de nodos de almacenamiento

Element 12.5 incluye actualizaciones de firmware para nodos de almacenamiento. ["Más información"](#).

Seguridad mejorada

El elemento 12.5 contiene la mitigación que cierra la exposición del software Element a la vulnerabilidad de Apache Log4j. Los clústeres de almacenamiento NetApp SolidFire con la función de volúmenes virtuales (VVols) habilitada están expuestos a la vulnerabilidad de Apache Log4j. Para obtener información sobre la solución alternativa para la vulnerabilidad de Apache Log4j en el software NetApp Element , consulte el artículo de la base de conocimientos [KB article](#).

Si está ejecutando Element 11.x, 12.0 o 12.2 o su clúster de almacenamiento ya está en Element 12.3 o 12.3.1 con la función VVols habilitada, debería actualizar a 12.5.

El elemento 12.5 también incluye más de 120 correcciones de vulnerabilidades de seguridad CVE.

Encuentra más información

- ["Notas de la versión de los servicios de control y gestión de la nube híbrida de NetApp"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Centro de documentación de SolidFire y Element Software para versiones anteriores"](#)
- ["Documentación de NetApp HCI"](#)
- ["Versiones de firmware de almacenamiento compatibles para nodos de almacenamiento SolidFire"](#)

Conceptos

Aprende conceptos básicos relacionados con el software Element.

- ["Descripción general del producto"](#)
- [Descripción general de la arquitectura de SolidFire](#)
- [Nodos](#)
- [Clústeres](#)
- ["Seguridad"](#)
- [Cuentas y permisos](#)
- ["Volúmenes"](#)
- [Protección de datos](#)
- [Rendimiento y calidad del servicio](#)

Descripción general del producto

Un sistema de almacenamiento all-flash SolidFire se compone de componentes de hardware discretos (unidades y nodos) que se combinan en un único conjunto de recursos de almacenamiento. Este clúster unificado se presenta como un único sistema de almacenamiento para uso de clientes externos y se gestiona con el software NetApp Element .

Utilizando la interfaz Element, la API u otras herramientas de administración, puede supervisar la capacidad y el rendimiento del almacenamiento del clúster SolidFire y administrar la actividad de almacenamiento en una infraestructura multiinquilino.

Características de SolidFire

Un sistema Solidfire ofrece las siguientes características:

- Ofrece almacenamiento de alto rendimiento para su infraestructura de nube privada a gran escala.
- Proporciona una escala flexible que le permite satisfacer las necesidades de almacenamiento cambiantes.
- Utiliza una interfaz de software Element para la gestión del almacenamiento basada en API.
- Garantiza el rendimiento mediante políticas de calidad de servicio.
- Incluye balanceo de carga automático en todos los nodos del clúster.
- Reequilibra los clústeres automáticamente cuando se añaden o se eliminan nodos.

Despliegue de SolidFire

Utilice nodos de almacenamiento proporcionados por NetApp e integrados con el software NetApp Element .

["Descripción general de la arquitectura de almacenamiento totalmente flash de SolidFire"](#)

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)

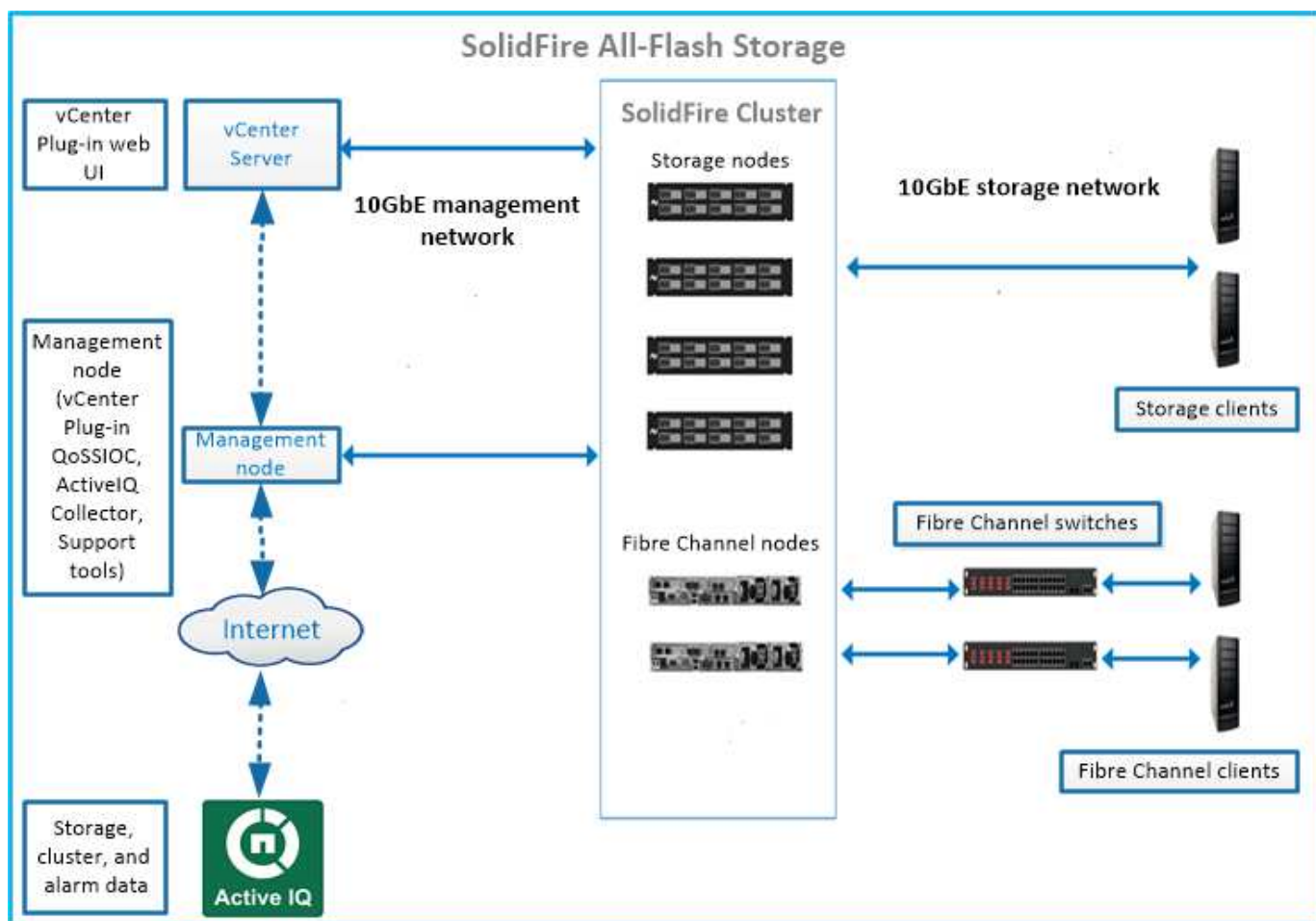
Arquitectura y componentes

Conozca la arquitectura de SolidFire

Un sistema de almacenamiento all-flash SolidFire se compone de componentes de hardware discretos (unidades y nodos) que se combinan en un conjunto de recursos de almacenamiento con el software NetApp Element ejecutándose de forma independiente en cada nodo. Este sistema de almacenamiento único se gestiona como una sola 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:

- **Clúster:** El núcleo del sistema de almacenamiento SolidFire que es una colección de nodos.
- **Nodos:** Los componentes de hardware agrupados en un clúster. 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
- **Unidades:** Se utilizan 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 volumen almacenan información que define los volúmenes y otros objetos dentro de un clúster.
 - Las unidades de bloque almacenan bloques de datos para volúmenes.



Puede administrar, supervisar y actualizar el sistema utilizando la interfaz web de Element y otras herramientas compatibles:

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

URL comunes

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

URL	Descripción
<code>https://[storage cluster MVIP address]</code>	Acceda a la interfaz de usuario del software NetApp Element .
<code>https://activeiq.solidfire.com</code>	Supervise los datos y reciba alertas sobre cualquier cuello de botella en el rendimiento o posibles problemas del sistema.
<code>https://[management node IP address]</code>	Acceda a NetApp Hybrid Cloud Control para actualizar su instalación de almacenamiento y los servicios de administración de actualizaciones.

URL	Descripción
<code>https://[IP address]:442</code>	Desde la interfaz de usuario de cada nodo, acceda a la configuración de red y clúster y utilice las pruebas y utilidades del sistema. "Más información."
<code>https://[management node IP address]/mnode</code>	Utilice la API REST de servicios de gestión y otras funcionalidades del nodo de gestión. "Más información."
<code>https://[management node IP address]:9443</code>	Registre el paquete de complementos de vCenter en el cliente web de vSphere. "Más información."

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

interfaces de software SolidFire

Puede administrar un sistema de almacenamiento SolidFire utilizando diferentes interfaces de software y utilidades de integración de NetApp Element .

Opciones

- [Interfaz de usuario del software NetApp Element](#)
- [API del software NetApp Element](#)
- [Plugin de NetApp Element para vCenter Server](#)
- [Control de nube híbrida de NetApp](#)
- [interfaces de usuario de nodos de administración](#)
- [Utilidades y herramientas de integración adicionales](#)

Interfaz de usuario del software NetApp Element

Le permite configurar el almacenamiento de Element, supervisar la capacidad y el rendimiento del clúster y gestionar la actividad de almacenamiento en una infraestructura multiinquilino. Element es el sistema operativo de almacenamiento que constituye el núcleo de un clúster SolidFire . El software Element se ejecuta de forma independiente en todos los nodos del clúster y permite que los nodos del clúster combinen recursos que se presentan como un único sistema de almacenamiento a los clientes externos. El software Element es responsable de toda la coordinación del clúster, la escalabilidad y la gestión del sistema en su conjunto. La interfaz de software está construida sobre la API de Element.

["Gestiona el almacenamiento con el software Element."](#)

API del software NetApp Element

Te permite utilizar un conjunto de objetos, métodos y rutinas para gestionar el almacenamiento de elementos. La API de Element se basa en el protocolo JSON-RPC sobre HTTPS. Puedes supervisar las operaciones de la API en la interfaz de usuario de Element habilitando el registro de la API; esto te permite ver los métodos que se están enviando al sistema. Puedes habilitar tanto las solicitudes como las respuestas para ver cómo responde el sistema a los métodos que se emiten.

["Gestiona el almacenamiento con la API de Element"](#)

Plugin de NetApp Element para vCenter Server

Le permite configurar y administrar clústeres de almacenamiento que ejecutan el software Element utilizando una interfaz alternativa para la interfaz de usuario de Element dentro de VMware vSphere.

["Plugin de NetApp Element para vCenter Server"](#)

Control de nube híbrida de NetApp

Le permite actualizar los servicios de almacenamiento y administración de Element y administrar los activos de almacenamiento utilizando la interfaz de NetApp Hybrid Cloud Control.

["Administre y supervise el almacenamiento con NetApp Hybrid Cloud Control."](#)

interfases de usuario de nodos de administración

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

Utilidades y herramientas de integración adicionales

Aunque normalmente se administra el almacenamiento con NetApp Element, NetApp Element API y NetApp Element Plug-in para vCenter Server, se pueden utilizar utilidades y herramientas de integración adicionales para acceder al almacenamiento.

CLI de Element

["CLI de Element"](#) le permite controlar un sistema de almacenamiento SolidFire mediante una interfaz de línea de comandos sin necesidad de utilizar la API de Element.

Herramientas de PowerShell de Element

["Herramientas de PowerShell de Element"](#) le permite utilizar una colección de funciones de Microsoft Windows PowerShell que utilizan la API de Element para administrar un sistema de almacenamiento SolidFire .

SDK de elementos

["SDK de elementos"](#) le permiten administrar su clúster SolidFire utilizando estas 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 Element con el lenguaje de programación Python.

Suite de pruebas de la API Postman de SolidFire

Permite a los programadores utilizar una colección de ["Cartero"](#) funciones que prueban las llamadas a la 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 SolidFire replicados y ejecutar flujos de trabajo compatibles.

SolidFire vRO

"[SolidFire vRO](#)" Proporciona una forma práctica de usar la API de Element para administrar su sistema de almacenamiento SolidFire con VMware vRealize Orchestrator.

Proveedor VSS de SolidFire

"[Proveedor VSS de SolidFire](#)" Integra las copias de sombra de VSS con las instantáneas y clones de Element.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

SolidFire Active IQ

"[SolidFire Active IQ](#)" Es una herramienta basada en la web que proporciona vistas históricas actualizadas continuamente de los datos de todo el clúster. Puedes configurar alertas para eventos, umbrales o métricas específicas. SolidFire Active IQ le permite supervisar el rendimiento y la capacidad del sistema, así como mantenerse informado sobre el estado del clúster.

En SolidFire Active IQ encontrará la siguiente información sobre su sistema:

- Número de nodos y estado de los nodos: sano, fuera de línea o con fallos.
- Representación gráfica del uso de CPU y memoria, y de la limitación de nodos.
- 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 de las máquinas virtuales

Para obtener más información sobre SolidFire Active IQ, consulte la "[Documentación de SolidFire Active IQ](#)".

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- [Sitio de soporte de NetApp](#) > [Herramientas para Active IQ](#)

Nodo de gestión para el software Element

El "[nodo de gestión \(mNode\)](#)" es una máquina virtual que se ejecuta en paralelo con uno o más clústeres de almacenamiento basados en software Element. Se utiliza para

actualizar y proporcionar servicios del sistema, incluyendo monitoreo y telemetría, administrar los activos y la configuración del clúster, ejecutar pruebas y utilidades del sistema y habilitar el acceso al soporte de NetApp para la resolución de problemas.

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

A partir de la versión Element 11.3, el nodo de administración funciona como un host de microservicios, lo que permite actualizaciones más rápidas de servicios de software seleccionados fuera de las versiones principales. Estos microservicios o "[servicios de administración](#)" se actualizan con frecuencia como paquetes de servicios.

Servicios de gestión para almacenamiento all-flash SolidFire

A partir de la versión 11.3 de Element, los **servicios de gestión** se alojan en el "[nodo de gestión](#)", lo que permite actualizaciones más rápidas de determinados servicios de software fuera de las versiones principales.

Los servicios de gestión proporcionan funcionalidades de gestión centralizadas y extendidas para el almacenamiento all-flash SolidFire. Estos servicios incluyen "[Control de nube híbrida de NetApp](#)", Telemetría, registro y actualizaciones de servicio del sistema Active IQ, así como el servicio QoSSIOC para el complemento Element para vCenter.



Obtenga más información sobre "[Lanzamientos de servicios de gestión](#)".

Nodos

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

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

- [Nodo de gestión](#)
- [Nodo de almacenamiento](#)
- [Nodo de canal de fibra](#)

[Estados de los nodos](#) varían según la asociación del grupo.

Nodo de gestión

Un nodo de administración es una máquina virtual que se utiliza para actualizar y proporcionar servicios del sistema, incluidos el monitoreo y la telemetría, administrar los activos y la configuración del clúster, ejecutar pruebas y utilidades del sistema y habilitar el acceso al soporte de NetApp para la resolución de problemas. "[Más información](#)"

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 del nodo contienen espacio de bloques y metadatos para el almacenamiento y la gestión de datos. Cada nodo contiene una imagen de fábrica del 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 utilizará por defecto SF-XXXX, donde XXXX son cuatro caracteres aleatorios generados por el sistema.
- Cada nodo tiene su propia memoria caché de escritura de memoria de acceso aleatorio no volátil (NVRAM) de alto rendimiento para mejorar el rendimiento general del sistema y reducir la latencia de escritura.
- Cada nodo está conectado a dos redes, una de almacenamiento y otra de gestión, cada una con dos enlaces independientes para redundancia y rendimiento. Cada nodo requiere una dirección IP en cada red.
- Puede crear un clúster con nuevos nodos de almacenamiento o agregar nodos de almacenamiento a un clúster existente para aumentar la capacidad y el rendimiento del almacenamiento.
- Puede agregar o eliminar nodos del clúster en cualquier momento sin interrumpir el servicio.

Nodo de canal de fibra

Los nodos Fibre Channel de SolidFire proporcionan conectividad a un conmutador Fibre Channel, al que puede conectar clientes Fibre Channel. Los nodos Fibre Channel actúan como un convertidor de protocolo entre los protocolos Fibre Channel e iSCSI; esto le permite agregar conectividad Fibre Channel a cualquier clúster SolidFire nuevo o existente.

Los nodos Fibre Channel tienen las siguientes características:

- Los conmutadores Fibre Channel gestionan el estado de la estructura, proporcionando interconexiones optimizadas.
- El tráfico entre dos puertos fluye únicamente a través de los conmutadores; no se transmite a ningún otro puerto.
- El fallo de un puerto es aislado y no afecta al funcionamiento de los demás puertos.
- En una estructura, varios pares de puertos pueden comunicarse simultáneamente.

Estados de operación de los nodos

Un nodo puede estar en uno de varios estados dependiendo del nivel de configuración.

- **Disponible**

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

- **Pendiente**

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

No se requiere autenticación para acceder al nodo.

- **Activo pendiente**

El sistema está en proceso de instalar el software Element compatible en el nodo. Una vez completado, el nodo pasará al estado Activo.

- **Activo**

El nodo participa en un clúster.

Se requiere autenticación para modificar el nodo.

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

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Clústeres

Un clúster es el centro de un sistema de almacenamiento SolidFire y está formado por una colección de nodos. Para aprovechar al máximo la eficiencia del almacenamiento de SolidFire, debe tener al menos cuatro nodos en un clúster. Un clúster aparece en la red como un único grupo lógico y, por lo tanto, se puede acceder a él como almacenamiento en bloque.

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

Puedes escalar horizontalmente un clúster añadiendo nodos adicionales. Al agregar un nuevo nodo, no se interrumpe el servicio y el clúster utiliza automáticamente el rendimiento y la capacidad del nuevo nodo.

Los administradores y los anfitriones pueden acceder al clúster utilizando direcciones IP virtuales. Cualquier nodo del clúster puede alojar las direcciones IP virtuales. La IP virtual de gestión (MVIP) permite la gestión del clúster a través de una conexión de 1 GbE, mientras que la IP virtual de almacenamiento (SVIP) permite el acceso del host al almacenamiento a través de una conexión de 10 GbE. Estas direcciones IP virtuales permiten conexiones consistentes independientemente del tamaño o la composición de un clúster SolidFire. Si falla un nodo que aloja una dirección IP virtual, 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 direcciones IPv4, IPv6 o ambas para su red de administración. Esto se aplica tanto a los nodos de almacenamiento como a los nodos de administración, excepto al nodo de administración 11.3 y posteriores, que no admiten IPv6. Al crear un clúster, solo se puede usar una única dirección IPv4 o IPv6 para MVIP y el tipo de dirección correspondiente debe configurarse en todos los nodos.

Más sobre clústeres

- [clústeres de almacenamiento autorizados](#)

- [Regla de los tercios](#)
- [capacidad varada](#)
- [Eficiencia de almacenamiento](#)
- [quórum del clúster de almacenamiento](#)

clústeres de almacenamiento autorizados

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

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

Muchas funciones de NetApp Hybrid Cloud Control están diseñadas para funcionar con múltiples clústeres de almacenamiento, pero la autenticación y la autorización tienen limitaciones. La limitación en torno a la autenticación y autorización es que el usuario del clúster autoritativo puede ejecutar acciones en otros clústeres vinculados a NetApp Hybrid Cloud Control incluso si no es usuario en los otros clústeres de almacenamiento.

Antes de proceder a administrar varios clústeres de almacenamiento, debe asegurarse de que los usuarios definidos en los clústeres autorizados estén definidos en todos los demás clústeres de almacenamiento con los mismos permisos. Puedes gestionar los usuarios desde el "[Interfaz de usuario del software Element](#)".

Ver "[crear y administrar activos de clúster de almacenamiento](#)" Para obtener más información sobre cómo trabajar con los recursos del clúster de almacenamiento del nodo de administración.

Regla de los tercios

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

capacidad varada

Si un nodo recién agregado representa más del 50 por ciento de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("varada"), de modo que cumpla con la regla de capacidad. Esta situación se mantendrá hasta que se añada más capacidad de almacenamiento. Si se añade un nodo muy grande que también incumple la regla de capacidad, el nodo que antes estaba aislado dejará de estarlo, mientras que el nodo recién añadido quedará aislado. La capacidad siempre debe añadirse por pares para evitar que esto suceda. Cuando un nodo queda aislado, se genera un fallo de clúster apropiado.

Eficiencia de almacenamiento

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

- **Compresión**

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

- **Desduplicación**

La deduplicación reduce la cantidad de almacenamiento físico necesario para un volumen al descartar bloques de datos duplicados.

- **Aprovisionamiento ligero**

Un volumen de aprovisionamiento ligero o LUN es aquel para el cual no se reserva almacenamiento por adelantado. En cambio, el almacenamiento se asigna dinámicamente, según se necesite. Cuando se eliminan datos del volumen o LUN, el espacio libre se devuelve al sistema de almacenamiento.

quórum del clúster de almacenamiento

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

Seguridad

Cuando utiliza su sistema de almacenamiento totalmente flash SolidFire, sus datos están protegidos por protocolos de seguridad estándar del sector.

Cifrado en reposo (hardware)

Todas las unidades en los nodos de almacenamiento son capaces de utilizar el cifrado AES de 256 bits a nivel de unidad. Cada unidad tiene su propia clave de cifrado, que se crea cuando la unidad se inicializa por primera vez. Al habilitar la función de cifrado, se crea una contraseña para todo el clúster y, a continuación, se distribuyen fragmentos de la contraseña a todos los nodos del clúster. Ningún nodo individual almacena la contraseña completa. La contraseña se utiliza entonces para proteger con contraseña todo el acceso a las unidades. La contraseña es necesaria para desbloquear la unidad y luego no se necesita a menos que se desconecte la alimentación de la unidad o se bloquee la unidad.

["Habilitar la función de cifrado de hardware en reposo"](#) No afecta al rendimiento ni a la eficiencia del clúster. Si se elimina una unidad o nodo con cifrado habilitado de la configuración del clúster mediante la API de Element o la interfaz de usuario de Element, se deshabilitará el cifrado en reposo en las unidades. Una vez extraída la unidad, se puede borrar de forma segura utilizando el método `SecureEraseDrives` Método API. Si se extrae por la fuerza una unidad o nodo físico, los datos permanecen protegidos por la contraseña de todo el clúster y las claves de cifrado individuales de la unidad.

Cifrado en reposo (software)

Otro tipo de cifrado en reposo, el cifrado en reposo por software, permite cifrar todos los datos escritos en las unidades SSD de un clúster de almacenamiento. ["Cuando está habilitado"](#) Encripta todos los datos escritos y descifra todos los datos leídos automáticamente en el software. El cifrado de software en reposo reproduce la implementación de la unidad de autocifrado (SED) en el hardware para proporcionar seguridad de los datos en ausencia de SED.



Para los clústeres de almacenamiento all-flash SolidFire , el cifrado de software en reposo debe habilitarse durante la creación del clúster y no puede deshabilitarse después de que se haya creado el clúster.

Tanto el cifrado en reposo basado en software como el basado en hardware pueden utilizarse de forma independiente o en combinación entre sí.

Gestión de claves externas

Puede configurar el software Element para que utilice un servicio de administración de claves (KMS) de terceros compatible con KMIP para administrar las claves de cifrado del clúster de almacenamiento. Cuando habilita esta función, la clave de cifrado de la contraseña de acceso a la unidad de todo el clúster de almacenamiento es administrada por un KMS que usted especifica.

Element puede utilizar los siguientes servicios de gestión de claves:

- Gemalto SafeNet KeySecure
- SafeNet en KeySecure
- Control de teclas HyTrust
- Administrador de seguridad de datos de Vormetric
- Administrador del ciclo de vida de las claves de seguridad de IBM

Para obtener más información sobre la configuración de la administración de claves externas, consulte ["Primeros pasos con la administración de claves externas"](#) documentación.

Autenticación multifactor

La autenticación multifactor (MFA) le permite exigir a los usuarios que presenten varios tipos de evidencia para autenticarse con la interfaz de usuario web de NetApp Element o la interfaz de usuario del nodo de almacenamiento al iniciar sesión. Puede configurar Element para que acepte únicamente la autenticación multifactor para los inicios de sesión, integrándose con su sistema de gestión de usuarios y proveedor de identidad existentes. Puedes configurar Element para que se integre con un proveedor de identidad SAML 2.0 existente que puede aplicar múltiples esquemas de autenticación, como contraseña y mensaje de texto, contraseña y mensaje de correo electrónico u otros métodos.

Puede combinar la autenticación multifactor con proveedores de identidad (IdP) comunes compatibles con SAML 2.0, como Microsoft Active Directory Federation Services (ADFS) y Shibboleth.

Para configurar la autenticación multifactor (MFA), consulte ["habilitar la autenticación multifactor"](#) documentación.

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

Los clústeres de almacenamiento NetApp SolidFire admiten cifrado que cumple con los requisitos del Estándar Federal de Procesamiento de Información (FIPS) 140-2 para módulos criptográficos. Puede habilitar el cumplimiento de FIPS 140-2 en su clúster SolidFire tanto para las comunicaciones HTTPS como para el cifrado de unidades.

Cuando habilita el modo de funcionamiento FIPS 140-2 en su clúster, este activa el Módulo de Seguridad Criptográfica de NetApp (NCSM) y aprovecha el cifrado certificado FIPS 140-2 Nivel 1 para todas las comunicaciones a través de HTTPS con la interfaz de usuario y la API de NetApp Element . Usted usa el `EnableFeature` API de elementos con la `fips` Parámetro para habilitar el cifrado HTTPS FIPS 140-2. En

clústeres de almacenamiento con hardware compatible con FIPS, también puede habilitar el cifrado de unidad FIPS para datos en reposo mediante `EnableFeature` API de elementos con la `FipsDrives` parámetro.

Para obtener más información sobre cómo preparar un nuevo clúster de almacenamiento para el cifrado FIPS 140-2, 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 ["API de elementos EnableFeature"](#) .

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Cuentas y permisos

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

Con el almacenamiento de Element, puede crear y administrar los siguientes tipos de cuentas:

- [Cuentas de usuario administrador para el clúster de almacenamiento](#)
- [Cuentas de usuario para el acceso al volumen de almacenamiento](#)
- [Cuentas de usuario de clúster autorizadas para NetApp Hybrid Cloud Control](#)

cuentas de administrador de clúster de almacenamiento

En un clúster de almacenamiento que ejecuta el software NetApp Element, pueden existir dos tipos de cuentas de administrador:

- **Cuenta de administrador principal del clúster:** Esta cuenta de administrador se crea cuando se crea el clúster. Esta cuenta es la cuenta administrativa principal con el nivel más alto de acceso al clúster. Esta cuenta es análoga a un usuario root en un sistema Linux. Puedes 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 asignadas a cada cuenta de administrador del clúster se utilizan para autenticar las solicitudes de API y de la interfaz de usuario de Element dentro del sistema de almacenamiento.



Se requiere una cuenta de administrador de clúster local (no LDAP) para acceder a los nodos activos de un clúster a través de la interfaz de usuario por nodo. No se requieren credenciales de cuenta para acceder a un nodo que aún no forma parte de un clúster.

Puede ["administrar cuentas de administrador de clúster"](#) mediante la creación, eliminación y edición de cuentas de administrador de clúster, el cambio de la contraseña de administrador de clúster y la configuración de los ajustes LDAP para gestionar el acceso al sistema para 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 NetApp Element . Se requiere al menos una cuenta de usuario antes de poder crear un

volumen.

Cuando se crea un volumen, este se asigna a una cuenta. Si ha creado un volumen virtual, la cuenta es el contenedor de almacenamiento.

Aquí hay algunas consideraciones adicionales:

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

cuentas de usuario de clúster autorizadas

Las cuentas de usuario autorizadas del clúster pueden autenticarse frente a cualquier recurso de almacenamiento asociado con la instancia de nodos y clústeres de NetApp Hybrid Cloud Control. Con esta cuenta, puede administrar volúmenes, cuentas, grupos de acceso y más en todos los clústeres.

Las cuentas de usuario autorizadas se gestionan desde la opción "Gestión de usuarios" del menú superior derecho en NetApp Hybrid Cloud Control.

El "[clúster de almacenamiento autorizado](#)" es el clúster de almacenamiento que NetApp Hybrid Cloud Control utiliza para autenticar a los usuarios.

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

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

Si bien muchas funciones de NetApp Hybrid Cloud Control funcionan con múltiples clústeres de almacenamiento, la autenticación y la autorización tienen limitaciones necesarias. La limitación en torno a la autenticación y autorización es que los usuarios del clúster autoritativo pueden ejecutar acciones en otros clústeres vinculados a NetApp Hybrid Cloud Control incluso si no son usuarios de los otros clústeres de almacenamiento. Antes de proceder a administrar varios clústeres de almacenamiento, debe asegurarse de que los usuarios definidos en los clústeres autorizados estén definidos en todos los demás clústeres de almacenamiento con los mismos permisos. Puede administrar los usuarios desde NetApp Hybrid Cloud Control.

Cuentas de volumen

Las cuentas específicas de volumen son específicas únicamente del clúster de almacenamiento en el que se crearon. Estas cuentas permiten establecer permisos en volúmenes específicos de la red, pero no tienen efecto fuera de esos volúmenes.

Las cuentas de volumen se gestionan dentro de la tabla de volúmenes de control de la nube híbrida de NetApp .

Almacenamiento

Volúmenes

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

El almacenamiento de elementos le permite crear, ver, editar, eliminar, clonar, realizar copias de seguridad o restaurar volúmenes para cuentas de usuario. También puede administrar cada volumen en un clúster y agregar o eliminar volúmenes en grupos de acceso a volúmenes.

Volúmenes persistentes

Los volúmenes persistentes permiten almacenar los datos de configuración del nodo de administración en un clúster de almacenamiento específico, 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 administración. Los volúmenes persistentes son una configuración de nodo de administración opcional, pero recomendada.

En los scripts de instalación y actualización se incluye una opción para habilitar volúmenes persistentes cuando ["despliegue de un nuevo nodo de gestión"](#). Los volúmenes persistentes son volúmenes en un clúster de almacenamiento basado en software Element que contienen información de configuración del nodo de administración para la máquina virtual del nodo de administración del host, la cual persiste más allá de la vida útil de la máquina virtual. Si se pierde el nodo de administración, una máquina virtual de nodo de administración de reemplazo puede reconectarse y recuperar los datos de configuración de la máquina virtual perdida.

La funcionalidad de volúmenes persistentes, si está habilitada durante la instalación o actualización, crea automáticamente varios volúmenes. Estos volúmenes, al igual que cualquier volumen basado en software Element, se pueden visualizar mediante la interfaz web del software Element, el complemento NetApp Element para vCenter Server o la API, según sus preferencias e instalación. Los volúmenes persistentes deben estar activos y funcionando con una conexión iSCSI al nodo de administración para mantener los datos de configuración actuales que se pueden utilizar para la recuperación.



Los volúmenes persistentes asociados a los servicios de gestión se crean y se asignan a una nueva cuenta durante la instalación o actualización. Si utiliza volúmenes persistentes, no modifique ni elimine los volúmenes ni sus cuentas asociadas.

Volúmenes virtuales (vVols)

vSphere Virtual Volumes es un paradigma de almacenamiento para VMware que traslada gran parte de la gestión del almacenamiento de vSphere desde el sistema de almacenamiento a VMware vCenter. Con los volúmenes virtuales (vVols), puede asignar almacenamiento de acuerdo con los requisitos de cada máquina virtual.

Fijaciones

El clúster NetApp Element elige un punto de conexión de protocolo óptimo, crea un enlace que asocia el host ESXi y el volumen virtual con el punto de conexión de protocolo y devuelve el enlace al host ESXi. Una vez enlazado, el host ESXi puede realizar operaciones de E/S con el volumen virtual enlazado.

puntos finales del protocolo

Los hosts VMware ESXi utilizan proxies de E/S lógicos conocidos como puntos finales de protocolo para comunicarse con volúmenes virtuales. Los hosts ESXi enlazan volúmenes virtuales a puntos finales de protocolo para realizar operaciones de E/S. Cuando una máquina virtual en el host realiza una operación de E/S, el punto final del protocolo asociado dirige la E/S al volumen virtual con el que está emparejado.

Los puntos finales del protocolo en un clúster NetApp Element funcionan como unidades lógicas administrativas SCSI. El clúster crea automáticamente cada punto final del protocolo. Para cada nodo de un clúster, se crea un punto final de protocolo correspondiente. Por ejemplo, un clúster de cuatro nodos tendrá cuatro puntos finales de protocolo.

iSCSI es el único protocolo compatible con el software NetApp Element . El protocolo Fibre Channel no es compatible. Los puntos de conexión del protocolo no pueden ser eliminados ni modificados por un usuario, no están asociados a una cuenta y no pueden agregarse a un grupo de acceso por volumen.

contenedores de almacenamiento

Los contenedores de almacenamiento son construcciones lógicas que se asignan a cuentas de NetApp Element y se utilizan para la generación de informes y la asignación de recursos. Agrupan la capacidad de almacenamiento en bruto o agregan las capacidades de almacenamiento que el sistema de almacenamiento puede proporcionar a los volúmenes virtuales. Un almacén de datos VVol que se crea en vSphere se asigna a un contenedor de almacenamiento individual. Un único contenedor de almacenamiento dispone de forma predeterminada de todos los recursos disponibles del clúster NetApp Element . Si se requiere una gobernanza más granular para la multitenencia, se pueden crear múltiples contenedores de almacenamiento.

Los contenedores de almacenamiento funcionan como las cuentas tradicionales y pueden contener tanto volúmenes virtuales como volúmenes tradicionales. Se admite un máximo de cuatro contenedores de almacenamiento por clúster. Se requiere un mínimo de un contenedor de almacenamiento para utilizar la funcionalidad VVols. Puede descubrir contenedores de almacenamiento en vCenter durante la creación de VVols.

Proveedor de VASA

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

El proveedor VASA se ejecuta como parte del maestro del clúster en el software Element. El maestro del clúster es un servicio de alta disponibilidad que realiza la conmutación por error a cualquier nodo del clúster según sea necesario. Si el maestro del clúster falla, el proveedor VASA se mueve con él, lo que garantiza una alta disponibilidad para el proveedor VASA. Todas las tareas de aprovisionamiento y gestión de almacenamiento utilizan el proveedor VASA, que se encarga de cualquier cambio necesario en el clúster Element.



Para Element 12.5 y versiones anteriores, no registre más de un proveedor NetApp Element VASA en una sola instancia de vCenter. Cuando se agrega un segundo proveedor NetApp Element VASA, todos los almacenes de datos VVOL quedan inaccesibles.



La compatibilidad con VASA para hasta 10 vCenters está disponible como parche de actualización si ya ha registrado un proveedor de VASA con su vCenter. Para instalarlo, siga las instrucciones del manifiesto VASA39 y descargue el archivo .tar.gz desde el ["Descargas de software de NetApp"](#) sitio. El proveedor NetApp Element VASA utiliza un certificado NetApp . Con este parche, vCenter utiliza el certificado sin modificaciones para admitir múltiples vCenters para el uso de VASA y VVols. No modifique el certificado. VASA no admite certificados SSL personalizados.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Grupos de acceso por volumen

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

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

Los grupos de acceso por volumen tienen los siguientes límites:

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

Iniciadores

Los iniciadores permiten que los clientes externos accedan a los volúmenes de un clúster, sirviendo como punto de entrada para la comunicación entre clientes y volúmenes. Puede utilizar iniciadores para el acceso basado en CHAP en lugar del acceso basado en cuentas a los volúmenes de almacenamiento. Un único iniciador, cuando se agrega a un grupo de acceso a volúmenes, permite a los miembros del grupo de acceso a volúmenes acceder a todos los volúmenes de almacenamiento agregados al grupo sin necesidad de autenticación. Un iniciador solo puede pertenecer a un grupo de acceso.

Protección de datos

Las funciones de protección de datos incluyen replicación remota, instantáneas de volumen, clonación de volumen, dominios de protección y alta disponibilidad con tecnología de doble hélice.

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

- [Tipos de replicación remota](#)
- [Instantáneas de volumen para la protección de datos](#)
- [clones de volumen](#)
- [Descripción general del proceso de copia de seguridad y restauración para el almacenamiento de 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 instantáneas](#)
- [Replicación entre clústeres Element y ONTAP mediante SnapMirror](#)

Para obtener más información, consulte ["TR-4741: Replicación remota de software NetApp Element"](#) .

Replicación síncrona y asíncrona entre clústeres

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

Puedes emparejar un clúster de almacenamiento con hasta cuatro clústeres de almacenamiento adicionales. Puede replicar datos de volumen de forma síncrona o asíncrona desde cualquiera de los clústeres de un par de clústeres para escenarios de conmutación por error y recuperación ante fallos.

Replicación sincrónica

La replicación síncrona replica continuamente los 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 apropiada para las siguientes situaciones:

- Replicación de varios sistemas a corta distancia
- Un sitio de recuperación ante desastres que se encuentra geográficamente cerca de la fuente.
- Aplicaciones sensibles al tiempo y la protección de bases de datos
- Aplicaciones de continuidad de negocio que requieren que el sitio secundario actúe como sitio principal cuando este último esté inactivo.

Replicación asíncrona

La replicación asíncrona replica continuamente los datos de un clúster de origen a un clúster de destino sin esperar las confirmaciones del clúster de destino. Durante la replicación asíncrona, las escrituras se confirman al cliente (aplicación) después de que se hayan confirmado en el clúster de origen.

La replicación asíncrona es apropiada para las siguientes situaciones:

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

Replicación solo de instantáneas

La protección de datos de solo instantáneas replica los datos modificados en momentos específicos en un clúster remoto. Solo se replican las instantáneas creadas en el clúster de origen. Las escrituras activas desde el volumen de origen no lo son.

Puedes configurar la frecuencia de las replicaciones de instantáneas.

La replicación de instantáneas no afecta a la replicación asíncrona ni a la síncrona.

Replicación entre clústeres Element y ONTAP mediante SnapMirror

Con la tecnología NetApp SnapMirror, puede replicar instantáneas tomadas con el software NetApp Element en ONTAP para fines de recuperación ante desastres. En una relación SnapMirror, Element es un punto final y ONTAP es el otro.

SnapMirror es una tecnología de replicación de instantáneas de NetApp que facilita la recuperación ante desastres, diseñada para la conmutación por error desde el almacenamiento primario al almacenamiento secundario en un sitio geográficamente remoto. La tecnología SnapMirror crea una réplica, o espejo, de los datos de trabajo en un almacenamiento secundario desde el cual se puede seguir proporcionando datos si se produce una interrupción en el sitio principal. Los datos se reflejan a 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 puntos finales en los que residen los volúmenes y los volúmenes que contienen los datos replicados deben estar interconectados. Una relación entre pares permite que los clústeres y volúmenes intercambien datos de forma segura.

SnapMirror se ejecuta de forma nativa en los controladores NetApp ONTAP y está integrado en Element, que se ejecuta en clústeres NetApp HCI y SolidFire. La lógica para controlar SnapMirror reside en el software ONTAP; por lo tanto, todas las relaciones de SnapMirror deben involucrar al menos un sistema ONTAP para realizar el trabajo de coordinación. Los usuarios gestionan las relaciones entre los clústeres Element y ONTAP principalmente a través de la interfaz de usuario de Element; sin embargo, algunas tareas de gestión residen en NetApp ONTAP System Manager. Los usuarios también pueden administrar SnapMirror a través de la CLI y la API, ambas disponibles en ONTAP y Element.

Ver ["TR-4651: Arquitectura y configuración de NetApp SolidFire SnapMirror"](#) (Se requiere iniciar sesión)

Debe habilitar manualmente la funcionalidad SnapMirror a nivel de clúster utilizando el software Element. La funcionalidad SnapMirror está desactivada por defecto y no se activa automáticamente como parte de una nueva instalación o actualización.

Tras habilitar SnapMirror, puede crear relaciones de SnapMirror desde la pestaña Protección de datos en el

software Element.

El software NetApp Element 10.1 y versiones posteriores admiten la funcionalidad SnapMirror para copiar y restaurar instantáneas con sistemas ONTAP .

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

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

Para obtener más información, consulte ["Replicación entre NetApp Element Software y ONTAP \(CLI de ONTAP \)"](#).

Instantáneas de volumen para la protección de datos

Una instantánea de volumen es una copia de un volumen en un momento dado que posteriormente se puede usar para restaurar un volumen a ese momento específico.

Aunque las instantáneas son similares a los clones de volumen, las instantáneas son simplemente réplicas de los metadatos del volumen, por lo que no se pueden montar ni escribir en ellas. La creación de una instantánea de volumen también requiere una cantidad mínima de recursos del sistema y espacio, lo que hace que la creación de instantáneas sea más rápida que la clonación.

Puede replicar instantáneas en un clúster remoto y utilizarlas como copia de seguridad del volumen. Esto le permite revertir un volumen a un punto específico en el tiempo mediante el uso de la instantánea replicada; también puede crear un clon de un volumen a partir de una instantánea replicada.

Puede realizar copias de seguridad de instantáneas desde un clúster de Element a un almacenamiento de objetos externo o a otro clúster de Element. Cuando se realiza una copia de seguridad de una instantánea en un almacenamiento de objetos externo, es necesario disponer de una conexión con dicho almacenamiento que permita operaciones de lectura/escritura.

Puede tomar una instantánea de un volumen individual o de varios para la protección de datos.

clones de volumen

Un clon de un único volumen o de varios volúmenes es una copia de los datos en un momento dado. Cuando se clona un volumen, el sistema crea una instantánea del volumen y luego crea una copia de los datos a los que hace referencia la instantánea.

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

El clúster admite hasta dos solicitudes de clonación en ejecución por volumen a la vez y hasta ocho operaciones de clonación de volumen activas a la vez. Las solicitudes que superen estos límites se pondrán en cola para su posterior procesamiento.

Descripción general del proceso de copia de seguridad y restauración para el almacenamiento de Element

Puede realizar copias de seguridad y restaurar volúmenes en otros almacenamientos SolidFire , así como en almacenes de objetos secundarios compatibles con Amazon S3 u OpenStack Swift.

Puedes realizar una copia de seguridad de un volumen en lo siguiente:

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

Al restaurar volúmenes desde OpenStack Swift o Amazon S3, se necesita la información del manifiesto del proceso de copia de seguridad original. Si está restaurando un volumen del que se realizó una copia de seguridad en un sistema de almacenamiento SolidFire , no se requiere información de manifiesto.

Dominios de protección

Un dominio de protección es un nodo o un conjunto de nodos agrupados de tal manera que cualquier parte o incluso la totalidad del mismo podría fallar, manteniendo al mismo tiempo la disponibilidad de los datos. Los dominios de protección permiten que un clúster de almacenamiento se recupere automáticamente de la pérdida de un chasis (afinidad de chasis) o de todo un dominio (grupo de chasis).

Puede habilitar manualmente la supervisión del dominio de protección mediante el punto de extensión de configuración de NetApp Element en el complemento NetApp Element para vCenter Server. Puede seleccionar un umbral de dominio de protección basado en dominios de nodo o chasis. También puede habilitar la supervisión del dominio de protección mediante la API de Element o la interfaz web.

Un diseño de Dominio de Protección asigna cada nodo a un Dominio de Protección específico.

Se admiten dos diseños diferentes de dominio de protección, denominados niveles de dominio de protección.

- A nivel de nodo, cada nodo se encuentra en su propio Dominio de Protección.
- A nivel de chasis, solo los nodos que comparten un chasis están en el mismo Dominio de Protección.
 - La disposición a nivel de chasis se determina automáticamente a partir del hardware cuando se agrega el nodo al clúster.
 - En un clúster donde cada nodo se encuentra en un chasis separado, estos dos niveles son funcionalmente idénticos.

Al crear un nuevo clúster, si utiliza nodos de almacenamiento que residen en un chasis compartido, es posible que desee considerar el diseño de una protección contra fallos a nivel de chasis mediante la función Dominios de protección.

Dominios de protección personalizados

Puede definir una disposición de dominio de protección personalizada que se ajuste a la disposición específica de su chasis y nodos, donde cada nodo esté asociado con un único dominio de protección personalizado. Por defecto, a cada nodo se le asigna el mismo dominio de protección personalizado predeterminado.

Si no se han asignado dominios de protección personalizados:

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

Cuando configura dominios de protección personalizados para un clúster, existen tres niveles de protección posibles, que puede ver en el panel de la interfaz web de Element:

- **No protegido:** El clúster de almacenamiento no está protegido contra el fallo de uno de sus dominios de protección personalizados. Para solucionar esto, agregue capacidad de almacenamiento adicional al clúster o reconfigure los dominios de protección personalizados del clúster para protegerlo de posibles pérdidas 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.
- **Resistente a fallos:** El clúster de almacenamiento tiene suficiente capacidad libre para autorrepararse tras el fallo de uno de sus dominios de protección personalizados. Una vez finalizado el proceso de recuperación, el clúster estará protegido contra la pérdida de datos en caso de que fallen dominios adicionales.

Si se asigna más de un dominio de protección personalizado, cada subsistema asignará los duplicados a dominios de protección personalizados separados. Si esto no es posible, recurre a asignar los duplicados a nodos separados. Cada subsistema (por ejemplo, contenedores, segmentos, proveedores de puntos finales de protocolo y conjunto) realiza esto de forma independiente.

Puedes usar la interfaz de usuario de Element para "[Configurar dominios de protección personalizados](#)" o bien puede utilizar los siguientes métodos de la API:

- "[ObtenerDiseñoDeDominioDeProtección](#)"- muestra en qué chasis y en qué dominio de protección personalizado se encuentra cada nodo.
- "[Establecer diseño de dominio de protección](#)"- Permite asignar un dominio de protección personalizado a cada nodo.

Alta disponibilidad de Double Helix

La protección de datos Double Helix es un método de replicación que distribuye al menos dos copias redundantes de los datos 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 se repare rápidamente.

Rendimiento y calidad del servicio

Un clúster de almacenamiento SolidFire tiene la capacidad de 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 QoS: IOPS mínimas, IOPS máximas e IOPS de ráfaga.



SolidFire Active IQ cuenta con una página de recomendaciones de QoS que ofrece consejos sobre la configuración óptima y la puesta en marcha de los ajustes de QoS.

Parámetros de calidad del servicio

Los parámetros IOPS se definen de las siguientes maneras:

- **IOPS mínimo** - El número mínimo de entradas y salidas sostenidas por segundo (IOPS) que el clúster de almacenamiento proporciona a un volumen. El valor de IOPS mínimo configurado para un volumen es el nivel de rendimiento garantizado para dicho volumen. El rendimiento no baja de este nivel.
- **IOPS máximo** - El número máximo de IOPS sostenidas que el clúster de almacenamiento proporciona a un volumen. Cuando los niveles de IOPS del clúster son críticamente altos, este nivel de rendimiento de IOPS no se supera.
- **IOPS de ráfaga** - El número máximo de IOPS permitido en un escenario de ráfaga corta. Si un volumen ha estado funcionando por debajo del IOPS máximo, se acumulan créditos de ráfaga. Cuando los niveles de rendimiento se vuelven muy altos y se llevan a niveles máximos, se permiten ráfagas cortas de IOPS en el volumen.

El software Element utiliza Burst IOPS cuando un clúster se encuentra en un estado de baja utilización de IOPS del clúster.

Un único volumen puede acumular IOPS de ráfaga y usar los créditos para realizar ráfagas por encima de sus IOPS máximas hasta su nivel de IOPS de ráfaga durante un "período de ráfaga" determinado. Un volumen puede generar ráfagas de hasta 60 segundos si el clúster tiene la capacidad para acomodarlas. Un volumen acumula un segundo de crédito de ráfaga (hasta un máximo de 60 segundos) por cada segundo que el volumen funcione por debajo de su límite de IOPS máximo.

Las IOPS de ráfaga están limitadas de dos maneras:

- Un volumen puede superar su IOPS máxima durante un número de segundos igual al número de créditos de ráfaga que haya acumulado el volumen.
 - Cuando un volumen supera su configuración de IOPS máximas, queda limitado por su configuración de IOPS de ráfaga. Por lo tanto, las IOPS de ráfaga nunca superan la configuración de IOPS de ráfaga para el volumen.
- **Ancho de banda máximo efectivo** - El ancho de banda máximo se calcula multiplicando el número de IOPS (según la curva QoS) por el tamaño de E/S.

Ejemplo: La configuración de parámetros QoS de 100 IOPS mínimas, 1000 IOPS máximas y 1500 IOPS de ráfaga tiene los siguientes efectos en la calidad del rendimiento:

- Las cargas de trabajo pueden alcanzar y mantener un máximo de 1000 IOPS hasta que la condición de contención de carga de trabajo por IOPS se haga evidente en el clúster. A continuación, las IOPS se reducen de forma incremental hasta que las IOPS en todos los volúmenes se encuentran dentro de los rangos QoS designados y se alivia la contención por el rendimiento.
- El rendimiento en todos los volúmenes se está llevando hacia el IOPS mínimo de 100. Los niveles no bajan del valor de IOPS mínimo establecido, pero podrían mantenerse por encima de 100 IOPS cuando se alivia la contención de la carga de trabajo.
- El rendimiento nunca es superior a 1000 IOPS, ni inferior a 100 IOPS durante un período prolongado. Se permite un rendimiento de 1500 IOPS (IOPS de ráfaga), pero solo para aquellos volúmenes que hayan acumulado créditos de ráfaga al funcionar por debajo de las IOPS máximas y solo durante períodos cortos de tiempo. Los niveles de ráfaga nunca se mantienen.

límites de valor de QoS

Aquí están los posibles valores mínimos y máximos para QoS.

Parámetros	Valor mínimo	Por defecto	4 KB	5 8KB	6 16 KB	262 KB
IOPS mínimas	50	50	15.000	9.375*	5556*	385*

Parámetros	Valor mínimo	Por defecto	4 KB	5 8KB	6 16 KB	262 KB
IOPS máximas	100	15.000	200.000**	125.000	74.074	5128
Burst IOPS	100	15.000	200.000**	125.000	74,074	5128

*Estas estimaciones son aproximadas. **Los valores de IOPS máximos e IOPS de ráfaga se pueden configurar hasta en 200.000; sin embargo, esta configuración solo se permite para desbloquear efectivamente el rendimiento de un volumen. El rendimiento máximo real de un volumen está limitado por el uso del clúster y el rendimiento por nodo.

Rendimiento de QoS

La curva de rendimiento QoS muestra la relación entre el tamaño del bloque y el porcentaje de IOPS.

El tamaño de bloque y el ancho de banda tienen un impacto directo en la cantidad de IOPS que una aplicación puede obtener. El software Element tiene en cuenta los tamaños de bloque que recibe normalizando los tamaños de bloque a 4k. En función de la carga de trabajo, el sistema podría aumentar el tamaño de los bloques. A medida que aumenta el tamaño de los bloques, el sistema incrementa el ancho de banda hasta el nivel necesario para procesar los bloques de mayor tamaño. A medida que aumenta el ancho de banda, disminuye el número de IOPS que el sistema puede alcanzar.

La curva de rendimiento QoS muestra la relación entre el aumento del tamaño de los bloques y la disminución del porcentaje de IOPS:

Por ejemplo, si los tamaños de bloque son de 4k y el ancho de banda es de 4000 KBps, las IOPS son 1000. Si el tamaño de los bloques aumenta a 8k, el ancho de banda aumenta a 5000 KBps y las IOPS disminuyen a 625. Al tener en cuenta el tamaño del bloque, el sistema garantiza que las cargas de trabajo de menor prioridad que utilizan tamaños de bloque más grandes, como las copias de seguridad y las actividades del hipervisor, no consuman demasiado rendimiento del tráfico de mayor prioridad que utiliza tamaños de bloque más pequeños.

Políticas de QoS

Una política de QoS le permite crear y guardar una configuración de calidad de servicio estandarizada que se puede aplicar a muchos volúmenes.

Las políticas de QoS son las más adecuadas para entornos de servicio, por ejemplo, con servidores de bases de datos, aplicaciones o infraestructura que rara vez se reinician y necesitan un acceso constante y equitativo al almacenamiento. La QoS de volumen individual es la mejor opción para máquinas virtuales de uso ligero, como escritorios virtuales o máquinas virtuales especializadas tipo quiosco, que pueden reiniciarse, encenderse o apagarse diariamente o varias veces al día.

No se deben utilizar juntas las políticas de QoS y QoS. Si está utilizando políticas de QoS, no utilice QoS personalizada en un volumen. La QoS personalizada anulará y ajustará los valores de la política de QoS para la configuración de QoS de volumen.



El clúster seleccionado debe ser Element 10.0 o posterior para utilizar las políticas de QoS; de lo contrario, las funciones de política de QoS no estarán disponibles.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)

Requisitos

Redes

La configuración de red para un sistema SolidFire consta de requisitos de conmutadores y puertos. La implementación de estas opciones depende de su sistema.

Para más información

- ["Configuración de conmutadores para clústeres que ejecutan el software Element"](#)
- ["Requisitos del puerto de red"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Configuración de conmutadores para clústeres que ejecutan el software Element

El sistema de software NetApp Element tiene ciertos requisitos de conmutación y mejores prácticas para un rendimiento de almacenamiento óptimo.

Los nodos de almacenamiento requieren conmutadores Ethernet de 10 o 25 GbE, según el hardware específico del nodo, para los servicios de almacenamiento iSCSI y la comunicación de servicios intraclúster del nodo. Los conmutadores 1GbE se pueden utilizar para estos tipos de tráfico:

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

Buenas prácticas: Al configurar los conmutadores Ethernet para el tráfico del clúster, debe implementar las siguientes buenas prácticas:

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

El despliegue de elementos requiere al menos dos segmentos de red, uno para cada uno de los siguientes tipos de tráfico:

- Gestión
- Almacenamiento/Datos

Dependiendo de los modelos de nodos de almacenamiento NetApp serie H y de la configuración de cableado prevista, puede separar físicamente estas redes mediante conmutadores independientes o separarlas lógicamente mediante VLAN. Sin embargo, para la mayoría de las implementaciones, es necesario separar

lógicamente estas redes utilizando VLAN.

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

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

NetApp Element requiere lo siguiente:

- Todos los puertos de conmutador conectados a los nodos de almacenamiento NetApp serie H deben configurarse como puertos de borde de árbol de expansión.
 - En los switches de Cisco , dependiendo 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, puedes hacerlo con el `spanning-tree port type edge dominio`.
- Los conmutadores que manejan el tráfico de almacenamiento deben admitir velocidades de al menos 10 GbE por puerto (se admiten hasta 25 GbE por puerto).
- Los conmutadores que gestionan el tráfico de administración deben admitir velocidades de al menos 1 GbE por puerto.
- Debe configurar tramas jumbo en los puertos del switch que manejan el tráfico de almacenamiento. Para que la instalación sea exitosa, los hosts deben poder enviar paquetes de 9000 bytes de extremo a extremo.
- La latencia de red de ida y vuelta entre todos los nodos de almacenamiento no debe superar los 2 ms.

Algunos nodos proporcionan capacidades 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, debería facilitar la administración remota configurando la administración fuera de banda para todos los nodos de su entorno.

Para más información

- ["Requisitos de red y conmutador NetApp HCI"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Requisitos del puerto de red

Es posible que necesite permitir los siguientes puertos TCP y UDP a través del firewall perimetral de su centro de datos para poder administrar el sistema de forma remota y permitir que los clientes fuera de su centro de datos se conecten a los recursos. Es posible que algunos de estos puertos no sean necesarios, dependiendo de cómo utilice

el sistema.

Todos los puertos son TCP a menos que se indique lo contrario, y todos los puertos TCP deben admitir comunicación de enlace de tres vías entre el servidor de soporte de NetApp , el nodo de administración y los nodos que ejecutan el software Element. Por ejemplo, el host en un nodo de administración de origen se comunica con el host en un clúster de almacenamiento MVIP de destino a través del puerto TCP 443, y el host de destino se comunica de vuelta al host de origen a través de cualquier puerto.



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

En la tabla se utilizan 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 administración
- SVIP: Dirección IP virtual de almacenamiento

Fuente	Destino	Puerto	Descripción
clientes iSCSI	MVIP de clúster de almacenamiento	443	(Opcional) Acceso a la interfaz de usuario y a la API
clientes iSCSI	Clúster de almacenamiento SVIP	3260	Comunicaciones iSCSI del cliente
clientes iSCSI	Nodo de almacenamiento SIP	3260	Comunicaciones iSCSI del cliente
Nodo de gestión	<code>sfsupport.solidfire.com</code>	22	Túnel SSH inverso para acceso de soporte
Nodo de gestión	Nodo de almacenamiento MIP	22	Acceso SSH para soporte
Nodo de gestión	servidores DNS	53 TCP/UDP	Búsqueda de DNS
Nodo de gestión	Nodo de almacenamiento MIP	442	Acceso mediante interfaz de usuario y API a las actualizaciones de software del nodo de almacenamiento y del elemento
Nodo de gestión	MVIP de clúster de almacenamiento	442	Acceso mediante interfaz de usuario y API a las actualizaciones de software del nodo de almacenamiento y del elemento

Fuente	Destino	Puerto	Descripción
Nodo de gestión	monitoring.solidfire.com	443	El clúster de almacenamiento informa a Active IQ.
Nodo de gestión	MVIP de clúster de almacenamiento	443	Acceso mediante interfaz de usuario y API a las actualizaciones de software del nodo de almacenamiento y del elemento
Nodo de gestión	repo.netapp.com	443	Proporciona acceso a los componentes necesarios para instalar/actualizar la implementación local.
Nodo de gestión	Nodo de almacenamiento BMC/IPMI	623 UDP	Puerto RMCP. Esto es necesario para gestionar sistemas habilitados para IPMI.
Nodo de gestión	Nodo testigo	9442	Servicio API de configuración por nodo
Nodo de gestión	Servidor vCenter	9443	Registro del complemento de vCenter. El puerto puede cerrarse una vez finalizado el registro.
Servidor SNMP	MVIP de clúster de almacenamiento	161 UDP	sondeo SNMP
Servidor SNMP	Nodo de almacenamiento MIP	161 UDP	sondeo SNMP
Nodo de almacenamiento BMC/IPMI	Nodo de gestión	623 UDP	Puerto RMCP. Esto es necesario para gestionar sistemas habilitados para IPMI.
Nodo de almacenamiento MIP	servidores DNS	53 TCP/UDP	Búsqueda de DNS
Nodo de almacenamiento MIP	Nodo de gestión	80	Actualizaciones de software de Element
Nodo de almacenamiento MIP	Punto de conexión S3/Swift	80	(Opcional) Comunicación HTTP con el punto de conexión S3/Swift para copias de seguridad y recuperación
Nodo de almacenamiento MIP	Servidor NTP	123 UDP	NTP

Fuente	Destino	Puerto	Descripción
Nodo de almacenamiento MIP	Nodo de gestión	162 UDP	(Opcional) Trampas SNMP
Nodo de almacenamiento MIP	Servidor SNMP	162 UDP	(Opcional) Trampas SNMP
Nodo de almacenamiento MIP	Servidor LDAP	389 TCP/UDP	(Opcional) Búsqueda LDAP
Nodo de almacenamiento MIP	Nodo de gestión	443	Actualizaciones de almacenamiento de elementos
Nodo de almacenamiento MIP	MVIP de clúster de almacenamiento remoto	443	Comunicación de emparejamiento de clústeres de replicación remota
Nodo de almacenamiento MIP	Nodo de almacenamiento remoto MIP	443	Comunicación de emparejamiento de clústeres de replicación remota
Nodo de almacenamiento MIP	Punto de conexión S3/Swift	443	(Opcional) Comunicación HTTPS con el punto de conexión S3/Swift para copias de seguridad y recuperación
Nodo de almacenamiento MIP	Nodo de gestión	514 TCP/UDP 10514 TCP/UDP	Reenvío de Syslog
Nodo de almacenamiento MIP	Servidor de syslog	514 TCP/UDP 10514 TCP/UDP	Reenvío de Syslog
Nodo de almacenamiento MIP	Servidor LDAPS	636 TCP/UDP	Búsqueda de LDAPS
Nodo de almacenamiento MIP	Nodo de almacenamiento remoto MIP	2181	Comunicación entre clústeres para replicación remota
Nodo de almacenamiento SIP	Nodo de almacenamiento remoto SIP	2181	Comunicación entre clústeres para replicación remota
Nodo de almacenamiento SIP	Nodo de almacenamiento SIP	3260	iSCSI internodo

Fuente	Destino	Puerto	Descripción
Nodo de almacenamiento SIP	Nodo de almacenamiento remoto SIP	4000 al 4020	Transferencia de datos de nodo a nodo mediante replicación remota
PC del administrador del sistema	Nodo de gestión	442	Acceso mediante interfaz de usuario HTTPS al nodo de administración
PC del administrador del sistema	Nodo de almacenamiento MIP	442	Interfaz de usuario HTTPS y acceso a la API del nodo de almacenamiento
PC del administrador del sistema	Nodo de gestión	443	Interfaz de usuario HTTPS y acceso a la API del nodo de administración
PC del administrador del sistema	MVIP de clúster de almacenamiento	443	Interfaz de usuario HTTPS y acceso a la API del clúster de almacenamiento
PC del administrador del sistema	Controlador de gestión de placa base (BMC)/Interfaz de gestión de plataforma inteligente (IPMI) de las series H410 y H600 del nodo de almacenamiento	443	Interfaz de usuario y acceso API HTTPS para el control remoto del nodo
PC del administrador del sistema	Nodo de almacenamiento MIP	443	Creación de clústeres de almacenamiento HTTPS, acceso a la interfaz de usuario del clúster de almacenamiento tras la implementación
PC del administrador del sistema	Nodo de almacenamiento BMC/IPMI serie H410 y H600	623 UDP	Puerto del protocolo de control de gestión remota. Esto es necesario para gestionar sistemas habilitados para IPMI.
PC del administrador del sistema	Nodo testigo	8080	Interfaz web por nodo de Witness Node
Servidor vCenter	MVIP de clúster de almacenamiento	443	Acceso a la API del complemento de vCenter
Servidor vCenter	Conexión remota	8333	Servicio de complementos remotos de vCenter
Servidor vCenter	Nodo de gestión	8443	(Opcional) Servicio QoSSIOC del complemento vCenter.

Fuente	Destino	Puerto	Descripción
Servidor vCenter	MVIP de clúster de almacenamiento	8444	Acceso del proveedor vCenter VASA (solo VVols)
Servidor vCenter	Nodo de gestión	9443	Registro del complemento de vCenter. El puerto puede cerrarse una vez finalizado el registro.

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Pruébalo

Conozca los recursos y herramientas que le ayudarán a comenzar a usar el software Element.

- ["Laboratorio a demanda para una mayor flexibilidad en el almacenamiento en la nube privada con Element \(se requiere inicio de sesión\)"](#) Este laboratorio presenta conceptos de escalabilidad horizontal sin limitaciones, rendimiento de carga de trabajo garantizado 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 utilizando el nodo de demostración de Element"](#) Element Demo Node es una versión de máquina virtual VMware del software Element, que proporciona una manera fácil de demostrar muchas de las características clave de almacenamiento de los productos NetApp HCI y SolidFire .

Pruebe las funciones de almacenamiento utilizando el nodo de demostración de Element

["Nodo de demostración de elemento"](#) Es una versión de máquina virtual (VM) VMware del software Element, que proporciona una manera fácil de demostrar muchas de las características clave de almacenamiento de los productos NetApp HCI y SolidFire . El nodo de demostración permite a los desarrolladores programar con la API de Element sin necesidad de hardware físico. Se empaqueta como un archivo OVA para facilitar su implementación en VMware.

Funcionalidad admitida:

El nodo de demostración Element Demo está destinado únicamente a ser utilizado 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 elementos no admite la agrupación en clústeres. Funciona únicamente como un clúster de un solo nodo.
- No admite actualizaciones de Element. Para probar una versión más reciente de Element, debe instalar una nueva máquina virtual de nodo de demostración.
- No pretende demostrar el rendimiento del almacenamiento. El rendimiento observado en el nodo de demostración no es en absoluto indicativo del rendimiento en los clústeres físicos.
- No se pueden agregar nodos de demostración a clústeres NetApp HCI o SolidFire .
- Las VLAN VRF no son compatibles (las VLAN etiquetadas estándar sí lo son).
- El servicio de segmentación de múltiples unidades (MDSS) no es compatible.
- El nodo de demostración de elementos solo es compatible con almacenes de datos VMFS. Los VVols no son compatibles.
- Las funciones de configuración y monitorización basadas en hardware no funcionan con el nodo de demostración.
- Admite un máximo de 10 instantáneas por volumen.
- Admite un máximo de 20 cuentas por nodo/clúster.

- Admite un máximo de 100 volúmenes por cuenta.
- Admite un máximo de 200 vVols por cuenta.
- Admite un tamaño de volumen máximo de 100 GiB.
- Admite un límite de clúster sostenido de 3000 IOPS.



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

Requisitos de VM

- Capacidad total de 240 GB (El tamaño y el número de discos virtuales para la máquina virtual no se pueden cambiar). Cualquier almacenamiento adicional presentado a través del hipervisor es ignorado por el sistema operativo invitado.
- disco raíz de 60 GB
- Aprovisionamiento grueso/borrado inmediato (una unidad de metadatos de 30 GB o tres unidades de bloque de 50 GB) o aprovisionamiento ligero/borrado inmediato (**recomendado**) (una unidad de metadatos de 30 GB o tres unidades de bloque de 50 GB)
- Dos vCPU (totalmente reservadas)
- 16 GB de RAM (totalmente reservada)
- Un único HBA para todos los discos, paralelo LSI Logic
- Dos vNIC, ambas vmxnet3 (una de administración, una de almacenamiento)

Requisitos del anfitrión

- ESXi 6.0 o 6.5 para la máquina virtual Element Demo Node 11.7
- ESXi 6.5 para máquinas virtuales Element Demo Node 12.0 y 12.2
- ESXi 6.7 y 7.0 para las máquinas virtuales Element Demo Node 12.3 y 12.5
- Arquitectura Intel® multinúcleo de 64 bits

Descargar nodo de demostración de Element

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

Instalar el nodo de demostración de Element en VMware ESXi

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

- [Configurar interfaces de red](#)
- [Registre el nodo de demostración en un servidor ESXi.](#)
- [Inicie el nodo de demostración en un servidor ESXi.](#)

Configurar interfaces de red

El nodo de demostración de Element requiere dos redes de máquinas virtuales 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 tramas jumbo.

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 utilizando el cliente vSphere.

Pasos

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

Se inicia el asistente para implementar plantillas OVF.

3. En la página **Seleccionar plantilla**, busque el archivo OVA que descargó y seleccione **Abrir**.
4. Seleccione **Siguiente**.
5. En la página **Nombre y ubicación**, especifique un nombre y una ubicación para la plantilla implementada y, a continuación, seleccione **Siguiente**.
6. En la página **Seleccionar un recurso**, navegue hasta la ubicación donde desea ejecutar la plantilla y seleccione **Siguiente**.
7. Verifique los detalles y seleccione **Siguiente**.
8. En la página **Seleccionar almacenamiento**, seleccione dónde desea almacenar los archivos de la máquina virtual y luego seleccione **Siguiente**.
9. En la página **Seleccionar redes**, asigne la red utilizada en el archivo OVA a las dos redes de máquinas virtuales separadas en su inventario y seleccione **Siguiente**.
10. En la página **Listo para completar**, verifique los detalles sobre la máquina virtual que está creando y, a continuación, seleccione **Finalizar**.



El despliegue del nodo de demostración puede tardar 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 a través de la consola de VMware ESXi.

Pasos

1. En vSphere Client, seleccione la máquina virtual del nodo de demostración que creó.
2. Seleccione la pestaña **Resumen** para ver los detalles sobre esta máquina virtual.
3. Seleccione **Encender** para iniciar la máquina virtual.
4. Seleccione **Iniciar consola web**.
5. Utilice la interfaz de usuario de texto (TUI) para configurar el nodo de demostración. Para obtener más información, consulte ["Configurar un nodo de almacenamiento"](#).

Cómo obtener ayuda

El nodo de demostración de Element está disponible con el mejor esfuerzo posible por parte de voluntarios. Para obtener ayuda, publique sus preguntas en el ["Foro de nodos de demostración de elementos"](#).

Encuentra más información

["Página de descarga del nodo de demostración de Element \(se requiere iniciar sesión\)"](#)

Instalar y mantener el hardware

Información de hardware H410S y H610S

Instalar nodos de almacenamiento de la serie H

Antes de comenzar a utilizar su sistema de almacenamiento totalmente flash, debe instalar y configurar correctamente los nodos de almacenamiento.



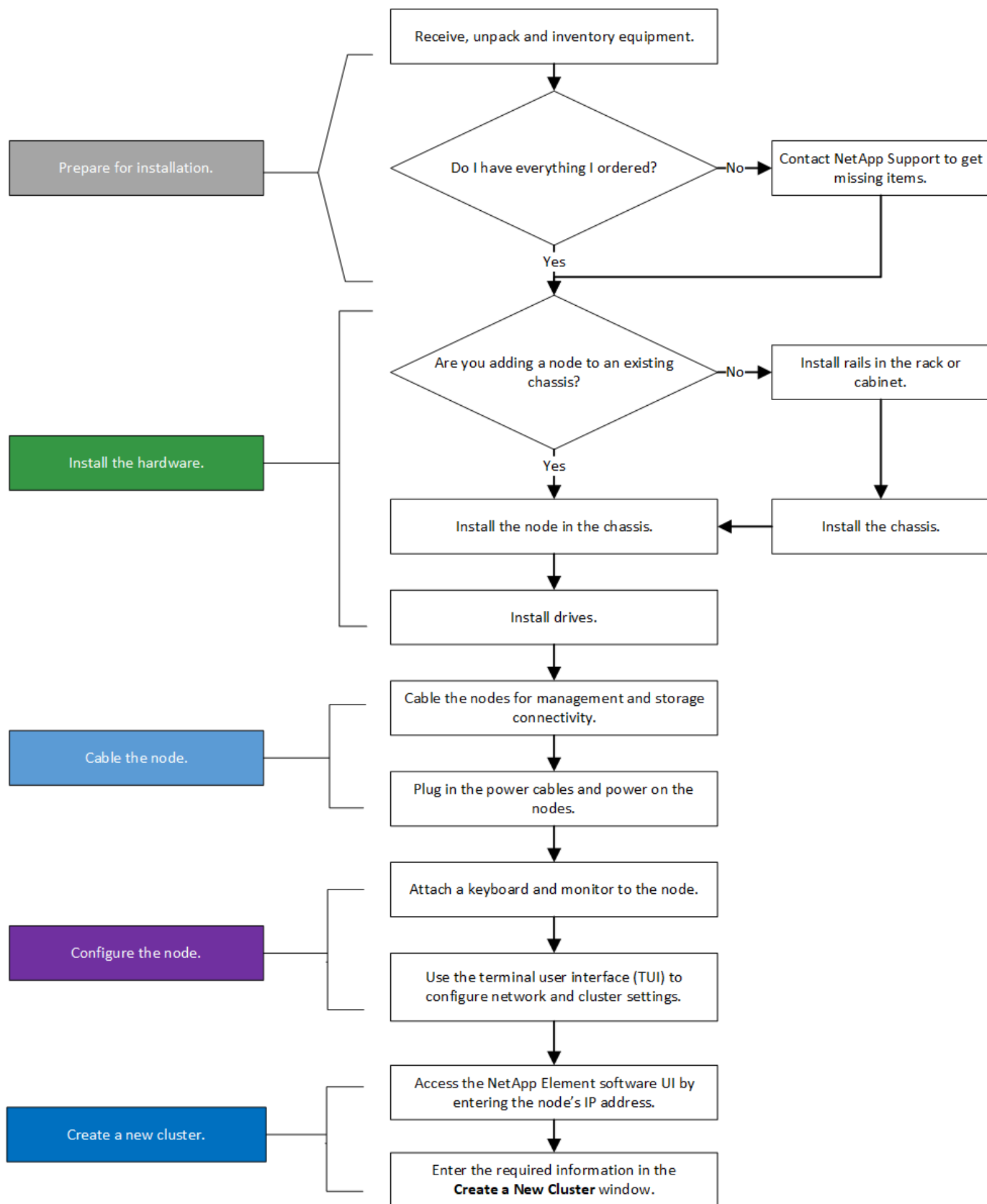
Ver el ["póster"](#) para una representación visual de las instrucciones.

- [Diagramas de flujo de trabajo](#)
- [Prepárese para la instalación](#)
- [Instala los rieles](#)
- [Instalar y cablear los nodos](#)
- [Configurar los nodos](#)
- [Crear un clúster](#)

Diagramas de flujo de trabajo

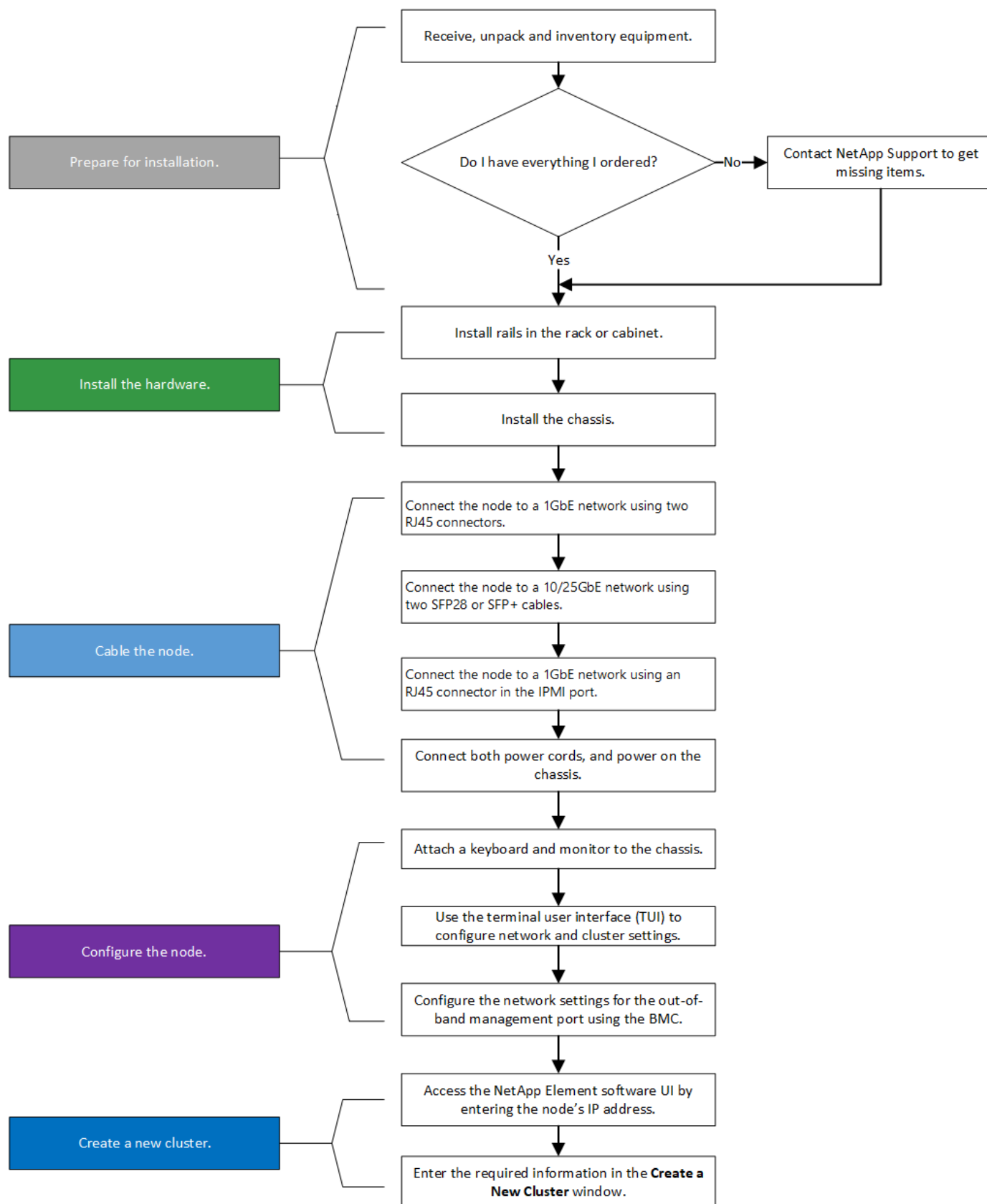
Los diagramas de flujo que se muestran aquí ofrecen una visión general de alto nivel de los pasos de instalación. Los pasos varían ligeramente dependiendo del modelo de la serie H.

H410S





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



Prepárese para la instalación

Para preparar la instalación, haga un inventario del hardware que se le envió y póngase en contacto con el soporte de NetApp si falta algún elemento.

Asegúrese de tener los siguientes elementos en el lugar de instalación:

- Espacio en rack para el sistema.

Tipo de nodo	espacio en 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 conmutador KVM (teclado, vídeo y ratón) para configurar su sistema.
- Memoria USB (opcional)



El hardware que se le envíe dependerá de lo que haya pedido. Un nuevo pedido de 2U y cuatro nodos incluye el chasis, el bisel, el kit de rieles deslizantes, las unidades, los nodos de almacenamiento y los cables de alimentación (dos por chasis). Si solicita nodos de almacenamiento H610S, las unidades vienen instaladas en el chasis.



Al instalar el hardware, asegúrese de retirar todo el material de embalaje y el envoltorio de la unidad. Esto evitará que los nodos se sobrecalienten y se apaguen.

Instala los rieles

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



Instale los soportes desde la parte inferior del rack hasta la parte superior para evitar que el equipo se vuelque. Si su rack incluye dispositivos estabilizadores, instálelos antes de instalar el hardware.

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

H410S

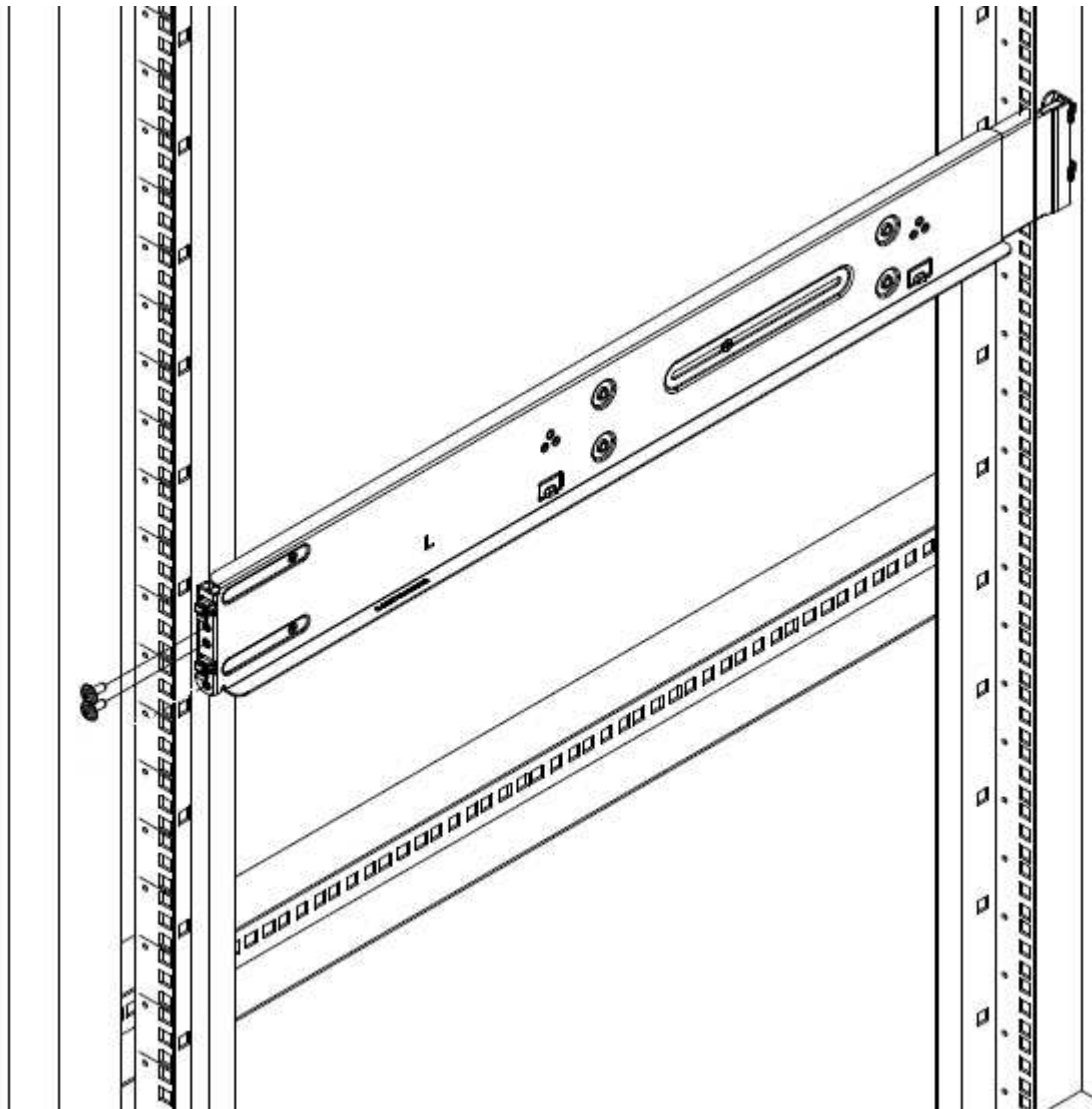
Los nodos H410S se instalan en un chasis de la serie H de 2U y cuatro nodos, que se envía con dos juegos de adaptadores. Si desea instalar el chasis en un rack con orificios redondos, utilice los adaptadores adecuados para un rack con orificios redondos. Los rieles para nodos H410S se ajustan a un rack de entre 29 y 33,5 pulgadas de profundidad. Cuando el riel está completamente contraído, mide 28 pulgadas de largo, y las secciones delantera y trasera del riel se mantienen unidas por un solo tornillo.



Si instala el chasis sobre un riel completamente contraído, las secciones delantera y trasera del riel podrían separarse.

Pasos

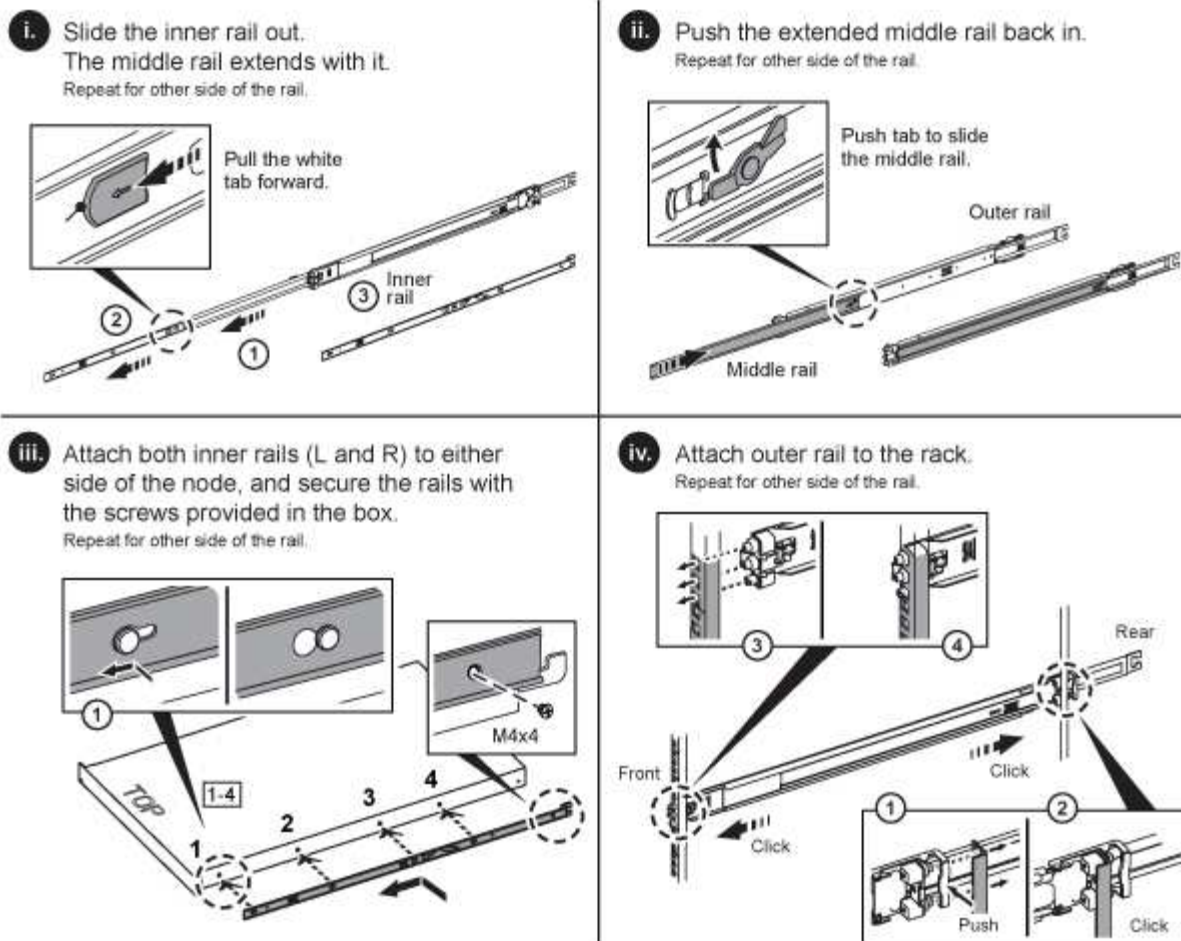
1. Alinea la parte delantera del riel con los agujeros del poste delantero del estante.
2. Empuja los ganchos de la parte delantera del riel hacia los orificios del poste delantero del portaequipajes y luego hacia abajo, hasta que las clavijas con resorte encajen en los orificios del portaequipajes.
3. Fije el riel al estante con tornillos. Aquí tenéis una ilustración del riel izquierdo fijado a la parte delantera del estante:



4. Extienda la sección trasera del riel hasta el poste trasero del portaequipajes.
5. Alinea los ganchos de la parte trasera del riel con los orificios correspondientes del poste trasero, asegurándote de que la parte delantera y la trasera del riel estén al mismo nivel.
6. Monte la parte trasera del riel en el soporte y fíjelo con tornillos.
7. Repita todos los pasos anteriores para el otro lado del estante.

H610S

Aquí se muestra una ilustración para la instalación de rieles para un nodo de almacenamiento H610S:



El H610S tiene rieles izquierdo y derecho. Coloque el orificio del tornillo hacia abajo para que el tornillo de mariposa H610S pueda fijar el chasis al riel.

Instalar y cablear los nodos

El nodo de almacenamiento H410S se instala en un chasis de 2U y cuatro nodos. Para el H610S, instale el chasis/nodo directamente sobre los rieles del rack.



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

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

H410S

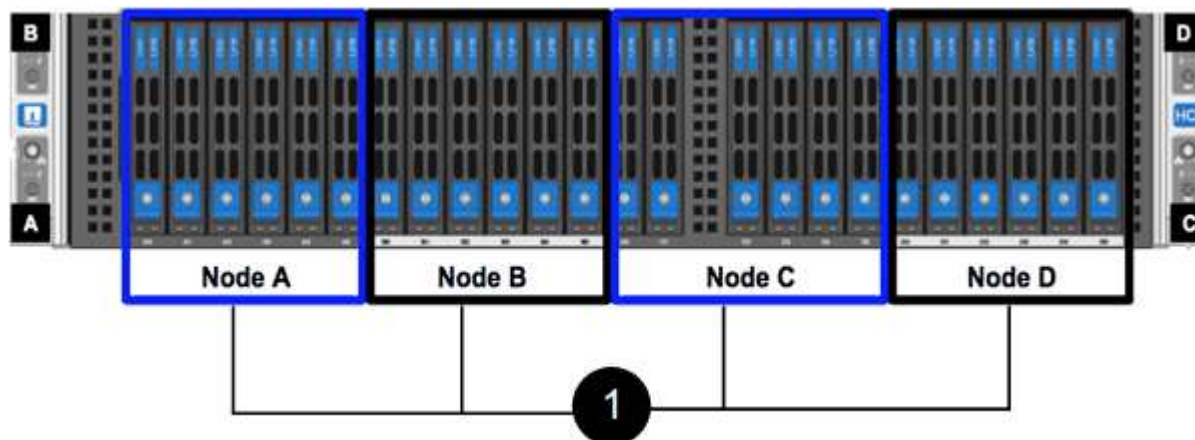
Pasos

1. Instale los nodos H410S en el chasis. Aquí tenéis un ejemplo de vista trasera de un chasis con cuatro nodos instalados:



Tenga cuidado al levantar los componentes e instalarlos en el bastidor. Un chasis vacío de dos unidades de rack (2U) y cuatro nodos pesa 54,45 lb (24,7 kg) y un nodo pesa 8,0 lb (3,6 kg).

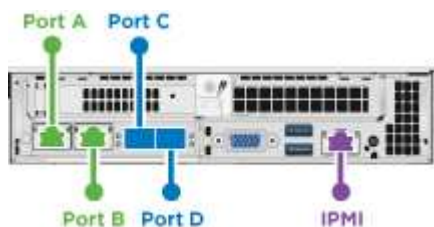
2. Instala las unidades.



3. Conectar los nodos mediante cable.



Si las rejillas de ventilación de la parte trasera del chasis están bloqueadas por cables o etiquetas, esto puede provocar fallos prematuros de los componentes debido al sobrecalentamiento.



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

4. Conecte los cables de alimentación a las dos unidades de alimentación por chasis y conéctelos a una PDU de 240 V o a una toma de corriente.

5. Encendido de los nodos.



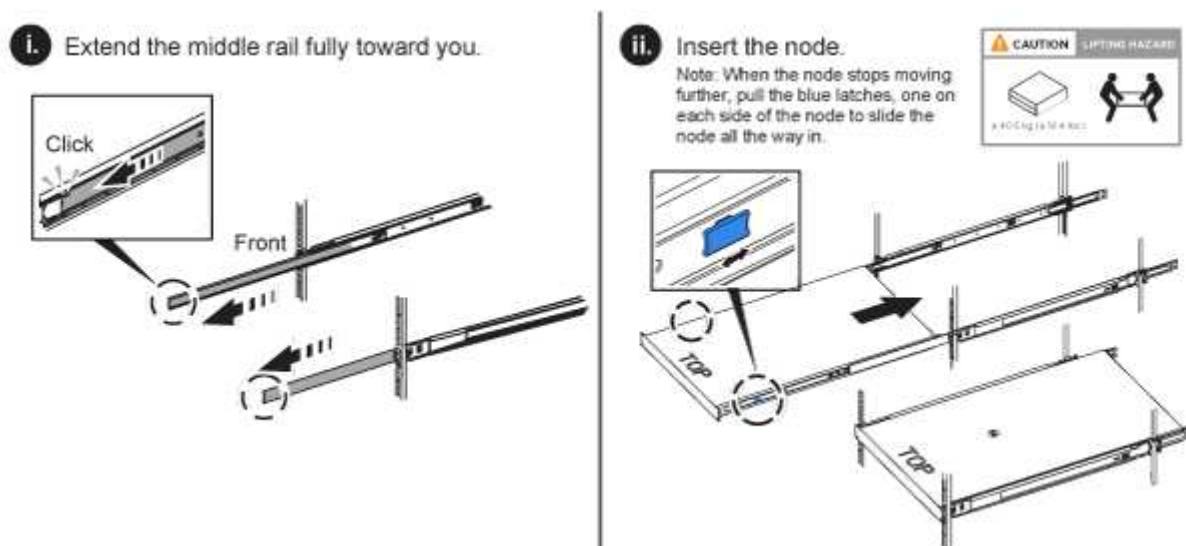
El nodo tarda aproximadamente seis minutos en arrancar.



H610S

Pasos

1. Instale el chasis H610S. Aquí se muestra una ilustración para la instalación del nodo/chasis en el rack:

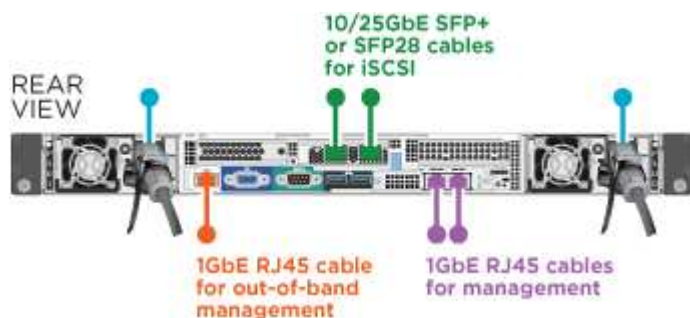


Tenga cuidado al levantar los componentes e instalarlos en el bastidor. Un chasis H610S pesa 40,5 lb (18,4 kg).

2. Conectar los nodos mediante cable.



Si las rejillas de ventilación de la parte trasera del chasis están bloqueadas por cables o etiquetas, esto puede provocar fallos prematuros de los componentes debido al sobrecalentamiento.



- Conecte el nodo a una red 10/25GbE utilizando dos cables SFP28 o SFP+.
- Conecte el nodo a una red 1GbE utilizando dos conectores RJ45.

- Conecte el nodo a una red 1GbE utilizando un conector RJ-45 en el puerto IPMI.
- Conecte ambos cables de alimentación al nodo.

3. Encendido de los nodos.



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



Configurar los nodos

Una vez instalados los racks y el cableado del hardware, ya puede configurar su nuevo recurso de almacenamiento.

Pasos

1. Conecta un teclado y un monitor al nodo.
2. En la interfaz de usuario del terminal (TUI) que se muestra, configure los ajustes de red y clúster para el nodo utilizando la navegación en pantalla.



Debes obtener la dirección IP del nodo desde la interfaz de usuario de texto (TUI). Esto es necesario cuando se agrega el nodo a un clúster. Después de guardar la configuración, el nodo queda en estado pendiente y puede añadirse a un clúster. Consulte la <insertar enlace a la sección de Configuración>.

3. Configure la administración fuera de banda utilizando el controlador de administración de la placa base (BMC). Estos pasos se aplican **únicamente a los nodos H610S**.
 - a. Utilice un navegador web y acceda a la dirección IP predeterminada de BMC : 192.168.0.120
 - b. Inicia sesión usando **root** como nombre de usuario y **calvin** como contraseña.
 - c. Desde la pantalla de administración del nodo, vaya a **Configuración > Configuración de red** y configure los parámetros de red para el puerto de administración fuera de banda.



Ver "[Este artículo de la base de conocimientos \(se requiere iniciar sesión\)](#)".

Crear un clúster

Después de agregar el nodo de almacenamiento a su instalación y 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 requerida en la ventana **Crear un nuevo clúster**. Ver el "[Descripción general de la configuración](#)" Para más información.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Reemplazar un nodo H410S

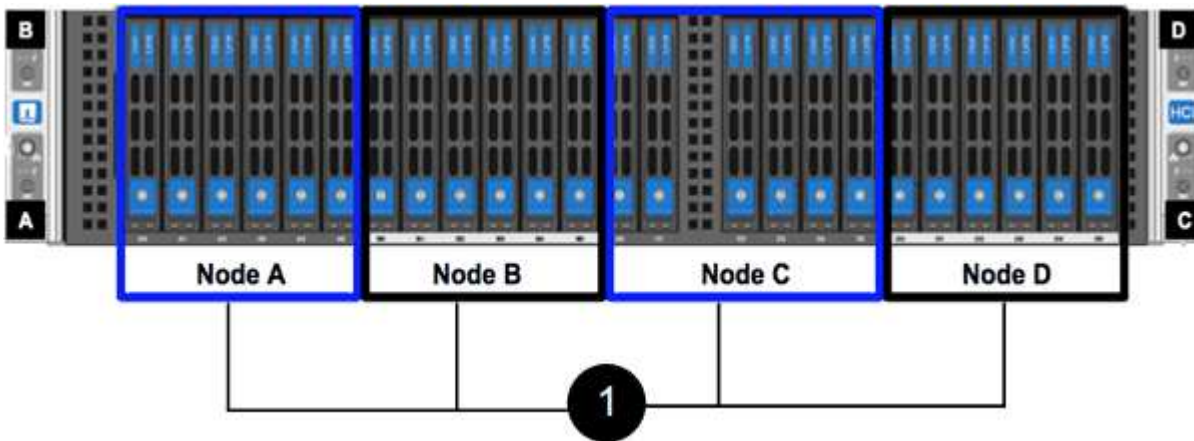
Debe reemplazar un nodo de almacenamiento en caso de fallo de la CPU, problemas con la tarjeta Radian, otros problemas con la placa base o si no se enciende. Las instrucciones se aplican a los nodos de almacenamiento H410S.

Las alarmas en la interfaz de usuario del software NetApp Element le avisan cuando falla un nodo de almacenamiento. Debe utilizar la interfaz de usuario de Element para obtener el número de serie (etiqueta de servicio) del nodo que falló. Necesitas esta información para localizar el nodo que ha fallado en el clúster.

Aquí está la parte posterior de un chasis de dos unidades de rack (2U) y cuatro nodos con cuatro nodos de almacenamiento:



Aquí se muestra la vista frontal de un chasis de cuatro nodos con nodos H410S, donde se aprecian las bahías que corresponden a cada nodo:



Lo que necesitarás

- Has verificado que tu nodo de almacenamiento está defectuoso y necesita ser reemplazado.
- Has obtenido un nodo de almacenamiento de reemplazo.
- Llevas una pulsera antiestática (ESD) o has tomado otra protección antiestática.
- Has etiquetado cada cable que está conectado al nodo de almacenamiento.

Aquí tenéis una descripción general de alto nivel de los pasos:

- [Prepárese para reemplazar el nodo](#)
- [Reemplace el nodo en el chasis](#)
- [Agrega el nodo al clúster](#)

Prepárese para reemplazar el nodo

Debe eliminar correctamente el nodo de almacenamiento defectuoso del clúster en la interfaz de usuario del software NetApp Element antes de instalar el nodo de reemplazo. Puedes hacerlo sin causar ninguna interrupción del servicio. Debe obtener el número de serie del nodo de almacenamiento defectuoso desde la interfaz de usuario de Element y compararlo con el número de serie que aparece en la etiqueta de la parte posterior del nodo.

Pasos

1. En la interfaz de usuario de Element, seleccione **Clúster > Unidades**.
2. Retire las unidades del nodo utilizando uno de los siguientes métodos:

Opción	Pasos
Para extraer unidades individuales	a. Haz clic en Acciones para la unidad que deseas eliminar. b. Haga clic en Eliminar.
Para extraer varias unidades	a. Seleccione todas las unidades que desea eliminar y haga clic en Acciones en lote. b. Haga clic en Eliminar.

3. Seleccione **Clúster > Nodos**.
4. Anote el número de serie (etiqueta de servicio) del nodo defectuoso. Debe coincidir con el número de serie que aparece en la etiqueta de la parte posterior del nodo.
5. Después de anotar el número de serie, elimine el nodo del clúster de la siguiente manera:
 - a. Seleccione el botón **Acciones** para el nodo que desea eliminar.
 - b. Seleccione **Eliminar**.

Reemplace el nodo en el chasis

Después de eliminar el nodo defectuoso del clúster mediante la interfaz de usuario del software NetApp Element, ya puede extraer físicamente el nodo del chasis. Debe instalar el nodo de reemplazo en la misma ranura del chasis de la que extrajo el nodo averiado.

Pasos

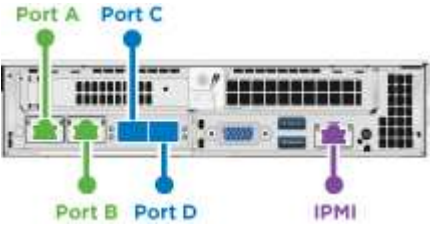
1. Utilice protección antiestática antes de continuar.
2. Desembale el nuevo nodo de almacenamiento y colóquelo sobre una superficie nivelada cerca del chasis.

Conserva el material de embalaje para cuando devuelvas el nodo defectuoso a NetApp.

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

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

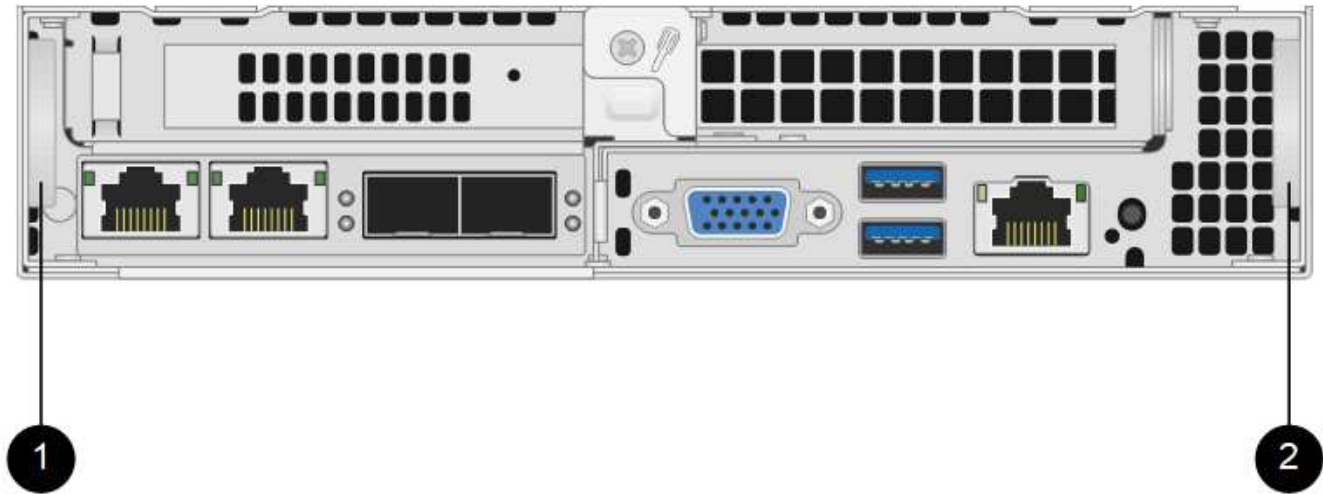
Aquí tenéis una imagen que muestra la parte posterior de un nodo de almacenamiento:



Puerto	Detalles
Puerto A	1 puerto RJ45 de 1/10 GbE
Puerto B	1 puerto RJ45 de 1/10 GbE
Puerto C	Puerto SFP+ o SFP28 de 10/25 GbE
Puerto D	Puerto SFP+ o SFP28 de 10/25 GbE
IPMI	1 puerto RJ45 de 1/10 GbE

- 4. Desconecta todos los cables del nodo de almacenamiento.
- 5. Tire hacia abajo de la manija de leva del lado derecho del nodo y extraiga el nodo utilizando ambas manijas de leva.

La manivela que se tira hacia abajo tiene una flecha que indica la dirección en la que se mueve. La otra manivela no se mueve y está ahí para ayudarte a extraer el nodo.



Artículo	Descripción
1	Mango de leva para ayudarte a extraer el nodo.

Artículo	Descripción
2	Manija de leva que se tira hacia abajo antes de extraer el nodo.



Sujete el nodo con ambas manos al extraerlo del chasis.

6. Coloca el nodo sobre una superficie nivelada.

Debes empaquetar el nodo y devolverlo a NetApp.

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



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

8. Traslada las unidades del nodo que retiraste e insértalas en el nuevo nodo.

9. Vuelva a conectar los cables a los puertos de los que los desconectó originalmente.

Las etiquetas que tenían los cables cuando los desconectaste te servirán de guía.



- a. Si las rejillas de ventilación de la parte trasera del chasis están bloqueadas por cables o etiquetas, esto puede provocar fallos prematuros de los componentes debido al sobrecalentamiento.
- b. No fuerce los cables en 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 demás nodos del chasis.

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

Agrega el nodo al clúster

Cuando se agrega un nodo al clúster o se instalan nuevas unidades en un nodo existente, las unidades se registran automáticamente como disponibles. Debe agregar las unidades al clúster utilizando la interfaz de usuario de Element o la API antes de que puedan participar en el clúster.

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

Pasos

1. Seleccione **Clúster > Nodos**.
2. Seleccione **Pendientes** 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 agregar varios nodos, seleccione la casilla de verificación de los nodos que desea agregar y luego **Acciones en lote**.



Si el nodo que está agregando tiene una versión del 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 del clúster. Después de que se actualiza el nodo, se agrega 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. Desde la interfaz de usuario de Element, seleccione **Clúster > Unidades**.

6. Seleccione **Disponible** 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 agregar varias unidades, seleccione las casillas de verificación de las unidades que desea agregar, seleccione **Acciones en lote** y, a continuación, seleccione **Agregar**.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Reemplazar un nodo H610S

Es posible que necesite reemplazar el chasis si falla el ventilador, la unidad central de procesamiento (CPU) o el módulo de memoria en línea dual (DIMM), o para solucionar problemas de sobrecalentamiento o problemas con el proceso de arranque. El LED ámbar parpadeante en la parte frontal del chasis indica una posible necesidad de reemplazar el chasis. Debe ponerse en contacto con el soporte de NetApp antes de continuar.



Ver el ["Artículo de la base de conocimientos"](#) Para obtener información sobre los requisitos de instalación para los nodos H610S. Los nodos de almacenamiento H610S nuevos y de repuesto podrían tener requisitos de instalación adicionales según la versión del software Element existente del clúster de almacenamiento. Póngase en contacto con el soporte de NetApp para obtener más información.



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

Mejores prácticas para agregar y eliminar unidades

Deberá seguir estas prácticas recomendadas para agregar unidades al clúster:

- Agrega todas las unidades de bloque y asegúrate de que la sincronización de bloques esté completa antes de agregar las unidades de partición.
- Para el software Element 10.x y versiones posteriores, agregue todas las unidades de bloque a la vez.

Asegúrese de no realizar esta operación con más de tres nodos a la vez.

- Para el software Element 9.x y versiones anteriores, agregue tres unidades a la vez, permitiendo que se sincronicen completamente antes de agregar el siguiente grupo de tres.
- Retire la unidad de partición y asegúrese de que la sincronización de la partición esté completa antes de retirar las unidades de bloque.
- Retire todas las unidades de bloque de un solo nodo a la vez. Asegúrese de que la sincronización de todos los bloques esté completa antes de pasar al siguiente nodo.

Lo que necesitarás

- Usted se ha puesto en contacto con el soporte de NetApp . Si va a solicitar un repuesto, debería tener un caso abierto con el soporte de NetApp .
- Has obtenido el nodo de reemplazo.
- Llevas una pulsera antiestática (ESD) o has tomado otra protección antiestática.
- Si necesita realizar el proceso de Restauración de Imagen de Fábrica (RTFI), ya ha obtenido la llave USB. El soporte de NetApp puede ayudarle a decidir si necesita realizar el proceso RTFI.
- Tienes un teclado y un monitor.
- Has eliminado correctamente el nodo averiado del clúster.
- Si un módulo DIMM ha fallado, significa que ha retirado unidades antes de eliminar el nodo del clúster.

Acerca de esta tarea

Las alarmas en la interfaz de usuario de Element te avisan cuando falla un host. Debe hacer coincidir el número de serie del host averiado del cliente web de VMware vSphere con el número de serie que figura en la etiqueta de la parte posterior del nodo.

Pasos

1. Localice la etiqueta de servicio en la parte delantera del chasis averiado.



2. Verifique que el número de serie en la etiqueta de servicio coincida con el número de caso de soporte de NetApp cuando solicitó el chasis de reemplazo.

3. Conecta el teclado y el monitor a la parte posterior del chasis averiado.
4. Verifique el número de serie del nodo averiado con el soporte de NetApp .
5. Apague el chasis.
6. Etiqueta las unidades de la parte delantera y los cables de la parte trasera con sus ubicaciones, para que puedas volver a colocarlos en los mismos lugares después del reemplazo. Consulte la siguiente imagen para ver la ubicación de las unidades en el chasis:



7. Retire los cables.
8. Retire el chasis aflojando los tornillos moleteados de las orejas de montaje. Deberá empaquetar y devolver el chasis defectuoso a NetApp.
9. Instale el chasis de repuesto.
10. Retire con cuidado las unidades del chasis averiado e insértelas en el chasis de repuesto.



Debes insertar las unidades en las mismas ranuras en las que estaban antes de extraerlas.

11. Retire las fuentes de alimentación del chasis averiado e insértelas en el chasis de repuesto.
12. Inserte los cables de alimentación y los cables de red en sus puertos originales.
13. Se podrían insertar transceptores conectables de factor de forma pequeño (SFP) en los puertos 10GbE del nodo de reemplazo. Debes quitarlos antes de conectar los puertos 10GbE.



Consulte la documentación del fabricante del switch si este 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.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Reemplazar unidades

Si una unidad está defectuosa o si su nivel de desgaste cae por debajo de un umbral, debe reemplazarla. Las alarmas en la interfaz de usuario del software Element le notifican cuando una unidad ha fallado o está a punto de fallar. Puedes reemplazar en caliente una unidad averiada.

Acerca de esta tarea

Este procedimiento sirve para reemplazar unidades en nodos de almacenamiento H410S y H610S. Al extraer una unidad, esta se desconecta de internet. Los datos que contiene la unidad se eliminan y se migran a otras unidades del clúster. La migración de datos a otras unidades activas del sistema puede tardar desde unos minutos hasta una hora, dependiendo de la utilización de la capacidad y las operaciones de E/S activas en el

clúster. Deberá seguir estas buenas prácticas para el manejo de unidades durante su extracción y reemplazo:

- Mantén la unidad en la bolsa ESD hasta que estés listo para instalarla.
- Abra la bolsa ESD a mano o corte la parte superior con unas tijeras.
- Utilice siempre una pulsera antiestática conectada a tierra a una superficie sin pintar de su chasis.
- Utilice siempre ambas manos al extraer, instalar o transportar una unidad.
- Nunca fuerce una unidad en el chasis.
- Utilice siempre embalaje homologado para el envío de unidades.
- No apile las unidades una encima de otra.

Mejores prácticas para agregar y eliminar unidades

- Agrega todas las unidades de bloque y asegúrate de que la sincronización de bloques esté completa antes de agregar las unidades de partición.
- Para el software Element 10.x y versiones posteriores, agregue todas las unidades de bloque a la vez. Asegúrese de no realizar esta operación con más de tres nodos a la vez.
- Para el software Element 9.x y versiones anteriores, agregue tres unidades a la vez, permitiendo que se sincronicen completamente antes de agregar el siguiente grupo de tres.
- Retire la unidad de partición y asegúrese de que la sincronización de la partición esté completa antes de retirar las unidades de bloque.
- Retire todas las unidades de bloque de un solo nodo a la vez. Asegúrese de que la sincronización de todos los bloques esté completa antes de pasar al siguiente nodo.

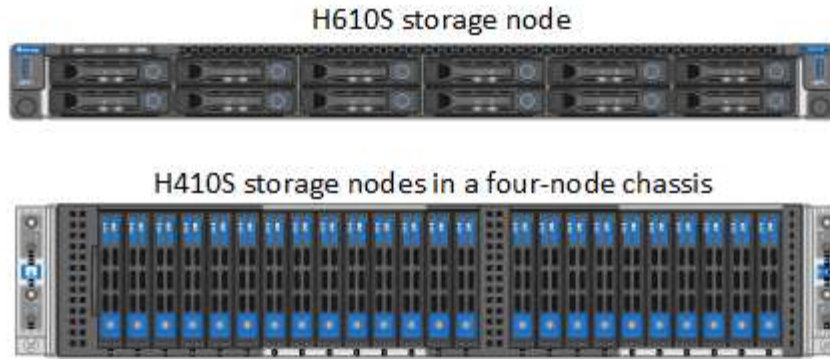
Pasos

1. Elimine la unidad del clúster utilizando la interfaz de usuario del software NetApp Element :
 - a. Desde la interfaz de usuario de Element, seleccione **Clúster > Unidades**.
 - b. Seleccione **Falló** para ver la lista de unidades que fallaron.
 - c. Anote el número de ranura de la unidad averiada. Necesitas esta información para localizar la unidad averiada en el chasis.
 - d. Seleccione **Acciones** para la unidad que desea eliminar.
 - e. Seleccione **Eliminar**.



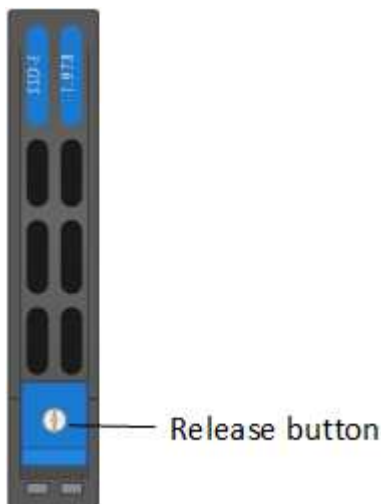
Si no hay suficiente capacidad para extraer las unidades activas antes de eliminar un nodo, aparecerá un mensaje de error al confirmar la extracción de la unidad. Una vez resuelto el error, ya puede extraer físicamente la unidad del chasis.

2. Reemplace la unidad del chasis:
 - a. Desembale la unidad de repuesto y colóquela sobre una superficie plana y libre de estática cerca del rack. Guarda los materiales de embalaje para cuando devuelvas la unidad defectuosa a NetApp. Aquí se muestra la vista frontal de los nodos de almacenamiento H610S y H410S con las unidades:



b. **(Solo H410S)** Realice los siguientes pasos:

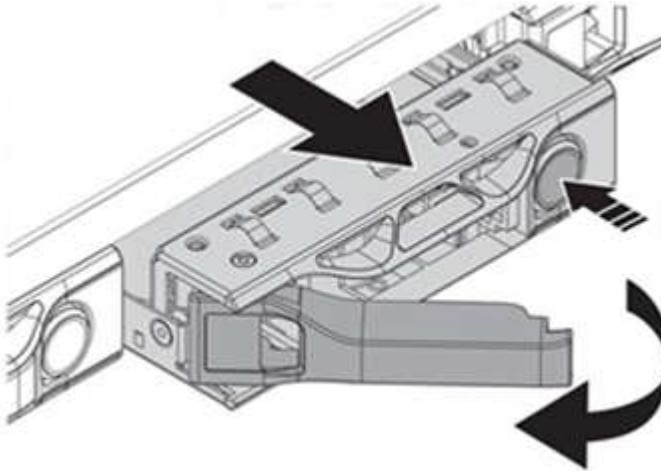
- i. Identifique el nodo haciendo coincidir el número de serie (etiqueta de servicio) con el número que anotó en la interfaz de usuario de Element. El número de serie se encuentra en una pegatina en la parte posterior de cada nodo. Una vez identificado el nodo, puede utilizar la información de la ranura para identificar la ranura en la que se encuentra la unidad averiada. Las unidades están ordenadas 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 averiada:



Al presionar el botón de liberación, la manija de leva del accionamiento se abre parcialmente y el accionamiento se libera del plano medio.

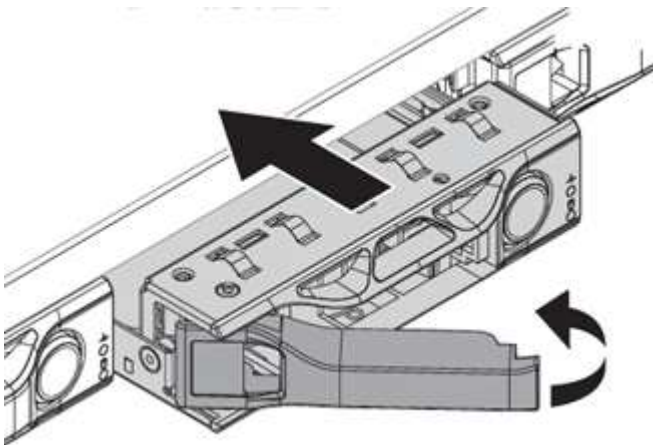
- i. Abra la manija de la leva y deslice la unidad hacia afuera con cuidado usando ambas manos.
 - ii. Coloque la unidad sobre una superficie antiestática y nivelada.
 - iii. Inserte la unidad de repuesto en la ranura hasta el fondo del chasis utilizando ambas manos.
 - iv. Presione la manija de la leva 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 le proporcionará instrucciones para devolver la unidad defectuosa.
- c. **(Solo H610S)** Realice los siguientes pasos:
- i. Haga coincidir el número de ranura de la unidad averiada en la interfaz de usuario de Element con el número del chasis. El LED del disco averiado está iluminado en color ámbar.

- ii. Retire el bisel.
- iii. Pulse el botón de liberación y retire la unidad averiada como se muestra en la siguiente ilustración:



Asegúrese de que el asa de la bandeja esté completamente abierta antes de intentar deslizar la unidad fuera del chasis.

- i. Deslice la unidad hacia afuera y colóquela sobre una superficie nivelada y libre de estática.
- ii. Pulse el botón de liberación de la unidad de repuesto antes de insertarla en la bahía de la unidad. El asa de la bandeja de la unidad se abre con un resorte.



- iii. Inserte la unidad de repuesto sin utilizar una fuerza excesiva. Cuando la unidad esté insertada completamente, se oirá un clic.
 - iv. Cierre con cuidado el asa de la bandeja de la unidad.
 - v. Vuelva a instalar el bisel.
 - vi. Notifique al soporte de NetApp sobre el reemplazo de la unidad. El soporte de NetApp le proporcionará instrucciones para devolver la unidad defectuosa.
3. Vuelva a agregar la unidad al clúster utilizando la interfaz de usuario de Element.



Cuando se instala una nueva unidad en un nodo existente, la unidad se registra automáticamente como **Disponible** en la interfaz de usuario de Element. Debes agregar la unidad al clúster antes de que pueda participar en él.

- a. Desde la interfaz de usuario de Element, seleccione **Clúster > Unidades**.
- b. Seleccione **Disponible** para ver la lista de unidades disponibles.
- c. Seleccione el icono de Acciones de la unidad que desea agregar y seleccione **Agregar**.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Reemplace una unidad de fuente de alimentación

Cada chasis incluye dos unidades de alimentación para redundancia de energía. Si una fuente de alimentación está defectuosa, debe reemplazarla lo antes posible para garantizar que el chasis tenga una fuente de alimentación redundante.

Lo que necesitarás

- Usted ha determinado que la fuente de alimentación está defectuosa.
- Tienes una fuente de alimentación de repuesto.
- Usted ha comprobado que la segunda fuente de alimentación está funcionando.
- Llevas una pulsera antiestática (ESD) o has tomado otras precauciones antiestáticas.

Acerca de esta tarea

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

- Chasis NetApp HCI de dos unidades de rack (2U) y cuatro nodos
- Chasis de almacenamiento H610S de una unidad de rack (1U).



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

Las alarmas en la interfaz de usuario de Element proporcionan información sobre la unidad de fuente de alimentación defectuosa, refiriéndose a ella como PS1 o PS2. En un chasis NetApp HCI 2U de cuatro nodos, PS1 se refiere a la unidad en la fila superior del chasis y PS2 se refiere a la unidad en la fila inferior del chasis. Puede sustituir la fuente de alimentación defectuosa mientras el chasis está encendido y funcionando, siempre que la fuente de alimentación de respaldo esté funcionando.



Si va a reemplazar ambas fuentes de alimentación en un nodo, las fuentes de alimentación deben tener el mismo número de pieza y potencia. El uso de fuentes de alimentación incompatibles podría dañar el sistema.

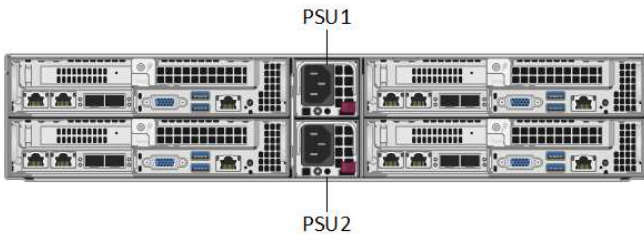
Pasos

1. Localice la fuente de alimentación defectuosa en el chasis. El LED de la unidad defectuosa muestra color ámbar.

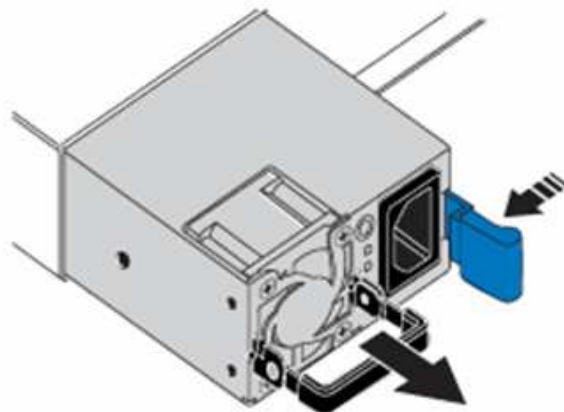
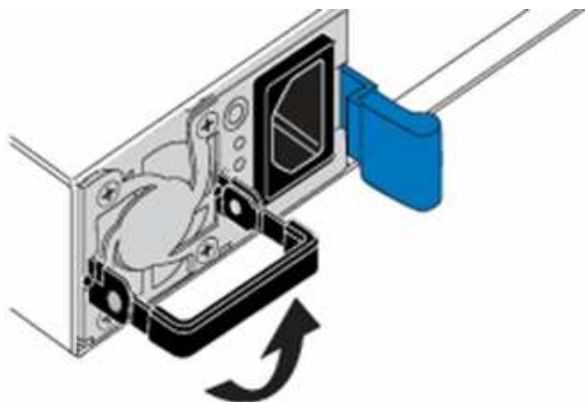


La ubicación de las fuentes de alimentación varía según el tipo de chasis.

Consulte las imágenes a continuación para ver la ubicación de las fuentes de alimentación:

Modelo	Ubicación de las unidades de alimentación
Chasis de almacenamiento NetApp HCI de 2U y cuatro nodos	 Los nodos de su chasis pueden tener un aspecto diferente según el tipo de nodos (almacenamiento o computación) que tenga.
Chasis H610S	

2. Identifique el nodo correcto utilizando la etiqueta azul extraíble o el número de serie. La etiqueta azul extraíble muestra el número de serie (S/N) y la disposición de la unidad. Confirme el número de serie del nodo que se va a reparar.
 - Si va a reemplazar ambas fuentes de alimentación, continúe con el paso 3.
 - Si va a reemplazar solo una unidad de fuente de alimentación, pase al paso 4.
3. Confirme que el nodo se ha apagado o está listo para apagarse para su mantenimiento. Tenga en cuenta lo siguiente:
 - Un nodo que se ha apagado no muestra ningún LED de encendido azul en las unidades ni en el botón de encendido.
 - Un nodo que aún no se ha apagado muestra LEDs azules en las unidades y en el botón de encendido.
 - Un nodo que ha sido apagado y está listo para el servicio muestra un LED de la fuente de alimentación parpadeante que se enciende (verde) y se apaga (sin color).
 - Un nodo que aún no se ha apagado muestra LEDs verdes fijos en las fuentes de alimentación.
4. Desconecte el cable de alimentación de la fuente de alimentación o de ambos cables de alimentación, si va a sustituir ambas unidades.
5. Levante la manija de leva y presione el pestillo azul para deslizar hacia afuera la unidad de fuente de alimentación.



La ilustración es un ejemplo. La ubicación de la(s) fuente(s) de alimentación en el 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 fuente de alimentación.

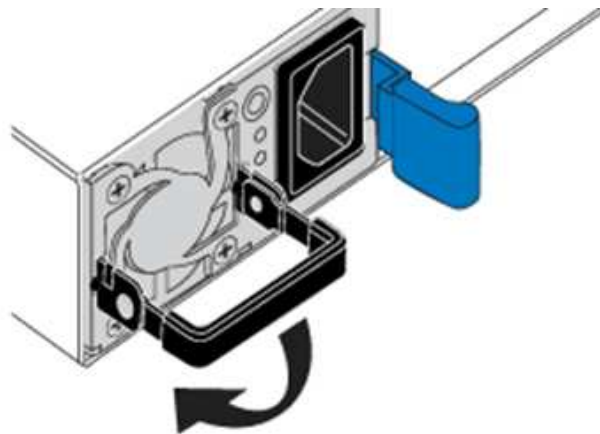
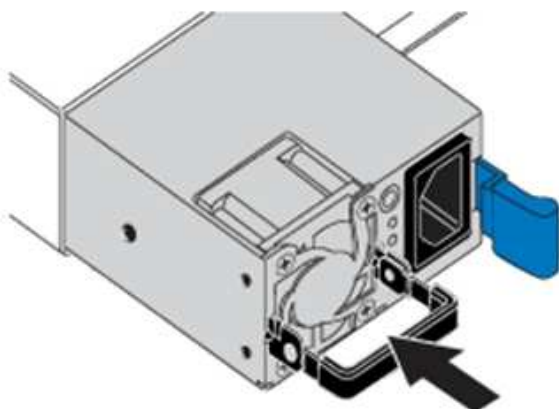
Repita los pasos 3, 4 y 5 si reemplaza una segunda unidad de fuente de alimentación.

6. Localice la etiqueta en la fuente de alimentación que retiró del chasis. La etiqueta contiene detalles del fabricante y la potencia de salida (en vatios).



No sustituya la fuente de alimentación si la potencia de la fuente de alimentación de su RMA no coincide con la potencia de la fuente de alimentación extraída. Póngase en contacto con el soporte de NetApp para conocer los siguientes pasos.

7. Utilizando ambas manos, alinee los bordes de la fuente de alimentación con la abertura del chasis, empuje suavemente la unidad dentro del chasis utilizando la manija de leva hasta que encaje en su lugar y vuelva a colocar la manija de leva en la posición vertical.



8. Conecte uno o ambos cables de alimentación.
9. Si reemplazó ambas fuentes de alimentación, vaya a la parte frontal del nodo y presione el botón de encendido para encender los nodos. Tras encender el dispositivo, el LED del botón de encendido se ilumina en color azul fijo. Los LED azules de las unidades y del botón de identificación comenzarán a parpadear.

10. Devuelva la unidad defectuosa a NetApp siguiendo las instrucciones de la caja que le fue enviada.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Información sobre el hardware de la serie SF

Reemplazar un chasis

Es posible que necesite reemplazar el chasis si falla el ventilador, la unidad central de procesamiento (CPU) o el módulo de memoria en línea dual (DIMM), o para solucionar problemas de sobrecalentamiento o problemas con el proceso de arranque. Los fallos de clúster en la interfaz de usuario (IU) del software NetApp Element y la luz ámbar parpadeante en la parte frontal del chasis son indicios de una posible necesidad de sustitución del chasis. Debe ponerse en contacto con el soporte de NetApp antes de continuar.

Lo que necesitarás

- Usted se ha puesto en contacto con el soporte de NetApp .

Si va a solicitar un repuesto, debe tener un caso abierto con el soporte de NetApp .

- Usted ha obtenido el chasis de repuesto.
- Llevas una pulsera antiestática (ESD) o has tomado otra protección antiestática.
- Si necesita realizar el proceso de Restauración de Imagen de Fábrica (RTFI), ya ha obtenido la llave USB.

El soporte de NetApp le ayudará a decidir si necesita RTFI. Ver ["Este artículo de la base de conocimientos \(se requiere iniciar sesión\)"](#) .

- Tienes un teclado y un monitor.

Acerca de esta tarea

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

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

Dependiendo de la versión de su software Element, los siguientes nodos no son compatibles:



- Comenzando con los nodos de almacenamiento Element 12.8, SF4805, SF9605, SF19210 y SF38410.
- Comenzando con los nodos de almacenamiento Element 12.7, SF2405 y SF9608 y los nodos FC FC0025 y SF-FCN-01.
- A partir de los nodos de almacenamiento Element 12.0, SF3010, SF6010 y SF9010.

Pasos

1. Localice la etiqueta de servicio del chasis averiado y verifique que el número de serie coincida con el número del caso que abrió con el soporte de NetApp cuando solicitó el reemplazo.

La etiqueta de servicio se encuentra en la parte delantera del chasis.

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



La figura anterior es un ejemplo. La ubicación exacta de la etiqueta de servicio puede variar según el modelo de su hardware.

2. Conecta el teclado y el monitor a la parte posterior del chasis averiado.
3. Verifique 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 fuentes de alimentación y los cables.
7. Retire las unidades con cuidado y colóquelas sobre una superficie antiestática y nivelada.



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

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

Deberá empaquetar y devolver el chasis defectuoso a NetApp.

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

Puedes optar por reutilizar los rieles existentes. Si va a reutilizar los rieles existentes, puede omitir este paso.

10. Deslice el chasis de repuesto sobre los rieles.

11. Para los nodos de almacenamiento, inserte las unidades del chasis averiado en el chasis de reemplazo.



Debes insertar las unidades en las mismas ranuras en las que estaban en el chasis averiado.

12. Instale las fuentes de alimentación.

13. Inserte los cables de alimentación y los cables 1GbE y 10GbE en sus puertos originales.

Los transceptores conectables de factor de forma pequeño (SFP) podrían insertarse en los puertos 10GbE del chasis de reemplazo. Debes quitarlos antes de conectar los puertos 10GbE.

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 de terminal (TUI). Pase al paso 16 y permita que el clúster vuelva a crear la imagen del nodo automáticamente cuando lo agregue mediante la interfaz de usuario.

15. **Opcional:** Si el soporte de NetApp recomienda reinstalar la imagen del nodo con una llave USB, realice los siguientes subpasos:

- a. Alimentación en el chasis. Se inicia con la imagen de clave RTFI.
- b. En la primera solicitud, escriba **Y** para crear una imagen del nodo de almacenamiento.
- c. En la segunda solicitud, escriba **N** para realizar comprobaciones del estado del hardware.

Si el script RTFI detecta un problema con un componente de hardware, muestra un error en la consola. Si ve algún error, póngase en contacto con el soporte de NetApp. Una vez finalizado el proceso RTFI, el nodo se apaga.

- d. Retire la llave USB de la ranura USB.
- e. Inicie el nodo recién configurado y espere a que aparezca la interfaz de usuario de texto (TUI).

16. Configure la información de red y clúster desde la interfaz de usuario de texto (TUI).

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

17. Agregue el nuevo nodo al clúster utilizando la interfaz de usuario del clúster.

18. Empaqueta y devuelve el chasis averiado.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Reemplazar las unidades de los nodos de almacenamiento de la serie SF

Puedes sustituir en caliente una unidad de estado sólido averiada por una unidad de

repuesto.

Lo que necesitarás

- Tienes una unidad de repuesto.
- Llevas una pulsera antiestática (ESD) o has tomado otras precauciones antiestáticas.
- Usted se ha puesto en contacto con el soporte de NetApp para verificar que la unidad SSD necesita ser reemplazada y para obtener ayuda con el procedimiento de resolución adecuado.

Necesitará la etiqueta de servicio o el número de serie cuando llame al soporte de NetApp . El equipo de soporte trabajará con usted para obtener una unidad de reemplazo 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 :

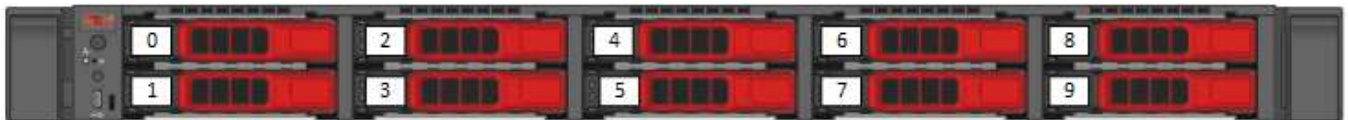
- SF2405
- SF4805
- SF9605
- SF9608
- SF19210
- SF38410

Dependiendo de la versión de su software Element, los siguientes nodos no son compatibles:



- Comenzando con los nodos de almacenamiento Element 12.8, SF4805, SF9605, SF19210 y SF38410.
- Comenzando con los nodos de almacenamiento Element 12.7, SF2405 y SF9608.
- A partir de los nodos de almacenamiento Element 12.0, SF3010, SF6010 y SF9010.

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



La figura anterior es un ejemplo. El SF9608 tiene una disposición de unidades diferente que incluye solo ocho unidades numeradas del uno al ocho, de izquierda a derecha.

La ranura 0 contiene la unidad de metadatos del nodo. Si va a sustituir la unidad en la ranura 0, debe pegar la etiqueta adhesiva incluida en la caja de envío en la unidad de repuesto, para poder identificarla por separado de las demás.

Siga estas buenas prácticas al manejar unidades:



- Evite las descargas electrostáticas (ESD) manteniendo la unidad en la bolsa ESD hasta que esté listo para instalarla.
- No introduzca herramientas metálicas ni cuchillos en la bolsa ESD.
- Abra la bolsa ESD a mano o corte la parte superior con unas tijeras.
- Conserva la bolsa ESD y cualquier material de embalaje por si necesitas devolver una unidad más adelante.
- Utilice siempre una pulsera antiestática conectada a tierra a una superficie sin pintar de su chasis.
- Utilice siempre ambas manos al extraer, instalar o transportar una unidad.
- Nunca fuerce una unidad en el chasis.
- No apile las unidades una encima de otra.
- Utilice siempre embalaje homologado para el envío de unidades.

Aquí tenéis una descripción general de alto nivel de los pasos:

- [Retire la unidad del clúster.](#)
- [Reemplace la unidad del chasis](#)
- [Agrega la unidad al clúster.](#)

Retire la unidad del clúster.

El sistema SolidFire marca una unidad como averiada si su autodiagnóstico indica al nodo que ha fallado o si la comunicación con la unidad se interrumpe durante cinco minutos y medio o más. El sistema muestra una lista de las unidades que han fallado. Debe eliminar una unidad defectuosa de la lista de unidades defectuosas en el software NetApp Element .

Pasos

1. En la interfaz de usuario de Element, seleccione **Clúster > Unidades**.
2. Seleccione **Falló** para ver la lista de unidades que fallaron.
3. Anote el número de ranura de la unidad averiada.

Necesitas esta información para localizar la unidad averiada en el chasis.

4. Retire la unidad defectuosa utilizando uno de los siguientes métodos:

Opción	Pasos
Para extraer unidades individuales	a. Seleccione Acciones para la unidad que desea eliminar. b. Seleccione Eliminar.

Opción	Pasos
Para extraer varias unidades	a. Seleccione todas las unidades que desea eliminar y, a continuación, seleccione Acciones en lote . b. Seleccione Eliminar .

Reemplace la unidad del chasis

Después de eliminar una unidad defectuosa de la lista de unidades defectuosas en la interfaz de usuario de Element, estará listo para reemplazar físicamente la unidad defectuosa del chasis.

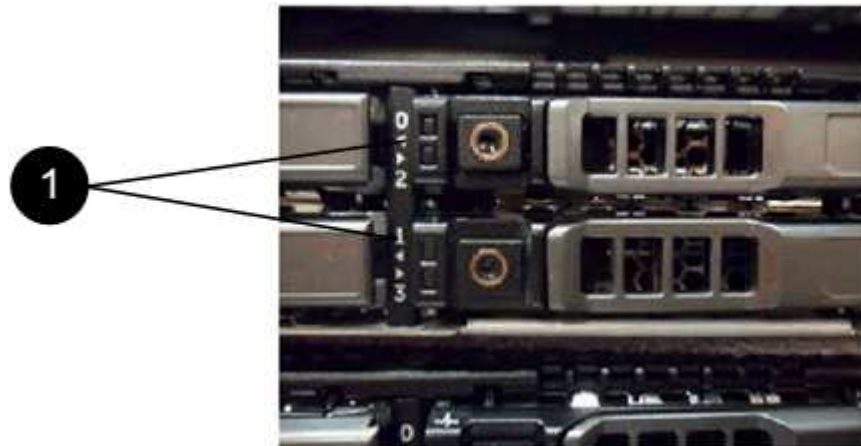
Pasos

1. Desembale la unidad de repuesto y colóquela sobre una superficie plana y libre de estática cerca del rack.

Guarda los materiales de embalaje para cuando devuelvas la unidad defectuosa a NetApp.

2. Haga coincidir el número de ranura de la unidad averiada en la interfaz de usuario de Element con el número del chasis.

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



Artículo	Descripción
1	Números de ranura de la unidad

3. Pulse el círculo rojo de la unidad que desea extraer para liberarla.

El pestillo se abre con un clic.

4. Deslice la unidad fuera del chasis y colóquela sobre una superficie nivelada y libre de estática.
5. Presione el círculo rojo en la unidad de repuesto antes de deslizarla en la ranura.
6. Inserte la unidad de repuesto 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 le proporcionará instrucciones para devolver la unidad defectuosa.

Agrega la unidad al clúster.

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

Pasos

1. En la interfaz de usuario de Element, haga clic en **Clúster > Unidades**.
2. Haz clic en **Disponible** para ver la lista de unidades disponibles.
3. Elija una de las siguientes opciones para agregar unidades:

Opción	Pasos
Para agregar unidades individuales	a. Seleccione el botón Acciones para la unidad que desea agregar. b. Seleccione Agregar.
Para agregar varias unidades	a. Seleccione las casillas de verificación de las unidades que desea agregar y, a continuación, seleccione Acciones en lote. b. Seleccione Agregar.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Reemplace una unidad de fuente de alimentación

Cada chasis SolidFire incluye dos unidades de alimentación para redundancia de energía. Si falla una fuente de alimentación, debe sustituirla lo antes posible para garantizar que el chasis tenga una fuente de alimentación redundante.

Lo que necesitarás

- Usted ha determinado que es necesario reemplazar la fuente de alimentación.
- Tienes una fuente de alimentación de repuesto.
- Usted ha comprobado que la segunda fuente de alimentación está funcionando.
- Llevas una pulsera antiestática (ESD) o has tomado otras precauciones antiestáticas.

Acerca de esta tarea

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

- SF2405
- SF4805
- SF9605
- SF9608

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



Dependiendo de la versión de su software Element, los siguientes nodos no son compatibles:

- Comenzando con los nodos de almacenamiento Element 12.8, SF4805, SF9605, SF19210 y SF38410.
- Comenzando con los nodos de almacenamiento Element 12.7, SF2405 y SF9608, y los nodos FC FC0025 y SF-FCN-01.
- A partir de los nodos de almacenamiento Element 12.0, SF3010, SF6010 y SF9010.

Pasos

1. Desconecte el cable de alimentación de la fuente de alimentación que está reemplazando.
2. Pulse el botón de liberación para deslizar la unidad de alimentación fuera del chasis.



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

3. Utilizando ambas manos, alinee los bordes de la fuente de alimentación de repuesto con la abertura del chasis y empuje suavemente la unidad hacia el interior del chasis.



No utilice una fuerza excesiva al deslizar la fuente de alimentación en el chasis para evitar daños en el hardware.

4. Enchufe el cable de alimentación.
5. Devuelva la unidad defectuosa a NetApp siguiendo las instrucciones de la caja que le fue enviada.

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

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Volver a la información de la imagen de fábrica

Configurar la imagen de retorno a fábrica

Los sistemas de almacenamiento NetApp SolidFire 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 NetApp Element sin configurar. El proceso RTFI está disponible para todos los nodos SolidFire .

Los sistemas SolidFire utilizan un único proceso RTFI para todas las instalaciones del software Element. Esto incluye instalaciones manuales internas realizadas por desarrolladores, instalaciones automáticas mediante pruebas automatizadas del marco de trabajo, instalaciones de campo realizadas por ingenieros de servicio y clientes, e instalaciones realizadas por diversos integradores y socios. El mismo proceso RTFI se utiliza en todos los nodos SolidFire, independientemente del chasis o tipo de nodo en uso, para solucionar automáticamente cualquier problema.

El público objetivo de esta guía son los integradores que instalan, configuran, utilizan o solucionan problemas relacionados con el almacenamiento.

- **Linux:** Tienes cierta experiencia con sistemas Linux.
- **Redes:** Posee conocimientos sobre redes de servidores y almacenamiento en red, incluyendo direcciones IP, máscaras de red y puertas de enlace.



El proceso RTFI destruye los datos y borra de forma segura todos los datos y detalles de configuración del nodo e instala un nuevo sistema operativo. Verifique que el nodo utilizado para el proceso RTFI no esté activo como parte de un clúster.

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

- [Opciones de instalación y despliegue de RTFI](#)
- [Realizar el proceso RTFI](#)
- [Menú de opciones RTFI](#)

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Opciones de instalación y despliegue de RTFI

El proceso Return To Factory Image (RTFI) utiliza un medio de arranque e instalable con un sistema operativo Linux completamente autónomo y minimalista para implementar el software Element en un nodo. Puedes descargar la imagen ISO RTFI específica para tu versión de software Element desde el ["Sitio de soporte de NetApp"](#).

Después de descargar la imagen ISO de RTFI, puede implementarla siguiendo uno de los siguientes métodos de uso común:

- **Llave USB física:** Puede grabar una imagen ISO de arranque del software Element en una llave USB. Para obtener instrucciones, consulte el artículo de la base de conocimientos. ["Cómo crear una clave RTFI para reinstalar la imagen de un nodo de almacenamiento SolidFire"](#). Inserte la llave USB con la ISO en el nodo e inicie desde la llave USB.
- **Medios virtuales que utilizan el puerto de administración del controlador de administración de la placa base (BMC):** Puede utilizar el BMC para conectarse dinámicamente a la ISO ubicada en su sistema cliente. La imagen ISO se pone a disposición del sistema operativo anfitrión como una unidad virtual (CD o DVD). Para obtener más información, consulte el artículo de la base de conocimientos. ["Cómo enviar información en tiempo real \(RTFI\) a un nodo mediante BMC"](#).
- **Arranque de red mediante un entorno de ejecución previo al arranque (PXE), protocolo de**

transferencia de archivos trivial (TFTP) o FTP: En lugar de descomprimir manualmente una imagen ISO, puede usar `autofs` extraer automáticamente una imagen cuando el proceso RTFI lo solicite. Este mecanismo de despliegue requiere una configuración inicial más compleja, pero permite una correcta automatización y escalabilidad de la instalación.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

El proceso RTFI

Puede iniciar el proceso de Restauración de la Imagen de Fábrica (RTFI) interactuando con el nodo a través de mensajes de consola de texto que aparecen antes de que arranque el sistema.



El proceso RTFI destruye los datos y borra de forma segura todos los datos y detalles de configuración del nodo e instala un nuevo sistema operativo. Verifique que el nodo utilizado para el proceso RTFI no esté 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 en un nodo.
3. Valida y actualiza el firmware.
4. Comprueba el hardware.
5. Prueba el hardware.
6. Borra de forma segura todas las unidades seleccionadas.

7. Divide 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 del host), la configuración predeterminada del clúster y el cargador de arranque GRUB.
10. Detiene todos los servicios, recopila registros y reinicia.

Para configurar su nodo después de que el proceso RTFI se complete correctamente, consulte la ["Documentación para su versión del software Element"](#) . Después de que un nodo completa con éxito el proceso RTFI, pasa al estado *disponible* (no configurado) de forma predeterminada.

Realizar el proceso RTFI

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

Para obtener información sobre cómo crear una llave USB o utilizar el BMC para realizar el proceso RTFI, consulte [Opciones de instalación y despliegue de RTFI](#) .

Antes de empezar

Verifique que cumple con los siguientes requisitos:

- Tienes acceso a una consola para el nodo SolidFire .
- El nodo en el que está realizando el proceso RTFI está encendido y conectado a una red.
- El nodo en el que está realizando el proceso RTFI no forma parte de un clúster activo.
- Tienes acceso a un medio de instalación de arranque que contiene la imagen de la versión del software Element correspondiente a tu 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 conéctese a la interfaz de usuario IP de BMC y abra la consola **iKVM/HTML5** desde la pestaña **Control remoto** en la interfaz de usuario.
2. Inserte una llave USB con una imagen apropiada en una de las dos ranuras USB de la parte posterior del nodo.
3. Encienda o reinicie el nodo. Durante el arranque, seleccione Dispositivo de arranque pulsando **F11**:



Debe seleccionar **F11** varias veces en rápida sucesión porque la pantalla del dispositivo de arranque pasa rápidamente.

4. En el menú de selección de dispositivo de arranque, resalte la opción USB.

Las opciones que aparecen dependen de la marca del USB que estás utilizando.



Si no aparece ningún dispositivo USB en la lista, acceda a la BIOS, verifique que el USB esté incluido en el orden de arranque, reinicie y vuelva a intentarlo.

Si eso no resuelve el problema, acceda a la BIOS, vaya a la pestaña **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 seleccionado. Seleccione la versión deseada y pulse Intro para iniciar el proceso RTFI.

Aparecen el nombre y el número de versión del software RTFI Image Element.

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



Una vez iniciado el proceso, todos los datos y detalles de configuración se borran permanentemente del nodo. Si decide no continuar, se le redirige a la [Menú de opciones RTFI](#).



Si desea ver la consola durante el proceso RTFI, puede presionar las teclas **ALT+F8** para alternar al modo detallado de la consola. Presione **ALT+F7** para regresar a la interfaz gráfica principal.

7. Ingrese **No** cuando se le solicite realizar pruebas de hardware exhaustivas, a menos que tenga motivos para sospechar una falla de hardware o que el Soporte de NetApp le indique que realice las pruebas.

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

8. Si es necesario, retire todos los medios de instalación de arranque después de apagar el nodo.

El nodo ya está listo para encenderse y configurarse. Ver el "[Documentación de almacenamiento de configuración del software Element](#)" para configurar el nodo de almacenamiento.

Si recibió un mensaje de error durante el proceso RTFI, consulte [Menú de opciones RTFI](#).

Encuentra más información

- "[Documentación del software SolidFire y Element](#)"
- "[Documentación para versiones anteriores de los productos NetApp SolidFire y Element](#)"

Menú de opciones RTFI

El siguiente menú de opciones aparece si el proceso RTFI no tiene éxito o si elige no continuar en la solicitud inicial del proceso RTFI.



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

Opción	Descripción
Reiniciar	Finaliza el proceso RTFI y reinicia el nodo en su estado actual. No se realiza ninguna limpieza.
Apagado	Apaga correctamente el nodo en su estado actual. No se realiza ninguna limpieza.
Salida	Finaliza el proceso RTFI y abre una ventana de comandos.
Registros de carga	Recopila todos los registros del sistema y carga un único archivo de registro consolidado en una URL específica.

Registros de carga

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

Pasos

1. En el menú de opciones RTFI, ingrese **UploadLogs**.
2. Introduzca la información del directorio remoto:
 - a. Escriba una URL que incluya el protocolo. Por ejemplo: `ftp://`, `scp://`, `http://`, or `https://`.
 - b. (Opcional) Agregue un nombre de usuario y una contraseña integrados. Por ejemplo:
`scp://user:password@URLaddress.com`.



Para conocer todas las opciones de sintaxis, consulte la ["rizo"](#) Manual de usuario.

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

Utilice el túnel de soporte

Si necesita asistencia técnica para su sistema NetApp HCI o su sistema de almacenamiento all-flash SolidFire, el soporte de NetApp puede conectarse de forma remota con su sistema. Para iniciar una sesión y obtener

acceso remoto, el soporte de NetApp puede abrir una conexión Secure Shell (SSH) inversa a su entorno.

Puede abrir un puerto TCP para una conexión de túnel inverso SSH con el soporte de NetApp . Esta conexión permite al soporte de NetApp iniciar sesión en su nodo de administración.

Antes de empezar

- Para los servicios de administración 2.18 y posteriores, la capacidad de acceso remoto está deshabilitada en el nodo de administración de forma predeterminada. Para habilitar la funcionalidad de acceso remoto, consulte ["Gestionar la funcionalidad SSH en el nodo de administración"](#) .
- Si su nodo de administración se encuentra detrás de un servidor proxy, se requieren los siguientes puertos TCP en el archivo sshd.config:

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

Pasos

- Inicie sesión en su nodo de administración y abra una sesión de terminal.
- Cuando se le solicite, ingrese 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) Desactivar ["funcionalidad de acceso remoto"](#) de nuevo.



SSH permanecerá habilitado en el nodo de administración si no lo deshabilita. La configuración habilitada para SSH persiste en el nodo de administración a través de actualizaciones y mejoras hasta que se deshabilita manualmente.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

nodos de almacenamiento

Versiones de firmware compatibles para los nodos de almacenamiento de la serie H y SolidFire .

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

H610S

Número de modelo (parte de la familia): H610S **Números de modelo completos:** H610S-1, H610S-1-NE, H610S-2, H610S-2-NE, H610S-4, H610S-4-NE y H610S-2F

Firmware de componentes gestionado por un paquete de firmware de almacenamiento

Durante el período 11.x, el software NetApp Element era la única forma de lanzar firmware. A partir de Element 12.0, se introdujo el concepto de **Paquete de Firmware de Almacenamiento** y las actualizaciones de firmware ahora eran posibles mediante un Paquete de Firmware de Almacenamiento publicado de forma independiente o un Paquete de Firmware de Almacenamiento incluido como parte de una versión de Element 12.x.



Un guion (-) en la siguiente tabla indica que el componente de hardware en cuestión NO era compatible con ese vehículo de lanzamiento determinado.

Ve hí cu lo de lib er aci ón	Fe ch a de la nza mi en to	BI OS	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de en DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de en DI M de ca ch é NV DI M M int eli ge nt e (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 2.1 82. 0	17 de oct ub re de 20 24	3B 14	4.0 1.0 7	12 2	14. 25. 10 20	16. 32. 10 10	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,5	2,1 7	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 A0 2Q	11 09 3A 10	11 0B 3A 10

Ve hí cu lo de lib er aci ón	Fe ch a de la nza mi en to	BI OS	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 2.1 75. 0	15 de jun io de 20 23	3B 11	3.9 4.0 7	12 2	14. 25. 10 20	16. 32. 10 10	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,5	2,1 7	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 60 2Q	11 09 2A 10	11 0B 2A 10

Ve hí cu lo de lib er aci ón	Fe ch a de la nza mi en to	BI OS	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M int eli ge nt e (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa quet e de fir m wa re de al mac en a mi en to 2.1 64. 0	20 de oct ub re de 20 22	3B 11	3.9 4.0 7	12 2	14. 25. 10 20	16. 32. 10 10	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,3	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 60 2Q	11 09 2A 10	11 0B 2A 10

Ve hí cu lo de lib er aci ón	Fe ch a de la nza mi en to	BI OS	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa quet e de fir m wa re de al ma cen a mi en to 2.1 64. 0 ha st a Ne tA pp El e m	20 de oct ub re de 20 22	3B 11	3.9 4.0 7	12 2	14. 25. 10 20	16. 32. 10 10	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,3	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 60 2Q	11 09 2A 10	11 0B 2A 10

Ve hí cu lo de lib er aci ón	Fe ch a de la n z a mi en to	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de NV DI M de ca ch é Mi cr on (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	Fu en te de NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)	
Pa qu et e de fir m wa re de al m ac en a mi en to 2.1 50. 4	8 de jun io de 20 22	3B 11	3.9 4.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,3	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 50 2Q	11 09 2A 10	11 0B 2A 10

Ve hí cu lo de lib er aci ón	Fe ch a de la n z a mi en to	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 2.1 50. 4 ha st a Ne tA pp El e m	8 de jun io de 20 22	3B 11	3.9 4.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,3	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 50 2Q	11 09 2A 10	11 0B 2A 10

Ve hí cu lo de lib er aci ón	Fe ch a de la nza mi en to	BI OS	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de en DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de en DI M de ca ch é NV DI M M int eli ge nt e (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 2.1 46. 2	22 de feb rer o de 20 22	3B 11	3.9 4.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,3	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 50 2Q	11 09 2A 10	11 0B 2A 10

Ve hí cu lo de lib er aci ón	Fe ch a de la nza mi en to	BI OS	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al ma cen a mi en to 2.9 9.4 ha st a Ne tA pp El e m en	16 de se pti em br e de 20 21	3B 06	3.9 1.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la n z a mi en to	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 2.9 9.4 ha st a Ne tA pp El e m en	6 de dic ie mb re de 20 21	3B 06	3.9 1.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la nz a mi en to	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 2.9 9.2	6 de dic ie mb re de 20 21	3B 06	3.9 1.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la nza mi en to	BI OS	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al ma c en a mi en to 2.9 9.1 ha st a Ne tA pp El e m en	16 de se pti em br e de 20 21	3B 06	3.8 6.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la n z a mi en to	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 2.9 9 ha st a Ne tA pp El e m en	15 de ab ril de 20 21	3B 06	3.8 6.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la nza mi en to	BI OS	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M int eli ge nt e (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 2.7 6.8	3 de feb rer o de 20 21	3B 06	3.8 6.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la nza mi en to	BI OS	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí M a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí M a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí M a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí M a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí M a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 2.2 7.1	29 de se pti em br e de 20 20	3B 03	3.8 4.0 7	12 2	14. 02. 10 02	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 30 2Q	ED A5 60 0Q	01 08	01 08	01 08	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la n z a mi en to	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 2.7 6.8 ha st a Ne tA pp El e m en	2 de jun io de 20 21	3B 06	3.8 6.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la n z a mi en to	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 2.2 1 a Ne tA pp El e m en t 96. 12. 2	29 de se pti em br e de 20 20	3B 03	3.8 4.0 7	12 2	14. 22. 10 02	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 30 2Q	ED A5 60 0Q	01 08	01 08	01 08	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la n z a mi en to	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 2.7 6.8 ha st a Ne tA pp El e m en	2 de jun io de 20 21	3B 06	3.8 6.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la n z a mi en to	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (B P M) int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 2)	Fu en te de en er gí a de ca ch é NV DI M M (P G E M) Ag ig at ec h (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
Pa qu et e de fir m wa re de al m ac en a mi en to 1.2 .17 ha st a Ne tA pp El e m en	20 de ma rzo de 20 20	3B 03	3.7 8.0 7	12 2	14. 22. 10 02	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	01 08	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la nza mi en to	BI OS	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)
* Ne tA pp El em ent 11. 8 *	11 de ma rzo de 20 20	3B 03	3.7 8.0 7	12 2	14. 22. 10 02	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	01 07	-	-	-
* Ne tA pp El em ent 11. 7 *	21 de no vie mb re de 20 19	3A 10	3.7 6.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	01 07	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la nza mi en to	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)	
* Ne ta pp El em ent 11. 5.1 *	20 de feb rer o de 20 20 5.1 *	3A 08	3.7 6.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	01 07	-	-	-
* Ne ta pp El em ent 11. 5 *	26 de se pti em br e de 20 19	3A 08	3.7 6.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	-	-	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	-	-	01 07	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la n z a m i e n t o	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)	
* Ne tA pp El em ent 11. 3.2 *	19 de feb rer o de 20 11. 3.2 *	3A 08	3.7 6.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	-	-	-	-
* Ne tA pp El em ent 11. 3.1 *	19 de ag ost o de 20 19 3.1 *	3A 08	3.7 6.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	-	-	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	-	-	-	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la nza mi en to	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é Mi cr on (G en 1)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é Mi cr on (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 A3 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)	
* Ne ta pp El em ent 11. 1.1 *	19 de feb rer o de 20 20 11. 1.1 *	3A 06	3.7 0.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	-	-	-	-
* Ne ta pp El em ent 11. 1 *	25 de ab ril de 20 19	3A 06	3.7 0.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	-	-	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	-	-	-	-	-	-

Ve hí cu lo de lib er aci ón	Fe ch a de la n z a mi en to	BI O S	B M C	CP LD	NI C CX 4 de 10/ 25 Gb E	NI C CX 5 de 10/ 25 Gb E	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 1)	M ód ul o NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 2)	Fu en te de NV DI M de ca ch é NV DI M M int eli ge nt e (G en 3)	Un id ad Sa m su ng P M9 63 (S ED)	Un id ad Sa m su ng P M9 63 (N- SE D)	Un id ad Sa m su ng P M9 83 (S ED)	Un id ad Sa m su ng P M9 83 (N- SE D)	Un id ad Ki ox ia C D5 (S ED)	Un id ad Ki ox ia C D5 (N- SE D)	Un id ad C D5 (FI PS)	Un id ad Sa m su ng P M9 80 (S ED)	Un id ad SK Hy ni x PE 80 (S ED)	Un id ad SK Hy ni x PE 80 (N- SE D)	
* Ne tA pp El em ent 11. 0.2 *	19 de feb rer o de 20 20	3A 06	3.7 0.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	-	-	-	-
* Ne tA pp El em ent *	29 de no vie mb re de 20 18	3A 06	3.7 0.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	-	-	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	-	-	-	-	-	-

Firmware de componentes no gestionado por un paquete de firmware de almacenamiento

El siguiente firmware no está gestionado por un paquete de firmware de almacenamiento:

Componente	Versión actual
NIC de 1/10 GbE	3.2d 0x80000b4b
dispositivo de arranque	M161225i

H410S

Número de modelo (parte de la familia): H410S **Números de modelo completos:** H410S-0, H410S-1, H410S-1-NE y H410S-2

Firmware de componentes gestionado por un paquete de firmware de almacenamiento

Firmware de componentes gestionado por un paquete de firmware de almacenamiento.

Vehículo de liberación	Fecha de lanzamiento	BIOS	BMC	NIC SMCI Mellanox de 10/25 GbE	Caché NVDIMM RMS200	Caché NVDIMM RMS300	Unidad Samsung PM863 (SED)	Unidad Samsung PM863 (N-SED)	Condu ce la Toshiba Hawk-4 (SED)	Condu ce la Toshiba Hawk-4 (N-SED)	Unidad Samsung PM883 (SED)
Paquete de firmware de almacenamiento 2.182.0	17 de octubre de 2024	NAT3.6	07.02.00	14.25.1020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Paquete de firmware de almacenamiento 2.175.0	15 de junio de 2023	NAT3.4	07.02.00	14.25.1020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Paquete de firmware de almacenamiento 2.164.0 hasta NetApp Element 12.7	20 de octubre de 2022	NAT3.4	6.98.00	14.25.1020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q

Vehículo de liberación	Fecha de lanzamiento	BIOS	BMC	NIC SMCI Mellanox de 10/25 GbE	Caché NVDIMM RMS200	Caché NVDIMM RMS300	Unidad Samsung PM863 (SED)	Unidad Samsung PM863 (N-SED)	Conduce la Toshiba Hawk-4 (SED)	Conduce la Toshiba Hawk-4 (N-SED)	Unidad Samsung PM883 (SED)
Paquete de firmware de almacenamiento 2.164.0	20 de octubre de 2022	NAT3.4	6.98.00	14.25.1020	ae3b8c	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Paquete de firmware de almacenamiento 2.164.0 hasta NetApp Element 12.7	20 de octubre de 2022	NAT3.4	6.98.00	14.25.1020	ae3b8c	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Paquete de firmware de almacenamiento 2.150.4 hasta NetApp Element 12.5	8 de junio de 2022	NAT3.4	6.98.00	14.25.1020	ae3b8c	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Paquete de firmware de almacenamiento 2.99 hasta NetApp Element 12.3	15 de abril de 2021	NA2.1	6.84.00	14.25.1020	ae3b8c	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q

Vehículo de liberación	Fecha de lanzamiento	BIOS	BMC	NIC SMCI Mellanox de 10/25 GbE	Caché NVDIMM RMS200	Caché NVDIMM RMS300	Unidad Samsung PM863 (SED)	Unidad Samsung PM863 (N-SED)	Conduce la Toshiba Hawk-4 (SED)	Conduce la Toshiba Hawk-4 (N-SED)	Unidad Samsung PM883 (SED)
Paquete de firmware de almacenamiento 2.76.8 hasta NetApp Element 12.2.1	2 de junio de 2021	NA2.1	6.84.00	14.25.1020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
Paquete de firmware de almacenamiento 1.2.17 hasta NetApp Element 12.0	20 de marzo de 2020	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.8.2 *	22 de febrero de 2022	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.8.1 *	2 de junio de 2021	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.8 *	11 de marzo de 2020	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.7 *	21 de noviembre de 2019	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q

Vehículo de liberación	Fecha de lanzamiento	BIOS	BMC	NIC SMCI Mellanox de 10/25 GbE	Caché NVDIMM RMS200	Caché NVDIMM RMS300	Unidad Samsung PM863 (SED)	Unidad Samsung PM863 (N-SED)	Conduce la Toshiba Hawk-4 (SED)	Conduce la Toshiba Hawk-4 (N-SED)	Unidad Samsung PM883 (SED)
* NetApp Element 11.5.1 *	19 de febrero de 2020	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.5 *	26 de septiembre de 2019	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.3.2 *	19 de febrero de 2020	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.3.1 *	19 de agosto de 2019	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.1.1 *	19 de febrero de 2020	NA2.1	3,25	14.17.2020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.1 *	25 de abril de 2019	NA2.1	3,25	14.17.2020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.0.2 *	19 de febrero de 2020	NA2.1	3,25	14.17.2020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.0 *	29 de noviembre de 2018	NA2.1	3,25	14.17.2020	ae3b8cc	-	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q

Firmware de componentes no gestionado por un paquete de firmware de almacenamiento

El siguiente firmware no está gestionado por un paquete de firmware de almacenamiento:

Componente	Versión actual
CPLD	01.A1.06
Adaptador SAS	16.00.01.00
Unidad de microcontrolador (MCU)	1,18
NIC SIOM 1/10 GbE	1,93
Fuente de alimentación	1,3
Dispositivo de arranque SSDSCKJB240G7	N2010121
Dispositivo de arranque MTFDDAV240TCB1AR	DOMU037

SF38410, SF19210, SF9605 y SF4805

Números de modelo completos: SF38410, SF19210, SF9605 y SF4805

Firmware de componentes gestionado por un paquete de firmware de almacenamiento

Durante el período 11.x, el software NetApp Element era la única forma de lanzar firmware. A partir de Element 12.0, se introdujo el concepto de **Paquete de Firmware de Almacenamiento** y las actualizaciones de firmware ahora eran posibles mediante un Paquete de Firmware de Almacenamiento publicado de forma independiente o un Paquete de Firmware de Almacenamiento incluido como parte de una versión de Element 12.x.



Un guion (-) en la siguiente tabla indica que el componente de hardware en cuestión NO era compatible con ese vehículo de lanzamiento determinado.

Vehículo de liberación	Fecha de lanzamiento	NIC	Memoria caché NVDIMM RMS200 (RMS200)	Memoria caché NVDIMM RMS200 (RMS300)	Unidad Samsung PM863 (SED)	Unidad Samsung PM863 (N-SED)	Conduce la Toshiba Hawk-4 (SED)	Conduce la Toshiba Hawk-4 (N-SED)	Unidad Samsung PM883 (SED)
Paquete de firmware de almacenamiento 2.164.0	20 de octubre de 2022	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7A04 Q

Vehículo de liberación	Fecha de lanzamiento	NIC	Memoria caché NVDIMM RMS200 (RMS200)	Memoria caché NVDIMM RMS200 (RMS300)	Unidad Samsung PM863 (SED)	Unidad Samsung PM863 (N-SED)	Conduce la Toshiba Hawk-4 (SED)	Conduce la Toshiba Hawk-4 (N-SED)	Unidad Samsung PM883 (SED)
Paquete de firmware de almacenamiento 2.164.0 hasta NetApp Element 12.7	20 de octubre de 2022	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7A04 Q
Paquete de firmware de almacenamiento 2.150.4	8 de junio de 2022	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7A04 Q
Paquete de firmware de almacenamiento 2.150.4 hasta NetApp Element 12.5	8 de junio de 2022	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7A04 Q
Paquete de firmware de almacenamiento 2.146.2	22 de febrero de 2022	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7A04 Q

Vehículo de liberación	Fecha de lanzamiento	NIC	Memoria caché NVDIMM RMS200 (RMS200)	Memoria caché NVDIMM RMS200 (RMS300)	Unidad Samsung PM863 (SED)	Unidad Samsung PM863 (N-SED)	Conduce la Toshiba Hawk-4 (SED)	Conduce la Toshiba Hawk-4 (N-SED)	Unidad Samsung PM883 (SED)
Paquete de firmware de almacenamiento 2.99.4 hasta NetApp Element 12.3.2	16 de septiembre de 2021	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q
Paquete de firmware de almacenamiento 2.99.4 hasta NetApp Element 12.3.1.16 5	6 de diciembre de 2021	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q
Paquete de firmware de almacenamiento 2.99.2	3 de agosto de 2021	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q
Paquete de firmware de almacenamiento 2.99.1 hasta NetApp Element 12.3.1.10 3	16 de septiembre de 2021	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q

Vehículo de liberación	Fecha de lanzamiento	NIC	Memoria caché NVDIMM RMS200 (RMS200)	Memoria caché NVDIMM RMS200 (RMS300)	Unidad Samsung PM863 (SED)	Unidad Samsung PM863 (N-SED)	Conduce la Toshiba Hawk-4 (SED)	Conduce la Toshiba Hawk-4 (N-SED)	Unidad Samsung PM883 (SED)
Paquete de firmware de almacenamiento 2.99 hasta NetApp Element 12.3	15 de abril de 2021	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q
Paquete de firmware de almacenamiento 2.76.8	3 de febrero de 2021	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q
Paquete de firmware de almacenamiento 2.27.1	29 de septiembre de 2020	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
Paquete de firmware de almacenamiento 2.76.8 hasta NetApp Element 12.2.1	2 de junio de 2021	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q

Vehículo de liberación	Fecha de lanzamiento	NIC	Memoria caché NVDIMM RMS200 (RMS200)	Memoria caché NVDIMM RMS200 (RMS300)	Unidad Samsung PM863 (SED)	Unidad Samsung PM863 (N-SED)	Conduce la Toshiba Hawk-4 (SED)	Conduce la Toshiba Hawk-4 (N-SED)	Unidad Samsung PM883 (SED)
Paquete de firmware de almacenamiento 2.21 a NetApp Element 12.2	29 de septiembre de 2020	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP7101	8ENP6101	HXT7104 Q
Paquete de firmware de almacenamiento 2.76.8 hasta NetApp Element 12.0.1	2 de junio de 2021	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP7101	8ENP6101	HXT7904 Q
Paquete de firmware de almacenamiento 1.2.17 hasta NetApp Element 12.0	20 de marzo de 2020	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP7101	8ENP6101	HXT7104 Q
* NetApp Element 11.8.2 *	22 de febrero de 2022	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP7101	8ENP6101	HXT7104 Q
* NetApp Element 11.8.1 *	2 de junio de 2021	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP7101	8ENP6101	HXT7104 Q
* NetApp Element 11.8 *	11 de marzo de 2020	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP7101	8ENP6101	HXT7104 Q

Vehículo de liberación	Fecha de lanzamiento	NIC	Memoria caché NVDIMM RMS200 (RMS200)	Memoria caché NVDIMM RMS200 (RMS300)	Unidad Samsung PM863 (SED)	Unidad Samsung PM863 (N-SED)	Conduce la Toshiba Hawk-4 (SED)	Conduce la Toshiba Hawk-4 (N-SED)	Unidad Samsung PM883 (SED)
* NetApp Element 11.7 *	21 de noviembre de 2019	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.5.1 *	19 de febrero de 2020	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.5 *	26 de septiembre de 2019	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.3.2 *	19 de febrero de 2020	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.3.1 *	19 de agosto de 2019	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.1.1 *	19 de febrero de 2020	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.1 *	25 de abril de 2019	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.0.2 *	19 de febrero de 2020	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element *	29 de noviembre de 2018	7.10.18	ae3b8cc	-	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q

Firmware de componentes no gestionado por un paquete de firmware de almacenamiento

El siguiente firmware no está gestionado por un paquete de firmware de almacenamiento:

Componente	Versión actual
BIOS	2.8.0
iDRAC	2.75.75.75
Módulo de identidad	N41WC 1.02
Adaptador SAS	16.00.01.00

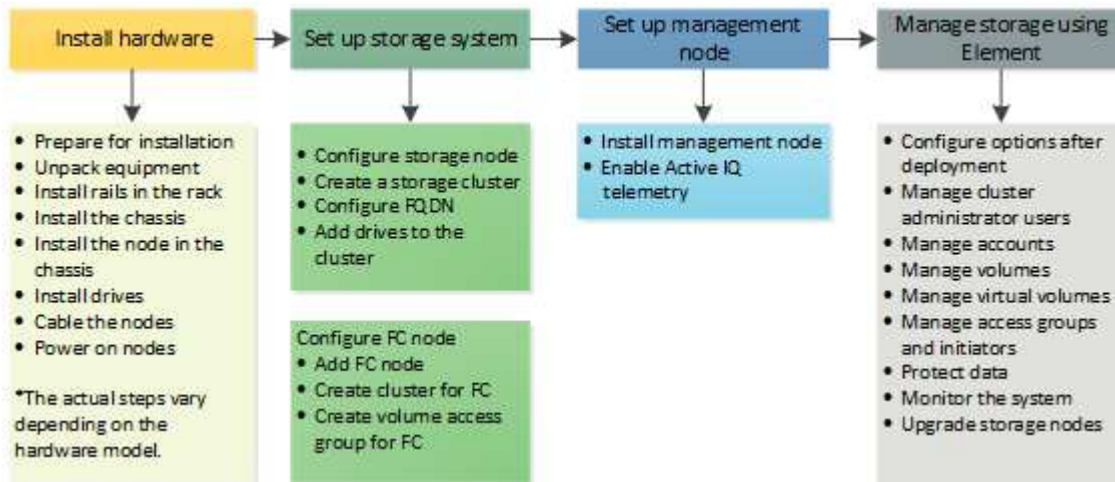
Componente	Versión actual
Fuente de alimentación	1,3
Dispositivo de arranque	M161225i

Configurar almacenamiento

Aprenda cómo configurar el almacenamiento

En este punto, ya deberías haber instalado el hardware. El hardware también incluye el software Element.

A continuación, deberá configurar el sistema de almacenamiento para su entorno. Puede configurar un clúster con nodos de almacenamiento o nodos Fibre Channel y administrarlo mediante el software Element después de instalar y cablear los nodos en una unidad de rack y encenderlos.



Pasos para configurar el almacenamiento

1. Seleccione una de las siguientes opciones:

- ["Configurar clúster con nodos de almacenamiento"](#)

Puede configurar un clúster con nodos de almacenamiento y administrarlo utilizando el software Element después de instalar y cablear los nodos en una unidad de rack y encenderlos. A continuación, podrá instalar y configurar componentes adicionales en su sistema de almacenamiento.

- ["Configurar clúster con nodos Fibre Channel"](#)

Puede configurar un clúster con nodos Fibre Channel y administrarlo mediante el software Element después de instalar y cablear los nodos en una unidad de rack y encenderlos. A continuación, podrá instalar y configurar componentes adicionales en su sistema de almacenamiento.

2. ["Determina qué componentes de SolidFire debes instalar."](#)

3. ["Configure un nodo de administración y habilite la telemetría de Active IQ ."](#)

Encuentra más información

- ["Descubre los siguientes pasos para usar el almacenamiento"](#)
- ["Documentación del software SolidFire y Element"](#)

Configurar un clúster con nodos de almacenamiento

Configurar un nodo de almacenamiento

Debes configurar los nodos individuales antes de poder agregarlos a un clúster. Después de instalar y cablear un nodo en una unidad de rack y encenderlo, puede configurar los ajustes de red del nodo utilizando la interfaz de usuario por nodo o la interfaz de usuario del terminal del nodo (TUI). Asegúrese de tener la información de configuración de red necesaria para el nodo antes de continuar.

Existen dos opciones para configurar los nodos de almacenamiento:

- **Interfaz de usuario por nodo** Utilice la interfaz de usuario por nodo. (https://<node_management_IP>:442) para configurar los ajustes de red del nodo.
- **TUI** Utilice la interfaz de usuario del terminal del nodo (TUI) para configurar el nodo.

No se puede agregar un nodo con direcciones IP asignadas por DHCP a un clúster. Puede utilizar la dirección IP DHCP para configurar inicialmente el nodo en la interfaz de usuario (UI), la interfaz de usuario de texto (TUI) o la API de cada nodo. Durante esta configuración inicial, puede agregar información de dirección IP estática para poder agregar el nodo a un clúster.

Tras la configuración inicial, puede acceder al nodo utilizando la dirección IP de gestión del nodo. Luego puedes cambiar la configuración del nodo, agregarlo a un clúster o usar el nodo para crear un clúster. También puede configurar un nuevo nodo utilizando los métodos de la API del software Element.



A partir de la versión 11.0 de Element, los nodos se pueden configurar con direcciones IPv4, IPv6 o ambas para su red de administración. Esto se aplica tanto a los nodos de almacenamiento como a los nodos de administración, excepto al nodo de administración 11.3 y posteriores, que no admiten IPv6. Al crear un clúster, solo se puede usar una única dirección IPv4 o IPv6 para MVIP y el tipo de dirección correspondiente debe configurarse en todos los nodos.

Configure un nodo de almacenamiento mediante la interfaz de usuario específica para cada nodo.

Puede configurar los nodos utilizando la interfaz de usuario de cada nodo.

Acerca de esta tarea

- Puedes configurar el nodo para que tenga una dirección IPv4 o IPv6.
- Necesitas la dirección DHCP que se muestra en la interfaz de usuario para acceder a un nodo. No se pueden usar direcciones DHCP para agregar un nodo a un clúster.



Debe configurar las interfaces de administración (Bond1G) y almacenamiento (Bond10G) para subredes separadas. Las interfaces Bond1G y Bond10G configuradas para la misma subred causan problemas de enrutamiento cuando el tráfico de almacenamiento se envía a través de la interfaz Bond1G. Si necesita utilizar la misma subred para el tráfico de administración y almacenamiento, configure manualmente el tráfico de administración para que utilice la interfaz Bond10G. Puedes hacerlo para cada nodo utilizando la página **Configuración del clúster** de la interfaz de usuario por nodo.

Pasos

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

Debes añadir la extensión : 442 para acceder al nodo; por ejemplo, <https://172.25.103.6:442>.

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

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



Este nombre debe añadirse a la configuración de todos los nodos antes de poder crear un clúster. Todos los nodos de un clúster deben tener nombres de clúster idénticos. Los nombres de los clústeres distinguen entre mayúsculas y minúsculas.

10. Haga clic en **Aplicar cambios**.

Configure un nodo de almacenamiento mediante la interfaz de usuario de texto (TUI).

Puede utilizar la interfaz de usuario de terminal (TUI) para realizar la configuración inicial de los nuevos nodos.

Debe configurar las interfaces Bond1G (Administración) y Bond10G (Almacenamiento) para subredes separadas. Las interfaces Bond1G y Bond10G configuradas para la misma subred provocan problemas de enrutamiento cuando el tráfico de almacenamiento se envía a través de la interfaz Bond1G. Si necesita utilizar la misma subred para el tráfico de administración y almacenamiento, configure manualmente el tráfico de administración para que utilice la interfaz Bond10G. Puedes hacerlo para cada nodo utilizando la página **Cluster > Nodos** de la interfaz de usuario de Element.

Pasos

1. Conecta un teclado y un monitor al nodo y luego enciende el nodo.

El menú principal de NetApp Storage de la interfaz de usuario de texto aparece en el terminal tty1.



Si el nodo no puede conectarse con su servidor de configuración, la interfaz de usuario mostrará un mensaje de error. Comprueba la conexión del servidor de configuración o la conexión de red para resolver el error.

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



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

3. Seleccione **Bond1G (Administración)** o **Bond10G (Almacenamiento)** para configurar los ajustes de red de 1G y 10G para el nodo.

4. Para los campos Modo de enlace y Estado, pulse **Tab** para seleccionar el botón Ayuda e identificar las opciones disponibles.

Todos los nodos de un clúster deben tener nombres de clúster idénticos. Los nombres de los clústeres distinguen entre mayúsculas y minúsculas. Si hay un servidor DHCP funcionando en la red con direcciones IP disponibles, la dirección 1GbE aparece en el campo Dirección.

5. Presione **Tab** para seleccionar el botón **Aceptar** y guardar los cambios.

El nodo se coloca en estado pendiente y se puede agregar a un clúster existente o a un nuevo clúster.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Cree un clúster de almacenamiento.

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

Lo que necesitarás

- Has instalado el nodo de gestión.
- Has configurado todos los nodos individuales.

Acerca de esta tarea

Durante la configuración de un nuevo nodo, se asignan direcciones IP de gestión (MIP) de 1G o 10G a cada nodo. Debe utilizar una de las direcciones IP de nodo creadas durante la configuración para abrir la página Crear un nuevo clúster. La dirección IP que utilice dependerá de la red que haya elegido para la gestión del clúster.



Si desea habilitarlo en todo el clúster. ["Cifrado de software en reposo"](#) Para los clústeres de almacenamiento all-flash SolidFire, debe hacerlo durante la creación del clúster. A partir de Element 12.5, debe habilitar el cifrado de software en reposo en la interfaz de usuario Crear clúster durante la creación del clúster. Para Element 12.3.x y versiones anteriores, debe crear el clúster utilizando el ["CrearClúster"](#) Método API y cambie el parámetro `enableSoftwareEncryptionAtRest` a `true`. Una vez habilitada la encriptación de software en reposo en el clúster, no se puede deshabilitar. Puede ["activar y desactivar"](#) Cifrado basado en hardware en reposo después de la creación del clúster.

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



- Si utiliza nodos de almacenamiento que residen en un chasis compartido, quizá le interese considerar el diseño de una protección contra fallos a nivel de chasis mediante la función de dominios de protección.
- Si no se utiliza un chasis compartido, puede definir una distribución de dominio de protección personalizada.

Pasos

1. En una ventana del navegador, ingrese `https://MIP:443`, donde MIP es la dirección IP del nodo de gestión.
2. En Crear un nuevo clúster, ingrese la siguiente información:
 - VIP de gestión: IP virtual enrutable en la red 1GbE o 10GbE para tareas de gestión de red.



 Puede crear un nuevo clúster utilizando direccionamiento IPv4 o IPv6.
 - VIP iSCSI (almacenamiento): IP virtual en la red 10GbE para almacenamiento y descubrimiento iSCSI.



 No se puede cambiar el MVIP, SVIP ni el nombre del clúster después de crearlo.
 - Nombre de usuario: El nombre de usuario del administrador principal del clúster para el acceso autenticado al clúster. Debe guardar el nombre de usuario para futuras consultas.



 Puedes utilizar letras mayúsculas y minúsculas, caracteres especiales y números para el nombre de usuario y la contraseña.
 - Contraseña: Contraseña para el acceso autenticado al clúster. Debe guardar la contraseña para futuras consultas. La protección de datos bidireccional está habilitada por defecto. No puedes cambiar esta configuración.
3. Lea el Acuerdo de Licencia de Usuario Final y seleccione **Acepto**.
4. **Opcional:** En la lista de nodos, asegúrese de que no estén seleccionadas las casillas de verificación de los nodos que no deben incluirse en el clúster.
5. Seleccione **Crear clúster**.

El sistema podría tardar varios minutos en crear el clúster, dependiendo del número de nodos que lo componen. En una red correctamente configurada, un pequeño clúster de cinco nodos debería tardar menos de un minuto. Una vez creado el clúster, la ventana Crear un nuevo clúster se redirige a la dirección URL de MVIP del clúster y muestra la interfaz de usuario de Element.

Para más información

- ["Gestionar el almacenamiento con la API de Element"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Acceda a la interfaz de usuario del software Element

Puede acceder a la interfaz de usuario de Element utilizando la dirección IP virtual de administración (MVIP) del nodo principal del clúster.

Debes asegurarte de que los bloqueadores de ventanas emergentes y la configuración de NoScript estén desactivados en tu navegador.

Puede acceder a la interfaz de usuario utilizando direcciones IPv4 o IPv6, según la configuración realizada durante la creación del clúster.

Pasos

1. Elija una de las siguientes opciones:

- IPv6: Introducir `https://[IPv6_MVIP_address]` . Por ejemplo:

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

- IPv4: Introducir `https://[IPv4_MVIP_address]` . Por ejemplo:

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

2. Para DNS, introduzca el nombre del host.

3. Ignore cualquier mensaje de certificado de autenticación.

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Agregar unidades a un clúster

Cuando se agrega un nodo al clúster o se instalan nuevas unidades en un nodo existente, las unidades se registran automáticamente como disponibles. Debe agregar las unidades al clúster utilizando la interfaz de usuario de Element o la API antes de que puedan participar en el clúster.

Las unidades no se muestran en la lista de Unidades disponibles cuando se dan las siguientes condiciones:

- Las unidades se encuentran en estado Activo, Extrayendo, Borrando o Fallido.
- El nodo del que forma parte la unidad se encuentra en estado Pendiente.

Pasos

1. Desde la interfaz de usuario de Element, seleccione **Clúster > Unidades**.

2. Haz 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 agregar varias unidades, seleccione las casillas de verificación de las unidades que desea agregar, haga clic en **Acciones en lote** y, a continuación, 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^]
```

Configurar un clúster con nodos Fibre Channel

Configurar un nodo Fibre Channel

Los nodos Fibre Channel permiten conectar el clúster a una estructura de red Fibre Channel. Los nodos Fibre Channel se agregan por pares y funcionan en modo activo-activo (todos los nodos procesan activamente el tráfico del clúster). Los clústeres que ejecutan la versión 9.0 y posteriores del software Element admiten hasta cuatro nodos; los clústeres que ejecutan versiones anteriores admiten un máximo de dos nodos.

Debe asegurarse de que se cumplen las siguientes condiciones antes de configurar un nodo Fibre Channel:

- Al menos dos nodos Fibre Channel están conectados a conmutadores Fibre Channel.
- Todos los puertos Fibre Channel de SolidFire deben estar conectados a su estructura Fibre Channel. Las cuatro conexiones de red SolidFire Bond10G deben conectarse en un grupo de enlace LACP a nivel de conmutador. Esto permitirá obtener el mejor rendimiento general de los sistemas Fibre Channel.
- Revise y valide todas las prácticas recomendadas para clústeres Fibre Channel incluidas en este artículo de la base de conocimientos de NetApp .

["Mejores prácticas para clústeres SolidFire FC"](#)

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

Cuando se crea un nuevo clúster con nodos Fibre Channel y nodos de almacenamiento SolidFire , las direcciones de nombre de puerto mundial (WWPN) para los nodos están disponibles en la interfaz de usuario de Element. Puede utilizar las direcciones WWPN para zonificar el conmutador Fibre Channel.

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

Encuentra más información

[Agregar nodos Fibre Channel a un clúster](#)

[Cree un nuevo clúster con nodos Fibre Channel](#)

Cree un nuevo clúster con nodos Fibre Channel

Puede crear un nuevo clúster después de haber configurado los nodos Fibre Channel individuales. Cuando se crea un clúster, también se crea automáticamente una cuenta de

usuario de administrador de clúster. El administrador del clúster tiene permiso para gestionar todos los atributos del clúster y puede crear otras cuentas de administrador del clúster.

Durante la configuración de un nuevo nodo, se asignan direcciones IP de gestión (MIP) de 1G o 10G a cada nodo. Debe utilizar una de las direcciones IP de nodo creadas durante la configuración para abrir la página Crear un nuevo clúster. La dirección IP que utilice dependerá de la red que haya elegido para la gestión del clúster.

Lo que necesitarás

Has configurado los nodos Fibre Channel individuales.

Pasos

1. En una ventana del navegador, introduzca una dirección MIP del nodo.
2. En Crear un nuevo clúster, ingrese la siguiente información:
 - VIP de gestión: IP virtual enrutable en la red 1GbE o 10GbE para tareas de gestión de red.
 - VIP iSCSI (almacenamiento): IP virtual en la red 10GbE para almacenamiento y descubrimiento iSCSI.



No se puede cambiar la SVIP después de crear el clúster.

- Nombre de usuario: El nombre de usuario del administrador principal del clúster para el acceso autenticado al clúster. Debe guardar el nombre de usuario para futuras consultas.



Para el nombre de usuario puedes utilizar letras mayúsculas y minúsculas, caracteres especiales y números.

- Contraseña: Contraseña para el acceso autenticado al clúster. Debe guardar el nombre de usuario para futuras consultas. La protección de datos bidireccional está habilitada por defecto. No puedes cambiar esta configuración.

3. Lea el Acuerdo de Licencia de Usuario Final y haga clic en **Acepto**.
4. **Opcional:** En la lista de nodos, asegúrese de que no estén seleccionadas las casillas de verificación de los nodos que no deben incluirse en el clúster.
5. Haz clic en **Crear clúster**.

El sistema podría tardar varios minutos en crear el clúster, dependiendo del número de nodos que lo componen. En una red correctamente configurada, un pequeño clúster de cinco nodos debería tardar menos de un minuto. Una vez creado el clúster, la ventana Crear un nuevo clúster se redirige a la dirección URL de MVIP del clúster y muestra la interfaz de usuario web.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Agregar nodos Fibre Channel a un clúster

Puede agregar nodos Fibre Channel a un clúster cuando se necesite más almacenamiento o durante la creación del clúster. Los nodos Fibre Channel requieren

una configuración inicial cuando se encienden por primera vez. Una vez configurado el nodo, aparece en la lista de nodos pendientes y se puede agregar a un clúster.

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

Pasos

1. Seleccione **Clúster > Nodos**.
2. Haz clic en **Pendientes** 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 agregar varios nodos, seleccione la casilla de verificación de los nodos que desea agregar y luego **Acciones en lote**.



Si el nodo que está agregando tiene una versión de Element 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 del clúster. Después de que se actualiza el nodo, se agrega automáticamente al clúster. Durante este proceso asíncrono, el nodo estará en estado pendingActive.

4. Haga clic en **Agregar**.

El nodo aparece en la lista de nodos activos.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Configurar zonas para nodos Fibre Channel

Cuando se crea un nuevo clúster con nodos Fibre Channel y nodos de almacenamiento SolidFire, las direcciones de nombre de puerto mundial (WWPN) para los nodos están disponibles en la interfaz de usuario web. Puede utilizar las direcciones WWPN para zonificar el conmutador Fibre Channel.

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

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Cree un grupo de acceso por volumen para clientes Fibre Channel.

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

También puede agregar iniciadores iSCSI a un grupo de acceso a volúmenes; esto les da a los iniciadores acceso a los mismos volúmenes en el grupo de acceso a volúmenes.

Pasos

1. Haz clic en **Administración > Grupos de acceso**.
2. Haga clic en **Crear grupo de acceso**.
3. Introduzca un nombre para el grupo de acceso al volumen en el campo **Nombre**.
4. Seleccione y agregue los iniciadores de Fibre Channel de la lista **Iniciadores de Fibre Channel no enlazados**.



Puedes añadir o eliminar iniciadores más adelante.

5. **Opcional:** Seleccione y agregue un iniciador iSCSI de la lista **Iniciadores**.
6. Para adjuntar volúmenes al grupo de acceso, siga los siguientes pasos:
 - a. Seleccione un volumen de la lista **Volúmenes**.
 - b. Haga clic en **Adjuntar volumen**.
7. Haga clic en **Crear grupo de acceso**.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Determina qué componentes de SolidFire debes instalar.

Es posible que desee comprobar qué componentes de SolidFire , como el nodo de administración, Active IQ y el agente de supervisión de NetApp (NMA), debe instalar, según las opciones de configuración y despliegue.

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

Componente	clúster de almacenamiento SolidFire independiente	Clúster NetApp HCI
Nodo de gestión	Recomendado	Instalado por defecto, obligatorio
Active IQ	Recomendado*	Recomendado*

Componente	clúster de almacenamiento SolidFire independiente	Clúster NetApp HCI
Agente de supervisión de NetApp	No compatible	Recomendado

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

Pasos

1. Determinar qué componentes deben instalarse.
2. Complete la instalación de acuerdo con las instrucciones. ["instalar el nodo de administración"](#) procedimiento.



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

3. Para obtener información sobre el agente de supervisión de NetApp , consulte este enlace. ["procedimiento"](#)

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Configurar un nodo de administración

Puede instalar el nodo de administración de software NetApp Element (mNode) para actualizar y proporcionar servicios del sistema, administrar los activos y la configuración del clúster, ejecutar pruebas y utilidades del sistema y habilitar el acceso al soporte de NetApp para la solución de problemas.

1. Ver el ["instalar el nodo de administración"](#) documentación.



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

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Configurar el acceso a la interfaz web del nombre de dominio completo

El almacenamiento totalmente flash SolidFire con el software NetApp Element 12.2 o posterior le permite acceder a las interfaces web del clúster de almacenamiento utilizando el nombre de dominio totalmente calificado (FQDN). Si desea utilizar el FQDN

para acceder a interfaces de usuario web como la interfaz web de Element, la interfaz de usuario por nodo o la interfaz de usuario del nodo de administración, primero debe agregar una configuración de clúster de almacenamiento para identificar el FQDN utilizado por el clúster.

Este proceso permite que el clúster redirija correctamente una sesión de inicio de sesión y mejora la integración con servicios externos como gestores de claves y proveedores de identidad para la autenticación multifactor.

Lo que necesitarás

- Esta función requiere Element 12.2 o posterior.
- La configuración de esta función mediante las API REST de NetApp Hybrid Cloud Control requiere los servicios de administración 2.15 o posterior.
- La configuración de esta función mediante la interfaz de usuario de NetApp Hybrid Cloud Control requiere los servicios de administración 2.19 o posterior.
- Para utilizar las API REST, debe haber implementado un nodo de administración que ejecute la versión 11.5 o posterior.
- Necesita nombres de dominio completos para el nodo de administración y cada clúster de almacenamiento que se resuelvan correctamente a la dirección IP del nodo de administración y a la dirección IP de cada clúster de almacenamiento.

Puede configurar o eliminar el acceso a la interfaz web FQDN mediante NetApp Hybrid Cloud Control y la API REST. También puede solucionar problemas relacionados con FQDN configurados incorrectamente.

- [Configure el acceso a la interfaz web de FQDN mediante NetApp Hybrid Cloud Control.](#)
- [Configure el acceso a la interfaz web mediante FQDN utilizando la API REST.](#)
- [Eliminar el acceso a la interfaz web de FQDN mediante NetApp Hybrid Cloud Control](#)
- [Eliminar el acceso a la interfaz web de FQDN mediante la API REST](#)
- [Solución de problemas](#)

Configure el acceso a la interfaz web de FQDN mediante NetApp Hybrid Cloud Control.

Pasos

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

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

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione el icono de menú situado en la parte superior derecha de la página.
4. Seleccione **Configurar**.
5. En el panel **Nombres de dominio totalmente calificados**, seleccione **Configurar**.
6. En la ventana resultante, ingrese los FQDN para el nodo de administración y cada clúster de almacenamiento.

7. Seleccione **Guardar**.

El panel **Nombres de dominio totalmente calificados** muestra cada clúster de almacenamiento con su MVIP y FQDN asociados.



En el panel **Nombres de dominio totalmente calificados** solo se muestran los clústeres de almacenamiento conectados con el FQDN configurado.

Configure el acceso a la interfaz web mediante FQDN utilizando la API REST.

Pasos

1. Asegúrese de que los nodos de almacenamiento de Element y el mNode tengan el DNS configurado correctamente para el entorno de red, de modo que se puedan resolver los FQDN del entorno. Para configurar el DNS, vaya a la interfaz de usuario de cada nodo de almacenamiento y al nodo de administración, luego seleccione **Configuración de red > Red de administración**.
 - a. Interfaz de usuario por nodo para nodos de almacenamiento:
`https://<storage_node_management_IP>:442`
 - b. Interfaz de usuario por nodo para el nodo de administración:
`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 de clúster utilizando "**CrearPreferenciaDeInterfazDeClúster**" Método API, insertando el FQDN 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 administración mediante la API REST en el nodo de administración:
 - a. Acceda a la interfaz de usuario de la API REST para el nodo de administración introduciendo la dirección IP del nodo de administración seguida de `/mnode/2/`

Por ejemplo:

`https://<management_node_IP>/mnode/2/`
 - a. Haga clic en **Autorizar** o en cualquier icono de candado e introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID del cliente como `mnode-client`.
 - c. Haz clic en **Autorizar** para comenzar la sesión y luego cierra la ventana.

- d. Desde la lista de servidores, seleccione `mnode2`.
- e. Haz clic en **GET /settings**.
- f. Haz clic en **Pruébalo**.
- g. Haz clic en **Ejecutar**.
- h. Registre cualquier configuración de proxy que se indique en el cuerpo de la respuesta.
- i. Haz clic en **PUT/settings**.
- j. Haz clic en **Pruébalo**.
- k. En el área del cuerpo de la solicitud, introduzca el FQDN del nodo de administración como valor para el `mnode_fqdn` parámetro.
- l. Introduzca los valores de configuración del proxy que registró 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 eliminarán los ajustes del proxy existentes.
- m. Haz clic en **Ejecutar**.

Eliminar el acceso a la interfaz web de FQDN mediante NetApp Hybrid Cloud Control

Puede utilizar este procedimiento para eliminar el acceso web FQDN para el nodo de administración y los clústeres de almacenamiento.

Pasos

1. En el panel **Nombres de dominio totalmente calificados**, seleccione **Editar**.
2. En la ventana resultante, borre el contenido del campo de texto **FQDN**.
3. Seleccione **Guardar**.

La ventana se cierra y el FQDN ya no aparece en el panel **Nombres de dominio totalmente calificados**.

Eliminar el acceso a la interfaz web de FQDN mediante la API 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 `DeleteClusterInterfacePreference` Método de la 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 administración mediante la API REST en el nodo de administración:
 - a. Acceda a la interfaz de usuario de la API REST para el nodo de administración introduciendo la dirección IP del nodo de administración seguida de `/mnode/2/`. Por ejemplo:

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

- b. Seleccione **Autorizar** o cualquier icono de candado e introduzca el nombre de usuario y la contraseña del clúster de Element.
- c. Introduzca el ID del cliente como `mnode-client`.
- d. Seleccione **Autorizar** para iniciar una sesión.
- e. Cerrar la ventana.
- f. Seleccione **PUT /settings**.
- g. Seleccione **Probarlo**.
- h. En el área del cuerpo de la solicitud, no introduzca ningún valor para el `mnode_fqdn` parámetro. Especifique también si se debe utilizar el proxy.(`true` o `false`) para el `use_proxy` parámetro.

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

- i. Seleccione **Ejecutar**.

Solución de problemas

Si los FQDN están configurados incorrectamente, podría tener problemas para acceder al nodo de administración, a un clúster de almacenamiento o a ambos. Utilice la siguiente información para ayudarle a solucionar el problema.

Asunto	Causa	Resolución
• Se produce un error del navegador al intentar acceder al nodo de administración o al clúster de almacenamiento utilizando el FQDN. • No se puede iniciar sesión ni en el nodo de administración ni en el clúster de almacenamiento utilizando una dirección IP.	Tanto el FQDN del nodo de administración como el FQDN del clúster de almacenamiento están configurados incorrectamente.	Utilice las instrucciones de la API REST de esta página para eliminar la configuración del nodo de administración y del FQDN del clúster de almacenamiento y configurarlos de nuevo.

Asunto	Causa	Resolución
- Se produce un error del navegador al intentar acceder al FQDN del clúster de almacenamiento. - No se puede iniciar sesión ni en el nodo de administración ni en el clúster de almacenamiento utilizando una dirección IP.	El nombre de dominio completo (FQDN) del nodo de administración está configurado correctamente, pero el FQDN del clúster de almacenamiento está configurado incorrectamente.	Siga las instrucciones de la API REST en esta página para eliminar la configuración del FQDN del clúster de almacenamiento y volver a configurarla.
- Se produce un error del navegador al intentar acceder al FQDN del nodo de administración. - Puede iniciar sesión en el nodo de administración y en el clúster de almacenamiento utilizando una dirección IP.	El nombre de dominio completo (FQDN) del nodo de administración está configurado incorrectamente, pero el FQDN del clúster de almacenamiento está configurado correctamente.	Inicie sesión en NetApp Hybrid Cloud Control para corregir la configuración FQDN del nodo de administración en la interfaz de usuario, o utilice las instrucciones de la API REST en esta página para corregir la configuración.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

¿Qué sigue?

Después de configurar el software Element, puede administrar 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"](#)
- ["Administra tu sistema"](#)
- ["Gestionar volúmenes y volúmenes virtuales"](#)
- ["Proteja sus datos"](#)
- ["Soluciona los problemas de tu sistema"](#)

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Gestiona el almacenamiento con el software Element.

Gestiona el almacenamiento con el software Element.

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

Element es el sistema operativo de almacenamiento que constituye el núcleo de un clúster 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 se presenten como un único sistema de almacenamiento a los clientes externos. El software Element es responsable de toda la coordinación del clúster, la escalabilidad y la gestión del sistema en su conjunto.

La interfaz de software está construida sobre la API de Element.

- ["Acceda a la interfaz de usuario del software Element"](#)
- ["Configure las opciones del sistema SolidFire después de la implementación."](#)
- ["Actualizar los componentes del sistema de almacenamiento"](#)
- ["Utilice las opciones básicas de la interfaz de usuario del software Element."](#)
- ["Gestionar cuentas"](#)
- ["Administra tu sistema"](#)
- ["Gestionar volúmenes y volúmenes virtuales"](#)
- ["Proteja sus datos"](#)
- ["Soluciona los problemas de tu sistema"](#)

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Acceda a la interfaz de usuario del software Element

Puede acceder a la interfaz de usuario de Element utilizando la dirección IP virtual de administración (MVIP) del nodo principal del clúster.

Debes asegurarte de que los bloqueadores de ventanas emergentes y la configuración de NoScript estén desactivados en tu navegador.

Puede acceder a la interfaz de usuario utilizando direcciones IPv4 o IPv6, según la configuración realizada durante la creación del clúster.

1. Elija una de las siguientes opciones:
 - IPv6: Introduzca [https://\[dirección IPv6 MVIP\]](https://[dirección IPv6 MVIP]). Por ejemplo:

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

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

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

2. Para DNS, introduzca el nombre del host.
3. Ignore cualquier mensaje de certificado de autenticación.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Configure las opciones del sistema SolidFire después de la implementación.

Configure las opciones del sistema SolidFire después de la implementación.

Después de configurar su sistema SolidFire , es posible que desee realizar algunas tareas opcionales.

Si modifica las credenciales del sistema, es posible que desee conocer el impacto en otros componentes.

Además, puede configurar los ajustes para la autenticación multifactor, la gestión de claves externas y la seguridad de los Estándares Federales de Procesamiento de Información (FIPS). También deberías considerar actualizar tus contraseñas cuando sea necesario.

Encuentra más información

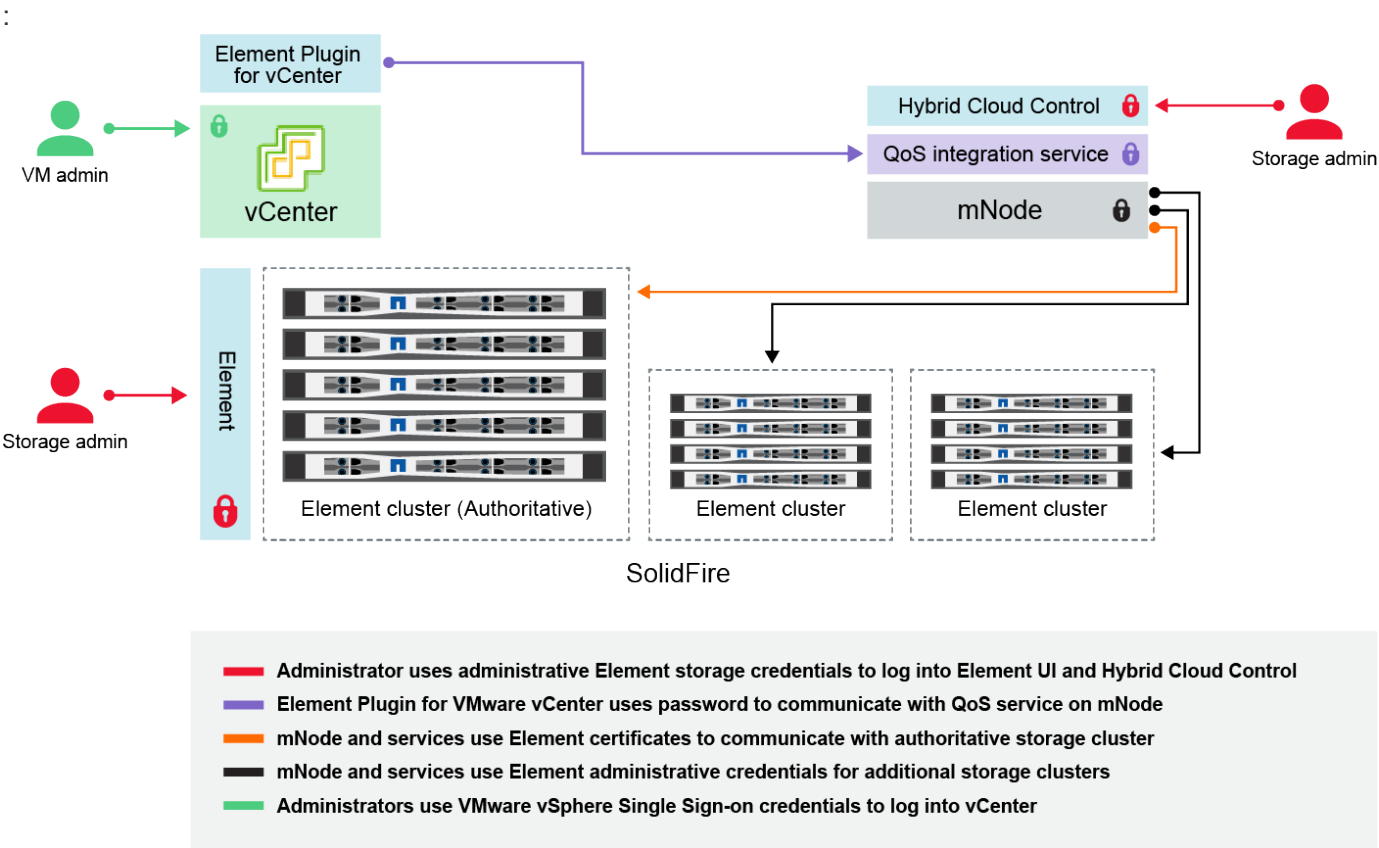
- ["Cambiar credenciales en NetApp HCI y NetApp SolidFire"](#)
- ["Cambiar el certificado SSL predeterminado del software Element"](#)
- ["Cambiar la contraseña IPMI para los nodos"](#)
- ["Habilitar la autenticación multifactor"](#)
- ["Comience con la administración de claves externas"](#)
- ["Cree un clúster que admita unidades FIPS."](#)

Cambiar credenciales en NetApp HCI y NetApp SolidFire

Dependiendo de las políticas de seguridad de la organización que implementó NetApp HCI o NetApp SolidFire, el cambio de credenciales o contraseñas suele formar parte de las prácticas de seguridad. Antes de cambiar las contraseñas, debe tener en cuenta el impacto que esto tendrá en otros componentes de software de la implementación.

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

Interacciones de componentes de NetApp SolidFire



Tipo de credencial e icono	Uso por parte del administrador	Consulte estas instrucciones
Credenciales de elemento 	Aplica a: NetApp HCI y SolidFire Los administradores utilizan estas credenciales para iniciar sesión en: • Interfaz de usuario de Element en el clúster de almacenamiento de Element • Control de nube híbrida en el nodo de administración (mnode) Cuando Hybrid Cloud Control administra varios clústeres de almacenamiento, solo acepta las credenciales de administrador para los clústeres de almacenamiento, conocidos como el <i>clúster autorizado</i> para el cual se configuró inicialmente el mnode. Para los clústeres de almacenamiento que se agreguen posteriormente a Hybrid Cloud Control, el nodo M almacena de forma segura las credenciales de administrador. Si se modifican las credenciales de los clústeres de almacenamiento añadidos posteriormente, también deben actualizarse las credenciales en el mnode utilizando la API de mnode.	• "Actualice las contraseñas de administrador del clúster de almacenamiento." • Actualice las credenciales de administrador del clúster de almacenamiento en el nodo M mediante el siguiente método: "API de modificación de administración de clústeres" .
Credenciales de inicio de sesión único de vSphere 	Aplica a: Solo NetApp HCI Los administradores utilizan estas credenciales para iniciar sesión en el cliente VMware vSphere. Cuando vCenter forma parte de la instalación de NetApp HCI , las credenciales se configuran en el motor de implementación de NetApp de la siguiente manera: • nombredeusuario@vsphere.local con la contraseña especificada, y • administrador@vsphere.local con la contraseña especificada. Cuando se utiliza un vCenter existente para implementar NetApp HCI, las credenciales de inicio de sesión único de vSphere son gestionadas por los administradores de TI de VMware.	"Actualizar las credenciales de vCenter y ESXi".

Tipo de credencial e icono	Uso por parte del administrador	Consulte estas instrucciones
Credenciales del controlador de gestión de la placa base (BMC) 	Aplica a: Solo NetApp HCI Los administradores utilizan estas credenciales para iniciar sesión en el BMC de los nodos de cómputo de NetApp en una implementación de NetApp HCI . El BMC proporciona funciones básicas de monitorización de hardware y de consola virtual. Las credenciales BMC (a veces denominadas <i>IPMI</i>) para cada nodo de cómputo de NetApp se almacenan de forma segura en el mnode en las implementaciones de NetApp HCI . NetApp Hybrid Cloud Control utiliza las credenciales de BMC en una cuenta de servicio para comunicarse con el BMC en los nodos de cómputo durante las actualizaciones de firmware de los nodos de cómputo. Cuando se cambian las credenciales de BMC , también deben actualizarse las credenciales de los nodos de cómputo respectivos en el mnode para conservar todas las funcionalidades de Hybrid Cloud Control.	• "Configure IPMI para cada nodo en NetApp HCI." • Para los nodos H410C, H610C y H615C, "cambiar la contraseña predeterminada de IPMI" . • Para los nodos H410S y H610S, "cambiar la contraseña predeterminada de IPMI" . • "Cambiar las credenciales de BMC en el nodo de administración".
credenciales de ESXi 	Aplica a: Solo NetApp HCI Los administradores pueden iniciar sesión en los hosts ESXi utilizando SSH o la DCUI local con una cuenta de root local. En las implementaciones de NetApp HCI , el nombre de usuario es 'root' y la contraseña se especificó durante la instalación inicial de ese nodo de cómputo en NetApp Deployment Engine. Las credenciales raíz de ESXi para cada nodo de cómputo de NetApp se almacenan de forma segura en el mnode en las implementaciones de NetApp HCI . NetApp Hybrid Cloud Control utiliza las credenciales en una cuenta de servicio para comunicarse directamente con los hosts ESXi durante las actualizaciones de firmware de los nodos de cómputo y las comprobaciones de estado. Cuando un administrador de VMware cambia las credenciales raíz de ESXi, las credenciales de los nodos de cómputo respectivos deben actualizarse en el mnode para conservar la funcionalidad de Hybrid Cloud Control.	"Actualizar las credenciales para los hosts de vCenter y ESXi".

Tipo de credencial e icono	Uso por parte del administrador	Consulte estas instrucciones
contraseña de integración de QoS 	Se aplica a: NetApp HCI y opcional en SolidFire No se utiliza para inicios de sesión interactivos por parte de los administradores. La integración de QoS entre VMware vSphere y Element Software se habilita mediante: • Complemento Element para vCenter Server, y • Servicio QoS en el nodo M. Para la autenticación, el servicio QoS utiliza una contraseña que se usa exclusivamente en este contexto. La contraseña de QoS se especifica durante la instalación inicial del complemento Element para vCenter Server, o se genera automáticamente durante la implementación de NetApp HCI . Sin impacto en otros componentes.	"Actualizar las credenciales de QoSSIOC en el complemento NetApp Element para vCenter Server". La contraseña SIOC del complemento NetApp Element para vCenter Server también se conoce como la contraseña QoSSIOC. Revise el artículo de la base de conocimientos Element Plug-in para vCenter Server.
Credenciales del dispositivo de servicio de vCenter 	Aplica a: NetApp HCI solo si se configura mediante NetApp Deployment Engine Los administradores pueden iniciar sesión en las máquinas virtuales del dispositivo vCenter Server. En las implementaciones de NetApp HCI , el nombre de usuario es 'root' y la contraseña se especificó durante la instalación inicial de ese nodo de cómputo en el motor de implementación de NetApp . Dependiendo de la versión de VMware vSphere implementada, ciertos administradores del dominio de inicio de sesión único de vSphere también pueden iniciar sesión en el dispositivo. Sin impacto en otros componentes.	No se necesitan cambios.
Credenciales de administrador del nodo de administración de NetApp 	Se aplica a: NetApp HCI y opcional en SolidFire Los administradores pueden iniciar sesión en las máquinas virtuales del nodo de administración de NetApp para realizar configuraciones avanzadas y solucionar problemas. Dependiendo de la versión del nodo de gestión implementada, el inicio de sesión mediante SSH no está habilitado de forma predeterminada. En las implementaciones de NetApp HCI , el nombre de usuario y la contraseña fueron especificados por el usuario durante la instalación inicial de ese nodo de cómputo en NetApp Deployment Engine. Sin impacto en otros componentes.	No se necesitan cambios.

Encuentra más información

- ["Cambiar el certificado SSL predeterminado del software Element"](#)
- ["Cambiar la contraseña IPMI para los nodos"](#)
- ["Habilitar la autenticación multifactor"](#)
- ["Comience con la administración de claves externas"](#)
- ["Cree un clúster que admita unidades FIPS."](#)

Cambiar el certificado SSL predeterminado del software Element

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

Cuando se crea un clúster de software NetApp Element , el clúster crea un certificado Secure Sockets Layer (SSL) autofirmado único y una clave privada que se utiliza para toda la comunicación 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 emitidos y verificados por una Autoridad de Certificación (CA) de confianza.

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

• Obtener certificado SSL

Puedes usar el ["Método GetSSLCertificate"](#) Para recuperar información sobre el certificado SSL actualmente instalado, incluyendo todos los detalles del certificado.

• Establecer certificado SSL

Puedes usar el ["Método SetSSLCertificate"](#) para configurar los certificados SSL del clúster y por nodo con el certificado y la clave privada que usted proporcione. El sistema valida el certificado y la clave privada para evitar que se aplique un certificado no válido.

• Eliminar certificado SSL

El ["Método RemoveSSLCertificate"](#) Elimina el certificado SSL y la clave privada actualmente instalados. A continuación, el clúster genera un nuevo certificado autofirmado y una clave privada.



El certificado SSL del clúster se aplica automáticamente a todos los nodos nuevos que se agreguen al clúster. Cualquier nodo eliminado del clúster vuelve a utilizar un certificado autofirmado y toda la información de certificado y clave definida por el usuario se elimina del nodo.

Encuentra más información

- ["Cambiar el certificado SSL predeterminado del nodo de administración"](#)
- ["¿Cuáles son los requisitos para configurar certificados SSL personalizados en Element Software?"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Cambiar la contraseña IPMI predeterminada para los nodos

Puede cambiar la contraseña de administrador predeterminada de la interfaz de administración de plataforma inteligente (IPMI) tan pronto como tenga acceso IPMI remoto al nodo. Es posible que desee hacer esto si hubiera alguna actualización de instalación.

Para obtener detalles sobre la configuración del acceso IPM para los nodos, consulte ["Configure IPMI para cada nodo"](#).

Puedes cambiar la contraseña de IPM para estos nodos:

- nodos H410S
- nodos H610S

Cambiar la contraseña IPMI predeterminada para los nodos H410S

Debe cambiar la contraseña predeterminada de la cuenta de administrador de IPMI en cada nodo de almacenamiento tan pronto como configure el puerto de red IPMI.

Lo que necesitarás

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

Pasos

1. Abra un navegador web en un ordenador que pueda acceder a la red IPMI y navegue hasta la dirección IP IPMI del nodo.
2. Introduzca el nombre de usuario `ADMIN` y contraseña `ADMIN` en la pantalla de inicio de sesión.
3. Tras iniciar sesión, haga clic en la pestaña **Configuración**.
4. Haz clic en **Usuarios**.
5. Seleccione el `ADMIN` usuario y 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. Haz clic en **Modificar** y luego en **Aceptar**.
9. Repita este procedimiento para cualquier otro nodo H410S con contraseñas IPMI predeterminadas.

Cambiar la contraseña IPMI predeterminada para los nodos H610S

Debe cambiar la contraseña predeterminada de la cuenta de administrador de IPMI en cada nodo de almacenamiento tan pronto como configure el puerto de red IPMI.

Lo que necesitarás

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

Pasos

1. Abra un navegador web en un ordenador que pueda acceder a la red IPMI y navegue hasta la dirección IP IPMI del nodo.
2. Introduzca el nombre de usuario `root` y contraseña `calvin` en la pantalla de inicio de sesión.

3. Tras iniciar sesión, haga clic en el icono de navegación del menú situado en la parte superior izquierda de la página para abrir el panel lateral.
4. Haz clic en **Configuración**.
5. Haz clic en **Gestión de usuarios**.
6. Seleccione el usuario **Administrador** de la lista.
7. Habilite la casilla de verificación **Cambiar contraseña**.
8. Introduzca una contraseña nueva y segura en los campos **Contraseña** y **Confirmar contraseña**.
9. Haz clic en **Guardar** en la parte inferior de la página.
10. Repita este procedimiento para cualquier otro nodo H610S con contraseñas IPMI predeterminadas.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Utilice las opciones básicas de la interfaz de usuario del software Element.

Utilice las opciones básicas de la interfaz de usuario del software Element.

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

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

- ["Ver actividad de la API"](#)
- ["Iconos en la interfaz de Elemento"](#)
- ["Enviar comentarios"](#)

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

actividad de la API

Ver actividad de la API

El sistema Element utiliza la API de NetApp Element como base para sus características y funcionalidades. La interfaz de usuario de Element le permite ver varios tipos de actividad de la API en tiempo real en el sistema mientras utiliza la interfaz. Con el registro de la API, puede ver la actividad de la API del sistema iniciada por el usuario y en segundo plano, así como las llamadas a la API realizadas en la página que está viendo actualmente.

Puedes usar el registro de la API para identificar qué métodos de la API se utilizan para determinadas tareas y ver cómo usar los métodos y objetos de la API para crear aplicaciones personalizadas.

Para obtener información sobre cada método, consulte ["Referencia de la API de Element Software"](#).

1. Desde la barra de navegación de la interfaz de usuario de Element, haga clic en **Registro de API**.
2. Para modificar el tipo de actividad de la API que se muestra en la ventana de registro de la API, siga los siguientes pasos:
 - a. Seleccione **Solicitudes** para mostrar el tráfico de solicitudes de la 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:
 - **Iniciado por el usuario:** Tráfico de API generado por sus actividades durante esta sesión de interfaz de usuario web.
 - **Consulta en segundo plano:** Tráfico de API generado por la actividad del sistema en segundo plano.
 - **Página actual:** Tráfico de la API generado por las tareas en la página que está viendo actualmente.

Encuentra más información

- ["Gestionar el almacenamiento con la API de Element"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

La frecuencia de actualización de la interfaz se ve 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 datos para ciertas partes de la página del software NetApp Element que está visualizando.

El intervalo de actualización se restablece al valor predeterminado cuando recargas la página en tu navegador. Puedes ver el intervalo de actualización actual haciendo clic en el nombre del clúster en la parte superior derecha de la página. Tenga en cuenta que el intervalo controla la frecuencia con la que se realizan las solicitudes a la API, no la rapidez con la que los datos regresan del servidor.

Cuando un clúster está bajo una carga elevada, puede poner en cola las solicitudes de API desde la interfaz de usuario de Element. En raras ocasiones, cuando la respuesta del sistema se retrasa significativamente, como por ejemplo una conexión de red lenta combinada con un clúster ocupado, es posible que se cierre su sesión en la interfaz de usuario de Element si el sistema no responde con la suficiente rapidez a las solicitudes de API en cola. Si se le redirige a la pantalla de cierre de sesión, puede volver a iniciar sesión después de descartar cualquier solicitud de autenticación inicial del navegador. Al regresar a la página de resumen, es posible que se le soliciten las credenciales del clúster si su navegador no las ha guardado.

Iconos en la interfaz de Elemento

La interfaz del software NetApp Element muestra iconos que representan las acciones que puede realizar sobre los recursos del sistema.

La siguiente tabla proporciona una referencia rápida:

Icono	Descripción
	Comportamiento
	Copia de seguridad a
	Clonar o copiar
	Eliminar o purgar
	Editar
	Filtrar
	Par
	Refrescar
	Restaurar
	Restaurar desde
	Reversión
	Snapshot

Enviar comentarios

Puedes ayudar a mejorar la interfaz de usuario web del software Element y solucionar cualquier problema de la interfaz utilizando el formulario de comentarios que está accesible en toda la interfaz.

1. Desde cualquier página de la interfaz de usuario de Element, haga clic en el botón **Comentarios**.
2. Introduzca la información pertinente en los campos Resumen y Descripción.

3. Adjunta cualquier captura de pantalla que pueda ser útil.
4. Introduzca un nombre y una dirección de correo electrónico.
5. Seleccione la casilla de verificación para incluir datos sobre su entorno actual.
6. Haga clic en **Enviar**.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Gestionar cuentas

Gestionar cuentas

En los sistemas de almacenamiento SolidFire , los inquilinos pueden usar cuentas para permitir que los clientes se conecten a volúmenes en un clúster. Cuando se crea un volumen, este se asigna a una cuenta específica. También puede administrar las cuentas de administrador de clúster para un sistema de almacenamiento SolidFire .

- ["Trabajar con cuentas que utilizan CHAP"](#)
- ["Administrar cuentas de usuario de administrador de clúster"](#)

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Trabajar con cuentas que utilizan CHAP

En los sistemas de almacenamiento SolidFire , los inquilinos pueden usar cuentas para permitir que los clientes se conecten a volúmenes en un clúster. Una cuenta contiene el protocolo de autenticación Challenge-Handshake Authentication Protocol (CHAP) necesario para acceder a los volúmenes que le han sido asignados. Cuando se crea un volumen, este se asigna a una cuenta específica.

Una cuenta puede tener asignados hasta dos mil volúmenes, pero un volumen solo puede pertenecer a una cuenta.

algoritmos CHAP

A partir del Elemento 12.7, se admiten los algoritmos CHAP seguros compatibles con FIPS SHA1, SHA-256 y SHA3-256. Cuando un iniciador iSCSI de host crea una sesión iSCSI con un destino iSCSI de Element, solicita una lista de algoritmos CHAP para usar. El destino iSCSI de Element elige el primer algoritmo que admite de la lista solicitada por el iniciador iSCSI del host. Para confirmar que el destino iSCSI de Element elige el algoritmo más seguro, debe configurar el iniciador iSCSI del host para que envíe una lista de algoritmos ordenados desde el más seguro, por ejemplo, SHA3-256, hasta el menos seguro, por ejemplo, SHA1 o MD5. Cuando el iniciador iSCSI del host no solicita algoritmos SHA, el destino iSCSI de Element elige MD5, suponiendo que la lista de algoritmos propuestos por el host contiene MD5. Es posible que deba

actualizar la configuración del iniciador iSCSI del host para habilitar la compatibilidad con los algoritmos de seguridad.

Durante una actualización a Element 12.7 o posterior, si ya ha actualizado la configuración del iniciador iSCSI del host para enviar una solicitud de sesión con una lista que incluye algoritmos SHA, a medida que se reinician los nodos de almacenamiento, se activan los nuevos algoritmos seguros y se establecen sesiones iSCSI nuevas o reconectadas utilizando el protocolo más seguro. Todas las sesiones iSCSI existentes pasarán de MD5 a SHA durante la actualización. Si no actualiza la configuración del iniciador iSCSI del host para solicitar SHA, las sesiones iSCSI existentes seguirán utilizando MD5. Posteriormente, después de actualizar los algoritmos CHAP del iniciador iSCSI del host, las sesiones iSCSI deberían pasar gradualmente de MD5 a SHA con el tiempo, en función de las actividades de mantenimiento que resulten en reconexiones de sesiones iSCSI.

Por ejemplo, el iniciador iSCSI de host predeterminado en Red Hat Enterprise Linux (RHEL) 8.3 tiene el `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5`. Se ha comentado la configuración, lo que provoca que el iniciador iSCSI solo utilice MD5. Descomentar esta configuración en el host y reiniciar el iniciador iSCSI activa las sesiones iSCSI desde ese host para que comiencen a usar SHA3-256.

Si es necesario, puede utilizar el "[Lista de sesiones iSCSI](#)" Método API para ver los algoritmos CHAP que se utilizan en cada sesión.

Crea una cuenta

Es posible crear una cuenta para permitir el acceso a los volúmenes.

Cada nombre de cuenta en el sistema debe ser único.

1. Seleccione **Administración > Cuentas**.
2. Haz clic en **Crear cuenta**.
3. Introduce un **Nombre de usuario**.
4. En la sección **Configuración CHAP**, introduzca la siguiente información:



Deje los campos de credenciales en blanco para generar automáticamente cualquiera de las contraseñas.

- **Secreto del iniciador** para la autenticación de sesión de nodo CHAP.
- **Secreto de destino** para la autenticación de sesión de nodo CHAP.

5. Haz clic en **Crear cuenta**.

Ver detalles de la cuenta

Puede visualizar la actividad de rendimiento de cuentas individuales en formato gráfico.

La información del gráfico proporciona información sobre las operaciones de entrada/salida y el rendimiento de la cuenta. Los niveles de actividad promedio y máximo se muestran en incrementos de períodos de reporte de 10 segundos. Estas estadísticas incluyen la actividad de todos los volúmenes asignados a la cuenta.

1. Seleccione **Administración > Cuentas**.
2. Haz clic en el icono de Acciones para una cuenta.
3. Haga clic en **Ver detalles**.

Aquí tenéis algunos detalles:

- **Estado:** El estado de la cuenta. Valores posibles:
 - activa: Una cuenta activa.
 - bloqueado: Una cuenta bloqueada.
 - Eliminada: Una cuenta que ha sido borrada y purgada.
- **Volúmenes activos:** El número de volúmenes activos asignados a la cuenta.
- **Compresión:** La puntuación de eficiencia de compresión para los volúmenes asignados a la cuenta.
- **Desduplicación:** La puntuación de eficiencia de deduplicación para los volúmenes asignados a la cuenta.
- **Aprovisionamiento ligero:** La puntuación de eficiencia del aprovisionamiento ligero para los volúmenes asignados a la cuenta.
- **Eficiencia general:** La puntuación de eficiencia general para los volúmenes asignados a la cuenta.

Editar una cuenta

Puedes editar una cuenta para cambiar el estado, cambiar las claves CHAP o modificar el nombre de la cuenta.

Modificar la configuración CHAP en una cuenta o eliminar iniciadores o volúmenes de un grupo de acceso puede provocar que los iniciadores pierdan el acceso a los volúmenes de forma inesperada. Para verificar que el acceso al volumen no se pierda inesperadamente, cierre siempre las sesiones iSCSI que se verán afectadas por un cambio de cuenta o de grupo de acceso, y verifique que los iniciadores puedan volver a conectarse a los volúmenes después de que se hayan completado los cambios en la configuración del iniciador y la configuración del clúster.



Los volúmenes persistentes asociados a los servicios de administración se asignan a una nueva cuenta que se crea durante la instalación o actualización. Si utiliza volúmenes persistentes, no modifique ni elimine la cuenta asociada.

1. Seleccione **Administración > Cuentas**.
2. Haz clic en el icono de Acciones para una cuenta.
3. En el menú que aparece, seleccione **Editar**.
4. **Opcional:** Edita el **Nombre de usuario**.
5. **Opcional:** Haga clic en la lista desplegable **Estado** y seleccione un estado diferente.



Al cambiar el estado a **bloqueado**, se terminan todas las conexiones iSCSI a la cuenta y esta deja de ser accesible. Los volúmenes asociados a la cuenta se mantienen; sin embargo, no son detectables mediante iSCSI.

6. **Opcional:** En **Configuración CHAP**, edite las credenciales **Secreto del iniciador** y **Secreto del destino** utilizadas para la autenticación de la sesión del nodo.



Si no modifica las credenciales de **Configuración CHAP**, estas permanecerán sin cambios. Si dejas en blanco los campos de credenciales, el sistema generará nuevas contraseñas.

7. Haz clic en **Guardar cambios**.

Eliminar una cuenta

Puedes eliminar una cuenta cuando ya no sea necesaria.

Elimine y purgue cualquier volumen asociado con la cuenta antes de eliminar la cuenta.



Los volúmenes persistentes asociados a los servicios de administración se asignan a una nueva cuenta que se crea durante la instalación o actualización. Si utiliza volúmenes persistentes, no modifique ni elimine la cuenta asociada.

1. Seleccione **Administración > Cuentas**.
2. Haz clic en el icono de Acciones de la cuenta que deseas eliminar.
3. En el menú que aparece, seleccione **Eliminar**.
4. Confirma la acción.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Administrar cuentas de usuario de administrador de clúster

Puede administrar las cuentas de administrador de clúster para un sistema de almacenamiento SolidFire creando, eliminando y editando cuentas de administrador de clúster, cambiando la contraseña de administrador de clúster y configurando los ajustes de LDAP para administrar el acceso al sistema para los usuarios.

tipos de cuentas de administrador de clúster de almacenamiento

En un clúster de almacenamiento que ejecuta el software NetApp Element , pueden existir dos tipos de cuentas de administrador: la cuenta de administrador principal del clúster y una cuenta de administrador del clúster.

- **Cuenta de administrador principal del clúster**

Esta cuenta de administrador se crea cuando se crea el clúster. Esta cuenta es la cuenta administrativa principal con el nivel más alto de acceso al clúster. Esta cuenta es análoga a un usuario root en un sistema Linux. Puedes cambiar la contraseña de esta cuenta de administrador.

- **Cuenta de administrador del 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 asignadas a cada cuenta de administrador del clúster se utilizan para autenticar las solicitudes de API y de la interfaz de usuario de Element dentro del sistema de almacenamiento.



Se requiere una cuenta de administrador de clúster local (no LDAP) para acceder a los nodos activos de un clúster a través de la interfaz de usuario por nodo. No se requieren credenciales de cuenta para acceder a un nodo que aún no forma parte de un clúster.

Ver detalles de administración del clúster

1. Para crear una cuenta de administrador de clúster (no LDAP) para todo el clúster, realice las siguientes acciones:

a. Haz clic en **Usuarios > Administradores del clúster**.

2. En la página Administradores del clúster de la pestaña Usuarios, puede ver la siguiente información.

- **ID:** Número secuencial asignado a la cuenta del administrador del clúster.
- **Nombre de usuario:** El nombre asignado a la cuenta de administrador del clúster cuando se creó.
- **Acceso:** Los permisos de usuario asignados a la cuenta de usuario. Valores posibles:
 - leer
 - informes
 - nodos
 - unidades
 - volúmenes
 - cuentas
 - administradores de clúster
 - administrador
 - Administrador de soporte



Todos los permisos están disponibles para el tipo de acceso de administrador.

Existen tipos de acceso disponibles a través de la API que no están disponibles en la interfaz de usuario de Element.

+

- **Tipo:** El tipo de administrador del clúster. Valores posibles:
 - Grupo
 - LDAP
- **Atributos:** Si la cuenta de administrador del clúster se creó utilizando la API de Element, esta columna muestra cualquier par nombre-valor que se haya establecido utilizando ese método.

Ver "[Referencia de la API de NetApp Element Software](#)".

Crea una cuenta de administrador de clúster

Puede crear nuevas cuentas de administrador de clúster con permisos para permitir o restringir el acceso a áreas específicas del sistema de almacenamiento. Cuando configuras los permisos de la cuenta de administrador del clúster, el sistema otorga derechos de solo lectura para cualquier permiso que no asignes 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 LDAP con la interfaz de usuario de Element.](#)"

Posteriormente, puede cambiar los privilegios de la cuenta de administrador del clúster para la generación de informes, nodos, unidades, volúmenes, cuentas y acceso a nivel de clúster. Cuando habilitas un permiso, el sistema asigna acceso de escritura para ese nivel. El sistema otorga al usuario administrador acceso de solo lectura para los niveles que usted no seleccione.

Posteriormente también podrá eliminar cualquier cuenta de usuario administrador del clúster creada por un administrador del sistema. No se puede eliminar la cuenta de administrador principal del clúster que se creó cuando se creó el clúster.

1. Para crear una cuenta de administrador de clúster (no LDAP) para todo el clúster, realice las siguientes acciones:
 - a. Haz clic en **Usuarios > Administradores del clúster**.
 - b. Haga clic en **Crear administrador de clúster**.
 - c. Seleccione el tipo de usuario **Cluster**.
 - d. Introduce un nombre de usuario y una contraseña para la cuenta y confirma la contraseña.
 - e. Seleccione los permisos de usuario que se aplicarán a la cuenta.
 - f. Seleccione la casilla de verificación para aceptar el Acuerdo de Licencia de Usuario Final.
 - 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 **Clúster > LDAP**.
 - b. Asegúrese de que la autenticación LDAP esté habilitada.
 - c. Haz clic en **Probar autenticación de usuario** y copia el nombre distintivo que aparece para el usuario o uno de los grupos a los que pertenece el usuario para que puedas pegarlo más tarde.
 - d. Haz clic en **Usuarios > Administradores del 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 distintivo completo para el usuario o grupo. Como alternativa, péguelo del nombre distinguido que copió anteriormente.

Si el nombre distinguido forma parte de un grupo, cualquier usuario que sea miembro de ese grupo en el servidor LDAP tendrá los permisos de esta cuenta de administrador.

Para agregar usuarios o grupos de administradores de clúster LDAP, el formato general del nombre de usuario es "LDAP:<Nombre distinguido completo>".

- a. Seleccione los permisos de usuario que se aplicarán a la cuenta.
- b. Seleccione la casilla de verificación para aceptar el Acuerdo de Licencia de Usuario Final.
- c. Haga clic en **Crear administrador de clúster**.

Editar permisos de administrador del clúster

Puede cambiar los privilegios de la cuenta de administrador del clúster para la generación de informes, nodos, unidades, volúmenes, cuentas y acceso a nivel de clúster. Cuando habilitas un permiso, el sistema asigna acceso de escritura para ese nivel. El sistema otorga al usuario administrador acceso de solo lectura para los niveles que usted no seleccione.

1. Haz clic en **Usuarios > Administradores del clúster**.
2. Haga clic en el icono Acciones del administrador del clúster que desea editar.
3. Haga clic en **Editar**.
4. Seleccione los permisos de usuario que se aplicarán a la cuenta.
5. Haz clic en **Guardar cambios**.

Cambiar las contraseñas de las cuentas de administrador del clúster

Puede utilizar la interfaz de usuario de Element para cambiar las contraseñas de administrador del clúster.

1. Haz clic en **Usuarios > Administradores del clúster**.
2. Haga clic en el icono Acciones del administrador del clúster que desea editar.
3. Haga clic en **Editar**.
4. En el campo Cambiar contraseña, introduzca una nueva contraseña y confírmela.
5. Haz clic en **Guardar cambios**.

Información relacionada

- ["Obtenga información sobre los tipos de acceso disponibles para las API de Element."](#)
- ["Habilite la autenticación LDAP con la interfaz de usuario de Element."](#)
- ["Deshabilitar LDAP"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Administrar LDAP

Puede configurar el Protocolo Ligero de Acceso a Directorios (LDAP) para habilitar la funcionalidad de inicio de sesión segura basada en directorios para el almacenamiento SolidFire . Puede configurar LDAP a nivel de clúster y autorizar usuarios y grupos LDAP.

La gestión de LDAP implica configurar la autenticación LDAP en un clúster SolidFire utilizando un entorno de Microsoft Active Directory existente y probar la configuración.



Puedes utilizar direcciones IPv4 e IPv6.

Habilitar LDAP implica los siguientes pasos generales, descritos en detalle:

1. **Complete los pasos de preconfiguración para la compatibilidad con LDAP**. Compruebe que dispone de todos los datos necesarios para configurar la autenticación LDAP.
2. **Habilitar la autenticación LDAP**. Utilice la interfaz de usuario de Element o la API de Element.
3. **Validar la configuración LDAP**. Opcionalmente, verifique que el clúster esté configurado con los valores correctos ejecutando el método de la API GetLdapConfiguration o revisando la configuración de LCAP mediante la interfaz de usuario de Element.
4. **Prueba la autenticación LDAP** (con el `readonly` usuario). Compruebe que la configuración LDAP es correcta ejecutando el método API TestLdapAuthentication o utilizando la interfaz de usuario de Element. Para esta prueba inicial, utilice el nombre de usuario "sAMAccountName" de `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. **Prueba la autenticación LDAP** (con una cuenta de usuario que quieras agregar). Repita el paso 4 con una cuenta de usuario que desee agregar como administrador del clúster de Element. Copia el distinguished nombre (DN) o el usuario (o el grupo). Este DN se utilizará en el paso 6.
6. **Agregue el administrador del clúster LDAP** (copie y pegue el DN del paso de prueba de autenticación LDAP). Utilizando la interfaz de usuario de Element o el método de la 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 copió en el paso 5. Esto garantiza que el DN esté formateado correctamente.
7. **Prueba el acceso de administrador del clúster**. Inicie sesión en el clúster utilizando el usuario administrador del clúster LDAP recién creado. Si has añadido un grupo LDAP, puedes iniciar sesión como cualquier usuario de ese grupo.

Complete los pasos de preconfiguración para la compatibilidad con LDAP.

Antes de habilitar la compatibilidad con LDAP en Element, debe configurar un servidor de Active Directory de Windows y realizar otras tareas de preconfiguración.

Pasos

1. Configurar un servidor de directorio activo de Windows.
2. **Opcional:** Habilitar la compatibilidad con LDAPS.
3. Crear usuarios y grupos.
4. Cree una cuenta de servicio de solo lectura (como “sfireadonly”) para usarla para buscar en el directorio LDAP.

Habilite la autenticación LDAP con la interfaz de usuario de Element.

Puede configurar la integración del sistema de almacenamiento con un servidor LDAP existente. Esto permite a los administradores de LDAP gestionar de forma centralizada el acceso de los usuarios al sistema de almacenamiento.

Puede configurar LDAP mediante la interfaz de usuario de Element o la API de Element. Este procedimiento describe cómo configurar LDAP utilizando la interfaz de usuario de Element.

Este ejemplo muestra cómo configurar la autenticación LDAP en SolidFire y utiliza `SearchAndBind` como tipo de autenticación. El ejemplo utiliza un único servidor Active Directory de Windows Server 2012 R2.

Pasos

1. Haga clic en **Clúster > LDAP**.
2. Haga clic en **Sí** para habilitar la autenticación LDAP.
3. Haz clic en **Añadir un servidor**.
4. Introduzca el **Nombre de host/Dirección IP**.



También se puede introducir un número de puerto personalizado opcional.

Por ejemplo, para agregar un número de puerto personalizado, ingrese <nombre de host o dirección IP>:<número de puerto>

5. **Opcional:** Seleccione **Usar protocolo LDAPS**.
6. Introduzca la información requerida en **Ajustes generales**.

LDAP Servers

Host Name/IP Address	192.168.9.99	Remove
☐ Use LDAPS Protocol		

[Add a Server](#)

General Settings

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

[Save Changes](#)

7. Haga clic en **Habilitar LDAP**.
8. Haz clic en **Probar autenticación de usuario** si quieres probar el acceso al servidor de un usuario.
9. Copie el nombre distintivo y la información del grupo de usuarios que aparece para utilizarlos posteriormente al crear administradores de clúster.
10. Haz clic en **Guardar cambios** para guardar la nueva configuración.
11. Para crear un usuario en este grupo para que cualquiera pueda iniciar sesión, complete lo siguiente:
 - a. Haz clic en **Usuario > Ver**.

Create a New Cluster Admin



Select User Type

☐ Cluster ☒ LDAP

Enter User Details

Distinguished Name

CN=StorageAdmins,OU=Home
users,DC=thesmyths,DC=ca

Select User Permissions

☐ Reporting	☐ Volumes
☐ Nodes	☐ Accounts
☐ Drives	☐ Cluster Admin

Accept the Following End User License Agreement

- Para el nuevo usuario, haga clic en **LDAP** para Tipo de usuario y pegue el grupo que copió en el campo Nombre distintivo.
- Seleccione los permisos, normalmente todos los permisos.
- Desplácese hacia abajo hasta el Acuerdo de Licencia de Usuario Final y haga clic en **Acepto**.
- Haga clic en **Crear administrador de clúster**.

Ahora tienes un usuario con el valor de un grupo de Active Directory.

Para probar esto, cierre sesión en la interfaz de usuario de Element y vuelva a iniciar sesión como usuario de ese grupo.

Habilite la autenticación LDAP con la API de Element.

Puede configurar la integración del sistema de almacenamiento con un servidor LDAP existente. Esto permite a los administradores de LDAP gestionar de forma centralizada el acceso de los usuarios al sistema de almacenamiento.

Puede configurar LDAP mediante la interfaz de usuario de Element o la API de Element. Este procedimiento describe cómo configurar LDAP utilizando 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 siguiente método: `EnableLdapAuthentication` Método API.

Pasos

- 1. Habilite primero la autenticación LDAP en el clúster utilizando `EnableLdapAuthentication` Método API.
- 2. Ingrese la información requerida.

```
{
  "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
Tipo de autenticación: Buscar y vincular	Indica que el clúster utilizará la cuenta de servicio de solo lectura para buscar primero al usuario que se está autenticando y, posteriormente, vincularlo si se encuentra y se autentica.
groupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica la ubicación en el árbol LDAP donde comenzar la búsqueda de grupos. Para este ejemplo, hemos utilizado la raíz de nuestro árbol. Si su árbol LDAP es muy grande, es posible que desee configurarlo en un subárbol más granular para disminuir los tiempos de búsqueda.

Parámetros utilizados	Descripción
userSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica la ubicación en el árbol LDAP donde comenzar la búsqueda de usuarios. Para este ejemplo, hemos utilizado la raíz de nuestro árbol. Si su árbol LDAP es muy grande, es posible que desee configurarlo en un subárbol más granular para disminuir los tiempos de búsqueda.
groupSearchType: ActiveDirectory	Utiliza el servidor Active Directory de Windows como servidor LDAP.
userSearchFilter: <pre>" (& (objectClass=person) (sAMAccountName=%USERNAME%)) "</pre> Para usar el nombre principal de usuario (dirección de correo electrónico para iniciar sesión), puede cambiar el filtro de búsqueda de usuario a: <pre>" (& (objectClass=person) (userPrincipalName=%USERNAME%)) "</pre> O bien, para buscar tanto userPrincipalName como sAMAccountName, puede utilizar el siguiente userSearchFilter: <pre>" (& (objectClass=person) (</pre>	(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%))" ----
Utilizamos sAMAccountName como nombre de usuario para iniciar sesión en el clúster SolidFire . Estos ajustes le indican a LDAP que busque el nombre de usuario especificado durante el inicio de sesión en el atributo sAMAccountName y también que limite la búsqueda a las entradas que tengan "person" como valor en el atributo objectClass.	searchBindDN
Este es el nombre distintivo del usuario de solo lectura que se utilizará para buscar en el directorio LDAP. Para Active Directory, lo más sencillo suele ser utilizar el nombre principal de usuario (formato de dirección de correo electrónico) para el usuario.	buscarContraseñaVinculada

Para probar esto, cierre sesión en la interfaz de usuario de Element y vuelva a iniciar sesión como usuario de ese grupo.

Ver detalles de LDAP

Consulte la información LDAP en la página LDAP de la pestaña Clúster.



Debe habilitar LDAP para ver esta configuración de LDAP.

1. Para ver los detalles de LDAP con la interfaz de usuario de Element, haga clic en **Clúster > LDAP**.

- **Nombre de host/Dirección IP:** Dirección de un servidor de directorio LDAP o LDAPS.
- **Tipo de autenticación:** El método de autenticación del usuario. Valores posibles:
 - Enlace directo
 - Buscar y enlazar
- **DN de enlace de búsqueda:** Un DN completo para iniciar sesión y realizar una búsqueda LDAP del usuario (necesita acceso de nivel de enlace al directorio LDAP).
- **Contraseña de enlace de búsqueda:** Contraseña utilizada para autenticar el acceso al servidor LDAP.
- **DN base de búsqueda de usuarios:** El DN base del árbol utilizado para iniciar la búsqueda de usuarios. El sistema busca en el subárbol desde la ubicación especificada.
- **Filtro de búsqueda de usuario:** Introduzca lo siguiente utilizando su nombre de dominio:

```
( & (objectClass=person) ( | (sAMAccountName=%USERNAME%) (userPrincipalName=%USERN  
AME%) ) )
```

- **Tipo de búsqueda de grupo:** Tipo de búsqueda que controla el filtro de búsqueda de grupo predeterminado utilizado. Valores posibles:
 - Active Directory: Membresía anidada de todos los grupos LDAP de un usuario.
 - Sin grupos: No hay soporte para grupos.
 - DN de miembro: Grupos de estilo DN de miembro (de un solo nivel).
- **DN base de búsqueda de grupo:** El DN base del árbol utilizado para iniciar la búsqueda de grupo. El sistema busca en el subárbol desde la ubicación especificada.
- **Prueba de autenticación de usuario:** Después de configurar LDAP, utilice esto para probar la autenticación de nombre de usuario y contraseña para el servidor LDAP. Introduce una cuenta que ya exista para probar esto. Aparece el nombre distintivo y la información del grupo de usuarios, que puede copiar para su uso posterior al crear administradores de clúster.

Prueba la configuración LDAP

Tras configurar LDAP, debe probarlo utilizando la interfaz de usuario de Element o la API de Element. `TestLdapAuthentication` método.

Pasos

1. Para probar la configuración LDAP con la interfaz de usuario de Element, haga lo siguiente:
 - a. Haga clic en **Clúster > LDAP**.
 - b. Haga clic en **Probar autenticación LDAP**.
 - c. Resuelva cualquier problema utilizando la información de la siguiente tabla:

Mensaje de error	Descripción
<code>xLDAPUserNotFound</code>	- No se encontró al usuario que se estaba probando en la configuración. <code>userSearchBaseDN</code> subárbol. - El <code>userSearchFilter</code> está configurado incorrectamente.
<code>xLDAPBindFailed (Error: Invalid credentials)</code>	- 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 actualmente deshabilitada.
<code>xLDAPSearchBindFailed (Error: Can't contact LDAP server)</code>	La URI del servidor LDAP es incorrecta.
<code>xLDAPSearchBindFailed (Error: Invalid credentials)</code>	El nombre de usuario o la contraseña de solo lectura están configurados incorrectamente.
<code>xLDAPSearchFailed (Error: No such object)</code>	El <code>userSearchBaseDN</code> no es una ubicación válida dentro del árbol LDAP.
<code>xLDAPSearchFailed (Error: Referral)</code>	- El <code>userSearchBaseDN</code> no es una ubicación válida dentro del árbol LDAP. - El <code>userSearchBaseDN</code> y <code>groupSearchBaseDN</code> están en una unidad organizativa anidada. Esto puede causar problemas de permisos. La solución alternativa consiste en incluir la OU en las entradas DN base de usuario y grupo, (por ejemplo: <code>ou=storage, cn=company, cn=com</code>)

2. Para probar la configuración LDAP con la API de Element, haga lo siguiente:

a. Llama al método `TestLdapAuthentication`.

```
{
  "method": "TestLdapAuthentication",
  "params": {
    "username": "admin1",
    "password": "admin1PASS"
  },
  "id": 1
}
```

- b. Revisa los resultados. Si la llamada a la API se realiza correctamente, los resultados incluyen el nombre distintivo del usuario especificado y una lista de los grupos a los que pertenece el usuario.

```
{
  "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"
  }
}
```

Deshabilitar LDAP

Puede deshabilitar la integración LDAP mediante la interfaz de usuario de Element.

Antes de comenzar, debe anotar todas las opciones de configuración, ya que deshabilitar LDAP borra todas las configuraciones.

Pasos

1. Haga clic en **Clúster > LDAP**.
2. Haga clic en **No**.
3. Haga clic en **Deshabilitar LDAP**.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Administra tu sistema

Administra tu sistema

Puedes gestionar tu sistema en la interfaz de usuario de Element. Esto incluye habilitar la autenticación multifactor, administrar la configuración del clúster, admitir los estándares federales de procesamiento de información (FIPS) y utilizar la administración de claves externas.

- ["Habilitar la autenticación multifactor"](#)
- ["Configurar los ajustes del clúster"](#)
- ["Cree un clúster que admita unidades FIPS."](#)
- ["Comience con la administración de claves externas"](#)

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Habilitar la autenticación multifactor

Configurar la autenticación multifactor

La autenticación multifactor (MFA) utiliza un proveedor de identidad (IdP) de terceros a través del lenguaje de marcado de aserción de seguridad (SAML) para gestionar las sesiones de usuario. La autenticación multifactor (MFA) permite a los administradores configurar factores de autenticación adicionales según sea necesario, como contraseña y mensaje de texto, y contraseña y mensaje de correo electrónico.

Puedes utilizar estos pasos básicos a través de la API de Element para configurar tu clúster para que utilice la autenticación multifactor.

Los detalles de cada método de la API se pueden encontrar en el ["Referencia de la API de elementos"](#).

1. Cree una nueva configuración de proveedor de identidad (IdP) de terceros para el clúster llamando al siguiente método de la API y pasando los metadatos del IdP en formato JSON:

`CreateIdpConfiguration`

Los metadatos del IdP, en formato de texto plano, se recuperan del IdP de terceros. Es necesario validar estos metadatos para asegurar que estén formateados correctamente en JSON. Existen numerosas aplicaciones de formato JSON disponibles que puedes utilizar, por ejemplo: <https://freeformatter.com/json-escape.html>.

2. Recupere los metadatos del clúster, a través de `spMetadataUrl`, para copiarlos al IdP de terceros llamando al siguiente método de API: `ListIdpConfigurations`

`spMetadataUrl` es una URL utilizada para recuperar metadatos del proveedor de servicios del clúster para el IdP con el fin de establecer una relación de confianza.

3. Configure las aserciones SAML en el IdP de terceros para incluir el atributo "NameID" para identificar de forma única a un usuario para el registro de auditoría y para que el cierre de sesión único funcione correctamente.

4. Cree una o más cuentas de usuario de administrador de clúster autenticadas por un IdP de terceros para la autorización llamando al siguiente método de API: `AddIdpClusterAdmin`



El nombre de usuario del administrador del clúster IdP debe coincidir con la asignación de nombre/valor del atributo SAML para lograr el 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.
- `grupo=administrador-de-clúster` - donde el IdP está configurado para liberar una propiedad de grupo a la que todos los usuarios deberían tener acceso. Tenga en cuenta que, por motivos de seguridad, el emparejamiento de nombre/valor del atributo SAML distingue entre mayúsculas y minúsculas.

5. Habilite la autenticación multifactor (MFA) para el clúster llamando al siguiente método de la API: `EnableIdpAuthentication`

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Información adicional sobre la autenticación multifactor

Debes tener en cuenta las siguientes advertencias en relación con la autenticación multifactor.

- Para actualizar los certificados IdP que ya no son válidos, deberá utilizar un usuario administrador que no sea IdP para llamar al siguiente método de la API: `UpdateIdpConfiguration`
- La autenticación multifactor (MFA) es incompatible con certificados de menos de 2048 bits de longitud. Por defecto, se crea un certificado SSL de 2048 bits en el clúster. Debe evitar establecer un certificado de tamaño reducido al llamar al método de la API: `SetSSLCertificate`



Si el clúster utiliza un certificado de menos de 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 posterior.

- Los usuarios administradores de IdP no pueden utilizarse para realizar llamadas a la API directamente (por ejemplo, a través de SDK o Postman) ni para otras integraciones (por ejemplo, OpenStack Cinder o el complemento de vCenter). Si necesita crear usuarios con estas capacidades, agregue usuarios administradores de clúster LDAP o usuarios administradores de clúster locales.

Encuentra más información

- ["Gestionar el almacenamiento con la API de Element"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Configurar los ajustes del clúster

Habilitar y deshabilitar el cifrado en reposo para un clúster

Con los clústeres SolidFire , puede cifrar todos los datos en reposo almacenados en las unidades del clúster. Puede habilitar la protección de unidades de autocifrado (SED) en todo el clúster mediante cualquiera de los siguientes métodos: ["Cifrado en reposo basado en hardware o software"](#) .

Puede habilitar el cifrado de hardware en reposo mediante la interfaz de usuario o la API de Element. Habilitar la función de cifrado de hardware en reposo no afecta al rendimiento ni a la eficiencia del clúster. Solo puede habilitar el cifrado de software en reposo utilizando la API de Element.

El cifrado de datos en reposo basado en hardware no está habilitado de forma predeterminada durante la creación del clúster y se puede habilitar y deshabilitar desde la interfaz de usuario de Element.



Para los clústeres de almacenamiento all-flash SolidFire , el cifrado de software en reposo debe habilitarse durante la creación del clúster y no puede deshabilitarse después de que se haya creado el clúster.

Lo que necesitarás

- Usted tiene privilegios de administrador de clúster para habilitar o cambiar la configuración de cifrado.
- Para el cifrado en reposo basado en hardware, debe asegurarse de que el clúster se encuentre en buen estado antes de cambiar la configuración de cifrado.
- Si va a deshabilitar el cifrado, dos nodos deben participar en un clúster para acceder a la clave para deshabilitar el cifrado en una unidad.

Comprobar el estado del cifrado en reposo

Para ver el estado actual del cifrado en reposo y/o del cifrado de software en reposo en el clúster, utilice la siguiente información: ["Obtener información del clúster"](#) método. Puedes usar el ["Obtener información de cifrado de software en reposo"](#) Método para obtener información sobre el clúster que utiliza para cifrar los datos en reposo.



El panel de control de la interfaz de usuario del software Element en <https://<MVIP>/> Actualmente solo se muestra el estado de cifrado en reposo para el cifrado basado en hardware.

Opciones

- [Habilitar el cifrado basado en hardware en reposo](#)
- [Habilitar el cifrado basado en software en reposo](#)
- [Deshabilitar el cifrado basado en hardware en reposo](#)

Habilitar el cifrado basado en hardware en reposo



Para habilitar el cifrado en reposo mediante una configuración de administración de claves externa, debe habilitar el cifrado en reposo a través de ["API"](#) . Habilitar esta función mediante el botón de la interfaz de usuario de Element existente hará que se vuelva a utilizar la generación interna de claves.

1. Desde la interfaz de usuario de Element, seleccione **Cluster > Settings**.

2. Seleccione **Habilitar cifrado en reposo**.

Habilitar el cifrado basado en software en reposo



El cifrado de software en reposo no se puede deshabilitar después de que se haya habilitado en el clúster.

1. Durante la creación del clúster, ejecute el ["método de creación de clúster"](#) con `enableSoftwareEncryptionAtRest` empezar a `true`.

Deshabilitar el cifrado basado en hardware en reposo

1. Desde la interfaz de usuario de Element, seleccione **Cluster > Settings**.
2. Seleccione **Deshabilitar el cifrado en reposo**.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Establezca el umbral completo del clúster

Puedes cambiar el nivel en el que el sistema genera una advertencia de llenado del clúster de bloques siguiendo los pasos que se indican a continuación. Además, puede utilizar el método de la API `ModifyClusterFullThreshold` para cambiar el nivel en el que el sistema genera una advertencia de bloqueo o de metadatos.

Lo que necesitarás

Debe tener privilegios de administrador de clúster.

Pasos

1. Haz clic en **Clúster > Configuración**.
2. En la sección Configuración completa del clúster, ingrese un porcentaje en **Generar una alerta de advertencia cuando quede un _% de capacidad antes de que Helix no pueda recuperarse de una falla de nodo**.
3. Haz clic en **Guardar cambios**.

Encuentra más información

["¿Cómo se calculan los umbrales de blockSpace para Element?"](#)

Habilitar y deshabilitar el balanceo de carga de volumen

A partir de Element 12.8, puede usar el balanceo de carga de volumen para equilibrar los volúmenes entre nodos según las IOPS reales de cada volumen en lugar de las IOPS mínimas configuradas en la política de QoS. Puede activar y desactivar el balanceo de carga de volumen, que está desactivado de forma predeterminada, mediante la interfaz de usuario o la API de Element.

Pasos

1. Seleccione **Clúster > Configuración**.
2. En la sección Específica del clúster, cambie el estado de Balanceo de carga de volumen:

Habilitar el equilibrio de carga de volumen

Seleccione **Habilitar balanceo de carga en IOPS reales** y confirme su selección.

Deshabilitar el equilibrio de carga de volumen:

Seleccione **Deshabilitar el balanceo de carga en IOPS reales** y confirme su selección.

3. Opcionalmente, seleccione **Informes > Resumen** para confirmar el cambio de estado de Balance en IOPS reales. Es posible que tengas que desplazarte hacia abajo en la información de estado del clúster para ver el estado.

Encuentra más información

- ["Habilite el balanceo de carga de volumen mediante la API"](#)
- ["Deshabilitar el balanceo de carga de volumen mediante la API"](#)
- ["Crear y gestionar políticas de QoS de volumen"](#)

Habilitar y deshabilitar el acceso de soporte

Puede habilitar el acceso de soporte para permitir temporalmente que el personal de soporte de NetApp acceda a los nodos de almacenamiento a través de SSH para la resolución de problemas.

Debe tener privilegios de administrador de clúster para cambiar el acceso de soporte.

1. Haz clic en **Clúster > Configuración**.
2. En la sección Habilitar/Deshabilitar acceso de soporte, ingrese la duración (en horas) durante la cual desea permitir que el soporte tenga acceso.
3. Haga clic en **Habilitar acceso de soporte**.
4. **Opcional:** Para deshabilitar el acceso al soporte, haga clic en **Deshabilitar acceso al soporte**.

Gestionar el banner de Condiciones de uso

Puedes habilitar, editar o configurar un banner que contenga un mensaje para el usuario.

Opciones

[Habilita el banner de Condiciones de uso](#) [Edita el banner de Condiciones de uso](#) [Desactivar el banner de Condiciones de uso](#)

Habilita el banner de Condiciones de uso

Puedes habilitar un banner de Condiciones de uso que aparezca cuando un usuario inicie 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 ha configurado para el clúster. El banner puede eliminarse en cualquier momento.

Debe tener privilegios de administrador de clúster para habilitar la funcionalidad de Términos de uso.

1. Haz clic en **Usuarios > Condiciones de uso**.
2. En el formulario **Condiciones de uso**, introduzca el texto que se mostrará en el cuadro de diálogo de Condiciones de uso.



No exceda los 4096 caracteres.

3. Haga clic en **Habilitar**.

Edita el banner de Condiciones de uso

Puedes editar el texto que ve un usuario cuando selecciona el banner de inicio de sesión de los Términos de uso.

Lo que necesitarás

- Para configurar las Condiciones de uso, debe tener privilegios de administrador de clúster.
- Asegúrese de que la función de Condiciones de uso esté habilitada.

Pasos

1. Haz clic en **Usuarios > Condiciones de uso**.
2. En el cuadro de diálogo **Condiciones de uso**, edite el texto que desea que aparezca.



No exceda los 4096 caracteres.

3. Haz clic en **Guardar cambios**.

Desactivar el banner de Condiciones de uso

Puedes desactivar el banner de Condiciones de uso. Con el banner desactivado, ya no se le solicita al usuario que acepte los términos de uso al utilizar la interfaz de usuario de Element.

Lo que necesitarás

- Para configurar las Condiciones de uso, debe tener privilegios de administrador de clúster.
- Asegúrese de que las Condiciones de uso estén habilitadas.

Pasos

1. Haz clic en **Usuarios > Condiciones de uso**.
2. Haga clic en **Desactivar**.

Configurar el protocolo de tiempo de red

Configure los servidores del Protocolo de Tiempo de Red (NTP) para que el clúster los consulte.

Puede instruir a cada nodo de un clúster para que consulte a un servidor de Protocolo de Tiempo de Red (NTP) para obtener actualizaciones. El clúster solo contacta con los servidores configurados y les solicita información NTP.

El protocolo NTP se utiliza para sincronizar los relojes a través de una red. La conexión a un servidor NTP interno o externo debe formar parte de la configuración inicial del clúster.

Configure NTP en el clúster para que apunte a un servidor NTP local. Puede utilizar la dirección IP o el

nombre de host FQDN. El servidor NTP predeterminado al momento de la creación del clúster se establece en us.pool.ntp.org; sin embargo, no siempre se puede establecer una conexión con este sitio dependiendo de la ubicación física del clúster SolidFire .

El uso del FQDN depende de si la configuración DNS del nodo de almacenamiento individual está implementada y operativa. Para ello, configure los servidores DNS en cada nodo de almacenamiento y asegúrese de que los puertos estén abiertos consultando la página de Requisitos de puertos de red.

Puedes introducir hasta cinco servidores NTP diferentes.



Puedes utilizar direcciones IPv4 e IPv6.

Lo que necesitarás

Para configurar este ajuste, debe tener privilegios de administrador de clúster.

Pasos

1. Configure una lista de direcciones IP y/o nombres de dominio completos (FQDN) en la configuración del servidor.
2. Asegúrese de que el DNS esté configurado correctamente en los nodos.
3. Haz clic en **Clúster > Configuración**.
4. En Configuración del protocolo de tiempo de red, seleccione **No**, que utiliza la configuración NTP estándar.
5. Haz clic en **Guardar cambios**.

Encuentra más información

- ["Configure el clúster para que escuche las transmisiones NTP."](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Configure el clúster para que escuche las transmisiones NTP.

Al utilizar el modo de difusión, puede indicar a cada nodo de un clúster que escuche en la red los mensajes de difusión del Protocolo de tiempo de red (NTP) procedentes de un servidor determinado.

El protocolo NTP se utiliza para sincronizar los relojes a través de una red. La conexión a un servidor NTP interno o externo debe formar parte de la configuración inicial del clúster.

Lo que necesitarás

- Para configurar este ajuste, debe tener privilegios de administrador de clúster.
- Debe configurar un servidor NTP en su red como servidor de difusión.

Pasos

1. Haz clic en **Clúster > Configuración**.
2. Introduzca en la lista de servidores el servidor o servidores NTP que utilizan el modo de difusión.
3. En Configuración del protocolo de tiempo de red, seleccione **Sí** para usar un cliente de difusión.
4. Para configurar el cliente de difusión, en el campo **Servidor**, introduzca el servidor NTP que configuró en modo de difusión.

5. Haz clic en **Guardar cambios**.

Encuentra más información

- ["Configure los servidores del Protocolo de Tiempo de Red \(NTP\) para que el clúster los consulte."](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Administrar SNMP

Obtenga más información sobre SNMP

Puede configurar el Protocolo Simple de Administración de Red (SNMP) en su clúster.

Puede seleccionar un solicitante SNMP, seleccionar qué versión de SNMP utilizar, identificar el usuario del modelo de seguridad basado en usuario (USM) de SNMP y configurar traps para monitorear el clúster SolidFire . También puede ver y acceder a los archivos de la base de datos de información de gestión.



Puedes utilizar direcciones IPv4 e IPv6.

Detalles SNMP

En la página SNMP de la pestaña Clúster, puede ver la siguiente información.

• MIB SNMP

Los archivos MIB que puede ver o descargar.

• Configuración general de SNMP

Puede habilitar o deshabilitar SNMP. Una vez habilitado SNMP, puede elegir qué versión utilizar. Si utiliza la versión 2, puede agregar solicitantes, y si utiliza la versión 3, puede configurar usuarios USM.

• Configuración de trampas SNMP

Puedes identificar qué trampas quieres capturar. Puede configurar el host, el puerto y la cadena de comunidad para cada destinatario de la trampa.

Configurar un solicitante SNMP

Cuando SNMP versión 2 está habilitada, puede habilitar o deshabilitar un solicitante y configurar los solicitantes para que reciban solicitudes SNMP autorizadas.

1. Menú de clic: Clúster[SNMP].
2. En **Configuración general de SNMP**, haga clic en **Sí** para habilitar SNMP.
3. De la lista **Versión**, seleccione **Versión 2**.
4. En la sección **Solicitantes**, ingrese la **Cadena de comunidad** y la información de **Red**.



Por defecto, la cadena de comunidad es pública y la red es localhost. Puedes cambiar esta configuración predeterminada.

5. **Opcional:** Para agregar otro solicitante, haga clic en **Agregar un solicitante** e ingrese la **Cadena de comunidad** y la información de **Red**.
6. Haz clic en **Guardar cambios**.

Encuentra más información

- [Configurar traps SNMP](#)
- [Visualización de datos de objetos gestionados mediante archivos de la base de información de gestión.](#)

Configurar un usuario SNMP USM

Cuando habilite SNMP versión 3, deberá configurar un usuario USM para que reciba las solicitudes SNMP autorizadas.

1. Haga clic en **Clúster > SNMP**.
2. En **Configuración general de SNMP**, haga clic en **Sí** para habilitar SNMP.
3. De la lista **Versión**, seleccione **Versión 3**.
4. En la sección **Usuarios de USM**, ingrese el nombre, la contraseña y la frase de contraseña.
5. **Opcional:** Para agregar otro usuario de USM, haga clic en **Agregar un usuario de USM** e ingrese el nombre, la contraseña y la frase de contraseña.
6. Haz clic en **Guardar cambios**.

Configurar traps SNMP

Los administradores de sistemas pueden usar traps SNMP, también conocidas como notificaciones, para monitorear el estado del clúster SolidFire .

Cuando las alertas SNMP están habilitadas, el clúster SolidFire genera alertas asociadas con entradas del registro de eventos y alertas del sistema. Para recibir notificaciones SNMP, debe elegir las trampas que se deben generar e identificar los destinatarios de la información de la trampa. Por defecto, no se generan trampas.

1. Haga clic en **Clúster > SNMP**.
2. Seleccione uno o más tipos de traps en la sección **Configuración de traps SNMP** que el sistema debería generar:
 - Trampas de fallos de clúster
 - Trampas de fallos resueltas en clúster
 - Trampas de eventos de clúster
3. En la sección **Destinatarios de la trampa**, ingrese la información del host, el puerto y la cadena de comunidad para un destinatario.
4. **Opcional:** Para agregar otro destinatario de trampa, haga clic en **Agregar un destinatario de trampa** e ingrese la información de host, puerto y cadena de comunidad.
5. Haz clic en **Guardar cambios**.

Visualización de datos de objetos gestionados mediante archivos de la base de información de gestión.

Puede ver y descargar los archivos de la base de información de gestión (MIB) utilizados

para definir cada uno de los objetos gestionados. La función SNMP admite el acceso de solo lectura a los objetos definidos en SolidFire-StorageCluster-MIB.

Los datos estadísticos proporcionados en la MIB muestran la actividad del sistema para lo siguiente:

- Estadísticas de clúster
- Estadísticas de volumen
- Estadísticas de volúmenes por cuenta
- Estadísticas de nodos
- Otros datos como informes, errores y eventos del sistema

El sistema también admite el acceso al archivo MIB que contiene los puntos de acceso de nivel superior (OIDs) a los productos de la serie SF.

Pasos

1. Haga clic en **Clúster > SNMP**.
2. En **SNMP MIBs**, haga clic en el archivo MIB que desea descargar.
3. En la ventana de descarga resultante, abra o guarde el archivo MIB.

Administrar unidades

Cada nodo contiene una o más 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 después de que esta se haya agregado correctamente al clúster. Puedes utilizar la interfaz de usuario de Element para administrar las unidades.

Detalles de las unidades

La página Unidades en la pestaña Clúster proporciona una lista de las unidades activas en el clúster. Puede filtrar la página seleccionando entre las pestañas Activos, Disponibles, Eliminando, Borrando y Fallidos.

Cuando se inicializa un clúster por primera vez, la lista de unidades activas está vacía. Puede agregar unidades que no estén asignadas a un clúster y que aparezcan en la pestaña Disponible después de crear un nuevo clúster SolidFire .

Los siguientes elementos aparecen en la lista de unidades activas.

- **Identificador de unidad**

El número secuencial asignado a la unidad.

- **ID del nodo**

El número de nodo asignado cuando el nodo se agrega al clúster.

- **Nombre del nodo**

El nombre del nodo que aloja la unidad.

- **Ranura**

El número de ranura donde se encuentra físicamente la unidad.

- **Capacidad**

Tamaño de la unidad, en GB.

- **De serie**

El número de serie de la unidad.

- **Desgaste restante**

El indicador del nivel de desgaste.

El sistema de almacenamiento informa la cantidad aproximada de desgaste disponible en cada unidad de estado sólido (SSD) para la escritura y el borrado de datos. Una unidad que ha consumido el 5 por ciento de sus ciclos de escritura y borrado diseñados reporta un desgaste restante del 95 por ciento. El sistema no actualiza automáticamente la información sobre el desgaste de la unidad; puede actualizar la página o cerrarla y volver a cargarla para actualizar la información.

- **Tipo**

El tipo de transmisión. El tipo puede ser bloque o metadatos.

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Gestionar nodos

Gestionar nodos

Puede administrar el almacenamiento SolidFire y los nodos Fibre Channel desde la página Nodos de la pestaña Clúster.

Si un nodo recién agregado representa más del 50 por ciento de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("varada"), de modo que cumpla con la regla de capacidad. Esto seguirá siendo así hasta que se añada más capacidad de almacenamiento. Si se añade un nodo muy grande que también incumple la regla de capacidad, el nodo que antes estaba aislado dejará de estarlo, mientras que el nodo recién añadido quedará aislado. La capacidad siempre debe añadirse por pares para evitar que esto ocurra. Cuando un nodo queda aislado, se genera un fallo de clúster apropiado.

Encuentra más información

[Agregar un nodo a un clúster](#)

Agregar un nodo a un clúster

Puedes agregar nodos a un clúster cuando se necesite más almacenamiento o después de la creación del clúster. Los nodos requieren una configuración inicial cuando se encienden por primera vez. Una vez configurado el nodo, aparece en la lista de nodos pendientes y se puede agregar a un clúster.

La versión del software en cada nodo de un clúster debe ser compatible. Cuando se agrega un nodo a un clúster, este instala la versión del software NetApp Element correspondiente en el nuevo nodo, según sea necesario.

Puedes agregar nodos de menor o mayor capacidad a un clúster existente. Puede agregar capacidades de nodo mayores a un clúster para permitir el crecimiento de la capacidad. Los nodos más grandes que se agreguen a un clúster con nodos más pequeños deben agregarse por pares. Esto proporciona espacio suficiente para que Double Helix pueda mover los datos en caso de que falle uno de los nodos más grandes. Puedes agregar nodos de menor capacidad a un clúster de nodos más grande para mejorar el rendimiento.



Si un nodo recién agregado representa más del 50 por ciento de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("varada"), de modo que cumpla con la regla de capacidad. Esto seguirá siendo así hasta que se añada más capacidad de almacenamiento. Si se añade un nodo muy grande que también incumple la regla de capacidad, el nodo que antes estaba aislado dejará de estarlo, mientras que el nodo recién añadido quedará aislado. La capacidad siempre debe añadirse por pares para evitar que esto ocurra. Cuando un nodo queda aislado, se produce un fallo de clúster strandedCapacity.

["Vídeo de NetApp : Escala a tu manera: Ampliación de un clúster SolidFire"](#)

Puedes agregar nodos a los dispositivos NetApp HCI .

Pasos

1. Seleccione **Clúster > Nodos**.
2. Haz clic en **Pendientes** para ver la lista de nodos pendientes.

Cuando finaliza el proceso de adición de nodos, estos aparecen en la lista de nodos activos. Hasta entonces, los nodos pendientes aparecerán en la lista de Nodos Activos Pendientes.

SolidFire instala la versión del software Element del clúster en los nodos pendientes cuando los agrega a un clúster. Esto podría tardar unos 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 agregar varios nodos, seleccione la casilla de verificación de los nodos que desea agregar y luego **Acciones en lote**. **Nota:** Si el nodo que está agregando tiene una versión del 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 del clúster. Después de que se actualiza el nodo, se agrega automáticamente al clúster. Durante este proceso asíncrono, el nodo estará en estado pendingActive.
4. Haga clic en **Agregar**.

El nodo aparece en la lista de nodos activos.

Encuentra más información

[Control de versiones y compatibilidad de nodos](#)

Control de versiones y compatibilidad de nodos

La compatibilidad de los nodos se basa en la versión del software Element instalada en

un nodo. Los clústeres de almacenamiento basados en software de Element crean automáticamente una imagen de un nodo a la versión del software de Element en el clúster si el nodo y el clúster no tienen versiones compatibles.

La siguiente lista describe los niveles de importancia de las versiones de software que componen el número de versión del software Element:

- **Importante**

El primer número designa una versión del software. No se puede agregar un nodo con un número de componente principal a un clúster que contenga nodos con un número de parche principal diferente, ni se puede crear un clúster con nodos de versiones principales mixtas.

- **Menor**

El segundo número designa características de software menores o mejoras a características de software existentes que se han añadido a una versión principal. Este componente se incrementa dentro de un componente de versión principal para indicar que esta versión incremental no es compatible con ninguna otra versión incremental del software Element que tenga un componente secundario diferente. Por ejemplo, la versión 11.0 no es compatible con la 11.1, y la versión 11.1 no es compatible con la 11.2.

- **Micro**

El tercer número designa un parche compatible (versión incremental) para la versión del software Element representada por los componentes mayor.menor. Por ejemplo, la versión 11.0.1 es compatible con la versión 11.0.2, y la versión 11.0.2 es compatible con la versión 11.0.3.

Para garantizar la compatibilidad, los números de versión principal y secundaria deben coincidir. Los números micro no tienen que coincidir para ser compatibles.

Capacidad del clúster en un entorno de nodos mixtos

Puedes mezclar diferentes tipos de nodos en un clúster. Las series SF 2405, 3010, 4805, 6010, 9605, 9010, 19210, 38410 y la serie H pueden coexistir en un clúster.

La serie H consta de los nodos H610S-1, H610S-2, H610S-4 y H410S. Estos nodos son compatibles tanto con 10GbE como con 25GbE.

Lo mejor es no mezclar nodos no cifrados con nodos cifrados. En un clúster de nodos mixtos, ningún nodo puede ser mayor que el 33 por ciento de la capacidad total del clúster. Por ejemplo, en un clúster con cuatro nodos SF-Series 4805, el nodo más grande que se puede agregar individualmente es un SF-Series 9605. El umbral de capacidad del clúster se calcula en función de la pérdida potencial del nodo más grande en esta situación.

Dependiendo de la versión del software Element, los siguientes nodos de almacenamiento de la serie SF no son compatibles:

A partir de...	Nodo de almacenamiento no compatible...
Elemento 12.8	• SF4805 • SF9605 • SF19210 • SF38410
Elemento 12.7	• SF2405 • SF9608
Elemento 12.0	• SF3010 • SF6010 • SF9010

Si intenta actualizar uno de estos nodos a una versión de Element no compatible, verá un error que indica que el nodo no es compatible con Element 12.x.

Ver detalles del nodo

Puede ver detalles de nodos individuales, como etiquetas de servicio, detalles de la unidad y gráficos de utilización y estadísticas de la unidad. La página Nodos de la pestaña Clúster proporciona la columna Versión, donde puede ver la versión de software de cada nodo.

Pasos

1. Haz clic en **Clúster > Nodos**.
2. Para ver los detalles de un nodo específico, haga clic en el icono **Acciones** del nodo.
3. Haga clic en **Ver detalles**.
4. Revisa los detalles del nodo:
 - **ID de nodo:** El ID generado por el sistema para el nodo.
 - **Nombre del nodo:** El nombre de host del nodo.
 - **Rol del nodo:** El rol que el nodo tiene en el clúster. Valores posibles:
 - **Maestro del clúster:** El nodo que realiza tareas administrativas en todo el clúster y contiene el MVIP y el SVIP.
 - **Nodo de conjunto:** Un nodo que participa en el clúster. Hay 3 o 5 nodos de conjunto dependiendo del tamaño del clúster.
 - **Canal de fibra:** Un nodo en el clúster.
 - **Tipo de nodo:** El tipo de modelo del nodo.
 - **Unidades activas:** El número de unidades activas en el nodo.
 - **Utilización del nodo:** Porcentaje de utilización del nodo basado en nodeHeat. El valor mostrado es recentPrimaryTotalHeat como porcentaje. Disponible a partir del Elemento 12.8.
 - **IP de gestión:** La dirección IP de gestión (MIP) asignada al nodo para tareas de administración de red de 1GbE o 10GbE.

- **IP del clúster:** La dirección IP del clúster (CIP) asignada al nodo y utilizada para la comunicación entre nodos del mismo clúster.
- **IP de almacenamiento:** La dirección IP de almacenamiento (SIP) asignada al nodo utilizada para el descubrimiento de la red iSCSI y todo el tráfico de datos de la red.
- **ID de VLAN de administración:** El ID virtual para la red de área local de administración.
- **ID de VLAN de almacenamiento:** El ID virtual para 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 único asignado al nodo.
- **Dominio de protección personalizado:** El dominio de protección personalizado asignado al nodo.

Ver detalles de los puertos Fibre Channel

En la página de puertos FC puede consultar los detalles de los puertos Fibre Channel, como su estado, nombre y dirección.

Consulte la información sobre los puertos Fibre Channel conectados al clúster.

Pasos

1. Haga clic en **Clúster > Puertos FC**.
2. Para filtrar la información de esta página, haga clic en **Filtrar**.
3. Revisa los detalles:
 - **ID de nodo:** El nodo que aloja la sesión para la conexión.
 - **Nombre del nodo:** Nombre del nodo generado por el sistema.
 - **Ranura:** Número de ranura donde se encuentra el puerto Fibre Channel.
 - **Puerto HBA:** Puerto físico en el adaptador de bus de host de Fibre Channel (HBA).
 - **WWNN:** Nombre del nodo mundial.
 - **WWPN:** Nombre del puerto mundial de destino.
 - **WWN del switch:** Nombre mundial del switch Fibre Channel.
 - **Estado del puerto:** Estado actual del puerto.
 - **nPort ID:** El ID del puerto del nodo en la estructura Fibre Channel.
 - **Velocidad:** La velocidad negociada del canal de fibra. Los valores posibles son los siguientes:
 - 4Gbps
 - 8Gbps
 - 16Gbps

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Gestionar redes virtuales

Gestionar redes virtuales

La virtualización de redes en el almacenamiento SolidFire permite que el tráfico entre múltiples clientes que se encuentran en redes lógicas separadas se conecte a un solo clúster. Las conexiones al clúster se segregan en la pila de red mediante el uso de etiquetado VLAN.

Encuentra más información

- [Agregar una red virtual](#)
- [Habilitar el enrutamiento y reenvío virtual](#)
- [Editar una red virtual](#)
- [Editar VLAN VRF](#)
- [Eliminar una red virtual](#)

Agregar una red virtual

Puede agregar una nueva red virtual a una configuración de clúster para habilitar una conexión de entorno multiinquilino a un clúster que ejecuta el software Element.

Lo que necesitarás

- 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 utilizará como punto final para todo el tráfico de almacenamiento de NetApp Element .



Para esta configuración, debe tener en cuenta los siguientes criterios:

- Las VLAN que no tienen habilitado VRF requieren que los iniciadores estén en la misma subred que la SVIP.
- Las VLAN que tienen habilitado VRF no requieren que los iniciadores estén en la misma subred que la SVIP, y se admite el enrutamiento.
- La SVIP predeterminada no requiere que los iniciadores estén en la misma subred que la SVIP, y admite el enrutamiento.

Cuando se agrega una red virtual, se crea una interfaz para cada nodo y cada una requiere una dirección IP de red virtual. El número de direcciones IP que especifique al crear una nueva red virtual debe ser igual o mayor que el número de nodos del clúster. Las direcciones de red virtuales se aprovisionan de forma masiva y se asignan a nodos individuales automáticamente. No es necesario asignar manualmente direcciones de red virtuales 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 los valores en los siguientes campos:
 - **Nombre de VLAN**

- **Etiqueta VLAN**
- **SVIP**
- **Máscara de red**
- (Opcional) **Descripción**

4. Ingrese la dirección **IP inicial** para el rango de direcciones IP en **Bloques de direcciones IP**.
5. Ingrese el **Tamaño** del rango de IP como el número de direcciones IP que se incluirán en el bloque.
6. Haz clic en **Agregar un bloque** para añadir un bloque no contiguo de direcciones IP para esta VLAN.
7. Haga clic en **Crear VLAN**.

Ver detalles de la red virtual

Pasos

1. Haga clic en **Clúster > Red**.
2. Revise los detalles.
 - **ID**: Identificador único de la red VLAN, asignado por el sistema.
 - **Nombre**: Nombre único 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.
 - **Máscara de red**: Máscara de red para esta red virtual.
 - **Puerta de enlace**: Dirección IP única de una puerta de enlace de red virtual. VRF debe estar habilitado.
 - **VRF habilitado**: Indicación de si el enrutamiento y reenvío virtual está habilitado o no.
 - **Direcciones IP utilizadas**: El rango de direcciones IP de red virtual utilizadas para la red virtual.

Habilitar el enrutamiento y reenvío virtual

Puede habilitar el enrutamiento y reenvío virtual (VRF), lo que permite que existan varias instancias de una tabla de enrutamiento en un enrutador y funcionen simultáneamente. Esta funcionalidad solo está disponible para redes de almacenamiento.

Solo puedes habilitar VRF al momento de crear una VLAN. Si desea volver a un modo no VRF, deberá eliminar y volver a crear la VLAN.

1. Haga clic en **Clúster > Red**.
2. Para habilitar VRF en una nueva VLAN, seleccione **Crear VLAN**.
 - a. Introduzca la información pertinente para la nueva VRF/VLAN. Consulte la sección "Agregar una red virtual".
 - b. Seleccione la casilla de verificación **Habilitar VRF**.
 - c. **Opcional**: Introduzca una puerta de enlace.
3. Haga clic en **Crear VLAN**.

Encuentra más información

[Agregar una red virtual](#)

Editar una red virtual

Puedes cambiar los atributos de la VLAN, como el nombre de la VLAN, la máscara de red y el tamaño de los bloques de direcciones IP. La etiqueta VLAN y la SVIP no se pueden modificar para una VLAN. El atributo de puerta de enlace no es un parámetro válido para VLAN que no sean VRF.

Si existen sesiones iSCSI, de replicación remota u otras sesiones de red, la modificación podría fallar.

Al administrar el tamaño de los rangos de direcciones IP de VLAN, debe tener en cuenta las siguientes limitaciones:

- Solo puedes eliminar direcciones IP del rango de direcciones IP inicial asignado en el momento de la creación de la VLAN.
- Puedes eliminar un bloque de direcciones IP que se agregó después del rango de direcciones IP inicial, pero no puedes cambiar el tamaño de un bloque de IP eliminando direcciones IP.
- Cuando intentas eliminar direcciones IP, ya sea del rango de direcciones IP inicial o de un bloque IP, que están en uso por nodos del clúster, la operación podría fallar.
- No se pueden reasignar direcciones IP específicas en uso a otros nodos del clúster.

Puede agregar un bloque de direcciones IP siguiendo el siguiente procedimiento:

1. Seleccione **Clúster > Red**.
2. Seleccione el icono Acciones para la VLAN que desea 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 contiguo de direcciones IP para la red virtual.
6. Seleccione **Guardar cambios**.

Enlace a artículos de la base de conocimientos para la resolución de problemas

Enlace a los artículos de la Base de conocimientos para obtener ayuda con la resolución de problemas relacionados con la administración de sus rangos de direcciones IP de VLAN.

- ["Advertencia de IP duplicada tras agregar un nodo de almacenamiento en la VLAN del clúster Element"](#)
- ["Cómo determinar qué direcciones IP de VLAN están en uso y a qué nodos están asignadas esas direcciones IP en Element"](#)

Editar VLAN VRF

Puede cambiar los atributos de VLAN de VRF, como el nombre de VLAN, la máscara de red, la puerta de enlace y los bloques de direcciones IP.

1. Haga clic en **Clúster > Red**.
2. Haz clic en el icono Acciones de la VLAN que deseas editar.

3. Haga clic en **Editar**.
4. Introduzca los nuevos atributos para la VLAN VRF en el cuadro de diálogo **Editar VLAN**.
5. Haz clic en **Guardar cambios**.

Eliminar una red virtual

Puedes eliminar un objeto de red virtual. Debes agregar los bloques de direcciones a otra red virtual antes de eliminar una red virtual.

1. Haga clic en **Clúster > Red**.
2. Haz clic en el icono de Acciones de la VLAN que deseas eliminar.
3. Haga clic en **Eliminar**.
4. Confirma el mensaje.

Encuentra más información

[Editar una red virtual](#)

Cree un clúster que admita unidades FIPS.

Preparar el clúster Element para la función de unidades FIPS

La seguridad se está convirtiendo en un aspecto cada vez más crítico para el despliegue de soluciones en muchos entornos de clientes. Las Normas Federales de Procesamiento de Información (FIPS) son normas para la seguridad informática y la interoperabilidad. El cifrado certificado FIPS 140-2 para datos en reposo es un componente de la solución de seguridad general.

Para preparar la activación de la función de unidades FIPS, debe evitar mezclar nodos en los que algunos sean compatibles con unidades FIPS y otros no.

Un clúster se considera compatible con las 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.
- La función de controladores FIPS está habilitada. Todas las unidades y nodos deben ser compatibles con FIPS y el cifrado en reposo debe estar habilitado para poder habilitar la función de unidad FIPS.

Habilitar el cifrado en reposo

Puede habilitar y deshabilitar el cifrado en reposo para todo el clúster. Esta función no está habilitada de forma predeterminada. Para admitir 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 **Habilitar cifrado en reposo**.

Encuentra más información

- [Habilitar y deshabilitar el cifrado para un clúster](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Identificar si los nodos están listos para la función de controladores FIPS

Debe comprobar si todos los nodos del clúster de almacenamiento están preparados para admitir unidades FIPS utilizando el método de la API `GetFipsReport` del software NetApp Element .

El informe resultante muestra uno de los siguientes estados:

- Ninguno: El nodo no es compatible con la función de unidades FIPS.
- Parcial: El nodo es compatible con FIPS, pero no todas las unidades son compatibles con FIPS.
- Listo: El nodo es compatible con FIPS y todas las unidades son unidades FIPS o no hay unidades presentes.

Pasos

1. Utilizando la API de Element, compruebe si los nodos y las unidades del clúster de almacenamiento son compatibles con unidades FIPS introduciendo el siguiente comando:

```
GetFipsReport
```

2. Revise los resultados y observe si algún nodo no mostró el estado "Listo".
3. Para cualquier nodo que no muestre el estado Listo, compruebe si la unidad es compatible con la función de unidades FIPS:
 - Utilizando la API de Element, ingrese: `GetHardwareList`
 - Tenga en cuenta el valor de **DriveEncryptionCapabilityType**. Si es "fips", el hardware puede admitir la función de controladores FIPS.

Ver detalles sobre `GetFipsReport` o `ListDriveHardware` en el ["Referencia de la API de elementos"](#).

4. Si la unidad no admite la función de unidades FIPS, reemplace el hardware con hardware FIPS (ya sea el nodo o las unidades).

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Habilitar la función de controladores FIPS

Puede habilitar la función de 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, como se indica cuando `GetFipsReport` muestra un estado Listo para todos los nodos.

Paso

1. Utilizando la API de Element, habilite FIPS en todas las unidades introduciendo:

```
EnableFeature params: FipsDrives
```

Encuentra más información

- ["Gestiona el almacenamiento con la API de Element"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Compruebe el estado de la unidad FIPS

Puede comprobar si la función de unidades FIPS está habilitada en el clúster mediante el software NetApp Element . `GetFeatureStatus` Método API que muestra si el estado de activación de las unidades FIPS es verdadero o falso.

1. Utilizando la API de Element, compruebe la función de unidades FIPS en el clúster introduciendo:

```
GetFeatureStatus
```

2. Revisar los resultados de `GetFeatureStatus` Llamada a la API. Si el valor de FIPS Drives enabled es True, la función FIPS drives está habilitada.

```
{ "enabled": true,  
  "feature": "FipsDrives"  
}
```

Encuentra más información

- ["Gestiona el almacenamiento con la API de Element"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Solucionar problemas de la función de la unidad FIPS

Mediante la interfaz de usuario del software NetApp Element , puede ver alertas con información sobre fallos del clúster o errores del sistema relacionados con la función de unidades FIPS.

1. Utilizando la interfaz de usuario de Element, seleccione **Informes > Alertas**.
2. Busque fallos en el clúster, incluidos los siguientes:
 - Las unidades FIPS no coinciden
 - FIPS genera incumplimiento
3. Para obtener sugerencias de resolución, consulte la información sobre el código de error del clúster.

Encuentra más información

- [Códigos de falla del clúster](#)
- ["Gestiona el almacenamiento con la API de Element"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Establecer una comunicación segura

Habilite FIPS 140-2 para HTTPS en su clúster.

Puede utilizar el método API EnableFeature para habilitar el modo de funcionamiento FIPS 140-2 para comunicaciones HTTPS.

Con el software NetApp Element , puede optar por habilitar el modo de funcionamiento de los Estándares Federales de Procesamiento de Información (FIPS) 140-2 en su clúster. Habilitar este modo activa el Módulo de Seguridad Criptográfica de NetApp (NCSM) y aprovecha el cifrado certificado FIPS 140-2 Nivel 1 para todas las comunicaciones a través de HTTPS con la interfaz de usuario y la API de NetApp Element .



Una vez habilitado el modo FIPS 140-2, no se puede deshabilitar. Cuando se habilita el modo FIPS 140-2, cada nodo del clúster se reinicia y ejecuta una autocomprobación para garantizar que el NCSM esté correctamente habilitado y funcionando en el modo certificado FIPS 140-2. Esto provoca una interrupción tanto en las conexiones de gestión como en las de almacenamiento del clúster. Debe planificar cuidadosamente y habilitar este modo solo si su entorno necesita el mecanismo de cifrado que ofrece.

Para obtener más información, consulte la información de la API de Element.

El siguiente es un ejemplo de la solicitud a la API para habilitar FIPS:

```
{
  "method": "EnableFeature",
  "params": {
    "feature" : "fips"
  },
  "id": 1
}
```

Una vez habilitado este modo de funcionamiento, todas las comunicaciones HTTPS utilizan los cifrados aprobados por FIPS 140-2.

Encuentra más información

- [cifrados SSL](#)
- ["Gestiona el almacenamiento con la API de Element"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

cifrados SSL

Los cifrados SSL son algoritmos de cifrado utilizados por los hosts para establecer una comunicación segura. Existen cifrados estándar que admite el software Element y cifrados no estándar cuando está habilitado el modo FIPS 140-2.

Las siguientes listas proporcionan los cifrados SSL (Secure Socket Layer) estándar compatibles con el software Element y los cifrados SSL compatibles 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_CON_AES_128_CBC_SHA256 (secp256r1) - A

TLS_ECDHE_RSA_CON_AES_128_GCM_SHA256 (secp256r1) - A

TLS_ECDHE_RSA_CON_AES_256_CBC_SHA384 (secp256r1) - A

TLS_ECDHE_RSA_CON_AES_256_GCM_SHA384 (secp256r1) - A

TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

TLS_RSA_CON_AES_128_CBC_SHA (rsa 2048) - A

TLS_RSA_CON_AES_128_CBC_SHA256 (rsa 2048) - A

TLS_RSA_CON_AES_128_GCM_SHA256 (rsa 2048) - A

TLS_RSA_CON_AES_256_CBC_SHA (rsa 2048) - A

TLS_RSA_CON_AES_256_CBC_SHA256 (rsa 2048) - A

TLS_RSA_CON_AES_256_GCM_SHA384 (rsa 2048) - A

TLS_RSA_CON_CAMELLIA_128_CBC_SHA (rsa 2048) - A

TLS_RSA_CON_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_CON_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_CON_AES_128_CBC_SHA256 (sección 571r1) - A
TLS_ECDHE_RSA_CON_AES_128_CBC_SHA256 (secp256r1) - A
TLS_ECDHE_RSA_CON_AES_128_GCM_SHA256 (secp256r1) - A
TLS_ECDHE_RSA_CON_AES_128_GCM_SHA256 (sect571r1) - A
TLS_ECDHE_RSA_CON_AES_256_CBC_SHA384 (sección 571r1) - A
TLS_ECDHE_RSA_CON_AES_256_CBC_SHA384 (secp256r1) - A
TLS_ECDHE_RSA_CON_AES_256_GCM_SHA384 (secp256r1) - A
TLS_ECDHE_RSA_CON_AES_256_GCM_SHA384 (sección 571r1) - A
TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
TLS_RSA_CON_AES_128_CBC_SHA (rsa 2048) - A
TLS_RSA_CON_AES_128_CBC_SHA256 (rsa 2048) - A
TLS_RSA_CON_AES_128_GCM_SHA256 (rsa 2048) - A
TLS_RSA_CON_AES_256_CBC_SHA (rsa 2048) - A
TLS_RSA_CON_AES_256_CBC_SHA256 (rsa 2048) - A
TLS_RSA_CON_AES_256_GCM_SHA384 (rsa 2048) - A

Encuentra más información

[Habilite FIPS 140-2 para HTTPS en su clúster.](#)

Comience con la administración de claves externas

Comience con la administración de claves externas

La gestión de claves externas (EKM) proporciona una gestión segura de claves de autenticación (AK) junto con un servidor de claves externas fuera del clúster (EKS). Las AK se utilizan para bloquear y desbloquear unidades de autocifrado (SED) cuando "cifrado en reposo" está habilitado en el clúster. El EKS proporciona generación y almacenamiento seguros de los AK. El clúster utiliza el protocolo de interoperabilidad de gestión de claves (KMIP), un protocolo estándar definido por OASIS, para comunicarse con el EKS.

- ["Establecer la gestión externa"](#)

- ["Rekey cifrado de software en reposo clave maestra"](#)
- ["Recuperar claves de autenticación inaccesibles o no válidas"](#)
- ["Comandos de la API de administración de claves externas"](#)

Encuentra más información

- ["API CreateCluster que se puede usar para habilitar el cifrado de software en reposo"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Configurar la gestión de claves externas

Puedes seguir estos pasos y usar los métodos de la API de Element que se enumeran para configurar tu función de administración de claves externas.

Lo que necesitarás

- Si está configurando la administración de claves externas en combinación con el cifrado de software en reposo, habrá habilitado el cifrado de software en reposo mediante el uso de ["CrearClúster"](#) 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 pública/privada para el clúster de Element que se utiliza para establecer una relación de confianza con el servidor de claves llamando al siguiente método de la API: ["Crear par de claves públicas y privadas"](#)
 - b. Obtenga la solicitud de firma de certificado (CSR) que la Autoridad de Certificación necesita firmar. La CSR permite al servidor de claves verificar que el clúster de Element que accederá a las claves esté autenticado como tal. Llama al siguiente método de la API: ["Solicitud de firma de certificado de cliente"](#)
 - c. Utilice la EKS/Autoridad de Certificación 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 EKS. Un proveedor de claves define dónde se debe obtener una clave, y un servidor define los atributos específicos del EKS con el que se comunicará.
 - a. Cree un proveedor de claves donde residirán los detalles del servidor de claves llamando al siguiente método de la API: ["CrearKeyProviderKmpip"](#)
 - b. Cree un servidor de claves que proporcione el certificado firmado y el certificado de clave pública de la Autoridad de Certificación llamando a los siguientes métodos de la API: ["CrearKeyServerKmpip"](#) ["Servidor de claves de prueba Kmpip"](#)

Si la prueba falla, verifique la conectividad y la configuración de su servidor. Luego, repita la prueba.
 - c. Agregue el servidor de claves al contenedor del proveedor de claves llamando a los siguientes métodos de la API: ["Agregar servidor de claves al proveedor Kmpip"](#) ["TestKeyProviderKmpip"](#)

Si la prueba falla, verifique la conectividad y la configuración de su servidor. Luego, repita la prueba.
3. Como siguiente paso para el cifrado en reposo, realice una de las siguientes acciones:
 - a. (Para cifrado de hardware en reposo) Habilitar ["Cifrado de hardware en reposo"](#) proporcionando el ID del proveedor de claves que contiene el servidor de claves utilizado para almacenar las claves

mediante una llamada a ["Habilitar cifrado en reposo"](#) Método API.



Debe habilitar el cifrado en reposo a través de ["API"](#) . Habilitar el cifrado en reposo mediante el botón existente de la interfaz de usuario de Element hará que la función vuelva a utilizar claves generadas internamente.

- b. (Para el cifrado de software en reposo) Para ["Cifrado de software en reposo"](#) Para utilizar el proveedor de claves recién creado, pase el ID del proveedor de claves al ["Clave maestra de cifrado de software en reposo"](#) Método API.

Encuentra más información

- ["Habilitar y deshabilitar el cifrado para un clúster"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Rekey cifrado de software en reposo clave maestra

Puedes usar la API de Element para volver a generar una clave existente. Este proceso crea una nueva clave maestra de reemplazo para su servidor de administración de claves externo. Las claves maestras siempre se reemplazan por nuevas claves maestras y nunca se duplican ni se sobrescriben.

Es posible que necesite volver a introducir las teclas como parte de uno de los siguientes procedimientos:

- Cree una nueva clave como parte de un cambio de gestión de claves interna a gestión de claves externa.
- Cree una nueva clave como reacción a un evento relacionado con la seguridad o como protección contra el mismo.



Este proceso es asíncrono y devuelve una respuesta antes de que se complete la operación de reenvío de claves. Puedes usar el ["ObtenerResultadoAsíncrono"](#) Método para consultar al sistema y comprobar cuándo ha finalizado el proceso.

Lo que necesitarás

- Has habilitado el cifrado de software en reposo mediante ["CrearClúster"](#) método en un nuevo clúster que no contiene volúmenes y no tiene E/S. Utilice el siguiente enlace: `../api/reference_element_api_getsoftwareencryptionatrestinfo.html[GetSoftwareEncryptionatRestInfo]` para confirmar que el estado es `enabled` antes de continuar.
- Tienes ["Se estableció una relación de confianza"](#) entre el clúster SolidFire y un servidor de claves externo (EKS). Ejecutar el ["TestKeyProviderKmp"](#) Método para verificar que se ha establecido una conexión con el proveedor de claves.

Pasos

1. Ejecutar el ["Proveedores de claves de lista Kmp"](#) comando y copia del ID del proveedor de claves(`keyProviderID`).
2. Ejecutar el ["Clave maestra de cifrado de software en reposo"](#) con el `keyManagementType` parámetro como `external` y `keyProviderID` como el número de identificación del proveedor de claves del paso anterior:


```
{
  "method": "rekeysoftwareencryptionatrestmasterkey",
  "params": {
    "keyManagementType": "external",
    "keyProviderID": "<ID number>"
  }
}
```

3. Copia el `asyncHandle` valor de la `RekeySoftwareEncryptionAtRestMasterKey` Respuesta al comando.
4. Ejecutar el ["ObtenerResultadoAsíncrono"](#) comando con el `asyncHandle` Valor del paso anterior para confirmar el cambio de configuración. En la respuesta del comando, debería ver que la configuración de la clave maestra anterior se ha actualizado con la nueva información de la clave. 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. Ejecutar el `GetSoftwareEncryptionatRestInfo` orden para confirmar que los nuevos detalles clave, incluyendo el `keyProviderID`, han sido actualizados.

```
{
  "id": null,
  "result": {
    "masterKeyInfo": {
      "keyCreatedTime": "2021-01-01T22:29:18Z",
      "keyID": "<updated value>",
      "keyManagementType": "external",
      "keyProviderID": <value>
    },
    "rekeyMasterKeyAsyncResultID": <value>
    "status": "enabled",
    "version": 1
  },
}
```

Encuentra más información

- ["Gestiona el almacenamiento con la API de Element"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Recuperar claves de autenticación inaccesibles o no válidas

Ocasionalmente, puede producirse un error que requiere la intervención del usuario. En caso de error, se generará un fallo de clúster (denominado código de fallo de clúster). Aquí se describen los dos casos más probables.

El clúster no puede desbloquear las unidades debido a un fallo de clúster KmpServerFault.

Esto puede ocurrir cuando el clúster se inicia por primera vez y el servidor de claves es inaccesible o la clave requerida no está disponible.

1. Siga los pasos de recuperación indicados en los códigos de error del clúster (si los hay).

Es posible que se establezca un fallo sliceServiceUnhealthy porque las unidades de metadatos se han marcado como fallidas y se han colocado en el estado "Disponible".

Pasos para despejar:

1. Vuelva a agregar las unidades.
2. Después de 3 a 4 minutos, compruebe que el sliceServiceUnhealthy La avería se ha solucionado.

Ver ["códigos de falla del clúster"](#) Para más información.

Comandos de la API de administración de claves externas

Lista de todas las API disponibles para gestionar y configurar EKM.

Se utiliza para establecer una relación de confianza entre el clúster y los servidores externos propiedad del cliente:

- Crear par de claves públicas y privadas
- Solicitud de firma de certificado de cliente

Se utiliza para definir los detalles específicos de los servidores externos propiedad del cliente:

- CrearKeyServerKmp
- ModificarKeyServerKmp
- EliminarKeyServerKmp
- ObtenerKeyServerKmp
- Lista de servidores clave Kmp
- Servidor de claves de prueba Kmp

Se utiliza para crear y mantener proveedores de claves que gestionan servidores de claves externos:

- CrearKeyProviderKmp
- EliminarKeyProviderKmp
- Agregar servidor de claves al proveedor Kmp
- Eliminar servidor de claves del proveedor Kmp
- ObtenerProveedorDeClavesKmp
- Proveedores de claves de lista Kmp
- Clave maestra de cifrado de software en reposo
- TestKeyProviderKmp

Para obtener información sobre los métodos de la API, consulte ["Información de referencia de la API"](#).

Gestionar volúmenes y volúmenes virtuales

Aprenda sobre la gestión de volúmenes y volúmenes virtuales.

Puede administrar los datos en un clúster que ejecuta el software Element desde la pestaña Administración en la interfaz de usuario de Element. Las funciones de gestión de clústeres disponibles incluyen la creación y gestión de volúmenes de datos, grupos de acceso a volúmenes, iniciadores y políticas de calidad de servicio (QoS).

Trabajar con volúmenes

El sistema SolidFire aprovisiona almacenamiento mediante volúmenes. Los volúmenes son dispositivos de bloque a los que acceden a través de la red los clientes iSCSI o Fibre Channel. Desde la página Volúmenes en la pestaña Administración, puede crear, modificar, clonar y eliminar volúmenes en un nodo. También puede consultar estadísticas sobre el ancho de banda del volumen y el uso de E/S.

["Aprenda a trabajar con volúmenes"](#)

Trabajar con volúmenes virtuales

Puede ver información y realizar tareas para volúmenes virtuales y sus contenedores de almacenamiento asociados, puntos finales de protocolo, enlaces y hosts utilizando la interfaz de usuario de Element.

El sistema de almacenamiento de software NetApp Element se suministra con la función de volúmenes virtuales (VVols) desactivada. Debe realizar una tarea única de habilitar manualmente la funcionalidad de vSphere VVol a través de la interfaz de usuario de Element.

Después de habilitar la funcionalidad VVol, aparece una pestaña VVols en la interfaz de usuario que ofrece opciones de monitoreo y administración limitadas relacionadas con VVols. Además, un componente de software del lado del almacenamiento conocido como Proveedor VASA actúa como un servicio de reconocimiento de almacenamiento para vSphere. La mayoría de los comandos de VVols, como la creación, clonación y edición de VVols, son iniciados por un servidor vCenter o un host ESXi y traducidos por el proveedor VASA a las API de Element para el sistema de almacenamiento de software Element. Los comandos para crear, eliminar y administrar contenedores de almacenamiento y eliminar volúmenes virtuales se pueden iniciar mediante la interfaz de usuario de Element.

La mayoría de las configuraciones necesarias para utilizar la funcionalidad de Volúmenes Virtuales con los sistemas de almacenamiento de software Element se realizan en vSphere. Consulte la [Guía de configuración de volúmenes virtuales de VMware vSphere para almacenamiento SolidFire](#) para registrar el proveedor VASA en vCenter, crear y administrar almacenes de datos VVol y administrar el almacenamiento según las políticas.



Para Element 12.5 y versiones anteriores, no registre más de un proveedor NetApp Element VASA en una sola instancia de vCenter. Cuando se agrega un segundo proveedor NetApp Element VASA, todos los almacenes de datos VVOL quedan inaccesibles.



La compatibilidad con VASA para múltiples vCenters está disponible como un parche de actualización si ya ha registrado un proveedor de VASA con su vCenter. Para instalar, descargue el archivo VASA39 .tar.gz desde el ["Descargas de software de NetApp"](#). Visite el sitio y siga las instrucciones del manifiesto. El proveedor NetApp Element VASA utiliza un certificado NetApp. Con este parche, vCenter utiliza el certificado sin modificaciones para admitir múltiples vCenters para el uso de VASA y VVols. No modifique el certificado. VASA no admite certificados SSL personalizados.

["Aprenda a trabajar con volúmenes virtuales"](#)

Trabajar con grupos de acceso por volumen e iniciadores

Puede utilizar iniciadores iSCSI o iniciadores Fibre Channel para acceder a los volúmenes definidos dentro de los grupos de acceso a volúmenes.

Puede crear grupos de acceso asignando IQN de iniciador iSCSI o WWPN de Fibre Channel en una colección de volúmenes. Cada IQN que agregue a un grupo de acceso puede acceder a cada volumen del grupo sin necesidad de autenticación CHAP.

Existen dos tipos de métodos de autenticación CHAP:

- Autenticación CHAP a nivel de cuenta: Puede asignar la autenticación CHAP a la cuenta.
- Autenticación CHAP a nivel de iniciador: Puede asignar un destino CHAP y secretos únicos para iniciadores específicos sin estar limitado a un único CHAP en una sola cuenta. Esta autenticación CHAP a nivel de iniciador reemplaza las credenciales a nivel de cuenta.

Opcionalmente, con CHAP por iniciador, puede exigir la autorización del iniciador y la autenticación CHAP por

iniciador. Estas opciones pueden definirse para cada iniciador y un grupo de acceso puede contener una combinación de iniciadores con diferentes opciones.

Cada WWPN que agregue a un grupo de acceso habilita el acceso a la red Fibre Channel a los volúmenes del grupo de acceso.



Los grupos de acceso por volumen tienen los siguientes límites:

- Se permite un máximo de 64 IQN o WWPN en un grupo de acceso.
- Un grupo de acceso puede estar compuesto por un máximo de 2000 volúmenes.
- Un IQN o WWPN solo puede pertenecer a un grupo de acceso.
- Un único volumen puede pertenecer a un máximo de cuatro grupos de acceso.

["Aprenda a trabajar con grupos de acceso por volumen e iniciadores."](#)

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Trabajar con volúmenes

Políticas de gestión de la calidad del servicio

Una política de Calidad de Servicio (QoS) le permite crear y guardar una configuración de calidad de servicio estandarizada que se puede aplicar a muchos volúmenes. Puede crear, editar y eliminar políticas de QoS desde la página Políticas de QoS en la pestaña Administración.



Si está utilizando políticas de QoS, no utilice QoS personalizada en un volumen. La QoS personalizada anulará y ajustará los valores de la política de QoS para la configuración de QoS de volumen.

["Vídeo de NetApp : Políticas de calidad de servicio de SolidFire"](#)

Ver ["Rendimiento y calidad del servicio"](#) .

- Crea una política de QoS
- Editar una política de QoS
- Eliminar una política de QoS

Crea una política de QoS

Puede crear políticas de QoS y aplicarlas al crear volúmenes.

1. Seleccione **Administración > Políticas de QoS**.
2. Haga clic en **Crear política QoS**.
3. Ingrese el **Nombre de la póliza**.

4. Ingrese los valores de **IOPS mínimos**, **IOPS máximos** e **IOPS de ráfaga**.
5. Haga clic en **Crear política QoS**.

Editar una política de QoS

Puede cambiar el nombre de una política QoS existente o editar los valores asociados a la política. Modificar una política de QoS afecta a todos los volúmenes asociados a dicha política.

1. Seleccione **Administración > Políticas de QoS**.
2. Haz clic en el icono Acciones de la política QoS que quieras editar.
3. En el menú resultante, seleccione **Editar**.
4. En el cuadro de diálogo **Editar política de QoS**, modifique las siguientes propiedades según sea necesario:
 - Nombre de la póliza
 - IOPS mínimas
 - IOPS máximas
 - Burst IOPS
5. Haz clic en **Guardar cambios**.

Eliminar una política de QoS

Puede eliminar una política QoS si ya no es necesaria. Cuando se elimina una política de QoS, todos los volúmenes asociados a la política mantienen la configuración de QoS pero dejan de estar asociados a la política.



Si en cambio intenta desvincular un volumen de una política QoS, puede cambiar la configuración QoS de ese volumen a personalizada.

1. Seleccione **Administración > Políticas de QoS**.
2. Haz clic en el icono Acciones de la política QoS que deseas eliminar.
3. En el menú que aparece, seleccione **Eliminar**.
4. Confirma la acción.

Encuentra más información

- ["Eliminar la asociación de política QoS de un volumen"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Administrar volúmenes

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

Desde la página Volúmenes en la pestaña Administración, puede crear, modificar, clonar y eliminar volúmenes en un nodo.

Crear un volumen

Puede crear un volumen y asociar ese volumen a una cuenta determinada. Cada volumen debe estar asociado a una cuenta. Esta asociación otorga a la cuenta acceso al volumen a través de los iniciadores iSCSI utilizando las credenciales CHAP.

Puede especificar la configuración de QoS para un volumen durante su creación.

1. Seleccione **Administración > Volúmenes**.
2. Haz clic en **Crear volumen**.
3. En el cuadro de diálogo **Crear un nuevo volumen**, introduzca el **Nombre del volumen**.
4. Introduzca el tamaño total del volumen.



La selección de tamaño de volumen predeterminada está en GB. Puede crear volúmenes utilizando tamaños medidos en GB o GiB:

- 1 GB = 1 000 000 000 bytes
- 1 GiB = 1 073 741 824 bytes

5. Seleccione un **Tamaño de bloque** para el volumen.
6. Haz clic en la lista desplegable **Cuenta** y selecciona la cuenta que debería tener acceso al volumen.

Si no existe una cuenta, haga clic en el enlace **Crear cuenta**, ingrese un nuevo nombre de cuenta y haga clic en **Crear**. La cuenta se crea y se asocia con el nuevo volumen.



Si hay más de 50 cuentas, la lista no aparece. Empieza a escribir y la función de autocompletar te mostrará los valores posibles para que elijas.

7. Para configurar la **Calidad del Servicio**, realice una de las siguientes acciones:
 - a. En **Política**, puede seleccionar una política QoS existente, si está disponible.
 - b. En **Configuración personalizada**, establezca valores mínimos, máximos y de ráfaga personalizados para IOPS o utilice los valores QoS predeterminados.

Los volúmenes que tienen un valor de IOPS máximo o de ráfaga superior a 20 000 IOPS podrían requerir una gran profundidad de cola o varias sesiones para alcanzar este nivel de IOPS en un solo volumen.

8. Haz clic en **Crear volumen**.

Ver detalles del volumen

1. Seleccione **Administración > Volúmenes**.
2. Revise los detalles.
 - **ID**: El ID generado por el sistema para el volumen.
 - **Nombre**: El nombre que se le dio al volumen cuando fue creado.
 - **Cuenta**: El nombre de la cuenta asignada al volumen.
 - **Grupos de acceso**: El nombre del grupo o grupos de acceso al volumen al que pertenece el volumen.
 - **Acceso**: El tipo de acceso asignado al volumen cuando se creó. Valores posibles:

- **Lectura/Escritura:** Se aceptan todas las lecturas y escrituras.
- **Solo lectura:** Se permite toda la actividad de lectura; no se permiten escrituras.
- **Bloqueado:** Solo se permite el acceso de administrador.
- **ReplicationTarget:** Designado como volumen de destino en un par de volúmenes replicados.
- **Usado:** El porcentaje de espacio utilizado en el volumen.
- **Tamaño:** El tamaño total (en GB) del volumen.
- **ID del nodo primario:** El nodo primario para este volumen.
- **ID de nodo secundario:** La lista de nodos secundarios para este volumen. Puede tener múltiples valores durante estados transitorios, como el cambio de nodos secundarios, pero normalmente tendrá un solo valor.
- **Limitación de QoS:** Identifica si el volumen está siendo limitado debido a una alta carga en el nodo de almacenamiento primario.
- **Política de QoS:** El nombre y el enlace a la política de QoS definida por el usuario.
- **IOPS mínimas:** El número mínimo de IOPS garantizado para el volumen.
- **IOPS máx.:** El número máximo de IOPS permitido para el volumen.
- **IOPS de ráfaga:** El número máximo de IOPS permitidos durante un corto período de tiempo para el volumen. Valor predeterminado = 15.000.
- **Instantáneas:** Número de instantáneas creadas para el volumen.
- **Atributos:** Atributos que se han asignado al volumen como un par clave/valor a través de un método de API.
- **512e:** Indicación de si 512e está habilitado en un volumen. Valores posibles:
 - Sí
 - No
- **Fecha de creación:** La fecha y hora en que se creó el volumen.

Ver detalles de cada volumen

Puedes consultar las estadísticas de rendimiento de volúmenes individuales.

1. Seleccione **Informes > Rendimiento del volumen**.
2. En la lista de volúmenes, haga clic en el icono Acciones de un volumen.
3. Haga clic en **Ver detalles**.

En la parte inferior de la página aparece una bandeja 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, así como gráficos de rendimiento del volumen.

Editar volúmenes activos

Puede modificar atributos de volumen como los valores QoS, el tamaño del volumen y la unidad de medida en la que se calculan los valores de bytes. También puede modificar el acceso a la cuenta para el uso de replicación o para restringir el acceso al volumen.

Puede cambiar el tamaño de un volumen cuando haya suficiente espacio en el clúster bajo las siguientes condiciones:

- Condiciones normales de funcionamiento.
- Se están reportando errores o fallos de volumen.
- Se está clonando el volumen.
- El volumen se está resincronizando.

Pasos

1. Seleccione **Administración > Volúmenes**.
2. En la ventana **Activa**, haga clic en el icono Acciones del volumen que desea editar.
3. Haga clic en **Editar**.
4. **Opcional:** Cambie el tamaño total del volumen.
 - Puedes aumentar, pero no disminuir, el tamaño del volumen. Solo se puede cambiar el tamaño de un volumen en una sola operación de cambio de tamaño. Las operaciones de recolección de basura y las actualizaciones de software no interrumpen la operación de cambio de tamaño.
 - Si está ajustando el tamaño del volumen para la replicación, primero debe aumentar el tamaño del volumen asignado como destino de la replicación. Luego puedes cambiar el tamaño del volumen de origen. El volumen objetivo puede ser mayor o igual en tamaño que el volumen de origen, pero no puede ser menor.

La selección de tamaño de volumen predeterminada está en GB. Puede crear volúmenes utilizando tamaños medidos 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 a la cuenta diferente de entre los siguientes:
 - Solo lectura
 - Leer/Escribir
 - 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**, ingrese un nuevo nombre de cuenta y haga clic en **Crear**. La cuenta se crea y se asocia al volumen.



Si hay más de 50 cuentas, la lista no aparece. Empieza a escribir y la función de autocompletar te mostrará los valores posibles para que elijas.

7. **Opcional:** Para cambiar la selección en **Calidad del servicio**, realice una de las siguientes acciones:
 - a. En **Política**, puede seleccionar una política QoS existente, si está disponible.
 - b. En **Configuración personalizada**, establezca valores mínimos, máximos y de ráfaga personalizados para IOPS o utilice los valores QoS predeterminados.



Si está utilizando políticas de QoS en un volumen, puede configurar una QoS personalizada para eliminar la asociación de la política de QoS con el volumen. La QoS personalizada anulará y ajustará los valores de la política de QoS para la configuración de QoS de volumen.



Cuando cambie los valores de IOPS, debe incrementarlos en decenas o centenas. Los valores de entrada deben ser números enteros válidos.



Configure volúmenes con un valor de ráfaga extremadamente alto. Esto permite que el sistema procese cargas de trabajo secuenciales de bloques grandes ocasionales más rápidamente, al tiempo que limita las IOPS sostenidas para un volumen.

8. Haz clic en **Guardar cambios**.

Eliminar un volumen

Puede eliminar uno o más volúmenes de un clúster de almacenamiento Element.

El sistema no elimina inmediatamente un volumen borrado; el volumen permanece disponible durante aproximadamente ocho horas. Si restaura un volumen antes de que el sistema lo elimine, el volumen vuelve a estar en línea y se restablecen las conexiones iSCSI.

Si se elimina un volumen utilizado para crear una instantánea, sus instantáneas asociadas quedan inactivas. Cuando se eliminan los volúmenes de origen borrados, las instantáneas inactivas asociadas también se eliminan del sistema.



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

Pasos

1. Seleccione **Administración > Volúmenes**.
2. Para eliminar un solo volumen, siga los siguientes pasos:
 - a. Haz clic en el icono Acciones del volumen que deseas eliminar.
 - b. En el menú que aparece, haga clic en **Eliminar**.
 - c. Confirma la acción.

El sistema mueve el volumen al área **Eliminados** en la página **Volúmenes**.

3. Para eliminar varios volúmenes, siga los siguientes pasos:
 - a. En la lista de volúmenes, marque la casilla junto a los volúmenes que desee eliminar.
 - b. Haz clic en **Acciones en lote**.
 - c. En el menú que aparece, haga clic en **Eliminar**.
 - d. Confirma la acción.

El sistema mueve los volúmenes al área **Eliminados** en la página **Volúmenes**.

Restaurar un volumen eliminado

Puedes restaurar un volumen en el sistema si ha sido eliminado pero aún no se ha purgado. El sistema elimina automáticamente un volumen aproximadamente ocho horas después de haber sido borrado. Si el sistema ha borrado el volumen, no podrá recuperarlo.

1. Seleccione **Administración > Volúmenes**.
2. Haz clic en la pestaña **Eliminados** para ver la lista de volúmenes eliminados.
3. Haz clic en el icono Acciones del volumen que deseas restaurar.
4. En el menú que aparece, haga clic en **Restaurar**.
5. Confirma la acción.

El volumen se coloca en la lista de volúmenes **activos** y se restablecen las conexiones iSCSI al volumen.

Purgar un volumen

Cuando se purga un volumen, se elimina permanentemente del sistema. Se pierden todos los datos del volumen.

El sistema elimina automáticamente los volúmenes borrados ocho horas después de su eliminación. Sin embargo, si desea purgar un volumen antes de la hora programada, puede hacerlo.

1. Seleccione **Administración > Volúmenes**.
2. Haz clic en el botón **Eliminado**.
3. Realice los pasos para purgar un solo volumen o varios volúmenes.

Opción	Pasos
Purgar un solo volumen	a. Haz clic en el icono Acciones del volumen que deseas purgar. b. Haga clic en Purgar. c. Confirma la acción.
Purgar varios volúmenes	a. Seleccione los volúmenes que desea purgar. b. Haz clic en Acciones en lote. c. En el menú que aparece, seleccione Purgar. d. Confirma la acción.

Clonar un volumen

Puede crear un clon de un solo volumen o de varios volúmenes para realizar una copia de los datos en un momento dado. Cuando se clona un volumen, el sistema crea una instantánea del volumen y luego crea una copia de los datos a los que hace referencia la instantánea. Este es un proceso asíncrono, y el tiempo que requiere depende del tamaño del volumen que se está clonando y de la carga actual del clúster.

El clúster admite hasta dos solicitudes de clonación en ejecución por volumen a la vez y hasta ocho operaciones de clonación de volumen activas a la vez. Las solicitudes que superen estos límites se pondrán en cola para su posterior procesamiento.



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 de instantánea. El volumen será un dispositivo disponible que se podrá utilizar para crear un nuevo almacén de datos. Para obtener más información sobre el montaje de volúmenes clonados y la gestión de LUN de instantáneas, consulte la documentación de VMware sobre "[Montando una copia del almacén de datos VMFS](#)" y "[gestión de almacenes de datos VMFS duplicados](#)".



Antes de truncar un volumen clonado clonándolo a un tamaño menor, asegúrese de preparar las particiones para que quepan en el volumen más pequeño.

Pasos

1. Seleccione **Administración > Volúmenes**.
2. Para clonar un solo volumen, siga los siguientes pasos:
 - a. En la lista de volúmenes de la página **Activos**, haga clic en el icono Acciones del volumen que desea clonar.
 - b. En el menú que aparece, haga clic en **Clonar**.
 - c. En la ventana **Clonar volumen**, introduzca un nombre para el volumen recién clonado.
 - d. Seleccione un tamaño y una medida para el volumen utilizando el cuadro de selección y la lista **Tamaño del volumen**.



La selección de tamaño de volumen predeterminada está en GB. Puede crear volúmenes utilizando tamaños medidos 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 recién clonado.
 - f. Seleccione una cuenta para asociarla con el volumen recién clonado de la lista **Cuenta**.



Puedes crear una cuenta durante este paso si haces clic en el enlace **Crear cuenta**, introduces un nombre de cuenta y haces clic en **Crear**. El sistema añade automáticamente la cuenta a la lista **Cuentas** después de crearla.

3. Para clonar varios volúmenes, siga los siguientes pasos:
 - a. En la lista de volúmenes de la página **Activos**, marque la casilla junto a los volúmenes que desee clonar.
 - b. Haz clic en **Acciones en lote**.
 - c. En el menú resultante, 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 asociar con los volúmenes clonados de la lista **Cuenta**.
 - f. Seleccione el tipo de acceso para los volúmenes clonados.
4. Haz clic en **Iniciar clonación**.



Al aumentar el tamaño del volumen de un clon, se obtiene un nuevo volumen con espacio libre adicional al final del volumen. Dependiendo del uso que le des al volumen, es posible que necesites extender particiones o crear nuevas particiones en el espacio libre para poder utilizarlo.

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Asignar LUN a volúmenes Fibre Channel

Puede cambiar la asignación de LUN para un volumen Fibre Channel en un grupo de acceso a volúmenes. También puede realizar asignaciones de LUN de volumen Fibre Channel al crear un grupo de acceso a volúmenes.

La asignación de nuevas LUN de Fibre Channel es una función avanzada y podría tener consecuencias desconocidas en el host conectado. Por ejemplo, es posible que el nuevo ID de LUN no se detecte automáticamente en el host, y que el host requiera un nuevo escaneo para detectar el nuevo ID de LUN.

1. Seleccione **Administración > Grupos de acceso**.
2. Haz clic en el icono Acciones del grupo de acceso que deseas editar.
3. En el menú resultante, seleccione **Editar**.
4. En el cuadro de diálogo **Editar grupo de acceso a volumen**, bajo **Asignar ID de LUN**, haga clic en la flecha de la lista **Asignaciones de LUN**.
5. Para cada volumen de la lista al que desee asignar un LUN, introduzca un nuevo valor en el campo **LUN** correspondiente.
6. Haz clic en **Guardar cambios**.

Aplicar una política de QoS a los volúmenes

Puede aplicar de forma masiva una política QoS existente a uno o más volúmenes.

La política de QoS que desea aplicar de forma masiva debe existir.

1. Seleccione **Administración > Volúmenes**.
2. En la lista de volúmenes, marque la casilla junto a los volúmenes a los que desee aplicar la política de QoS.
3. Haz clic en **Acciones en lote**.
4. En el menú que aparece, haga clic en **Aplicar política de QoS**.
5. Seleccione la política de QoS de la lista desplegable.
6. Haga clic en **Aplicar**.

Encuentra más información

[Políticas de calidad del servicio](#)

Eliminar la asociación de política QoS de un volumen

Puede eliminar una asociación de política QoS de un volumen seleccionando una configuración QoS personalizada.

El volumen que desea modificar debe estar asociado a una política de QoS.

1. Seleccione **Administración > Volúmenes**.
2. Haga clic en el icono Acciones del volumen que contiene la política QoS 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 **IOPS mínimas**, **IOPS máximas** e **IOPS de ráfaga**, o mantenga la configuración predeterminada.
6. Haz clic en **Guardar cambios**.

Encuentra más información

[Eliminar una política de QoS](#)

Trabajar con volúmenes virtuales

Habilitar volúmenes virtuales

Debe habilitar manualmente la funcionalidad de vSphere Virtual Volumes (VVols) a través del software NetApp Element . El sistema de software Element viene con la funcionalidad VVols desactivada por defecto, y no se activa automáticamente como parte de una nueva instalación o actualización. Habilitar la función VVols es una tarea de configuración que se realiza una sola vez.

Lo que necesitarás

- El clúster debe estar ejecutando Element 9.0 o posterior.
- El clúster debe estar conectado a un entorno ESXi 6.0 o posterior que sea compatible con VVols.
- Si está utilizando Element 11.3 o posterior, el clúster debe estar conectado a un entorno ESXi 6.0 actualización 3 o posterior.



Habilitar la funcionalidad de volúmenes virtuales de vSphere modifica permanentemente la configuración del software Element. Solo debe habilitar la funcionalidad VVols si su clúster está conectado a un entorno compatible con VMware ESXi VVols. Solo se puede desactivar la función VVols y restaurar la configuración predeterminada devolviendo el clúster a la imagen de fábrica, lo que elimina todos los datos del sistema.

Pasos

1. Seleccione **Clústeres > Configuración**.
2. Encuentre la configuración específica del clúster para volúmenes virtuales.
3. Haga clic en **Habilitar volúmenes virtuales**.
4. Haga clic en **Sí** para confirmar el cambio de configuración de volúmenes virtuales.

La pestaña **VVols** aparece en la interfaz de usuario de Element.



Cuando se habilita la funcionalidad VVols, el clúster SolidFire inicia el proveedor VASA, abre el puerto 8444 para el tráfico VASA y crea puntos de conexión de protocolo que pueden ser detectados por vCenter y todos los hosts ESXi.

5. Copie la URL del proveedor VASA de la configuración de Volúmenes Virtuales (VVols) en **Clústeres > Configuración**. Utilizará esta URL 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 las máquinas virtuales puedan aprovisionarse en un almacén de datos VVol.

7. Seleccione **VVols > Puntos finales del protocolo**.

8. Verifique que se haya creado un punto final de protocolo para cada nodo del clúster.



En vSphere se requieren tareas de configuración adicionales. Consulte la [_Guía de configuración de volúmenes virtuales de VMware vSphere para almacenamiento SolidFire](#) para registrar el proveedor VASA en vCenter, crear y administrar almacenes de datos VVol y administrar el almacenamiento según las políticas.

Encuentra más información

["Guía de configuración de VMware vSphere Virtual Volumes para SolidFire Storage"](#)

Ver detalles del volumen virtual

En la interfaz de usuario de Element puede consultar la información de volumen virtual para todos los volúmenes virtuales activos en el clúster. También puede ver la actividad de rendimiento de cada volumen virtual, incluyendo entrada, salida, rendimiento, latencia, profundidad de cola e información del volumen.

Lo que necesitarás

- Deberías haber habilitado la funcionalidad VVols en la interfaz de usuario de Element para el clúster.
- Deberías haber creado un contenedor de almacenamiento asociado.
- Deberías haber configurado tu clúster vSphere para usar la funcionalidad VVols del software Element.
- Deberías haber creado al menos una máquina virtual en vSphere.

Pasos

1. Haga clic en **VVols > Volúmenes virtuales**.

Se muestra la información de todos los volúmenes virtuales activos.

2. Haga clic en el icono **Acciones** del volumen virtual que desea revisar.

3. En el menú que aparece, seleccione **Ver detalles**.

Detalles

La página Volúmenes virtuales de la pestaña VVols proporciona información sobre cada volumen virtual activo en el clúster, como el ID del volumen, el ID de la instantánea, el ID del volumen virtual principal y el ID del 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 instantánea de SolidFire .
- **ID de volumen virtual principal:** El ID de volumen virtual del volumen virtual principal. Si el ID está compuesto únicamente por ceros, el volumen virtual es independiente y no tiene vínculo con un elemento principal.
- **ID de volumen virtual:** El UUID del volumen virtual.
- **Nombre:** El 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:** El tipo de volumen virtual: Configuración, Datos, Memoria, Intercambio u Otro.
- **Acceso:** 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. Haz clic en el número para acceder a los detalles de la captura de pantalla.
- **IOPS mínimas:** La configuración QoS de IOPS mínima del volumen virtual.
- **IOPS máx.:** La configuración QoS de IOPS máxima del volumen virtual.
- **IOPS de ráfaga:** La configuración QoS de ráfaga máxima del volumen virtual.
- **VMW_VmID:** La información en los campos precedidos por "VMW_" está definida por VMware.
- **Hora de creación:** Hora en que se completó la tarea de creación del volumen virtual.

Detalles de volumen virtual individual

La página Volúmenes virtuales en la pestaña VVols proporciona la siguiente información sobre el volumen virtual cuando selecciona un volumen virtual individual y ve sus detalles.

- **VMW_XXX:** La información en los campos precedidos por "VMW_" está definida por VMware.
- **ID de volumen virtual principal:** El ID de volumen virtual del volumen virtual principal. Si el ID está compuesto únicamente por ceros, el volumen virtual es independiente y no tiene vínculo con un elemento principal.
- **ID de volumen virtual:** El UUID del volumen virtual.
- **Tipo de volumen virtual:** El tipo de volumen virtual: Configuración, Datos, Memoria, Intercambio u Otro.
- **ID de volumen:** El ID del volumen subyacente.
- **Acceso:** Los permisos de lectura y escritura asignados al volumen virtual.
- **Nombre de la cuenta:** Nombre de la cuenta que contiene el volumen.
- **Grupos de acceso:** Grupos de acceso a volúmenes asociados.
- **Tamaño total del volumen:** Capacidad total aprovisionada en bytes.
- **Bloques distintos de cero:** Número total de bloques de 4 KiB con datos después de que se haya

completado la última operación de recolección de basura.

- **Bloques Cero:** Número total de bloques de 4 KiB sin datos después de que se haya completado la última ronda de operación de recolección de basura.
- **Instantáneas:** El número de instantáneas asociadas. Haz clic en el número para acceder a los detalles de la captura de pantalla.
- **IOPS mínimas:** La configuración QoS de IOPS mínima del volumen virtual.
- **IOPS máx.:** La configuración QoS de IOPS máxima del volumen virtual.
- **IOPS de ráfaga:** La configuración QoS de ráfaga máxima del volumen virtual.
- **Habilitar 512:** Debido a que los volúmenes virtuales siempre usan la emulación de tamaño de bloque de 512 bytes, el valor siempre es sí.
- **Volúmenes emparejados:** Indica si un volumen está emparejado.
- **Hora de creación:** Hora en que se completó la tarea de creación del 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 límite de sector de 4k. Un número elevado de escrituras no alineadas podría indicar una alineación de particiones incorrecta.
- **Lecturas no alineadas:** Para volúmenes 512e, el número de operaciones de lectura que no estaban en un límite de sector de 4k. Un elevado número de lecturas no alineadas podría indicar una alineación de particiones incorrecta.
- **scsiEUIDeviceID:** Identificador de dispositivo SCSI único global para el volumen en formato de 16 bytes basado en EUI-64.
- **scsiNAADeviceID:** Identificador de dispositivo SCSI único a nivel mundial para el volumen en formato NAA IEEE Registered Extended.
- **Atributos:** Lista de pares nombre-valor en formato de objeto JSON.

Eliminar un volumen virtual

Aunque los volúmenes virtuales siempre deben eliminarse desde la capa de administración de VMware, la funcionalidad para eliminar volúmenes virtuales está habilitada desde la interfaz de usuario de Element. Solo debes eliminar un volumen virtual desde la interfaz de usuario de Element cuando sea absolutamente necesario, por ejemplo, cuando vSphere no pueda limpiar los volúmenes virtuales en el almacenamiento SolidFire .

1. Seleccione **VVols > Volúmenes virtuales**.
2. Haz clic en el icono Acciones del volumen virtual que deseas eliminar.
3. En el menú que aparece, seleccione **Eliminar**.



Debe eliminar un volumen virtual de la capa de administración de VMware para asegurarse de que el volumen virtual se desvincule correctamente antes de su eliminación. Solo debes eliminar un volumen virtual desde la interfaz de usuario de Element cuando sea absolutamente necesario, por ejemplo, cuando vSphere no pueda limpiar los volúmenes virtuales en el almacenamiento SolidFire . Si elimina un volumen virtual desde la interfaz de usuario de Element, el volumen se eliminará inmediatamente.

4. Confirma la acción.
5. Actualice la lista de volúmenes virtuales para confirmar que el volumen virtual se ha eliminado.
6. **Opcional:** Seleccione **Informes > Registro de eventos** para confirmar que la purga se ha realizado correctamente.

Gestionar contenedores de almacenamiento

Un contenedor de almacenamiento es una representación de un almacén de datos de vSphere creado en un clúster que ejecuta el software Element.

Los contenedores de almacenamiento se crean y se vinculan a las cuentas de NetApp Element . Un contenedor de almacenamiento creado en Element Storage aparece como un almacén de datos de vSphere en vCenter y ESXi. Los contenedores de almacenamiento no asignan ningún espacio en el almacenamiento de Element. Simplemente se utilizan para asociar lógicamente volúmenes virtuales.

Se admite un máximo de cuatro contenedores de almacenamiento por clúster. Se requiere un mínimo de un contenedor de almacenamiento para habilitar la funcionalidad VVols.

Crea un contenedor de almacenamiento

Puede crear contenedores de almacenamiento en la interfaz de usuario de Element y descubrirlos en vCenter. Debe crear al menos un contenedor de almacenamiento para comenzar a aprovisionar máquinas virtuales respaldadas por VVol.

Antes de comenzar, habilite la funcionalidad VVols en la interfaz de usuario de Element para el clúster.

Pasos

1. Seleccione **VVols > Contenedores de almacenamiento**.
2. Haz clic en el botón **Crear contenedores de almacenamiento**.
3. Introduzca la información del contenedor de almacenamiento en el cuadro de diálogo **Crear un nuevo contenedor de almacenamiento**:
 - a. Introduzca un nombre para el contenedor de almacenamiento.
 - b. Configure los secretos de iniciador y destino para CHAP.
- c. Haz clic en el botón **Crear contenedor de almacenamiento**.
4. Verifique que el nuevo contenedor de almacenamiento aparezca en la lista de la subpestaña **Contenedores de almacenamiento**.



Deje en blanco los campos de Configuración CHAP para generar secretos automáticamente.



Dado que se crea automáticamente un ID de cuenta de NetApp Element y se asigna al contenedor de almacenamiento, no es necesario crear una cuenta manualmente.

Ver detalles del contenedor de almacenamiento

En la página Contenedores de almacenamiento de la pestaña VVols, puede ver información sobre todos los contenedores de almacenamiento activos en el clúster.

- **ID de cuenta:** El ID de la cuenta de NetApp Element asociada con el contenedor de almacenamiento.
- **Nombre:** El nombre del contenedor de almacenamiento.
- **Estado:** El estado del contenedor de almacenamiento. Valores posibles:
 - Activo: El contenedor de almacenamiento está en uso.
 - Bloqueado: El contenedor de almacenamiento está bloqueado.
- **Tipo de PE:** El tipo de punto final del 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.
- **Volúmenes virtuales activos:** El número de volúmenes virtuales activos asociados al contenedor de almacenamiento.

Ver detalles de cada contenedor de almacenamiento

Puede ver la información del contenedor de almacenamiento para un contenedor de almacenamiento individual seleccionándolo en la página Contenedores de almacenamiento de la pestaña VVols.

- **ID de cuenta:** El ID de la cuenta de NetApp Element asociada con el contenedor de almacenamiento.
- **Nombre:** El nombre del contenedor de almacenamiento.
- **Estado:** El estado del contenedor de almacenamiento. Valores posibles:
 - Activo: El contenedor de almacenamiento está en uso.
 - Bloqueado: El contenedor de almacenamiento está bloqueado.
- **Secreto del Iniciador del Capítulo:** El secreto único del Capítulo para el iniciador.
- **Secreto del Objetivo CHAP:** El secreto CHAP único para el objetivo.
- **ID del contenedor de almacenamiento:** El UUID del contenedor de almacenamiento del volumen virtual.
- **Tipo de punto final de protocolo:** Indica el tipo de punto final de protocolo (SCSI es el único protocolo disponible).

Editar un contenedor de almacenamiento

Puede modificar la autenticación CHAP del contenedor de almacenamiento en la interfaz de usuario de Element.

1. Seleccione **VVols > Contenedores de almacenamiento**.
2. Haz clic en el icono **Acciones** del contenedor de almacenamiento que deseas editar.
3. En el menú que aparece, seleccione **Editar**.
4. En la configuración de CHAP, edite las credenciales de Secreto de Iniciador y Secreto de Destino utilizadas para la autenticación.



Si no modifica las credenciales de configuración CHAP, estas permanecerán sin cambios. Si dejas en blanco los campos de credenciales, el sistema generará automáticamente nuevos secretos.

5. Haz clic en **Guardar cambios**.

Eliminar un contenedor de almacenamiento

Puedes eliminar contenedores de almacenamiento desde la interfaz de usuario de Element.

Lo que necesitarás

Asegúrese de que todas las máquinas virtuales se hayan eliminado del almacén de datos VVol.

Pasos

1. Seleccione **VVols > Contenedores de almacenamiento**.
2. Haz clic en el icono **Acciones** del contenedor de almacenamiento que deseas eliminar.
3. En el menú que aparece, seleccione **Eliminar**.
4. Confirma la acción.
5. Actualice la lista de contenedores de almacenamiento en la subpestaña **Contenedores de almacenamiento** para confirmar que el contenedor de almacenamiento se ha eliminado.

puntos finales del protocolo

Aprenda sobre los puntos finales del protocolo

Los puntos de conexión del protocolo son puntos de acceso utilizados por un host para direccionar el almacenamiento en un clúster que ejecuta el software NetApp Element . Los puntos de conexión del protocolo no pueden ser eliminados ni modificados por un usuario, no están asociados a una cuenta y no pueden agregarse a un grupo de acceso por volumen.

Un clúster que ejecuta el software Element crea automáticamente un punto final de protocolo por cada nodo de almacenamiento en el clúster. Por ejemplo, un clúster de almacenamiento de seis nodos tiene seis puntos finales de protocolo que están asignados a cada host ESXi. Los puntos finales del protocolo son gestionados dinámicamente por el software Element y se crean, mueven o eliminan según sea necesario sin ninguna intervención. Los puntos finales del protocolo son el destino del enrutamiento múltiple y actúan como un proxy de E/S para las LUN subsidiarias. Cada extremo del protocolo consume una dirección SCSI disponible, al igual que un destino iSCSI estándar. Los puntos finales del protocolo aparecen como un dispositivo de almacenamiento de un solo bloque (512 bytes) en el cliente vSphere, pero este dispositivo de almacenamiento no está disponible para formatearse ni utilizarse como almacenamiento.

iSCSI es el único protocolo compatible. El protocolo Fibre Channel no es compatible.

Detalles de los puntos de conexión del protocolo

La página Puntos de conexión del protocolo en la pestaña VVols proporciona información sobre los puntos de conexión del protocolo.

- **ID del proveedor principal**

El ID del proveedor del punto final del protocolo principal.

- **ID del proveedor secundario**

El ID del proveedor del punto final del protocolo secundario.

- **ID del punto final del protocolo**

El UUID del punto final del protocolo.

- **Estado del punto final del protocolo**

Estado del punto final del protocolo. Los valores posibles son los siguientes:

- Activo: El punto final del protocolo está en uso.
- Inicio: El punto final del protocolo se está iniciando.
- Conmutación por error: El extremo del protocolo ha conmutado por error.
- Reservado: El punto final del protocolo está reservado.

- **Tipo de proveedor**

El tipo de proveedor del punto final del protocolo. Los valores posibles son los siguientes:

- Primario
- Secundario

- **ID de dispositivo SCSI NAA**

El identificador de dispositivo SCSI único a nivel mundial para el punto final del protocolo en formato extendido registrado IEEE NAA.

Fijaciones

Aprende sobre encuadernaciones

Para realizar operaciones de E/S con un volumen virtual, un host ESXi primero debe enlazar el volumen virtual.

El clúster SolidFire elige un punto final de protocolo óptimo, crea un enlace que asocia el host ESXi y el volumen virtual con el punto final de protocolo y devuelve el enlace al host ESXi. Una vez enlazado, el host ESXi puede realizar operaciones de E/S con el volumen virtual enlazado.

Detalles de encuadernación

La página de enlaces en la pestaña VVols proporciona información de enlace sobre cada volumen virtual.

Se muestra la siguiente información:

- **ID del host**

El UUID del host ESXi que aloja volúmenes virtuales y que es conocido por el clúster.

- **ID del punto final del protocolo**

Identificadores de punto final del protocolo que corresponden a cada nodo en el clúster SolidFire .

- **Punto final del protocolo en la ID de banda**

El ID de dispositivo SCSI de NAA del extremo del protocolo.

- **Tipo de punto final del protocolo**

El tipo de punto final del protocolo.

- **ID de enlace VVol**

El UUID de enlace del volumen virtual.

- **ID de VVol**

El identificador único universal (UUID) del volumen virtual.

- **ID secundaria de VVol**

El ID secundario del volumen virtual que es un ID de LUN SCSI de segundo nivel.

Detalles del anfitrión

La página Hosts de la pestaña VVols proporciona información sobre los hosts VMware ESXi que alojan volúmenes virtuales.

Se muestra la siguiente información:

- **ID del host**

El UUID del host ESXi que aloja volúmenes virtuales y que es conocido por el clúster.

- **Dirección del host**

La dirección IP o el nombre DNS del host ESXi.

- **Encuadernaciones**

Identificadores de enlace para todos los volúmenes virtuales enlazados por el host ESXi.

- **ID de clúster ESX**

El ID del clúster de host de vSphere o el GUID de vCenter.

- **Números de identificación de iniciador**

IQN de iniciador para el host de volumen virtual.

- *** Identificadores de punto final del protocolo SolidFire ***

Los puntos finales del protocolo que actualmente son visibles para el host ESXi.

Trabajar con grupos de acceso por volumen e iniciadores

Crear un grupo de acceso por volumen

Puede crear grupos de acceso a volúmenes asignando iniciadores a una colección de volúmenes para un acceso seguro. Luego puede 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 agregar credenciales CHAP para un único iniciador en un grupo de acceso por volumen, lo que proporciona mayor seguridad. Esto le permite aplicar esta opción a los grupos de acceso por volumen que ya existen.

Pasos

- 1. Haz clic en **Administración > Grupos de acceso.**
- 2. Haga clic en **Crear grupo de acceso.**
- 3. Introduzca un nombre para el grupo de acceso al volumen en el campo **Nombre.**
- 4. Agregue un iniciador al grupo de acceso al volumen de una de las siguientes maneras:

Opción	Descripción
Agregar un iniciador de canal de fibra	a. En Agregar iniciadores, seleccione un iniciador de canal de fibra existente de la lista Iniciadores de canal de fibra no enlazados. b. Haga clic en Agregar iniciador FC. i Puedes crear un iniciador durante este paso si haces clic en el enlace Crear iniciador, introduces un nombre para el iniciador y haces clic en Crear. El sistema añade automáticamente el iniciador a la lista de Iniciadores después de crearlo. Un ejemplo del formato es el siguiente: 5f:47:ac:c0:5c:74:d4:02

Opción	Descripción
Agregar un iniciador iSCSI	En Agregar iniciadores, seleccione un iniciador existente de la lista de Iniciadores. Nota: Puede crear un iniciador durante este paso si hace clic en el enlace Crear iniciador, introduce un nombre de iniciador y hace clic en Crear. El sistema añade automáticamente el iniciador a la lista de Iniciadores después de crearlo. Un ejemplo del formato es el siguiente: 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 Administración > Volúmenes > Activos. Al modificar un iniciador, puede cambiar el atributo requiredCHAP a True, lo que le permite establecer el secreto del iniciador de destino. Para obtener más detalles, consulte la información de la API sobre el método de la API ModifyInitiator. "Gestiona 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 de **Volúmenes adjuntos**.
7. **Opcional:** Añada más volúmenes según sea necesario.
8. Haga clic en **Crear grupo de acceso**.

Encuentra más información

[Agregar volúmenes a un grupo de acceso](#)

Ver detalles del grupo de acceso individual

Puede ver los detalles de un grupo de acceso individual, como los volúmenes conectados y los iniciadores, en formato gráfico.

1. Haz clic en **Administración > Grupos de acceso**.
2. Haz clic en el icono de Acciones para un grupo de acceso.
3. Haga clic en **Ver detalles**.

Detalles del grupo de acceso por volumen

La página Grupos de acceso en la pestaña Administración proporciona información sobre los grupos de acceso a volúmenes.

Se muestra la siguiente información:

- **ID:** El ID generado por el sistema para el grupo de acceso.
- **Nombre:** El nombre asignado al grupo de acceso cuando se creó.
- **Volúmenes activos:** El número de volúmenes activos en el grupo de acceso.
- **Compresión:** Puntuación de eficiencia de compresión para el grupo de acceso.
- **Desduplicación:** La puntuación de eficiencia de deduplicación para el grupo de acceso.
- **Aprovisionamiento ligero:** La puntuación de eficiencia del aprovisionamiento ligero para el grupo de acceso.
- **Eficiencia general:** La puntuación de eficiencia general para el grupo de acceso.
- **Iniciadores:** El número de iniciadores conectados al grupo de acceso.

Agregar volúmenes a un grupo de acceso

Puede agregar volúmenes a un grupo de acceso a volúmenes. Cada volumen puede pertenecer a más de un grupo de acceso a volúmenes; puede ver los grupos a los que pertenece cada volumen en la página de volúmenes **activos**.

También puede utilizar este procedimiento para agregar volúmenes a un grupo de acceso a volúmenes de Fibre Channel.

1. Haz clic en **Administración > Grupos de acceso**.
2. Haga clic en el icono Acciones del grupo de acceso al que desea agregar volúmenes.
3. Haz clic en el botón **Editar**.
4. En Agregar volúmenes, seleccione un volumen de la lista **Volúmenes**.

Puedes añadir más volúmenes repitiendo este paso.

5. Haz clic en **Guardar cambios**.

Eliminar volúmenes de un grupo de acceso

Cuando se elimina un volumen de un grupo de acceso, el grupo ya no tiene acceso a ese volumen.

Modificar la configuración CHAP en una cuenta o eliminar iniciadores o volúmenes de un grupo de acceso puede provocar que los iniciadores pierdan el acceso a los volúmenes de forma inesperada. Para verificar que el acceso al volumen no se pierda inesperadamente, cierre siempre las sesiones iSCSI que se verán afectadas por un cambio de cuenta o de grupo de acceso, y verifique que los iniciadores puedan volver a conectarse a los volúmenes después de que se hayan completado los cambios en la configuración del iniciador y la configuración del clúster.

1. Haz clic en **Administración > Grupos de acceso**.
2. Haga clic en el icono Acciones del grupo de acceso del que desea eliminar volúmenes.
3. Haga clic en **Editar**.
4. En Agregar volúmenes del cuadro de diálogo **Editar grupo de acceso a volúmenes**, haga clic en la flecha de la lista **Volúmenes conectados**.

5. Seleccione el volumen que desea eliminar de la lista y haga clic en el icono **x** para eliminar el volumen de la lista.

Puedes eliminar más volúmenes repitiendo este paso.

6. Haz clic en **Guardar cambios**.

Crear un iniciador

Puede crear iniciadores iSCSI o Fibre Channel y, opcionalmente, asignarles alias.

También puede asignar atributos CHAP basados en el iniciador mediante una llamada a la API. Para agregar un nombre de cuenta CHAP y credenciales por iniciador, debe usar el `CreateInitiator` Llamada a la API para eliminar y agregar acceso y atributos CHAP. El acceso del iniciador se puede restringir a una o más VLAN especificando uno o más ID de red virtual a través de `CreateInitiators` y `ModifyInitiators` Llamadas a la API. Si no se especifican redes virtuales, el iniciador puede acceder a todas las redes.

Para obtener más detalles, consulte la información de referencia de la API. "[Gestiona el almacenamiento con la API de Element](#)"

Pasos

1. Haz clic en **Administración > Iniciadores**.
2. Haz clic en **Crear iniciador**.
3. Siga los pasos para crear un único iniciador o varios iniciadores:

Opción	Pasos
Crea un único iniciador	a. Haga clic en Crear un único iniciador. b. Introduzca el IQN o WWPN del iniciador en el campo IQN/WWPN. c. Introduzca un nombre amigable para el iniciador en el campo Alias. d. Haz clic en Crear iniciador.
Crear múltiples iniciadores	a. Haga clic en Crear iniciadores en masa. b. Introduzca una lista de IQN o WWPN en el cuadro de texto. c. Haz clic en Añadir iniciadores. d. Elija un iniciador de la lista resultante y haga clic en el icono Agregar correspondiente en la columna Alias para agregar un alias al iniciador. e. Haz clic en la marca de verificación para confirmar el nuevo alias. f. Haz clic en Crear iniciadores.

Editar un iniciador

Puedes cambiar el alias de un iniciador existente o agregar un alias si aún no existe.

Para agregar un nombre de cuenta CHAP y credenciales por iniciador, debe usar el `ModifyInitiator` Llamada a la API para eliminar y agregar acceso y atributos CHAP.

Ver "[Gestiona el almacenamiento con la API de Element](#)".

Pasos

1. Haz clic en **Administración > Iniciadores**.
2. Haz clic en el icono de Acciones del iniciador que deseas editar.
3. Haga clic en **Editar**.
4. Introduzca un nuevo alias para el iniciador en el campo **Alias**.
5. Haz clic en **Guardar cambios**.

Agregar un único iniciador a un grupo de acceso a volumen

Puede agregar un iniciador a un grupo de acceso a volúmenes existente.

Cuando se agrega un iniciador a un grupo de acceso a volúmenes, dicho iniciador tiene acceso a todos los volúmenes de ese grupo de acceso a volúmenes.



Puede encontrar el iniciador de cada volumen haciendo clic en el icono Acciones y luego seleccionando **Ver detalles** para el volumen en la lista de volúmenes activos.

Si utiliza CHAP basado en iniciador, puede agregar credenciales CHAP para un único iniciador en un grupo de acceso por volumen, lo que proporciona mayor seguridad. Esto le permite aplicar esta opción a los grupos de acceso por volumen que ya existen.

Pasos

1. Haz 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 agregar un iniciador Fibre Channel al grupo de acceso a volúmenes, siga los siguientes pasos:
 - a. En Agregar iniciadores, seleccione un iniciador de canal de fibra existente de la lista **Iniciadores de canal de fibra no enlazados**.
 - b. Haga clic en **Agregar iniciador FC**.



Puedes crear un iniciador durante este paso si haces clic en el enlace **Crear iniciador**, introduces un nombre para el iniciador y haces clic en **Crear**. El sistema añade automáticamente al iniciador a la lista de **Iniciadores** después de crearlo.

Un ejemplo del formato es el siguiente:

```
5f:47:ac:c0:5c:74:d4:02
```

5. Para agregar un iniciador iSCSI al grupo de acceso al volumen, en Agregar iniciadores, seleccione un iniciador existente de la lista **Iniciadores**.



Puedes crear un iniciador durante este paso si haces clic en el enlace **Crear iniciador**, introduces un nombre para el iniciador y haces clic en **Crear**. El sistema añade automáticamente al iniciador a la lista de **Iniciadores** después de crearlo.

El formato aceptado de un IQN iniciador es el siguiente: iqn.yyyy-mm, donde y y m son dígitos, seguido de

texto que solo debe contener dígitos, caracteres alfabéticos en minúscula, un punto (.), dos puntos (:) o un guion (-).

Un ejemplo del formato es el siguiente:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```



Puede encontrar el IQN del iniciador para cada volumen en la página **Administración > Volúmenes** Volúmenes activos haciendo clic en el icono Acciones y luego seleccionando **Ver detalles** para el volumen.

6. Haz clic en **Guardar cambios**.

Agregue varios iniciadores a un grupo de acceso por volumen.

Puede agregar varios iniciadores a un grupo de acceso a volúmenes existente para permitir el acceso a los volúmenes del grupo de acceso a volúmenes con o sin necesidad de autenticación CHAP.

Cuando se agregan iniciadores a un grupo de acceso a volúmenes, los iniciadores tienen acceso a todos los volúmenes de ese grupo de acceso a volúmenes.



Puede encontrar el iniciador de cada volumen haciendo clic en el icono Acciones y luego en **Ver detalles** para el volumen en la lista de volúmenes activos.

Puede agregar varios iniciadores a un grupo de acceso a volúmenes existente para habilitar el acceso a los volúmenes y asignar credenciales CHAP únicas para cada iniciador dentro de ese grupo de acceso a volúmenes. Esto le permite aplicar esta opción a los grupos de acceso por volumen que ya existen.

Puede asignar atributos CHAP basados en el iniciador mediante una llamada a la API. Para agregar un nombre de cuenta CHAP y credenciales por iniciador, debe usar la llamada a la API ModifyInitiator para eliminar y agregar el acceso y los atributos CHAP.

Para más detalles, consulte "[Gestiona el almacenamiento con la API de Element](#)".

Pasos

1. Haz clic en **Administración > Iniciadores**.
2. Seleccione los iniciadores que desea agregar a un grupo de acceso.
3. Haz clic en el botón **Acciones en lote**.
4. Haga clic en **Agregar al grupo de acceso por volumen**.
5. En el cuadro de diálogo Agregar a grupo de acceso por volumen, seleccione un grupo de acceso de la lista **Grupo de acceso por volumen**.
6. Haga clic en **Agregar**.

Eliminar iniciadores de un grupo de acceso

Cuando se elimina un iniciador de un grupo de acceso, este ya no puede acceder a los volúmenes de ese grupo de acceso a volúmenes. El acceso normal de la cuenta al

volumen no se ve interrumpido.

Modificar la configuración CHAP en una cuenta o eliminar iniciadores o volúmenes de un grupo de acceso puede provocar que los iniciadores pierdan el acceso a los volúmenes de forma inesperada. Para verificar que el acceso al volumen no se pierda inesperadamente, cierre siempre las sesiones iSCSI que se verán afectadas por un cambio de cuenta o de grupo de acceso, y verifique que los iniciadores puedan volver a conectarse a los volúmenes después de que se hayan completado los cambios en la configuración del iniciador y la configuración del clúster.

Pasos

1. Haz clic en **Administración > Grupos de acceso**.
2. Haz clic en el icono **Acciones** del grupo de acceso que deseas eliminar.
3. En el menú que aparece, seleccione **Editar**.
4. En Agregar iniciadores en el cuadro de diálogo **Editar grupo de acceso a volumen**, haga clic en la flecha de la lista **Iniciadores**.
5. Seleccione el icono x para cada iniciador que desee eliminar del grupo de acceso.
6. Haz clic en **Guardar cambios**.

Eliminar un grupo de acceso

Puede eliminar un grupo de acceso cuando ya no sea necesario. No es necesario eliminar los ID de iniciador ni los ID de volumen del grupo de acceso a volúmenes antes de eliminar el grupo. Una vez eliminado el grupo de acceso, se interrumpe el acceso del grupo a los volúmenes.

1. Haz clic en **Administración > Grupos de acceso**.
2. Haz clic en el icono **Acciones** del grupo de acceso que deseas eliminar.
3. En el menú que aparece, haga clic en **Eliminar**.
4. Para eliminar también los iniciadores asociados a este grupo de acceso, seleccione la casilla de verificación **Eliminar iniciadores en este grupo de acceso**.
5. Confirma la acción.

Eliminar un iniciador

Puedes eliminar un iniciador cuando ya no sea necesario. Cuando se elimina un iniciador, el sistema lo quita de cualquier grupo de acceso a volúmenes asociado. Las conexiones que utilizan el iniciador permanecen válidas hasta que se restablece la conexión.

Pasos

1. Haz clic en **Administración > Iniciadores**.
2. Siga los pasos para eliminar un único iniciador o varios iniciadores:

Opción	Pasos
Eliminar iniciador único	- Haz clic en el icono Acciones del iniciador que deseas eliminar. - Haga clic en Eliminar. - Confirma la acción.
Eliminar varios iniciadores	- Seleccione las casillas de verificación junto a los iniciadores que desea eliminar. - Haz clic en el botón Acciones en lote. - En el menú que aparece, seleccione Eliminar. - Confirma la acción.

Proteja sus datos

Proteja sus datos

El software NetApp Element le permite proteger sus datos de diversas maneras con funcionalidades como instantáneas para volúmenes individuales o grupos de volúmenes, replicación entre clústeres y volúmenes que se ejecutan en Element y replicación a sistemas ONTAP .

- **Instantáneas**

La protección de datos de solo instantáneas replica los datos modificados en momentos específicos en un clúster remoto. Solo se replican las instantáneas creadas en el clúster de origen. Las escrituras activas desde el volumen de origen no lo son.

[Utilice instantáneas de volumen para la protección de datos.](#)

- **Replicación remota entre clústeres y volúmenes que se ejecutan en Element**

Puede replicar datos de volumen de forma síncrona o asíncrona desde cualquiera de los clústeres de un par de clústeres que se ejecutan en Element para escenarios de conmutación por error y recuperación ante fallos.

[Realizar replicación remota entre clústeres que ejecutan el software NetApp Element .](#)

- ***Replicación entre clústeres Element y ONTAP mediante la tecnología SnapMirror ***

Con la tecnología NetApp SnapMirror , puede replicar instantáneas tomadas con Element en ONTAP para fines de recuperación ante desastres. En una relación SnapMirror , Element es un punto final y ONTAP es el otro.

[Utilice la replicación SnapMirror entre los clústeres Element y ONTAP.](#)

- **Realizar copias de seguridad y restaurar volúmenes desde SolidFire, S3 o almacenes de objetos Swift**

Puede realizar copias de seguridad y restaurar volúmenes en otros almacenamientos SolidFire , así como

en almacenes de objetos secundarios compatibles con Amazon S3 u OpenStack Swift.

[Realice copias de seguridad y restaure volúmenes en almacenes de objetos SolidFire, S3 o Swift.](#)

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Utilice instantáneas de volumen para la protección de datos.

Utilice instantáneas de volumen para la protección de datos.

Una instantánea de volumen es una copia de un volumen en un momento dado. Puedes tomar una instantánea de un volumen y usarla más tarde si necesitas restaurar un volumen al estado en el que se encontraba en el momento en que se creó la instantánea.

Las instantáneas son similares a los clones de volumen. Sin embargo, las instantáneas son simplemente réplicas de los metadatos del volumen, por lo que no se pueden montar ni escribir en ellas. La creación de una instantánea de volumen también requiere una cantidad mínima de recursos del sistema y espacio, lo que hace que la creación de instantáneas sea más rápida que la clonación.

Puede tomar una instantánea de un volumen individual o de un conjunto de volúmenes.

Opcionalmente, replique las instantáneas en un clúster remoto y utilícelas como copia de seguridad del volumen. Esto le permite revertir un volumen a un punto específico en el tiempo mediante el uso de la instantánea replicada. Como alternativa, puede crear un clon de un volumen a partir de una instantánea replicada.

Encuentra más información

- [Utilice instantáneas de volumen individuales para la protección de datos.](#)
- [Utilizar instantáneas de grupo para la tarea de protección de datos](#)
- [Programar una instantánea](#)

Utilice instantáneas de volumen individuales para la protección de datos.

Utilice instantáneas de volumen individuales para la protección de datos.

Una instantánea de volumen es una copia de un volumen en un momento dado. Puede utilizar un volumen individual en lugar de un grupo de volúmenes para la instantánea.

Encuentra más información

- [Cree una instantánea de volumen](#)
- [Editar retención de instantáneas](#)
- [Eliminar una instantánea](#)
- [Clonar un volumen a partir de una instantánea](#)

- [Revertir un volumen a una instantánea](#)
- [Realizar una copia de seguridad de una instantánea de volumen en un almacenamiento de objetos de Amazon S3](#)
- [Realizar una copia de seguridad de una instantánea de volumen en un almacén de objetos Swift de OpenStack](#)
- [Realizar una copia de seguridad de una instantánea de volumen en un clúster SolidFire](#)

Cree una instantánea de volumen

Puede crear una instantánea de un volumen activo para conservar la imagen del volumen en cualquier momento. Puedes crear hasta 32 instantáneas para un solo volumen.

1. Haz clic en **Administración > Volúmenes**.
2. Haga clic en el icono **Acciones** del volumen que desea utilizar para la instantánea.
3. En el menú que aparece, seleccione **Instantánea**.
4. En el cuadro de diálogo **Crear instantánea del volumen**, introduzca el nombre de la nueva instantánea.
5. **Opcional:** Seleccione la casilla de verificación **Incluir instantánea en la replicación cuando se empareje** para garantizar que la instantánea se capture en la replicación cuando se empareje el volumen principal.
6. Para configurar el período de retención de la instantánea, seleccione una de las siguientes opciones:
 - Haz clic en **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
 - Haz clic en **Establecer período de retención** y usa los controles de fecha para elegir el tiempo durante el cual el sistema conservará la instantánea.
7. Para tomar una instantánea única e inmediata, siga los siguientes pasos:
 - a. Haz clic en **Tomar instantánea ahora**.
 - b. Haz clic en **Crear instantánea**.
8. Para programar la ejecución de la instantánea en un momento futuro, siga los siguientes pasos:
 - a. Haga clic en **Crear programación de instantáneas**.
 - b. Ingrese un **Nuevo Nombre de Horario**.
 - c. Elige un **Tipo de horario** de la lista.
 - d. **Opcional:** Seleccione la casilla de verificación **Programación recurrente** para repetir la instantánea programada periódicamente.
 - e. Haz clic en **Crear horario**.

Encuentra más información

[Programa una instantánea](#)

Editar retención de instantáneas

Puedes cambiar el período de retención de una instantánea para controlar cuándo o si el sistema elimina las instantáneas. El período de retención que especifique comienza cuando ingrese el nuevo intervalo. Al establecer un período de retención, puede

seleccionar un período que comience en el momento actual (la retención no se calcula a partir del momento de creación de la instantánea). Puedes especificar intervalos en minutos, horas y días.

Pasos

1. Haz clic en **Protección de datos > Instantáneas**.
2. Haz clic en el icono **Acciones** de la instantánea que quieras editar.
3. En el menú que aparece, haga clic en **Editar**.
4. **Opcional:** Seleccione la casilla de verificación **Incluir instantánea en la replicación cuando se empareje** para garantizar que la instantánea se capture en la replicación cuando se empareje el volumen principal.
5. **Opcional:** Seleccione una opción de retención para la instantánea:
 - Haz clic en **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
 - Haga clic en **Establecer período de retención** y utilice los controles numéricos de fecha para seleccionar el período de tiempo durante el cual el sistema conservará la instantánea.
6. Haz clic en **Guardar cambios**.

Eliminar una instantánea

Puede eliminar una instantánea de volumen de un clúster de almacenamiento que ejecuta el software Element. Cuando borras una instantánea, el sistema la elimina inmediatamente.

Puedes eliminar las instantáneas que se están replicando desde el clúster de origen. Si una instantánea se está sincronizando con el clúster de destino cuando la eliminas, la replicación de sincronización se completa y la instantánea se elimina del clúster de origen. La instantánea no se elimina del clúster de destino.

También puede eliminar instantáneas que se hayan replicado en el destino desde el clúster de destino. La instantánea eliminada se mantiene en una lista de instantáneas eliminadas en el destino hasta que el sistema detecta que usted ha eliminado la instantánea en el clúster de origen. Cuando el destino detecta que has eliminado la instantánea de origen, detiene la replicación de la misma.

Cuando se elimina una instantánea del clúster de origen, la instantánea del clúster de destino no se ve afectada (y viceversa).

1. Haz clic en **Protección de datos > Instantáneas**.
2. Haz clic en el icono **Acciones** de la instantánea que deseas eliminar.
3. En el menú que aparece, seleccione **Eliminar**.
4. Confirma la acción.

Clonar un volumen a partir de una instantánea

Puedes crear un nuevo volumen a partir de una instantánea de un volumen. Al hacer esto, el sistema utiliza la información de la instantánea para clonar un nuevo volumen utilizando los datos que contenía el volumen en el momento en que se creó la instantánea. Este proceso almacena información sobre otras instantáneas del volumen en el volumen recién creado.

1. Haz clic en **Protección de datos > Instantáneas**.
2. Haga clic en el icono **Acciones** de la instantánea que desea utilizar para la clonación del volumen.
3. En el menú que aparece, haga clic en **Clonar volumen desde instantánea**.
4. Introduzca un **Nombre de volumen** en el cuadro de diálogo **Clonar volumen desde instantánea**.
5. Seleccione un **Tamaño total** y las unidades de tamaño para el nuevo volumen.
6. Seleccione un tipo de **Acceso** para el volumen.
7. Seleccione una **Cuenta** de la lista para asociarla con el nuevo volumen.
8. Haz clic en **Iniciar clonación**.

Revierte un volumen a una instantánea

Puedes restaurar un volumen a una instantánea anterior en cualquier momento. Esto revierte cualquier cambio realizado en el volumen desde que se creó la instantánea.

Pasos

1. Haz clic en **Protección de datos > Instantáneas**.
2. Haga clic en el icono **Acciones** de la instantánea que desea utilizar para la reversión de volumen.
3. En el menú resultante, seleccione **Revertir volumen a instantánea**.
4. **Opcional:** Para guardar el estado actual del volumen antes de volver a la instantánea:
 - a. En el cuadro de diálogo **Revertir a instantánea**, seleccione **Guardar el estado actual del volumen como una instantánea**.
 - b. Introduzca un nombre para la nueva instantánea.
5. Haga clic en **Revertir instantánea**.

Realizar una copia de seguridad de una instantánea de volumen

Realizar una copia de seguridad de una instantánea de volumen

Puede utilizar la función de copia de seguridad integrada para realizar una copia de seguridad de una instantánea de volumen. Puede realizar copias de seguridad de instantáneas desde un clúster SolidFire a un almacenamiento de objetos externo o a otro clúster SolidFire . Cuando se realiza una copia de seguridad de una instantánea en un almacenamiento de objetos externo, es necesario disponer de una conexión con dicho almacenamiento que permita operaciones de lectura/escritura.

- ["Realizar una copia de seguridad de una instantánea de volumen en un almacenamiento de objetos de Amazon S3"](#)
- ["Realizar una copia de seguridad de una instantánea de volumen en un almacén de objetos Swift de OpenStack"](#)
- ["Realizar una copia de seguridad de una instantánea de volumen en un clúster SolidFire"](#)

Realizar una copia de seguridad de una instantánea de volumen en un almacenamiento de objetos de Amazon S3

Puede realizar copias de seguridad de las instantáneas de SolidFire en almacenes de

objetos externos compatibles con Amazon S3.

1. Haga clic en **Protección de datos > Instantáneas**.
2. Haz clic en el icono **Acciones** de la instantánea que deseas respaldar.
3. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
4. En el cuadro de diálogo **Copia de seguridad integrada**, en **Realizar copia de seguridad en**, seleccione **S3**.
5. Seleccione una opción en **Formato de datos**:
 - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
 - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Introduzca un nombre de host para acceder al almacén de objetos en el campo **Nombre de host**.
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 bucket de S3 en el que se almacenará la copia de seguridad en el campo **Bucket de S3**.
10. **Opcional**: Introduzca una etiqueta de nombre para añadir al prefijo en el campo **Etiqueta de nombre**.
11. Haz clic en **Iniciar lectura**.

Realizar una copia de seguridad de una instantánea de volumen en un almacén de objetos Swift de OpenStack

Puede realizar copias de seguridad de las instantáneas de SolidFire en almacenes de objetos secundarios que sean compatibles con OpenStack Swift.

1. Haz clic en **Protección de datos > Instantáneas**.
2. Haz clic en el icono **Acciones** de la instantánea que deseas respaldar.
3. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
4. En el cuadro de diálogo **Copia de seguridad integrada**, en **Realizar copia de seguridad en**, seleccione **Swift**.
5. Seleccione una opción en **Formato de datos**:
 - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
 - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Ingrese una **URL** para acceder al almacén de objetos.
7. Introduce un **Nombre de usuario** para la cuenta.
8. Introduzca la **Clave de autenticación** de la cuenta.
9. Introduzca el **Contenedor** en el que se almacenará la copia de seguridad.
10. **Opcional**: Introduzca una **etiqueta de nombre**.
11. Haz clic en **Iniciar lectura**.

Realizar una copia de seguridad de una instantánea de volumen en un clúster SolidFire

Puede realizar copias de seguridad de instantáneas de volumen que residen en un clúster SolidFire en un clúster SolidFire remoto.

Asegúrese de que los clústeres de origen y destino estén emparejados.

Al realizar copias de seguridad o restauraciones de un clúster a otro, el sistema genera una clave que se utilizará para la autenticación entre los clústeres. Esta clave de escritura de volumen masivo permite que el clúster de origen se autentique con el clúster de destino, proporcionando un nivel de seguridad al escribir en el volumen de destino. Como parte del proceso de copia de seguridad o restauración, debe generar una clave de escritura de volumen masivo 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 aparece, haga clic en **Restaurar desde**.
4. En el cuadro de diálogo **Restauración integrada**, en **Restaurar desde**, seleccione * SolidFire*.
5. Seleccione un formato de datos en **Formato de datos**:
 - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
 - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Haz clic en **Generar clave**.
7. Copie la clave del cuadro **Clave de escritura de volumen masivo** al portapapeles.
8. En el clúster de origen, haga clic en **Protección de datos > Instantáneas**.
9. Haz clic en el icono Acciones de la instantánea que quieras usar para la copia de seguridad.
10. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
11. En el cuadro de diálogo **Copia de seguridad integrada**, en **Realizar copia de seguridad en**, seleccione * SolidFire*.
12. Seleccione el mismo formato de datos que seleccionó anteriormente en el campo **Formato de datos**.
13. Introduzca la dirección IP virtual de gestión del clúster del volumen de destino en el campo **MVIP de clúster remoto**.
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 **Contraseña del clúster remoto**.
16. En el campo **Clave de escritura de volumen masivo**, pegue la clave que generó anteriormente en el clúster de destino.
17. Haz clic en **Iniciar lectura**.

Utilice instantáneas de grupo para la protección de datos.

Utilizar instantáneas de grupo para la tarea de protección de datos

Puede crear una instantánea de grupo de un conjunto de volúmenes relacionados para conservar una copia puntual de los metadatos de cada volumen. En el futuro, puede utilizar la instantánea del grupo como copia de seguridad o para revertir cambios y restaurar el estado del grupo de volúmenes a un estado anterior.

Encuentra más información

- [Crea una instantánea de grupo](#)
- [Editar instantáneas de grupo](#)

- [Editar miembros de la instantánea del grupo](#)
- [Eliminar una instantánea de grupo](#)
- [Revertir volúmenes a una instantánea de grupo](#)
- [Clonar múltiples volúmenes](#)
- [Clonar varios volúmenes a partir de una instantánea de grupo](#)

Detalles de la instantánea del grupo

La página Instantáneas de grupo en la pestaña Protección de datos proporciona información sobre las instantáneas de grupo.

- **IDENTIFICACIÓN**

El ID generado por el sistema para la instantánea del grupo.

- **UUID**

El identificador único de la instantánea del grupo.

- **Nombre**

Nombre definido por el usuario para la instantánea del grupo.

- **Crear tiempo**

La hora en la que se creó la instantánea del grupo.

- **Estado**

Estado actual de la instantánea. Valores posibles:

- Preparación: La instantánea se está preparando para su uso y aún no se puede escribir en ella.
- Listo: Esta instantánea ha finalizado su preparación y ya se puede utilizar.
- Activa: La instantánea corresponde a la rama activa.

- **# Volúmenes**

El número de volúmenes en el grupo.

- **Conservar hasta**

El día y la hora en que se eliminará la instantánea.

- **Replicación remota**

Indicación de si la instantánea está habilitada o no para la replicación a un clúster SolidFire remoto. Valores posibles:

- Habilitado: La instantánea está habilitada para la replicación remota.
- Deshabilitado: La instantánea no está habilitada para la replicación remota.

Creación de una instantánea de grupo

Puede crear una instantánea de un grupo de volúmenes, y también puede crear una programación de instantáneas de grupo para automatizar las instantáneas de grupo. Una única instantánea de grupo puede capturar de forma consistente hasta 32 volúmenes a la vez.

Pasos

1. Haz clic en **Administración > Volúmenes**.
2. Utilice las casillas de verificación para seleccionar varios volúmenes para un grupo de volúmenes.
3. Haz clic en **Acciones en lote**.
4. Haga clic en **Instantánea de grupo**.
5. Introduzca un nuevo nombre para la instantánea de grupo en el cuadro de diálogo Crear instantánea de grupo de volúmenes.
6. **Opcional:** Seleccione la casilla de verificación **Incluir cada miembro de la instantánea del grupo en la replicación cuando se emparejen** para garantizar que cada instantánea se capture en la replicación cuando se empareje el volumen principal.
7. Seleccione una opción de retención para la instantánea del grupo:
 - Haz clic en **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
 - Haz clic en **Establecer período de retención** y usa los controles de fecha para elegir el tiempo durante el cual el sistema conservará la instantánea.
8. Para tomar una instantánea única e inmediata, siga los siguientes pasos:
 - a. Haz clic en **Tomar instantánea de grupo ahora**.
 - b. Haz clic en **Crear instantánea de grupo**.
9. Para programar la ejecución de la instantánea en un momento futuro, siga los siguientes pasos:
 - a. Haga clic en **Crear programación de instantáneas de grupo**.
 - b. Ingrese un **Nuevo Nombre de Horario**.
 - c. Seleccione un **Tipo de horario** de la lista.
 - d. **Opcional:** Seleccione la casilla de verificación **Programación recurrente** para repetir la instantánea programada periódicamente.
 - e. Haz clic en **Crear horario**.

Edición de instantáneas de grupo

Puede editar la configuración de replicación y retención para las instantáneas de grupo existentes.

1. Haz clic en **Protección de datos > Instantáneas de grupo**.
2. Haz clic en el icono Acciones de la instantánea de grupo que quieras editar.
3. En el menú que aparece, 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. Seleccione la casilla de verificación **Incluir cada miembro de la instantánea del grupo en la**

replicación cuando se emparejen para garantizar que cada instantánea se capture en la replicación cuando se empareje el volumen principal.

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 instantánea del grupo:
 - Haz clic en **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
 - Haz clic en **Establecer período de retención** y usa los controles de fecha para elegir el tiempo durante el cual el sistema conservará la instantánea.
6. Haz clic en **Guardar cambios**.

Eliminar una instantánea de grupo

Puedes eliminar una instantánea de grupo del sistema. Al eliminar la instantánea del grupo, puede elegir si desea que se eliminen todas las instantáneas asociadas al grupo o que se conserven como instantáneas individuales.

Si elimina un volumen o una instantánea que sea miembro de una instantánea de grupo, ya no podrá revertir a la instantánea de grupo. Sin embargo, puede revertir cada volumen individualmente.

1. Haz clic en **Protección de datos > Instantáneas de grupo**.
2. Haz clic en el icono de Acciones de la instantánea que deseas eliminar.
3. En el menú que aparece, 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 la instantánea de grupo** para eliminar la instantánea de grupo y todas las instantáneas de los miembros.
 - Haz clic en **Conservar miembros de instantáneas de grupo como instantáneas individuales** para eliminar la instantánea de grupo pero conservar todas las instantáneas de los miembros.
5. Confirma la acción.

Revertir volúmenes a una instantánea de grupo

Puede revertir un grupo de volúmenes en cualquier momento a una instantánea de grupo.

Cuando se revierte un grupo de volúmenes, todos los volúmenes del grupo se restauran al estado en el que se encontraban en el momento en que se creó la instantánea del grupo. La reversión también restaura los tamaños de volumen al tamaño registrado en la instantánea original. Si el sistema ha eliminado un volumen, todas las instantáneas de ese volumen también se eliminaron en el momento de la eliminación; el sistema no restaura ninguna instantánea de volumen eliminada.

1. Haz clic en **Protección de datos > Instantáneas de grupo**.
2. Haga clic en el icono Acciones de la instantánea de grupo que desea utilizar para la reversión de volumen.
3. En el menú resultante, seleccione **Revertir volúmenes a instantánea de grupo**.
4. **Opcional:** Para guardar el estado actual de los volúmenes antes de volver a la instantánea:
 - a. En el cuadro de diálogo **Revertir a instantánea**, seleccione **Guardar el estado actual de los**

volúmenes como una instantánea de grupo.

b. Introduzca un nombre para la nueva instantánea.

5. Haga clic en **Revertir instantánea de grupo**.

Edición de la instantánea del grupo

Puedes editar la configuración de retención para los miembros de una instantánea de grupo existente.

1. Haz clic en **Protección de datos > Instantáneas**.
2. Haz clic en la pestaña **Miembros**.
3. Haz clic en el icono de Acciones del miembro de la instantánea del grupo que quieras editar.
4. En el menú que aparece, seleccione **Editar**.
5. Para cambiar la configuración de replicación de la instantánea, seleccione una de las siguientes opciones:
 - Haz clic en **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
 - Haz clic en **Establecer período de retención** y usa los controles de fecha para elegir el tiempo durante el cual el sistema conservará la instantánea.
6. Haz clic en **Guardar cambios**.

Clonar múltiples volúmenes

Puede crear varios clones de volumen en una sola operación para crear una copia puntual de los datos en un grupo de volúmenes.

Cuando se clona un volumen, el sistema crea una instantánea del volumen y luego crea un nuevo volumen a partir de los datos de la instantánea. Puede montar y escribir en el nuevo clon de volumen. La clonación de múltiples volúmenes es un proceso asíncrono y requiere un tiempo variable dependiendo del tamaño y la cantidad de volúmenes que se clonan.

El tamaño del volumen y la carga actual del clúster afectan al tiempo necesario para completar una operación de clonación.

Pasos

1. Haz clic en **Administración > Volúmenes**.
2. Haz clic en la pestaña **Activa**.
3. Utilice las casillas de verificación para seleccionar varios volúmenes y crear un grupo de volúmenes.
4. Haz clic en **Acciones en lote**.
5. Haz clic en **Clonar** en el menú que aparece.
6. Introduzca un **Prefijo de nombre de volumen nuevo** en el cuadro de diálogo **Clonar varios volúmenes**.

El prefijo se aplica a todos los volúmenes del grupo.

7. **Opcional:** Seleccione una cuenta diferente a la que pertenecerá el clon.

Si no selecciona una cuenta, el sistema asigna los nuevos volúmenes a la cuenta de volumen actual.

8. **Opcional:** Seleccione un método de acceso diferente para los volúmenes en el clon.

Si no selecciona un método de acceso, el sistema utiliza el acceso al volumen actual.

9. Haz clic en **Iniciar clonación**.

Clonación de varios volúmenes a partir de una instantánea de grupo

Puede clonar un grupo de volúmenes a partir de una instantánea de grupo en un momento dado. Esta operación requiere que ya exista una instantánea de grupo de los volúmenes, ya que dicha instantánea se utiliza como base para crear los volúmenes. Una vez creados los volúmenes, podrá utilizarlos como cualquier otro volumen del sistema.

El tamaño del volumen y la carga actual del clúster afectan al tiempo necesario para completar una operación de clonación.

1. Haz clic en **Protección de datos > Instantáneas de grupo**.
2. Haga clic en el icono Acciones de la instantánea de grupo que desea utilizar para los clones de volumen.
3. En el menú resultante, seleccione **Clonar volúmenes desde instantánea de grupo**.
4. Introduzca un **Nuevo prefijo de nombre de volumen** en el cuadro de diálogo **Clonar volúmenes desde instantánea de grupo**.

El prefijo se aplica a todos los volúmenes creados a partir de la instantánea del grupo.

5. **Opcional:** Seleccione una cuenta diferente a la que pertenecerá el clon.

Si no selecciona una cuenta, el sistema asigna los nuevos volúmenes a la cuenta de volumen actual.

6. **Opcional:** Seleccione un método de acceso diferente para los volúmenes en el clon.

Si no selecciona un método de acceso, el sistema utiliza el acceso al volumen actual.

7. Haz clic en **Iniciar clonación**.

Programa una instantánea

Programa una instantánea

Puede proteger los datos de un volumen o un grupo de volúmenes programando instantáneas de volumen para que se realicen a intervalos específicos. Puede programar la ejecución automática de instantáneas de un solo volumen o de instantáneas de grupo.

Al configurar una programación de instantáneas, puede elegir intervalos de tiempo basados en días de la semana o días del mes. También puedes especificar los días, horas y minutos antes de que se tome la siguiente instantánea. Puede almacenar las instantáneas resultantes en un sistema de almacenamiento remoto si el volumen se está replicando.

Encuentra más información

- [Crea un cronograma de instantáneas](#)
- [Editar un cronograma de instantáneas](#)
- [Eliminar una programación de instantáneas](#)

- [Copiar un cronograma de instantánea](#)

Detalles del cronograma de instantáneas

En la página Protección de datos > Programaciones, puede ver la siguiente información en la lista de programaciones de instantáneas.

- **IDENTIFICACIÓN**

El ID generado por el sistema para la instantánea.

- **Tipo**

El tipo de horario. Actualmente, solo se admite el tipo de instantánea.

- **Nombre**

El nombre que se le dio al horario cuando se creó. Los nombres de programación de instantáneas pueden tener hasta 223 caracteres de longitud y contener caracteres az, 0-9 y guion (-).

- **Frecuencia**

La frecuencia con la que se ejecuta la programación. La frecuencia se puede configurar en horas y minutos, semanas o meses.

- **Periódico**

Indicación de si la programación debe ejecutarse solo una vez o a intervalos regulares.

- **Pausa manual**

Indicación de si la programación se ha pausado manualmente o no.

- **Identificadores de volumen**

El identificador del volumen que utilizará la programación cuando se ejecute.

- **Última carrera**

La última vez que se ejecutó el horario.

- **Estado de la última ejecución**

El resultado de la última ejecución programada. Valores posibles:

- Éxito
- Falla

Crea un cronograma de instantáneas

Puede programar la toma de instantáneas de uno o varios volúmenes para que se realicen automáticamente a intervalos específicos.

Al configurar una programación de instantáneas, puede elegir intervalos de tiempo basados en días de la semana o días del mes. También puedes crear una programación recurrente y especificar los días, horas y

minutos antes de que se produzca la siguiente instantánea.

Si programas una instantánea para que se ejecute en un período de tiempo que no sea divisible por 5 minutos, la instantánea se ejecutará en el siguiente período de tiempo que sea divisible por 5 minutos. Por ejemplo, si programa una instantánea para que se ejecute a las 12:42:00 UTC, se ejecutará a las 12:45:00 UTC. No se puede programar una instantánea para que se ejecute a intervalos inferiores a 5 minutos.

A partir de Element 12.5, puede habilitar la creación serial y seleccionar conservar las instantáneas en base a las primeras en entrar, primeras en salir (FIFO) desde la interfaz de usuario.

- La opción **Habilitar creación serial** especifica que solo se replica una instantánea a la vez. La creación de una nueva instantánea falla cuando la replicación de una instantánea anterior aún está en curso. Si la casilla de verificación no está seleccionada, se permite la creación de una instantánea cuando otra replicación de instantánea aún está en curso.
- La opción **FIFO** añade la capacidad de conservar un número constante de las últimas instantáneas. Cuando se selecciona la casilla de verificación, las instantáneas se conservan en orden FIFO (primero en entrar, primero en salir). Una vez que la cola de instantáneas FIFO alcanza su profundidad máxima, la instantánea FIFO más antigua se descarta cuando se inserta una nueva.

Pasos

1. Seleccione **Protección de datos > Programaciones**.
2. Seleccione **Crear horario**.
3. En el campo **CSV de ID de volumen**, introduzca un único ID de volumen o una lista de ID de volumen separados por comas para incluir en la operación de instantánea.
4. Introduzca un nuevo nombre para el horario.
5. Seleccione un tipo de horario y configúrelo a partir de las opciones proporcionadas.
6. **Opcional:** Seleccione **Programación recurrente** para repetir la programación de instantáneas indefinidamente.
7. **Opcional:** Introduzca un nombre para la nueva instantánea en el campo **Nombre de la nueva instantánea**.

Si deja el campo en blanco, el sistema utilizará la fecha y hora de creación de la instantánea como nombre.

8. **Opcional:** Seleccione la casilla de verificación **Incluir instantáneas en la replicación cuando se emparejan** para garantizar que las instantáneas se capturen en la replicación cuando se empareje el volumen principal.
9. **Opcional:** Seleccione la casilla de verificación **Habilitar creación serial** para garantizar que solo se replique una instantánea a la vez.
10. Para configurar el período de retención de la instantánea, seleccione una de las siguientes opciones:
 - **Opcional:** Seleccione la casilla de verificación **FIFO (Primero en entrar, primero en salir)** para conservar un número constante de las instantáneas más recientes.
 - Seleccione **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
 - Seleccione **Establecer período de retención** y utilice los controles numéricos de fecha para elegir el período de tiempo durante el cual el sistema conservará la instantánea.
11. Seleccione **Crear horario**.

Editar un cronograma de instantáneas

Puede modificar las programaciones de instantáneas existentes. Tras la modificación, la próxima vez que se ejecute la programación, utilizará los atributos actualizados. Las instantáneas creadas por la programación original permanecen en el sistema de almacenamiento.

Pasos

1. Haz clic en **Protección de datos > Programaciones**.
2. Haz clic en el icono **Acciones** del horario que quieras cambiar.
3. En el menú que aparece, haga clic en **Editar**.
4. En el campo **CSV de ID de volumen**, modifique el ID de volumen único o la lista de ID de volumen separados por comas que se incluyen actualmente 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** de la lista **Pausar programación manualmente**.
 - Para reanudar una programación pausada, seleccione **No** de la lista **Pausar programación manualmente**.
6. Si lo desea, introduzca un nombre diferente para el horario en el campo **Nombre del nuevo horario**.
7. Para cambiar la programación para que se ejecute en diferentes días de la semana o del mes, seleccione **Tipo de programación** y cambie la programación de las opciones proporcionadas.
8. **Opcional:** Seleccione **Programación recurrente** para repetir la programación de instantáneas indefinidamente.
9. **Opcional:** Introduzca o modifique el nombre de la nueva instantánea en el campo **Nombre de la nueva instantánea**.

Si deja el campo en blanco, el sistema utilizará la fecha y hora de creación de la instantánea como nombre.

10. **Opcional:** Seleccione la casilla de verificación **Incluir instantáneas en la replicación cuando se emparejan** para garantizar que las instantáneas se capturen en la replicación cuando se empareje el volumen principal.
11. Para cambiar la configuración de retención, seleccione una de las siguientes opciones:
 - Haz clic en **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
 - Haga clic en **Establecer período de retención** y utilice los controles numéricos de fecha para seleccionar el período de tiempo durante el cual el sistema conservará la instantánea.
12. Haz clic en **Guardar cambios**.

Copiar un cronograma de instantánea

Puede copiar una programación y mantener sus atributos actuales.

1. Haz clic en **Protección de datos > Programaciones**.
2. Haz clic en el icono de Acciones del horario que quieras copiar.
3. En el menú que aparece, haga clic en **Hacer una copia**.

Aparece el cuadro de diálogo **Crear horario**, que se completa con los atributos actuales del horario.

4. **Opcional:** Introduzca un nombre y atributos actualizados para el nuevo horario.
5. Haz clic en **Crear horario**.

Eliminar una programación de instantáneas

Puedes eliminar una programación de instantáneas. Después de eliminar la programación, no se ejecutarán más instantáneas programadas. Las instantáneas creadas por la programación permanecen en el sistema de almacenamiento.

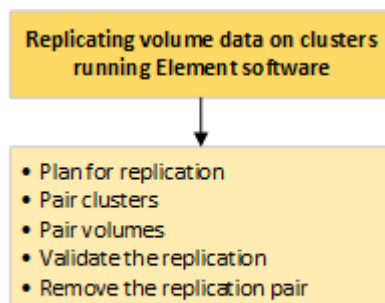
1. Haz clic en **Protección de datos > Programaciones**.
2. Haz clic en el icono **Acciones** del horario que deseas eliminar.
3. En el menú que aparece, haga clic en **Eliminar**.
4. Confirma la acción.

Realizar replicación remota entre clústeres que ejecutan el software NetApp Element .

Realizar replicación remota entre 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. Puedes emparejar un clúster de almacenamiento con hasta cuatro clústeres de almacenamiento adicionales. Puede replicar datos de volumen de forma síncrona o asíncrona desde cualquiera de los clústeres de un par de clústeres para escenarios de conmutación por error y recuperación ante fallos.

El proceso de replicación incluye los siguientes pasos:



- "Planificar el emparejamiento de clústeres y volúmenes para la replicación en tiempo real."
- "Agrupaciones de pares para replicación"
- "Volúmenes de pares"
- "Validar la replicación de volumen"
- "Eliminar una relación de volumen después de la replicación"
- "Gestionar las relaciones de volumen"

Planificar el emparejamiento de clústeres y volúmenes para la replicación en tiempo real.

La replicación remota en tiempo real requiere que se emparejen dos clústeres de almacenamiento que ejecuten el software Element, se emparejen los volúmenes en cada clúster y se valide la replicación. Una vez finalizada la replicación, debe eliminar la relación de volumen.

Lo que necesitarás

- Debe tener privilegios de administrador de clúster en uno o ambos clústeres que se están emparejando.
- Todas las direcciones IP de los nodos en las redes de administración y almacenamiento para clústeres emparejados están enrutadas entre sí.
- La MTU de todos los nodos emparejados debe ser la misma y debe ser compatible de extremo a extremo entre los clústeres.
- Ambos clústeres de almacenamiento deben tener nombres de clúster únicos, MVIP, SVIP y direcciones IP de todos los nodos.
- La diferencia entre las versiones del software Element en los clústeres no es mayor que una versión principal. Si la diferencia es mayor, uno de los clústeres debe actualizarse para realizar la replicación de datos.



NetApp no ha certificado los dispositivos WAN Accelerator para su uso en la replicación de datos. Estos dispositivos pueden interferir con la compresión y la deduplicación si se implementan entre dos clústeres que replican datos. Asegúrese de evaluar completamente los efectos de cualquier dispositivo WAN Accelerator antes de implementarlo en un entorno de producción.

Encuentra más información

- [Agrupaciones de pares para replicación](#)
- [Volúmenes de pares](#)
- [Asignar una fuente y un destino de replicación a los volúmenes emparejados.](#)

Agrupaciones de pares para replicación

Agrupaciones de pares para replicación

Como primer paso para utilizar la funcionalidad de replicación en tiempo real, debe emparejar dos clústeres. Después de emparejar y conectar dos clústeres, puede configurar los volúmenes activos de un clúster para que se repliquen continuamente en un segundo clúster, lo que proporciona protección continua de datos (CDP).

Lo que necesitarás

- Debe tener privilegios de administrador de clúster en uno o ambos clústeres que se están emparejando.
- Todas las MIP y SIP de los nodos están enrutadas 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 direcciones IP de todos los nodos.
- La diferencia entre las versiones del software Element en los clústeres no es mayor que una versión

principal. Si la diferencia es mayor, uno de los clústeres debe actualizarse para realizar la replicación de datos.



El emparejamiento de clústeres requiere conectividad completa entre los nodos de la red de gestión. La replicación requiere conectividad entre los nodos individuales de la red del clúster de almacenamiento.

Puedes emparejar un clúster con hasta cuatro clústeres más para replicar volúmenes. También puedes emparejar clústeres dentro del grupo de clústeres entre sí.

Emparejar clústeres usando MVIP o una clave de emparejamiento

Puede emparejar un clúster de origen y un clúster de destino utilizando el MVIP del clúster de destino si existe acceso de administrador de clúster a ambos clústeres. Si el acceso de administrador de clúster solo está disponible en uno de los clústeres de un par, se puede utilizar una clave de emparejamiento en el clúster de destino para completar el emparejamiento del clúster.

1. Seleccione uno de los siguientes métodos para emparejar clústeres:
 - **"Agrupamiento de pares mediante MVIP"** Utilice este método si existe acceso de administrador de clúster a ambos clústeres. Este método utiliza el MVIP del clúster remoto para emparejar dos clústeres.
 - **"Agrupar grupos mediante una clave de emparejamiento"** Utilice este método si solo uno de los clústeres tiene acceso de administrador. Este método genera una clave de emparejamiento que se puede utilizar en el clúster de destino para completar el emparejamiento del clúster.

Encuentra más información

[Requisitos del puerto de red](#)

Agrupamiento de pares mediante MVIP

Puede emparejar dos clústeres para la replicación en tiempo real utilizando el MVIP de un clúster para establecer una conexión con el otro clúster. Para utilizar este método se requiere acceso de administrador de clúster en ambos clústeres. El nombre de usuario y la contraseña del administrador del clúster se utilizan para autenticar el acceso al clúster antes de que los clústeres puedan emparejarse.

1. En el clúster local, seleccione **Protección de datos > Pares de clústeres**.
2. Haga clic en **Par de clústeres**.
3. Haga clic en **Iniciar emparejamiento** y haga clic en **Sí** para indicar que tiene acceso al clúster remoto.
4. Introduzca la dirección MVIP del clúster remoto.
5. Haga clic en **Completar el emparejamiento en el clúster remoto**.

En la ventana **Autenticación requerida**, ingrese 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 **Par de clústeres**.
8. Haga clic en **Completar emparejamiento**.

9. Haz clic en el botón **Completar emparejamiento**.

Encuentra más información

- [Agrupar grupos mediante una clave de emparejamiento](#)
- ["Emparejamiento de clústeres mediante MVIP \(vídeo\)"](#)

Agrupar grupos mediante una clave de emparejamiento

Si tiene acceso de administrador de clúster a un clúster local pero no al clúster remoto, puede emparejar los clústeres utilizando una clave de emparejamiento. Se genera una clave de emparejamiento en un clúster local y luego se envía de forma segura a un administrador de clúster en un sitio remoto para establecer una conexión y completar el emparejamiento del clúster para la replicación en tiempo real.

1. En el clúster local, seleccione **Protección de datos > Pares de clústeres**.
2. Haga clic en **Par de clústeres**.
3. Haga clic en **Iniciar emparejamiento** y haga clic en **No** para indicar que no tiene acceso al clúster remoto.
4. Haz clic en **Generar clave**.



Esta acción genera una clave de texto para el emparejamiento y crea un par de clúster no configurado en el clúster local. Si no completa el procedimiento, deberá eliminar manualmente el par de clústeres.

5. Copie la clave de emparejamiento del clúster al portapapeles.
6. Proporcione la clave de emparejamiento al administrador del clúster en el sitio remoto del clúster.



La clave de emparejamiento del clúster contiene una versión de MVIP, nombre de usuario, contraseña e información de la base de datos para permitir conexiones de volumen para la replicación remota. Esta clave debe tratarse de forma segura y no almacenarse de manera que permita el acceso accidental o no seguro al nombre de usuario o la contraseña.



No modifique ninguno de los caracteres de la clave de emparejamiento. La clave pierde validez si se modifica.

7. En el clúster remoto, seleccione **Protección de datos > Pares de clústeres**.
8. Haga clic en **Par de clústeres**.
9. Haga clic en **Completar emparejamiento** e ingrese la clave de emparejamiento en el campo **Clave de emparejamiento** (se recomienda pegar).
10. Haga clic en **Completar emparejamiento**.

Encuentra más información

- [Agrupamiento de pares mediante MVIP](#)
- ["Emparejamiento de clústeres mediante una clave de emparejamiento de clústeres \(vídeo\)"](#)

Validar la conexión del par de clústeres

Una vez completado el emparejamiento de clústeres, es posible que desee verificar la conexión del par de clústeres para garantizar el éxito de la replicación.

1. En el clúster local, seleccione **Protección de datos > Pares de clústeres**.
2. En la ventana **Pares de clústeres**, verifique que el par de clústeres esté conectado.
3. **Opcional:** Vuelva al clúster local y a la ventana **Pares de clústeres** y verifique que el par de clústeres esté conectado.

Volúmenes de pares

Volúmenes de pares

Una vez que haya establecido una conexión entre clústeres en un par de clústeres, puede emparejar un volumen de un clúster con un volumen del otro clúster del par. Cuando se establece una relación de emparejamiento de volúmenes, debe identificar cuál es el volumen de destino de la replicación.

Puede emparejar dos volúmenes para la replicación en tiempo real que estén almacenados en diferentes clústeres de almacenamiento en un par de clústeres conectados. Después de emparejar dos clústeres, puede configurar los volúmenes activos de un clúster para que se repliquen continuamente en un segundo clúster, lo que proporciona protección continua de datos (CDP). También puede asignar cualquiera de los volúmenes como origen o destino de la replicación.

Las relaciones de volumen son siempre uno a uno. Una vez que un volumen forma parte de un emparejamiento con un volumen en otro clúster, no se puede volver a emparejar con ningún otro volumen.

Lo que necesitarás

- Has establecido una conexión entre clústeres en un par de clústeres.
- Usted tiene privilegios de administrador de clúster en uno o ambos clústeres que están emparejados.

Pasos

1. [Cree un volumen de destino con acceso de lectura o escritura.](#)
2. [Empareje los volúmenes utilizando un ID de volumen o una clave de emparejamiento.](#)
3. [Asignar una fuente y un destino de replicación a los volúmenes emparejados.](#)

Cree un volumen de destino con acceso de lectura o escritura.

El proceso de replicación involucra dos puntos finales: el volumen de origen y el volumen de destino. Al crear el volumen de destino, este se configura automáticamente en modo de lectura/escritura para aceptar los datos durante la replicación.

1. Seleccione **Administración > Volúmenes**.
2. Haz clic en **Crear volumen**.
3. En el cuadro de diálogo Crear un nuevo volumen, introduzca el nombre del volumen.
4. Ingrese el tamaño total del volumen, seleccione un tamaño de bloque para el volumen y seleccione la cuenta que debe tener acceso al volumen.

5. Haz clic en **Crear volumen**.
6. En la ventana Activa, haga clic en el icono Acciones del volumen.
7. Haga clic en **Editar**.
8. Cambie el nivel de acceso de la cuenta a Destino de replicación.
9. Haz clic en **Guardar cambios**.

Empareje los volúmenes utilizando un ID de volumen o una clave de emparejamiento.

Emparejar volúmenes utilizando un ID de volumen

Puede emparejar un volumen con otro volumen en un clúster remoto si tiene acceso de administrador de clúster a ambos clústeres en los que se van a emparejar los volúmenes. Este método utiliza el ID del volumen en el clúster remoto para iniciar una conexión.

Lo que necesitarás

- Asegúrese de que los clústeres que contienen los volúmenes estén emparejados.
- Cree un nuevo volumen en el clúster remoto.



Puede asignar un origen y un destino de replicación después del proceso de emparejamiento. Una fuente o destino de replicación puede ser cualquiera de los volúmenes de un par de volúmenes. Debe crear un volumen de destino que no contenga datos y tenga las características exactas del volumen de origen, como el tamaño, la configuración del tamaño de bloque para los volúmenes (ya sea 512e o 4k) y la configuración de QoS. Si asigna un volumen existente como destino de replicación, los datos de ese volumen se sobrescribirán. El volumen objetivo puede ser mayor o igual en tamaño que el volumen de origen, pero no puede ser menor.

- Conozca el ID del volumen de destino.

Pasos

1. Seleccione **Administración > Volúmenes**.
2. Haz clic en el icono **Acciones** del volumen que desees emparejar.
3. Haga clic en **Emparejar**.
4. En el cuadro de diálogo **Emparejar volumen**, seleccione **Iniciar emparejamiento**.
5. Seleccione **Sí** para indicar que tiene acceso al clúster remoto.
6. Seleccione un **Modo de replicación** de la lista:
 - **Tiempo real (asíncrono)**: Las escrituras se confirman al cliente después de que se hayan confirmado en el clúster de origen.
 - **En tiempo real (síncrono)**: Las escrituras se confirman al cliente después de que se hayan confirmado tanto en el clúster de origen como en el de destino.
 - **Solo instantáneas**: Solo se replican las instantáneas creadas en el clúster de origen. Las escrituras activas desde el volumen de origen no se replican.
7. Seleccione un clúster remoto de la lista.
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 Element del clúster remoto. Es posible que se le solicite iniciar sesión en el clúster remoto con las credenciales de administrador del clúster.

10. En la interfaz de usuario de Element del clúster remoto, seleccione **Completar emparejamiento**.

11. Confirme los detalles en **Confirmar emparejamiento de volumen**.

12. Haga clic en **Completar emparejamiento**.

Una vez confirmado el emparejamiento, los dos grupos inician 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**. El par de pantallas de volumen PausedMisconfigured hasta que se asignen el origen y el destino del par de volúmenes.

Una vez completado correctamente el emparejamiento, se recomienda actualizar la tabla Volúmenes para eliminar la opción **Emparejar** de la lista **Acciones** del volumen emparejado. Si no actualiza la tabla, la opción **Par** seguirá disponible para su selección. Si vuelve a seleccionar la opción **Emparejar**, se abrirá una nueva pestaña y, dado que el volumen ya está emparejado, el sistema informará de un StartVolumePairing Failed: xVolumeAlreadyPaired Mensaje de error en la ventana **Emparejar volumen** de la página de la interfaz de usuario de Element.

Encuentra más información

- [Mensajes de emparejamiento de volumen](#)
- [Advertencias de emparejamiento de volumen](#)
- [Asignar una fuente y un destino de replicación a los volúmenes emparejados.](#)

Emparejar volúmenes mediante una clave de emparejamiento

Si solo tiene acceso de administrador de clúster al clúster de origen (no tiene credenciales de administrador de clúster para un clúster remoto), puede emparejar un volumen con otro volumen en un clúster remoto mediante una clave de emparejamiento.

Lo que necesitarás

- Asegúrese de que los clústeres que contienen los volúmenes estén emparejados.
- Asegúrese de que exista un volumen en el clúster remoto para utilizarlo para el emparejamiento.



Puede asignar un origen y un destino de replicación después del proceso de emparejamiento. Una fuente o destino de replicación puede ser cualquiera de los volúmenes de un par de volúmenes. Debe crear un volumen de destino que no contenga datos y tenga las características exactas del volumen de origen, como el tamaño, la configuración del tamaño de bloque para los volúmenes (ya sea 512e o 4k) y la configuración de QoS. Si asigna un volumen existente como destino de replicación, los datos de ese volumen se sobrescribirán. El volumen objetivo puede ser mayor o igual en tamaño que el volumen de origen, pero no puede ser menor.

Pasos

1. Seleccione **Administración > Volúmenes**.

2. Haz clic en el icono **Acciones** del volumen que quieras emparejar.
3. Haga clic en **Emparejar**.
4. En el cuadro de diálogo **Emparejar volumen**, seleccione **Iniciar emparejamiento**.
5. Seleccione **No tengo** para indicar que no tiene acceso al clúster remoto.
6. Seleccione un **Modo de replicación** de la lista:
 - **Tiempo real (asíncrono)**: Las escrituras se confirman al cliente después de que se hayan confirmado en el clúster de origen.
 - **En tiempo real (síncrono)**: Las escrituras se confirman al cliente después de que se hayan confirmado tanto en el clúster de origen como en el de destino.
 - **Solo instantáneas**: Solo se replican las instantáneas creadas en el clúster de origen. Las escrituras activas desde el volumen de origen no se replican.
7. Haz clic en **Generar clave**.



Esta acción genera una clave de texto para el emparejamiento y crea un par de volúmenes no configurados en el clúster local. Si no completa el procedimiento, deberá eliminar manualmente el par de volúmenes.

8. Copia la clave de emparejamiento al portapapeles de tu ordenador.
9. Proporcione la clave de emparejamiento al administrador del clúster en el sitio del clúster remoto.



La clave de emparejamiento de volumen debe tratarse de forma segura y no utilizarse de manera que permita un acceso accidental o no seguro.



No modifique ninguno de los caracteres de la clave de emparejamiento. La clave pierde validez si se modifica.

10. En la interfaz de usuario de Element del clúster remoto, seleccione **Administración > Volúmenes**.
11. Haz clic en el icono de Acciones del volumen que desees emparejar.
12. Haga clic en **Emparejar**.
13. En el cuadro de diálogo **Emparejar volumen**, seleccione **Completar emparejamiento**.
14. Pegue la clave de emparejamiento del otro grupo en el cuadro **Clave de emparejamiento**.
15. Haga clic en **Completar emparejamiento**.

Una vez confirmado el emparejamiento, los dos grupos inician 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**. El par de pantallas de volumen PausedMisconfigured hasta que se asignen el origen y el destino del par de volúmenes.

Una vez completado correctamente el emparejamiento, se recomienda actualizar la tabla Volúmenes para eliminar la opción **Emparejar** de la lista **Acciones** del volumen emparejado. Si no actualiza la tabla, la opción **Par** seguirá disponible para su selección. Si vuelve a seleccionar la opción **Emparejar**, se abrirá una nueva pestaña y, dado que el volumen ya está emparejado, el sistema informará de un StartVolumePairing Failed: xVolumeAlreadyPaired Mensaje de error en la ventana **Emparejar volumen** de la página de la interfaz de usuario de Element.

Encuentra más información

- [Mensajes de emparejamiento de volumen](#)
- [Advertencias de emparejamiento de volumen](#)
- [Asignar una fuente y un destino de replicación a los volúmenes emparejados.](#)

Asignar una fuente y un destino de replicación a los volúmenes emparejados.

Una vez emparejados los volúmenes, debe asignar un volumen de origen y su volumen de destino de replicación. Una fuente o destino de replicación puede ser cualquiera de los volúmenes de un par de volúmenes. También puede utilizar este procedimiento para redirigir los datos enviados a un volumen de origen a un volumen de destino remoto en caso de que el volumen de origen deje de estar disponible.

Lo que necesitarás

Tienes acceso a los clústeres que contienen los volúmenes de origen y destino.

Pasos

1. Prepare el volumen fuente:

- Desde el clúster que contiene el volumen que desea asignar como origen, seleccione **Administración > Volúmenes**.
- Haz clic en el icono **Acciones** del volumen que deseas asignar como fuente y haz clic en **Editar**.
- En la lista desplegable **Acceso**, seleccione **Lectura/Escritura**.



Si está invirtiendo la asignación de origen y destino, esta acción hará que el par de volúmenes muestre el siguiente mensaje hasta que se asigne un nuevo destino de replicación: `PausedMisconfigured`

Cambiar el acceso pausa la replicación del volumen y provoca que se detenga la transmisión de datos. Asegúrese de haber coordinado estos cambios en ambos sitios.

- Haz clic en **Guardar cambios**.

2. Prepare el volumen objetivo:

- Desde el clúster que contiene el volumen que desea asignar como destino, seleccione **Administración > Volúmenes**.
- Haz clic en el icono **Acciones** del volumen que deseas asignar como destino y haz clic en **Editar**.
- En la lista desplegable **Acceso**, seleccione **Destino de replicación**.



Si asigna un volumen existente como destino de replicación, los datos de ese volumen se sobrescribirán. Debe utilizar un nuevo volumen de destino que no contenga datos y tenga las características exactas del volumen de origen, como el tamaño, la configuración 512e y la configuración QoS. El volumen objetivo puede ser mayor o igual en tamaño que el volumen de origen, pero no puede ser menor.

- Haz clic en **Guardar cambios**.

Encuentra más información

- [Emparejar volúmenes utilizando un ID de volumen](#)
- [Emparejar volúmenes mediante una clave de emparejamiento](#)

Validar la replicación de volumen

Después de replicar un volumen, debe asegurarse de que los volúmenes de origen y destino estén activos. Cuando se encuentra en estado activo, los volúmenes están emparejados, los datos se envían desde el volumen de origen al volumen de destino y los datos están sincronizados.

1. Desde ambos clústeres, seleccione **Protección de datos > Pares de volúmenes**.
2. Verifique que el estado del volumen sea Activo.

Encuentra más información

[Advertencias de emparejamiento de volumen](#)

Eliminar una relación de volumen después de la replicación

Una vez completada la replicación y cuando ya no necesite la relación de pares de volúmenes, puede eliminar dicha relación.

1. Seleccione **Protección de datos > Pares de volúmenes**.
2. Haz clic en el icono **Acciones** del par de volúmenes que deseas eliminar.
3. Haga clic en **Eliminar**.
4. Confirma el mensaje.

Gestionar las relaciones de volumen

Pausar la replicación

Puede pausar manualmente la replicación si necesita detener el procesamiento de E/S durante un corto período de tiempo. Puede que desee pausar la replicación si hay un aumento repentino en el procesamiento de E/S y desea reducir la carga de procesamiento.

1. Seleccione **Protección de datos > Pares de volúmenes**.
2. Haz clic en el icono de Acciones para el par de volúmenes.
3. Haga clic en **Editar**.
4. En el panel **Editar par de volúmenes**, pause manualmente el proceso de replicación.



Pausar o reanudar manualmente la replicación de volúmenes provoca que la transmisión de datos se detenga o se reanude. Asegúrese de haber coordinado estos cambios en ambos sitios.

5. Haz clic en **Guardar cambios**.

Cambiar el modo de replicación

Puede editar las propiedades del par de volúmenes para cambiar el modo de replicación de la relación del par de volúmenes.

1. Seleccione **Protección de datos > Pares de volúmenes**.
2. Haz clic en el icono de Acciones para el par 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 confirman al cliente después de que se hayan confirmado en el clúster de origen.
 - **En tiempo real (síncrono)**: Las escrituras se confirman al cliente después de que se hayan confirmado tanto en el clúster de origen como en el de destino.
 - **Solo instantáneas**: Solo se replican las instantáneas creadas en el clúster de origen. Las escrituras activas desde el volumen de origen no se replican. **Atención**: Cambiar el modo de replicación cambia el modo inmediatamente. Asegúrese de haber coordinado estos cambios en ambos sitios.
5. Haz clic en **Guardar cambios**.

Eliminar pares de volúmenes

Puede eliminar un par de volúmenes si desea eliminar la asociación entre dos volúmenes.

1. Seleccione **Protección de datos > Pares de volúmenes**.
2. Haz clic en el icono Acciones del par de volúmenes que deseas eliminar.
3. Haga clic en **Eliminar**.
4. Confirma el mensaje.

Eliminar un par de clústeres

Puedes eliminar un par de clústeres desde la interfaz de usuario de Element de cualquiera de los clústeres del par.

1. Haz clic en **Protección de datos > Pares de clústeres**.
2. Haz clic en el icono de Acciones para un par de clústeres.
3. En el menú que aparece, haga clic en **Eliminar**.
4. Confirma la acción.
5. Repita los pasos desde el segundo clúster en el emparejamiento de clústeres.

Detalles del par de clústeres

La página Pares de clústeres en la pestaña Protección de datos proporciona información sobre los clústeres que se han emparejado o que están en proceso de emparejamiento. El sistema muestra mensajes de emparejamiento y progreso en la columna de Estado.

• IDENTIFICACIÓN

Se asigna un ID generado por el sistema a cada par de clústeres.

- **Nombre del clúster remoto**

El nombre del otro grupo del par.

- **MVIP remoto**

La dirección IP virtual de gestión del otro clúster del par.

- **Estado**

Estado de replicación del clúster remoto

- **Replicación de volúmenes**

El número de volúmenes contenidos en el clúster que están emparejados para la replicación.

- **UUID**

Se asigna un identificador único a cada clúster del par.

pares de volumen

Detalles del par de volúmenes

La página "Pares de volúmenes" en la pestaña "Protección de datos" proporciona información sobre los volúmenes que se han emparejado o que están en proceso de emparejamiento. El sistema muestra mensajes de emparejamiento y progreso en la columna Estado del volumen.

- **IDENTIFICACIÓN**

Identificador generado por el sistema para el volumen.

- **Nombre**

El nombre que se le dio al volumen cuando fue creado. Los nombres de volumen pueden tener hasta 223 caracteres y contener az, 0-9 y guion (-).

- **Cuenta**

Nombre de la cuenta asignada al volumen.

- **Estado del volumen**

Estado de replicación del volumen

- **Estado de la instantánea**

Estado del volumen de instantáneas.

- **Modo**

Método de replicación de escritura del cliente. Los valores posibles son los siguientes:

- Asíncrono
- Solo instantánea
- Sincronizar

- **Dirección**

La dirección de los datos de volumen:

- Icono de volumen de origen (→) indica que se están escribiendo datos en un destino fuera del clúster.
- Icono de volumen objetivo (←) indica que se están escribiendo datos en el volumen local desde una fuente externa.

- **Retardo asíncrono**

Tiempo transcurrido desde la última sincronización del volumen con el clúster remoto. Si el volumen no está emparejado, el valor es nulo.

- **Clúster remoto**

Nombre del clúster remoto en el que reside el volumen.

- **ID de volumen remoto**

Identificador del volumen en el clúster remoto.

- **Nombre del volumen remoto**

Nombre asignado al volumen remoto cuando se creó.

Mensajes de emparejamiento de volumen

Puede ver los mensajes de emparejamiento de volúmenes durante el proceso de emparejamiento inicial en la página "Pares de volúmenes" que se encuentra en la pestaña "Protección de datos". Estos mensajes pueden mostrarse tanto en el extremo de origen como en el de destino del par en la vista de lista de volúmenes replicados.

- **PausadoDesconectado**

Se agotó el tiempo de espera de las RPC de replicación de origen o de sincronización. Se ha perdido la conexión con el clúster remoto. Compruebe las conexiones de red al clúster.

- **Reanudando conexión**

La sincronización de replicación remota ya está activa. Iniciando el proceso de sincronización y esperando datos.

- **Reanudando RRSync**

Se está realizando una copia helicoidal única de los metadatos del volumen en el clúster emparejado.

- **Reanudando LocalSync**

Se está realizando una copia de doble hélice de los metadatos del volumen en el clúster emparejado.

- **Reanudando la transferencia de datos**

Se ha reanudado 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 está produciendo ninguna actividad de replicación.

Advertencias de emparejamiento de volumen

La página "Pares de volúmenes" en la pestaña "Protección de datos" muestra estos mensajes después de emparejar volúmenes. Estos mensajes pueden mostrarse tanto en el extremo de origen como en el de destino del par (a menos que se indique lo contrario) en la vista de lista de volúmenes replicados.

- **ClústerCompleto en Pausa**

Debido a que el clúster de destino está lleno, la replicación de origen y la transferencia masiva de datos no pueden continuar. El mensaje se muestra únicamente en el extremo de origen del par.

- **Pausa superada el número máximo de instantáneas**

El volumen de destino ya tiene el número máximo de instantáneas y no puede replicar instantáneas adicionales.

- **Pausa manual**

El volumen local se ha pausado manualmente. Debe reanudarse antes de que se reanude la replicación.

- **Control remoto manual en pausa**

El volumen remoto está en modo de pausa manual. Se requiere intervención manual para reanudar la replicación del volumen remoto.

- **PausadoDesconfigurado**

Esperando una fuente y un objetivo activos. Se requiere intervención manual para reanudar la replicación.

- **QoS en pausa**

La QoS objetivo no pudo soportar la E/S entrante. La replicación se reanuda automáticamente. El mensaje se muestra únicamente en el extremo de origen del par.

- **Enlace lento en pausa**

Se detectó un enlace lento y se detuvo la replicación. La replicación se reanuda automáticamente. El mensaje se muestra únicamente en el extremo de origen del par.

- **Desajuste en el tamaño del volumen en pausa**

El volumen de destino no tiene el mismo tamaño que el volumen de origen.

- **PausadoXCOPY**

Se está enviando un comando SCSI XCOPY a un volumen de origen. El comando debe completarse antes de que se pueda reanudar la replicación. El mensaje se muestra únicamente en el extremo de origen del par.

- **Detenido por mala configuración**

Se ha detectado un error de configuración permanente. El volumen remoto se ha borrado o desvinculado. No es posible ninguna acción correctiva; debe establecerse un nuevo emparejamiento.

Utilice la replicación SnapMirror entre los clústeres Element y ONTAP (interfaz de usuario de Element).

Utilice la replicación SnapMirror entre los clústeres Element y ONTAP (interfaz de usuario de Element).

Puede crear relaciones SnapMirror desde la pestaña Protección de datos en la interfaz de usuario de NetApp Element . Para ver esto en la interfaz de usuario, debe estar habilitada la funcionalidad SnapMirror .

IPv6 no es compatible con la replicación SnapMirror entre el software NetApp Element y los clústeres ONTAP .

["Vídeo de NetApp : SnapMirror para NetApp HCI y Element Software"](#)

Los sistemas que ejecutan el software NetApp Element admiten la funcionalidad SnapMirror para copiar y restaurar copias de instantáneas con sistemas NetApp ONTAP . La razón principal para utilizar esta tecnología es la recuperación ante desastres de NetApp HCI a ONTAP. Los puntos de conexión incluyen ONTAP, ONTAP Select y Cloud Volumes ONTAP. Consulte TR-4641 Protección de datos NetApp HCI .

["Informe técnico 4641 de NetApp : Protección de datos NetApp HCI"](#)

Encuentra más información

- ["Creación de su estructura de datos con NetApp HCI, ONTAP e infraestructura convergente"](#)
- ["Replicación entre NetApp Element Software y ONTAP \(CLI de ONTAP \)"](#)

Descripción general de SnapMirror

Los sistemas que ejecutan el software NetApp Element admiten la funcionalidad SnapMirror para copiar y restaurar instantáneas con sistemas NetApp ONTAP .

Los sistemas que ejecutan Element pueden comunicarse directamente con SnapMirror en sistemas ONTAP 9.3 o superiores. La API de NetApp Element proporciona métodos para habilitar la funcionalidad SnapMirror en clústeres, volúmenes e instantáneas. Además, la interfaz de usuario de Element incluye todas las funcionalidades necesarias para gestionar las relaciones SnapMirror entre el software Element y los sistemas ONTAP .

En casos de uso específicos, puede replicar volúmenes originados en ONTAP a volúmenes de Element con funcionalidad limitada. Para obtener más información, consulte ["Replicación entre el software Element y ONTAP \(ONTAP CLI\)"](#).

Habilite SnapMirror en el clúster.

Debe habilitar manualmente la funcionalidad SnapMirror a nivel de clúster a través de la interfaz de usuario de NetApp Element . El sistema viene con la funcionalidad SnapMirror desactivada por defecto, y no se activa automáticamente como parte de una nueva instalación o actualización. Habilitar la función SnapMirror es una tarea de configuración que se realiza una sola vez.

SnapMirror solo se puede habilitar para clústeres que ejecutan el software Element utilizado junto con volúmenes en un sistema NetApp ONTAP . Solo debe habilitar la funcionalidad SnapMirror si su clúster está conectado para su uso con volúmenes NetApp ONTAP .

Lo que necesitarás

El clúster de almacenamiento debe estar ejecutando el software NetApp Element .

Pasos

1. Haz clic en **Clústeres > Configuración**.
2. Encuentre la configuración específica del clúster para SnapMirror.
3. Haz clic en **Habilitar SnapMirror**.



Habilitar la funcionalidad SnapMirror modifica permanentemente la configuración del software Element. Solo puede desactivar la función SnapMirror y restaurar la configuración predeterminada devolviendo el clúster a la imagen de fábrica.

4. Haga clic en **Sí** para confirmar el cambio de configuración de SnapMirror .

Habilita 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 ONTAP específicos. Este es un permiso del administrador del clúster que ejecuta el software NetApp Element para que SnapMirror controle un volumen.

Lo que necesitarás

- Has habilitado SnapMirror en la interfaz de usuario de Element para el clúster.
- Hay disponible un punto de conexión SnapMirror .
- El volumen debe tener un tamaño de bloque de 512e.
- El volumen no participa en la replicación remota.
- El tipo de acceso al volumen no es Destino de replicación.



También puede configurar esta propiedad al crear o clonar un volumen.

Pasos

1. Haz clic en **Administración > Volúmenes**.
2. Haz clic en el icono **Acciones** del volumen para el que quieras habilitar SnapMirror .
3. En el menú que aparece, seleccione **Editar**.

4. En el cuadro de diálogo **Editar volumen**, seleccione la casilla de verificación **Habilitar SnapMirror**.
5. Haz clic en **Guardar cambios**.

Crea un punto de conexión de SnapMirror

Debe crear un punto de conexión SnapMirror en la interfaz de usuario de NetApp Element antes de poder crear una relación.

Un punto de conexión SnapMirror es un clúster ONTAP que sirve como destino de replicación para un clúster que ejecuta el software Element. Antes de crear una relación SnapMirror, primero debe crear un punto de conexión SnapMirror.

Puede crear y administrar hasta cuatro puntos de conexión SnapMirror en un clúster de almacenamiento que ejecute el software Element.



Si un punto de conexión existente se creó originalmente utilizando la API y no se guardaron las credenciales, puede ver el punto de conexión en la interfaz de usuario de Element y verificar su existencia, pero no se puede administrar mediante la interfaz de usuario de Element. Este punto de conexión solo se puede gestionar mediante la API de Element.

Para obtener más detalles sobre los métodos de la API, consulte ["Gestiona el almacenamiento con la API de Element"](#).

Lo que necesitarás

- Deberías haber habilitado SnapMirror en la interfaz de usuario de Element para el clúster de almacenamiento.
- Conoces las credenciales ONTAP para el punto final.

Pasos

1. Haga clic en **Protección de datos** > *Puntos de conexión de SnapMirror*.
2. Haz clic en **Crear punto de conexión**.
3. En el cuadro de diálogo **Crear un nuevo punto de conexión**, introduzca la dirección IP de administración del clúster del sistema ONTAP.
4. Introduzca las credenciales de administrador de ONTAP asociadas al punto de conexión.
5. Revisar detalles adicionales:
 - LIFs: Enumera las interfaces lógicas intercluster de ONTAP utilizadas para comunicarse con Element.
 - Estado: Muestra el estado actual del punto de conexión de SnapMirror. Los valores posibles son: conectado, desconectado y no administrado.
6. Haz clic en **Crear punto de conexión**.

Crear una relación SnapMirror

Debe crear una relación SnapMirror en la interfaz de usuario de NetApp Element.



Cuando un volumen aún no está habilitado para SnapMirror y usted selecciona crear una relación desde la interfaz de usuario de Element, SnapMirror se habilita automáticamente en ese volumen.

Lo que necesitarás

SnapMirror está habilitado en el volumen.

Pasos

1. Haz clic en **Administración > Volúmenes**.
2. Haga clic en el icono **Acciones** del volumen que formará parte de la relación.
3. Haga clic en ***Crear una relación SnapMirror ***.
4. En el cuadro de diálogo **Crear una relación SnapMirror ***, **seleccione un punto de conexión de la lista *Punto de conexión**.
5. Seleccione si la relación se creará utilizando un volumen ONTAP nuevo o un volumen ONTAP existente.
6. Para crear un nuevo volumen ONTAP en la interfaz de usuario de Element, haga clic en **Crear nuevo volumen**.
 - a. Seleccione la **Máquina Virtual de Almacenamiento** para esta relación.
 - b. Seleccione **Agregado** de la lista desplegable.
 - c. En el campo **Sufijo del nombre del volumen**, introduzca un sufijo.



El sistema detecta el nombre del volumen de origen y lo copia al campo **Nombre del volumen**. El sufijo que introduzcas añadirá un elemento al nombre.

- d. Haga clic en **Crear volumen de destino**.
7. Para utilizar un volumen ONTAP existente, haga clic en **Usar volumen existente**.
 - a. Seleccione la **Máquina Virtual de Almacenamiento** 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 póliza. Si la política seleccionada tiene reglas de retención, la tabla de reglas muestra las reglas y las etiquetas asociadas.
 9. **Opcional:** Seleccione un horario.

Esto determina con qué frecuencia la relación crea copias.
 10. **Opcional:** En el campo **Limitar ancho de banda a**, ingrese la cantidad máxima de ancho de banda que pueden consumir las transferencias de datos asociadas con esta relación.
 11. Revisar detalles adicionales:
 - **Estado:** Estado actual de la relación del volumen de destino. Los valores posibles son:
 - no inicializado: El volumen de destino no se ha inicializado.
 - snapmirrored: El volumen de destino se ha inicializado y está listo para recibir actualizaciones de SnapMirror.
 - volumen interrumpido: El volumen de destino es de lectura/escritura y existen instantáneas.
 - **Estado:** Estado actual de la relación. Los valores posibles son: inactivo, transfiriendo, comprobando, en reposo, en reposo, en cola, preparando, finalizando, abortando y rompiendo.
 - **Tiempo de retardo:** Cantidad de tiempo en segundos que el sistema de destino se retrasa con respecto al sistema de origen. El tiempo de demora no debe ser mayor que el intervalo del programa de transferencia.
 - **Límite de ancho de banda:** La cantidad máxima de ancho de banda que pueden consumir las transferencias de datos asociadas con esta relación.

- **Última transferencia:** Marca de tiempo de la última instantánea transferida. Haz clic para obtener más información.
- **Nombre de la política:** El nombre de la política ONTAP SnapMirror para la relación.
- **Tipo de política:** Tipo de política ONTAP SnapMirror seleccionada para la relación. Los valores posibles son:
 - espejo asíncrono
 - bóveda_espejo
- **Nombre de la programación:** Nombre de la programación preexistente en el sistema ONTAP seleccionada para esta relación.

12. Para no inicializar en este momento, asegúrese de que la casilla de verificación **Inicializar** no esté seleccionada.



La inicialización puede llevar mucho tiempo. Quizás te convenga ejecutarlo durante las horas de menor tráfico. La inicialización realiza una transferencia básica; crea una copia instantánea del volumen de origen y luego 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 establecida.

13. Haz clic en **Crear relación**.

14. Haz clic en **Protección de datos** > *Relaciones de SnapMirror * para ver esta nueva relación de SnapMirror .

acciones de relación de SnapMirror

Puede configurar una relación desde la página Relaciones de SnapMirror de la pestaña Protección de datos. Aquí se describen las opciones del icono Acciones.

- **Editar:** Modifica la política utilizada o el cronograma para la relación.
- **Eliminar:** Elimina la relación SnapMirror . Esta función no elimina el volumen de destino.
- **Inicializar:** Realiza la primera transferencia inicial de datos de referencia para establecer una nueva relación.
- **Actualización:** Realiza una actualización a petición de la relación, replicando en el destino cualquier dato nuevo y copias de instantáneas incluidas desde la última actualización.
- **Quiesce:** Impide cualquier actualización adicional de una relación.
- **Reanudar:** Reanuda una relación que se encontraba en pausa.
- **Interrupción:** Hace que el volumen de destino sea de lectura y escritura y detiene todas las transferencias actuales y futuras. Compruebe que los clientes no están utilizando el volumen de origen original, ya que la operación de resincronización inversa hace que el volumen de origen original sea de solo lectura.
- **Resincronizar:** Restablece una relación rota en la misma dirección en la que se produjo la ruptura.
- **Resincronización inversa:** Automatiza los pasos necesarios para crear e inicializar una nueva relación en la dirección opuesta. Esto solo puede hacerse si la relación existente está rota. Esta operación no eliminará la relación actual. El volumen de origen original vuelve a la copia Snapshot común más reciente y se resincroniza con el destino. Se perderán todos los cambios realizados en el volumen de origen original desde la última actualización correcta de SnapMirror . Cualquier modificación realizada o nuevos datos escritos en el volumen de destino actual se envían de vuelta al volumen de origen original.

- **Abortar:** Cancela una transferencia en curso. Si se emite una actualización de SnapMirror para una relación interrumpida, la relación continúa con la última transferencia del último punto de control de reinicio que se creó antes de que se produjera la interrupción.

Etiquetas de SnapMirror

Etiquetas de SnapMirror

Una etiqueta SnapMirror sirve como marcador para transferir una instantánea específica de acuerdo con las reglas de retención de la relación.

Al aplicar una etiqueta a una instantánea, esta se marca como objetivo para la replicación de SnapMirror. La función de esta relación es hacer cumplir las reglas durante la transferencia de datos, seleccionando la instantánea etiquetada correspondiente, copiándola al volumen de destino y asegurando que se conserve el número correcto de copias. Se refiere a la política para determinar el número de copias a conservar y el período de retención. La política puede tener cualquier número de reglas y cada regla tiene una etiqueta única. Esta etiqueta sirve de enlace entre la instantánea y la regla de retención.

Es la etiqueta SnapMirror la que indica qué regla se aplica a la instantánea, instantánea de grupo o programación seleccionada.

Agregar etiquetas de SnapMirror a las instantáneas

Las etiquetas de SnapMirror especifican la política de retención de instantáneas en el punto final de SnapMirror. Puedes añadir etiquetas a las instantáneas y agrupar instantáneas.

Puede ver las etiquetas disponibles desde un cuadro de diálogo de relación SnapMirror existente o desde NetApp ONTAP System Manager.



Al agregar una etiqueta a una instantánea de grupo, se sobrescriben las etiquetas existentes en las instantáneas individuales.

Lo que necesitarás

- SnapMirror está habilitado en el clúster.
- La etiqueta que desea agregar ya existe en ONTAP.

Pasos

1. Haz clic en **Protección de datos > Instantáneas** o en la página **Instantáneas de grupo**.
2. Haga clic en el icono **Acciones** de la instantánea o instantánea de grupo a la que desea agregar una etiqueta de SnapMirror.
3. En el cuadro de diálogo **Editar instantánea**, introduzca el texto en el campo ***Etiqueta de SnapMirror ***. La etiqueta debe coincidir con una etiqueta de regla en la política aplicada a la relación SnapMirror.
4. Haz clic en **Guardar cambios**.

Agregar etiquetas de SnapMirror a las programaciones de instantáneas

Puedes agregar etiquetas SnapMirror a las programaciones de instantáneas para asegurarte de que se aplique una política SnapMirror. Puede ver las etiquetas disponibles desde un cuadro de diálogo de relación SnapMirror existente o desde el

Administrador del sistema NetAppONTAP.

Lo que necesitarás

- SnapMirror debe estar habilitado a nivel de clúster.
- La etiqueta que desea agregar ya existe en ONTAP.

Pasos

1. Haz clic en **Protección de datos > Programaciones**.
2. Agregue una etiqueta de SnapMirror a una programación de una de las siguientes maneras:

Opción	Pasos
Crear un nuevo horario	a. Seleccione Crear horario. b. Introduzca todos los demás datos relevantes. c. Seleccione Crear horario.
Modificar el cronograma existente	a. Haz clic en el icono Acciones del calendario al que quieras añadir una etiqueta y selecciona Editar. b. En el cuadro de diálogo resultante, introduzca el texto en el campo *Etiqueta de SnapMirror *. c. Seleccione Guardar cambios.

Encuentra más información

[Crea un cronograma de instantáneas](#)

Recuperación ante desastres mediante SnapMirror

Recuperación ante desastres mediante SnapMirror

En caso de que se produzca un problema con un volumen o clúster que ejecute el software NetApp Element , utilice la funcionalidad SnapMirror para romper la relación y realizar una conmutación por error al volumen de destino.



Si el clúster original ha fallado por completo o no existe, póngase en contacto con el soporte de NetApp para obtener más ayuda.

Realizar una conmutación por error desde un clúster de Element

Puede realizar una conmutación por error desde el clúster Element para que el volumen de destino sea de lectura/escritura y accesible para los hosts en el lado de destino. Antes de realizar una conmutación por error desde el clúster Element, debe romper la relación SnapMirror .

Utilice la interfaz de usuario de NetApp Element para realizar la conmutación por error. Si la interfaz de usuario de Element no está disponible, también puede usar ONTAP System Manager o ONTAP CLI para ejecutar el comando para romper la relación.

Lo que necesitarás

- Existe una relación SnapMirror y tiene al menos una instantánea válida en el volumen de destino.
- Necesitas realizar una conmutación por error al volumen de destino debido a una interrupción 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. Encuentre la relación con el volumen de origen que desea conmutar por error.
3. Haz clic en el icono **Acciones**.
4. Haga clic en **Interrupción**.
5. Confirma la acción.

El volumen en el clúster de destino ahora tiene acceso de lectura y escritura y se puede montar en los hosts de la aplicación para reanudar las cargas de trabajo de producción. Como resultado de esta acción, se detiene toda la replicación de SnapMirror . La relación muestra un estado de ruptura.

Realizar una recuperación a Element

Aprenda cómo realizar una recuperación ante fallos a Element

Una vez mitigado el problema en el lado primario, debe volver a sincronizar el volumen de origen original y recurrir al software NetApp Element . Los pasos a seguir varían dependiendo de si el volumen de origen original aún existe o si necesita recurrir a un volumen recién creado.

escenarios de recuperación ante fallos de SnapMirror

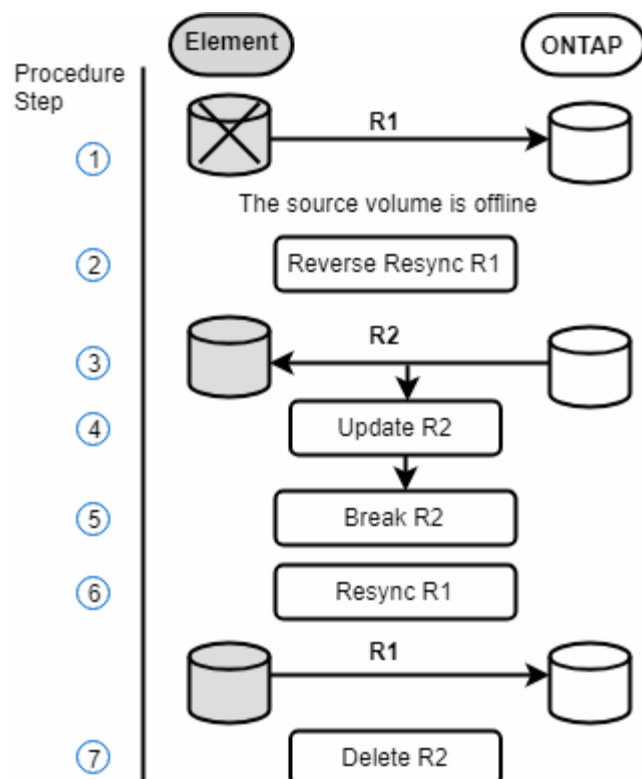
La funcionalidad de recuperación ante desastres de SnapMirror se ilustra en dos escenarios de recuperación tras fallo. Esto presupone que la relación original ha fracasado (se ha roto).

Los pasos de los procedimientos correspondientes se añaden como referencia.

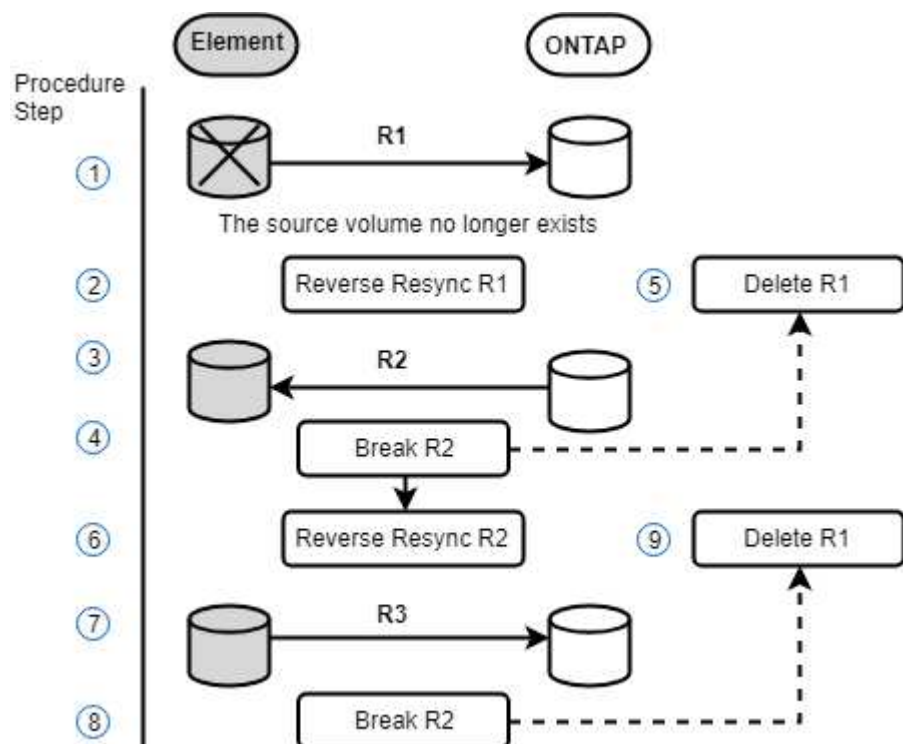


En los ejemplos aquí presentes, R1 = la relación original en la que el clúster que ejecuta el software NetApp Element es el volumen de origen original (Element) y ONTAP es el volumen de destino original (ONTAP). R2 y R3 representan las relaciones inversas creadas a través de la operación de resincronización inversa.

La siguiente imagen muestra el escenario de recuperación ante fallos cuando el volumen de origen aún existe:



La siguiente imagen muestra el escenario de recuperación ante fallos cuando el volumen de origen ya no existe:



Encuentra más información

- Realizar una recuperación tras fallo cuando el volumen de origen aún exista
- Realizar una recuperación tras fallo cuando el volumen de origen ya no exista

- [escenarios de recuperación ante fallos de SnapMirror](#)

Realizar una recuperación tras fallo cuando el volumen de origen aún exista

Puede volver a sincronizar el volumen de origen original y realizar la recuperación tras un fallo utilizando la interfaz de usuario de NetApp Element . Este procedimiento se aplica a escenarios donde el volumen fuente original aún existe.

1. En la interfaz de usuario de Element, busque la relación que rompió para realizar la conmutación por error.
2. Haz clic en el icono Acciones y luego en **Revertir resincronización**.
3. Confirma la acción.



La operación de resincronización inversa crea una nueva relación en la que se invierten las funciones de los volúmenes de origen y destino originales (esto da como resultado dos relaciones, ya que la relación original persiste). Los nuevos datos procedentes del volumen de destino original se transfieren al volumen de origen original como parte de la operación de resincronización inversa. Puede seguir accediendo y escribiendo datos en el volumen activo en el lado de destino, pero deberá desconectar todos los hosts del volumen de origen y realizar una actualización de SnapMirror antes de redirigir de nuevo al primario original.

4. Haz clic en el icono de Acciones de la relación inversa que acabas de crear y haz clic en **Actualizar**.

Una vez completada la resincronización inversa y comprobado 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, puede realizar los siguientes pasos para completar la recuperación ante fallos y reactivar el volumen primario original:

5. Haz clic en el icono de Acciones de la relación inversa y haz clic en **Romper**.
6. Haz clic en el icono Acciones de la relación original y haz clic en **Resincronizar**.



Ahora se puede montar el volumen primario original para reanudar las cargas de trabajo de producción en dicho volumen. La replicación original de SnapMirror se reanuda según la política y la programación configuradas para la relación.

7. Después de confirmar que el estado de la relación original es “snapmirred”, haga clic en el icono de Acciones de la relación inversa y haga clic en **Eliminar**.

Encuentra más información

[escenarios de recuperación ante fallos de SnapMirror](#)

Realizar una recuperación tras fallo cuando el volumen de origen ya no exista

Puede volver a sincronizar el volumen de origen original y realizar la recuperación tras un fallo utilizando la interfaz de usuario de NetApp Element . Esta sección se aplica a escenarios en los que se ha perdido el volumen de origen original, pero el clúster original permanece intacto. Para obtener instrucciones sobre cómo restaurar un nuevo clúster, consulte la documentación en el sitio de soporte de NetApp .

Lo que necesitarás

- Existe una relación de replicación interrumpida entre los volúmenes de Element y ONTAP .
- El volumen de Element se ha perdido irremediablemente.
- El nombre del volumen original aparece como NO ENCONTRADO.

Pasos

1. En la interfaz de usuario de Element, busque la relación que rompió para realizar la conmutación por error.

Buenas prácticas: Tome nota de la política de SnapMirror y de los detalles del calendario de la relación original que se interrumpió. Esta información será necesaria para restablecer la relación.

2. Haz clic en el icono **Acciones** y luego en **Revertir resincronización**.
3. Confirma la acción.



La operación de resincronización inversa crea una nueva relación en la que se invierten las funciones del volumen de origen original y del volumen de destino (esto da como resultado dos relaciones, ya que la relación original persiste). Dado que el volumen original ya no existe, el sistema crea un nuevo volumen Element con el mismo nombre y tamaño que el volumen de origen original. Al nuevo volumen se le asigna una política QoS predeterminada llamada sm-recovery y se asocia con una cuenta predeterminada llamada sm-recovery. Deberá editar manualmente la cuenta y la política de QoS para todos los volúmenes creados por SnapMirror para reemplazar los volúmenes de origen originales que fueron destruidos.

Los datos de la última instantánea se transfieren al nuevo volumen como parte de la operación de resincronización inversa. Puede continuar accediendo y escribiendo datos en el volumen activo 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. Después de completar la resincronización inversa y asegurarse de que no haya sesiones activas conectadas al volumen en el lado de destino y que los datos más recientes se encuentren en el volumen primario original, continúe con los siguientes pasos para completar la recuperación ante fallos y reactivar el volumen primario original:

4. Haga clic en el icono **Acciones** de la relación inversa que se creó durante la operación de resincronización inversa y haga clic en **Romper**.
5. Haga clic en el icono **Acciones** de la relación original, en la que no existe el volumen de origen, y haga clic en **Eliminar**.
6. Haz clic en el icono **Acciones** de la relación inversa, que rompiste en el paso 4, y haz clic en **Revertir resincronización**.
7. Esto invierte el origen y el destino, dando como resultado una relación con el mismo origen y destino de volumen que la relación original.
8. Haz clic en el icono **Acciones** y en **Editar** para actualizar esta relación con la política QoS original y la configuración de programación que anotaste.
9. Ahora es seguro eliminar la relación inversa que resincronizaste en el paso 6.

Encuentra más información

[escenarios de recuperación ante fallos de SnapMirror](#)

Realice una transferencia o migración única de ONTAP a Element

Normalmente, cuando se utiliza SnapMirror para la recuperación ante desastres desde

un clúster de almacenamiento 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 servir como origen y Element como destino.

- Existen dos escenarios:
 - No existe ninguna relación previa de recuperación ante desastres. Siga todos los pasos de este procedimiento.
 - Existe una relación previa de recuperación ante desastres, pero no entre los volúmenes que se utilizan para esta mitigación. En este caso, siga únicamente los pasos 3 y 4 a continuación.

Lo que necesitarás

- El nodo de destino del elemento debe haber sido hecho accesible para ONTAP.
- El volumen Element debe haber estado habilitado para la replicación SnapMirror .

Debe especificar la ruta de destino del elemento en el formato `hostip:/lun/<id_number>`, donde `lun` es la cadena real "lun" e `id_number` es el ID del volumen del elemento.

Pasos

1. Utilizando ONTAP, cree la relación con el clúster 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. Verifique que la relación SnapMirror se haya creado utilizando el comando ONTAP `snapmirror show`.

Consulte la información sobre cómo crear una relación de replicación en la documentación de ONTAP y para conocer la sintaxis completa de los comandos, consulte la página del manual de ONTAP .

3. Utilizando el `ElementCreateVolume` API, cree el volumen de destino y configure el modo de acceso al volumen de destino en SnapMirror:

Crea un volumen de Element utilizando la API de Element.

```
{
  "method": "CreateVolume",
  "params": {
    "name": "SMTargetVolumeTest2",
    "accountID": 1,
    "totalSize": 1000000000000,
    "enable512e": true,
    "attributes": {},
    "qosPolicyID": 1,
    "enableSnapMirrorReplication": true,
    "access": "snapMirrorTarget"
  },
  "id": 1
}
```

4. Inicialice la relación de replicación utilizando ONTAP. `snapmirror initialize` dominio:

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

Replicación entre el software NetApp Element y ONTAP (CLI de ONTAP)

Descripción general de la replicación entre el software NetApp Element y ONTAP (CLI de ONTAP)

Puede garantizar la continuidad del negocio en un sistema Element utilizando SnapMirror para replicar copias de instantáneas de un volumen Element en un destino ONTAP . En caso de desastre en el sitio de Element, puede proporcionar datos a los clientes desde el sistema ONTAP y luego reactivar el sistema Element cuando se restablezca el servicio.

A partir de ONTAP 9.4, puede replicar copias de instantáneas de una LUN creada en un nodo ONTAP de vuelta a un sistema Element. Es posible que haya creado un LUN durante una interrupción en el sitio de Element, o que esté utilizando un LUN para migrar datos de ONTAP al software de Element.

Deberías trabajar con la copia de seguridad de Element a ONTAP si se cumplen las siguientes condiciones:

- Lo que se busca es utilizar las mejores prácticas, no explorar todas las opciones disponibles.
- Desea utilizar la interfaz de línea de comandos (CLI) de ONTAP , no System Manager ni una herramienta de scripting automatizada.
- Estás utilizando iSCSI para proporcionar datos a los clientes.

Si necesita información adicional sobre la configuración o los conceptos de SnapMirror , consulte ["Resumen de protección de datos"](#) .

Acerca de la replicación entre Element y ONTAP

A partir de ONTAP 9.3, puede usar SnapMirror para replicar copias de instantáneas de un volumen Element en un destino ONTAP. En caso de desastre en el sitio de Element, puede proporcionar datos a los clientes desde el sistema ONTAP y luego reactivar el volumen de origen de Element cuando se restablezca el servicio.

A partir de ONTAP 9.4, puede replicar copias de instantáneas de una LUN creada en un nodo ONTAP de vuelta a un sistema Element. Es posible que haya creado un LUN durante una interrupción en el sitio de Element, o que esté utilizando un LUN para migrar datos de ONTAP al software de Element.

Tipos de relación de protección de datos

SnapMirror ofrece dos tipos de relación de protección de datos. Para cada tipo, SnapMirror crea una copia instantánea del volumen de origen del elemento antes de inicializar o actualizar la relación:

- En una relación de protección de datos de *recuperación ante desastres (DR)*, el volumen de destino contiene únicamente la copia instantánea creada por SnapMirror, desde la cual puede continuar sirviendo datos en caso de una catástrofe en el sitio principal.
- En una relación de protección de datos de *retención a largo plazo*, el volumen de destino contiene copias de instantáneas puntuales creadas por el software Element, así como la copia de instantánea creada por SnapMirror. Por ejemplo, es posible que desee conservar copias de instantáneas mensuales creadas durante un período de 20 años.

Políticas predeterminadas

La primera vez que se invoca SnapMirror, se realiza una transferencia básica desde el volumen de origen al volumen de destino. La política *SnapMirror* define el contenido de la línea base y cualquier actualización.

Puede utilizar una política predeterminada o personalizada al crear una relación de protección de datos. El *tipo de política* determina qué copias de instantáneas se incluirán y cuántas copias se conservarán.

La tabla siguiente muestra las políticas predeterminadas. Utilice el *MirrorLatest* política para crear una relación de DR tradicional. Utilice el *MirrorAndVault* o *Unified7year* política para crear una relación de replicación unificada, en la que la recuperación ante desastres y la retención a largo plazo se configuran en el mismo volumen de destino.

Política	Tipo de póliza	comportamiento de actualización
MirrorLatest	espejo asíncrono	Transfiera la copia de instantánea creada por SnapMirror.
Espejo y bóveda	bóveda de espejos	Transfiera la copia de instantánea creada por SnapMirror y cualquier copia de instantánea menos reciente realizada desde la última actualización, siempre que tengan las etiquetas de SnapMirror “daily” o “weekly”.
Unified7year	bóveda de espejos	Transfiera la copia de instantánea creada por SnapMirror y cualquier copia de instantánea menos reciente realizada desde la última actualización, siempre que tengan las etiquetas de SnapMirror “daily”, “weekly” o “monthly”.



Para obtener información completa sobre las políticas de SnapMirror , incluyendo orientación sobre qué política utilizar, consulte ["Resumen de protección de datos"](#) .

Comprender las etiquetas de SnapMirror

Cada política con el tipo de política “mirror-vault” debe tener una regla que especifique qué copias de instantáneas replicar. La regla “daily”, por ejemplo, indica que solo se deben replicar las copias de instantáneas a las que se les haya asignado la etiqueta SnapMirror “daily”. La etiqueta SnapMirror se asigna al configurar las copias de instantáneas de Element.

Replicación desde un clúster de origen Element a un clúster de destino ONTAP

Puede utilizar SnapMirror para replicar copias de instantáneas de un volumen Element en un sistema de destino ONTAP . En caso de desastre en el sitio de Element, puede proporcionar datos a los clientes desde el sistema ONTAP y luego reactivar el volumen de origen de Element cuando se restablezca el servicio.

Un volumen Element es aproximadamente equivalente a un LUN de ONTAP . SnapMirror crea un LUN con el nombre del volumen de Element cuando se inicializa una relación de protección de datos entre el software Element y ONTAP . SnapMirror replica datos a una LUN existente si la LUN cumple con los requisitos para la replicación de Element a ONTAP .

Las reglas de replicación son las siguientes:

- Un volumen ONTAP solo puede contener datos de un volumen Element.
- No se pueden replicar datos de un volumen ONTAP a varios volúmenes Element.

Replicación desde un clúster de origen ONTAP a un clúster de destino Element

A partir de ONTAP 9.4, puede replicar copias de instantáneas de una LUN creada en un sistema ONTAP en un volumen Element:

- Si ya existe una relación SnapMirror entre una fuente Element y un destino ONTAP , una LUN creada mientras se sirven datos desde el destino se replica automáticamente cuando se reactiva la fuente.
- De lo contrario, deberá crear e inicializar una relación SnapMirror entre el clúster de origen ONTAP y el clúster de destino Element.

Las reglas de replicación son las siguientes:

- La relación de replicación debe tener una política de tipo “async-mirror”.

Las políticas de tipo “mirror-vault” no son compatibles.

- Solo se admiten LUN iSCSI.
- No se puede replicar más de un LUN desde un volumen ONTAP a un volumen Element.
- No se puede replicar un LUN desde un volumen ONTAP a varios volúmenes Element.

Prerrequisitos

Debe haber completado las siguientes tareas antes de configurar una relación de protección de datos entre Element y ONTAP:

- El clúster Element debe estar ejecutando el software NetApp Element versión 10.1 o posterior.

- El clúster ONTAP debe estar ejecutando ONTAP 9.3 o posterior.
- SnapMirror debe haber sido licenciado en el clúster ONTAP .
- Debe haber configurado volúmenes en los clústeres Element y ONTAP que sean lo suficientemente grandes como para manejar las transferencias de datos previstas.
- Si está utilizando el tipo de política “mirror-vault”, debe haberse configurado una etiqueta SnapMirror para que se repliquen las copias de instantáneas de Element.



Solo puedes realizar esta tarea en el ["Interfaz web del software Element"](#) o utilizando el ["Métodos API"](#) .

- Debes haberte asegurado de que el puerto 5010 esté disponible.
- Si prevé que podría necesitar mover un volumen de destino, debe haberse asegurado de que exista conectividad de malla completa entre el origen y el destino. Cada nodo del clúster de origen Element debe poder comunicarse con cada nodo del clúster de destino ONTAP .

Detalles de soporte

La siguiente tabla muestra los detalles de soporte para la copia de seguridad de Element a ONTAP .

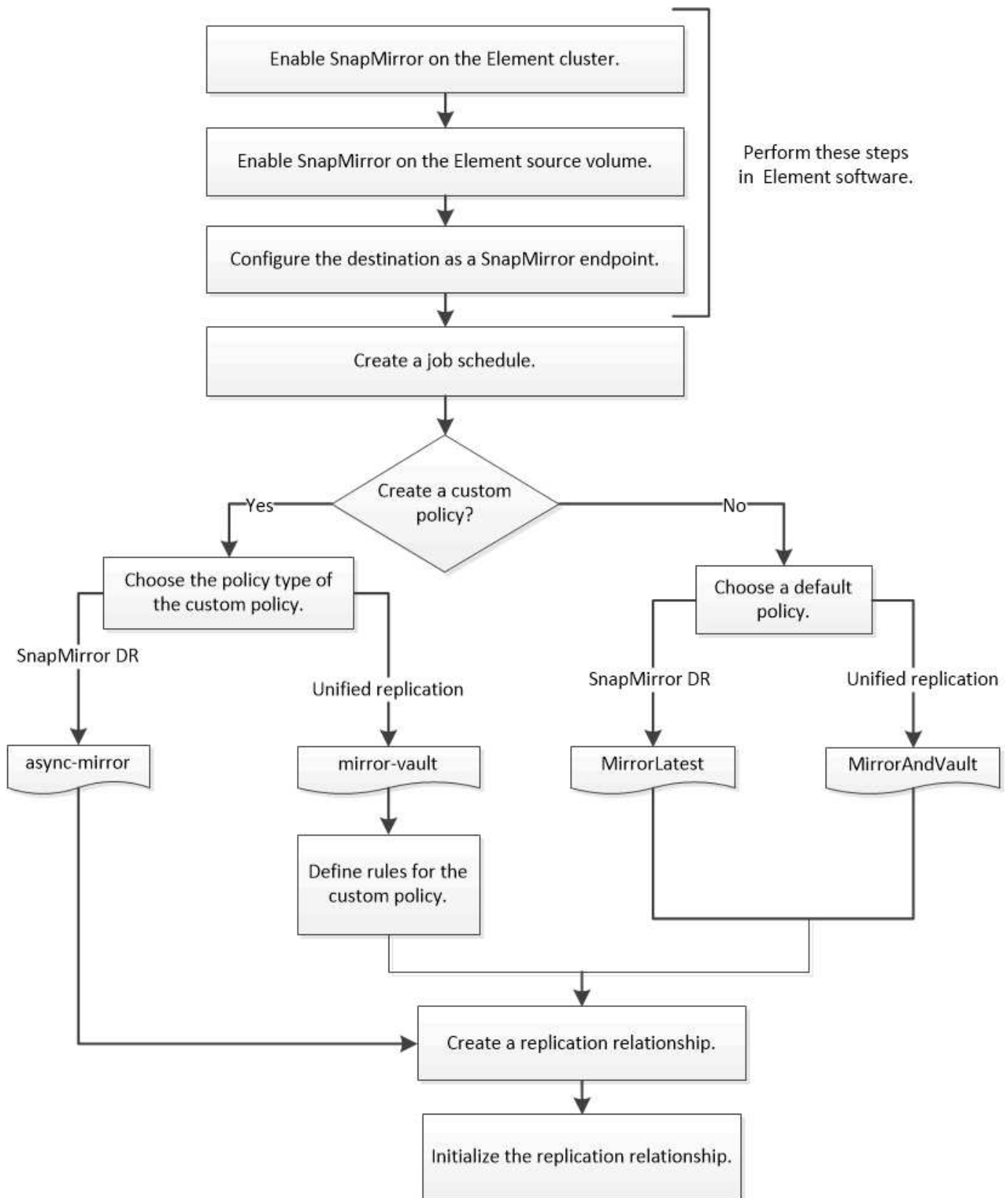
Recurso o función	Detalles de soporte
SnapMirror	• La función de restauración de SnapMirror no es compatible. • El <code>MirrorAllSnapshots</code> y <code>XDPDefault</code> Las políticas no son compatibles. • El tipo de política “vault” no es compatible. • La regla definida por el sistema “all_source_snapshots” no es compatible. • El tipo de política “mirror-vault” solo es compatible con la replicación desde el software Element a ONTAP. Utilice “async-mirror” para la replicación desde ONTAP al software Element. • El <code>-schedule</code> y <code>-prefix</code> opciones para <code>snapmirror policy add-rule</code> No son compatibles. • El <code>-preserve</code> y <code>-quick-resync</code> opciones para <code>snapmirror resync</code> No son compatibles. • La eficiencia del almacenamiento no se conserva. • No se admiten implementaciones de protección de datos en cascada ni de tipo fan-out.
ONTAP	• ONTAP Select es compatible a partir de ONTAP 9.4 y Element 10.3. • Cloud Volumes ONTAP es compatible a partir de ONTAP 9.5 y Element 11.0.

Elemento	• El límite de tamaño del volumen es de 8 TiB. • El tamaño del bloque de volumen debe ser de 512 bytes. No se admite un tamaño de bloque de 4K bytes. • El tamaño del volumen debe ser un múltiplo de 1 MiB. • Los atributos de volumen no se conservan. • El número máximo de copias de instantáneas que se replicarán es 30.
Red	• Se permite una única conexión TCP por transferencia. • El nodo Element debe especificarse como una dirección IP. La búsqueda de nombres de host DNS no es compatible. • Los espacios IP no son compatibles.
SnapLock	Los volúmenes SnapLock no son compatibles.
FlexGroup	Los volúmenes FlexGroup no son compatibles.
SVM DR	Los volúmenes ONTAP en una configuración SVM DR no son compatibles.
MetroCluster	Los volúmenes ONTAP en una configuración MetroCluster no son compatibles.

Flujo de trabajo para la replicación entre Element y ONTAP

Tanto si replica datos de Element a ONTAP como de ONTAP a Element, deberá configurar una programación de trabajos, especificar una política y crear e inicializar la relación. Puede utilizar una política predeterminada o personalizada.

El flujo de trabajo presupone que usted ha completado las tareas previas que se enumeran en ["Prerrequisitos"](#) . Para obtener información completa sobre las políticas de SnapMirror , incluyendo orientación sobre qué política utilizar, consulte ["Resumen de protección de datos"](#) .



Habilita SnapMirror en el software Element.

Habilite SnapMirror en el clúster de Element.

Debe habilitar SnapMirror en el clúster de Element antes de poder crear una relación de

replicación. Esta tarea solo se puede realizar en la interfaz web del software Element o utilizando "[Método API](#)".

Antes de empezar

- El clúster Element debe estar ejecutando el software NetApp Element versión 10.1 o posterior.
- SnapMirror solo se puede habilitar para clústeres Element utilizados con volúmenes NetApp ONTAP.

Acerca de esta tarea

El sistema Element viene con SnapMirror desactivado por defecto. SnapMirror no se habilita automáticamente como parte de una nueva instalación o actualización.



Una vez activado, SnapMirror no se puede desactivar. Solo puedes desactivar la función SnapMirror y restaurar la configuración predeterminada devolviendo el clúster a la imagen de fábrica.

Pasos

1. Haz clic en **Clústeres > Configuración**.
2. Encuentre la configuración específica del clúster para SnapMirror.
3. Haz clic en **Habilitar SnapMirror**.

Habilite SnapMirror en el volumen de origen Element.

Debe habilitar SnapMirror en el volumen de origen Element antes de poder crear una relación de replicación. Esta tarea solo se puede realizar en la interfaz web del software Element o utilizando "[Modificar volumen](#)" y "[Modificar volúmenes](#)" Métodos de la API.

Antes de empezar

- Debes haber habilitado SnapMirror en el clúster Element.
- El tamaño del bloque de volumen debe ser de 512 bytes.
- El volumen no debe participar en la replicación remota de Element.
- El tipo de acceso al volumen no debe ser "Objetivo de replicación".

Acerca de esta tarea

El procedimiento que se describe a continuación presupone que el volumen ya existe. También puedes habilitar SnapMirror al crear o clonar un volumen.

Pasos

1. Seleccione **Administración > Volúmenes**.
2. Seleccione el  botón para el volumen.
3. En el menú desplegable, seleccione **Editar**.
4. En el cuadro de diálogo **Editar volumen**, seleccione **Habilitar SnapMirror**.
5. Seleccione **Guardar cambios**.

Crea un punto de conexión de SnapMirror

Debes crear un punto de conexión SnapMirror antes de poder crear una relación de replicación. Esta tarea solo se puede realizar en la interfaz web del software Element o

utilizando ["Métodos de la API de SnapMirror"](#).

Antes de empezar

Debes haber habilitado SnapMirror en el clúster Element.

Pasos

1. Haga clic en **Protección de datos** > *Puntos de conexión de SnapMirror *.
2. Haz clic en **Crear punto de conexión**.
3. En el cuadro de diálogo **Crear un nuevo punto de conexión**, introduzca la dirección IP de administración del clúster ONTAP .
4. Introduzca el ID de usuario y la contraseña del administrador del clúster ONTAP .
5. Haz clic en **Crear punto de conexión**.

Configurar una relación de replicación

Cree un programa de trabajo de replicación.

Tanto si replica datos de Element a ONTAP como de ONTAP a Element, deberá configurar una programación de trabajos, especificar una política y crear e inicializar la relación. Puede utilizar una política predeterminada o personalizada.

Puedes usar el `job schedule cron create` comando para crear una programación de trabajos de replicación. La programación de tareas determina cuándo SnapMirror actualiza automáticamente la relación de protección de datos a la que está asignada dicha programación.

Acerca de esta tarea

Se asigna un cronograma de trabajo al crear una relación de protección de datos. Si no asigna un horario de trabajo, deberá actualizar la relación manualmente.

Paso

1. Crear un horario de trabajo:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week  
-day day_of_month -hour hour -minute minute
```

Para `-month`, `-dayofweek`, y `-hour`, puedes especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.

A partir de ONTAP 9.10.1, puede incluir el Vserver en su planificación de trabajos:

```
job schedule cron create -name job_name -vserver Vserver_name -month month  
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```

El siguiente ejemplo crea una programación de trabajos llamada `my_weekly` que se emite los sábados a las 3:00 am:

```
cluster_dst:> job schedule cron create -name my_weekly -dayofweek  
"Saturday" -hour 3 -minute 0
```

Crear una política de replicación personalizada

Puede utilizar una política predeterminada o personalizada al crear una relación de replicación. Para una política de replicación unificada personalizada, debe definir una o más *reglas* que determinen qué copias de instantáneas se transfieren durante la inicialización y la actualización.

Puede crear una política de replicación personalizada si la política predeterminada para una relación no es adecuada. Es posible que desee comprimir los datos en una transferencia de red, por ejemplo, o modificar el número de intentos que realiza SnapMirror para transferir copias de instantáneas.

Acerca de esta tarea

El *tipo de política* de la política de replicación determina el tipo de relación que admite. La tabla siguiente muestra los tipos de políticas disponibles.

Tipo de política	Tipo de relación
espejo asíncrono	SnapMirror DR
bóveda de espejos	replicación unificada

Paso

1. Cree una política de replicación personalizada:

```
snapmirror policy create -vserver SVM -policy policy -type async-  
mirror|mirror-vault -comment comment -tries transfer_tries -transfer-priority  
low|normal -is-network-compression-enabled true|false
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

A partir de ONTAP 9.5, puede especificar la programación para crear una programación de copia de instantánea común para las relaciones síncronas de SnapMirror mediante el uso de `-common-snapshot -schedule` parámetro. Por defecto, la programación común de copia de instantáneas para las relaciones síncronas de SnapMirror es de una hora. Puede especificar un valor de entre 30 minutos y dos horas para la programación de copia de instantáneas para las relaciones síncronas de SnapMirror .

El siguiente ejemplo crea una política de replicación personalizada para SnapMirror DR que habilita la compresión de red para las transferencias de datos:

```
cluster_dst::> snapmirror policy create -vserver svml -policy  
DR_compressed -type async-mirror -comment "DR with network compression  
enabled" -is-network-compression-enabled true
```

El siguiente ejemplo crea una política de replicación personalizada para la replicación unificada:

```
cluster_dst::> snapmirror policy create -vserver svml -policy my_unified  
-type mirror-vault
```

Después de terminar

Para los tipos de políticas “mirror-vault”, debe definir reglas que determinen qué copias de instantáneas se transfieren durante la inicialización y la actualización.

Utilice el `snapmirror policy show` comando para verificar que se creó la política de SnapMirror. Para conocer la sintaxis completa del comando, consulte la página del manual.

Defina una regla para una política

Para las políticas personalizadas con el tipo de política “mirror-vault”, debe definir al menos una regla que determine qué copias de instantáneas se transfieren durante la inicialización y la actualización. También puede definir reglas para políticas predeterminadas con el tipo de política “mirror-vault”.

Acerca de esta tarea

Cada política con el tipo de política “mirror-vault” debe tener una regla que especifique qué copias de instantáneas replicar. La regla “bimensual”, por ejemplo, indica que solo deben replicarse las copias de instantáneas a las que se les haya asignado la etiqueta SnapMirror “bimensual”. La etiqueta SnapMirror se asigna al configurar las copias de instantáneas de Element.

Cada tipo de política está asociado con una o más reglas definidas por el sistema. Estas reglas se asignan automáticamente a una política cuando se especifica su tipo de política. La tabla siguiente muestra las reglas definidas por el sistema.

regla definida por el sistema	Utilizado en tipos de políticas	Resultado
sm_creado	espejo asíncrono, bóveda de espejos	Una copia instantánea creada por SnapMirror se transfiere durante la inicialización y la actualización.
a diario	bóveda de espejos	Las nuevas copias de instantáneas en la fuente con la etiqueta SnapMirror “daily” se transfieren durante la inicialización y la actualización.
semanalmente	bóveda de espejos	Las nuevas copias de instantáneas en la fuente con la etiqueta SnapMirror “weekly” se transfieren durante la inicialización y la actualización.

mensual	bóveda de espejos	Las nuevas copias de instantáneas en la fuente con la etiqueta SnapMirror “mensual” se transfieren durante la inicialización y la actualización.

Puede especificar reglas adicionales según sea necesario, para políticas predeterminadas o personalizadas. Por ejemplo:

- Por defecto `MirrorAndVault` En cuanto a la política, podría crear una regla llamada “bimensual” para que coincidan las copias de instantáneas en la fuente con la etiqueta SnapMirror “bimensual”.
- Para una política personalizada con el tipo de política “mirror-vault”, puede crear una regla llamada “bi-weekly” para que coincida con las copias de instantáneas en el origen con la etiqueta SnapMirror “bi-weekly”.

Paso

1. Defina una regla para una política:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -keep retention_count
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo agrega una regla con la etiqueta SnapMirror. `bi-monthly` al valor predeterminado `MirrorAndVault` política:

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

El siguiente ejemplo agrega una regla con la etiqueta SnapMirror. `bi-weekly` a la costumbre `my_snapvault` política:

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

El siguiente ejemplo agrega una regla con la etiqueta SnapMirror. `app_consistent` a la costumbre `Sync` política:

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy Sync
-snapmirror-label app_consistent -keep 1
```

A continuación, puede replicar copias de instantáneas del clúster de origen que coincidan con esta etiqueta de SnapMirror :

```
cluster_src::> snapshot create -vserver vs1 -volume voll -snapshot  
snapshot1 -snapmirror-label app_consistent
```

Crear una relación de replicación

Cree una relación desde un origen Element a un destino ONTAP .

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*. Puedes usar el `snapmirror create` comando para crear una relación de protección de datos desde una fuente Element a un destino ONTAP , o desde una fuente ONTAP a un destino Element.

Puede utilizar SnapMirror para replicar copias de instantáneas de un volumen Element en un sistema de destino ONTAP . En caso de desastre en el sitio de Element, puede proporcionar datos a los clientes desde el sistema ONTAP y luego reactivar el volumen de origen de Element cuando se restablezca el servicio.

Antes de empezar

- El nodo Element que contiene el volumen que se va a replicar debe haber sido hecho accesible para ONTAP.
- El volumen Element debe haber estado habilitado para la replicación SnapMirror .
- Si está utilizando el tipo de política “mirror-vault”, debe haberse configurado una etiqueta SnapMirror para que se repliquen las copias de instantáneas de Element.



Solo puedes realizar esta tarea en el ["Interfaz web del software Element"](#) o utilizando el ["Métodos API"](#) .

Acerca de esta tarea

Debe especificar la ruta de origen del elemento en el formulario `<hostip:>/lun/<name>` , donde “lun” es la cadena real “lun” y name es el nombre del volumen de Element.

Un volumen Element es aproximadamente equivalente a un LUN de ONTAP . SnapMirror crea un LUN con el nombre del volumen de Element cuando se inicializa una relación de protección de datos entre el software Element y ONTAP . SnapMirror replica los datos a una LUN existente si la LUN cumple los requisitos para la replicación desde el software Element a ONTAP.

Las reglas de replicación son las siguientes:

- Un volumen ONTAP solo puede contener datos de un volumen Element.
- No se pueden replicar datos de un volumen ONTAP a varios volúmenes Element.

En ONTAP 9.3 y versiones anteriores, un volumen de destino puede contener hasta 251 copias de instantáneas. En ONTAP 9.4 y versiones posteriores, un volumen de destino puede contener hasta 1019 copias de instantáneas.

Paso

1. Desde el clúster de destino, cree una relación de replicación desde un origen Element a un destino ONTAP :

```
snapmirror create -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume> -type XDP -schedule schedule -policy  
<policy>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo crea una relación de recuperación ante desastres de SnapMirror utilizando la configuración predeterminada. MirrorLatest política:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy MirrorLatest
```

El siguiente ejemplo crea una relación de replicación unificada utilizando la configuración predeterminada. MirrorAndVault política:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy MirrorAndVault
```

El siguiente ejemplo crea una relación de replicación unificada utilizando Unified7year política:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy Unified7year
```

El siguiente ejemplo crea una relación de replicación unificada utilizando la opción personalizada. my_unified política:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy my_unified
```

Después de terminar

Utilice el `snapmirror show` comando para verificar que se creó la relación SnapMirror . Para conocer la sintaxis completa del comando, consulte la página del manual.

Cree una relación desde un origen ONTAP a un destino Element.

A partir de ONTAP 9.4, puede usar SnapMirror para replicar copias de instantáneas de una LUN creada en una fuente ONTAP de vuelta a un destino Element. Es posible que esté utilizando la LUN para migrar datos desde ONTAP al software Element.

Antes de empezar

- El nodo de destino del elemento debe haber sido hecho accesible para ONTAP.
- El volumen Element debe haber estado habilitado para la replicación SnapMirror .

Acerca de esta tarea

Debe especificar la ruta de destino del elemento en el formulario. <hostip:>/lun/<name> , donde “lun” es la cadena real “lun” y name es el nombre del volumen de Element.

Las reglas de replicación son las siguientes:

- La relación de replicación debe tener una política de tipo “async-mirror”.

Puede utilizar una política predeterminada o personalizada.

- Solo se admiten LUN iSCSI.
- No se puede replicar más de un LUN desde un volumen ONTAP a un volumen Element.
- No se puede replicar un LUN desde un volumen ONTAP a varios volúmenes Element.

Paso

1. Cree una relación de replicación desde un origen ONTAP a un destino Element:

```
snapmirror create -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name> -type XDP -schedule schedule -policy
<policy>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo crea una relación de recuperación ante desastres de SnapMirror utilizando la configuración predeterminada. MirrorLatest política:

```
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
```

El siguiente ejemplo crea una relación de recuperación ante desastres de SnapMirror utilizando la configuración personalizada. my_mirror política:

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy my_mirror
```

Después de terminar

Utilice el `snapmirror show` comando para verificar que se creó la relación SnapMirror . Para conocer la sintaxis completa del comando, consulte la página del manual.

Inicializar una relación de replicación

Para todos los tipos de relaciones, la inicialización realiza una *transferencia de línea*

base: crea una copia instantánea del volumen de origen y luego transfiere esa copia y todos los bloques de datos a los que hace referencia al volumen de destino.

Antes de empezar

- El nodo Element que contiene el volumen que se va a replicar debe haber sido hecho accesible para ONTAP.
- El volumen Element debe haber estado habilitado para la replicación SnapMirror .
- Si está utilizando el tipo de política “mirror-vault”, debe haberse configurado una etiqueta SnapMirror para que se repliquen las copias de instantáneas de Element.



Solo puedes realizar esta tarea en el ["Interfaz web del software Element"](#) o utilizando el ["Métodos API"](#) .

Acerca de esta tarea

Debe especificar la ruta de origen del elemento en el formulario `<hostip:>/lun/<name>` , donde “lun” es la cadena real “lun” y *name* es el nombre del volumen de Element.

La inicialización puede llevar mucho tiempo. Quizás te interese realizar la transferencia de referencia en horas de menor tráfico.

Si la inicialización de una relación desde una fuente ONTAP a un destino Element falla por cualquier motivo, seguirá fallando incluso después de que haya corregido el problema (un nombre de LUN no válido, por ejemplo). La solución alternativa es la siguiente:



1. Eliminar la relación.
2. Elimine el volumen de destino del elemento.
3. Crea un nuevo volumen de destino de Elemento.
4. Cree e inicialice una nueva relación desde la fuente ONTAP al volumen de destino Element.

Paso

1. Inicializar una relación de replicación:

```
snapmirror initialize -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume|cluster://SVM/volume>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo inicializa la relación entre el volumen fuente 0005 en la dirección IP 10.0.0.11 y el volumen de destino volA_dst en svm_backup :

```
cluster_dst:> snapmirror initialize -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

Servir datos desde un volumen de destino de SnapMirror DR

Haga que el volumen de destino sea escribible.

Cuando un desastre inhabilita el sitio principal para una relación de recuperación ante desastres de SnapMirror , puede servir datos desde el volumen de destino con una interrupción mínima. Puede reactivar el volumen de origen cuando se restablezca el servicio en el sitio principal.

Debes hacer que el volumen de destino sea escribible antes de poder servir datos desde el volumen a los clientes. Puedes usar el `snapmirror quiesce` comando para detener las transferencias programadas al destino, el `snapmirror abort` orden de detener las transferencias en curso, y la `snapmirror break` comando para hacer que el destino sea escribible.

Acerca de esta tarea

Debe especificar la ruta de origen del elemento en el formulario `<hostip:>/lun/<name>` , donde “lun” es la cadena real “lun” y name es el nombre del volumen de Element.

Pasos

1. Suspender los traslados programados al destino:

```
snapmirror quiesce -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo detiene las transferencias programadas entre el volumen de origen 0005 en la dirección IP 10.0.0.11 y el volumen de destino volA_dst en svm_backup :

```
cluster_dst:> snapmirror quiesce -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

2. Detener las transferencias en curso al destino:

```
snapmirror abort -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo detiene las transferencias en curso entre el volumen de origen 0005 en la dirección IP 10.0.0.11 y el volumen de destino volA_dst en svm_backup :

```
cluster_dst:> snapmirror abort -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

3. Romper la relación de recuperación ante desastres de SnapMirror :

```
snapmirror break -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo rompe la relación entre el volumen de origen 0005 en la dirección IP 10.0.0.11 y el volumen de destino volA_dst en svm_backup y el volumen de destino volA_dst en svm_backup :

```
cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

Configure el volumen de destino para el acceso a datos.

Después de habilitar la escritura en el volumen de destino, debe configurar el volumen para el acceso a los datos. Los hosts SAN pueden acceder a los datos del volumen de destino hasta que se reactive el volumen de origen.

1. Asigne el LUN del elemento al grupo iniciador apropiado.
2. Cree sesiones iSCSI desde los iniciadores del host SAN a las LIF de la SAN.
3. En el cliente SAN, realice un nuevo escaneo de almacenamiento para detectar la LUN conectada.

Reactivar el volumen de la fuente original

Puede restablecer la relación original de protección de datos entre los volúmenes de origen y destino cuando ya no necesite servir datos desde el destino.

Acerca de esta tarea

El procedimiento que se describe a continuación presupone que la línea base en el volumen de la fuente original está intacta. Si la línea base no está intacta, debe crear e inicializar la relación entre el volumen desde el que está sirviendo datos y el volumen de origen original antes de realizar el procedimiento.

Debe especificar la ruta de origen del elemento en el formulario <hostip:>/lun/<name> , donde “lun” es la cadena real “lun” y name es el nombre del volumen de Element.

A partir de ONTAP 9.4, las copias de instantáneas de una LUN creadas mientras se sirven datos desde el destino ONTAP se replican automáticamente cuando se reactiva la fuente Element.

Las reglas de replicación son las siguientes:

- Solo se admiten LUN iSCSI.
- No se puede replicar más de un LUN desde un volumen ONTAP a un volumen Element.
- No se puede replicar un LUN desde un volumen ONTAP a varios volúmenes Element.

Pasos

1. Eliminar la relación original de protección de datos:

```
snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>  
-destination-path <hostip:>/lun/<name> -policy <policy>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo elimina la relación con el volumen fuente original, 0005 en la dirección IP 10.0.0.11 y el volumen desde el que está sirviendo datos, volA_dst en svm_backup :

```
cluster_dst:> snapmirror delete -source-path 10.0.0.11:/lun/0005  
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

2. Invertir la relación original de protección de datos:

```
snapmirror resync -source-path <SVM:volume>|<cluster://SVM/volume>  
-destination-path <hostip:>/lun/<name> -policy <policy>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

Aunque la resincronización no requiere una transferencia de referencia, puede llevar mucho tiempo. Quizás te convenga ejecutar la resincronización en horas de menor actividad.

El siguiente ejemplo invierte la relación entre el volumen de la fuente original, 0005 en la dirección IP 10.0.0.11 y el volumen desde el que está sirviendo datos, volA_dst en svm_backup :

```
cluster_dst:> snapmirror resync -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

3. Actualizar la relación inversa:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>  
-destination-path <hostip:>/lun/<name>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.



El comando falla si no existe una copia de instantánea común en el origen y el destino. Usar `snapmirror initialize` para reiniciar la relación.

El siguiente ejemplo actualiza la relación entre el volumen desde el que se sirven los datos, volA_dst en svm_backup , y el volumen fuente original, 0005 en la dirección IP 10.0.0.11:

```
cluster_dst:> snapmirror update -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

4. Detener las transferencias programadas para la relación inversa:

```
snapmirror quiesce -source-path <SVM:volume>|<cluster://SVM/volume>  
-destination-path <hostip:>/lun/<name>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo detiene las transferencias programadas entre el volumen desde el que se están sirviendo los datos, volA_dst en svm_backup , y el volumen fuente original, 0005 en la dirección IP 10.0.0.11:


```
cluster_dst:> snapmirror quiesce -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

5. Detener las transferencias en curso para la relación inversa:

```
snapmirror abort -source-path <SVM:volume>|<cluster://SVM/volume> -destination  
-path <hostip:>/lun/<name>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo detiene las transferencias en curso entre el volumen desde el que se están sirviendo los datos, volA_dst en svm_backup , y el volumen fuente original, 0005 en la dirección IP 10.0.0.11:

```
cluster_dst:> snapmirror abort -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

6. Romper la relación inversa:

```
snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume> -destination  
-path <hostip:>/lun/<name>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo rompe la relación entre el volumen desde el que se sirven los datos, volA_dst en svm_backup , y el volumen fuente original, 0005 en la dirección IP 10.0.0.11:

```
cluster_dst:> snapmirror break -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

7. Eliminar la relación de protección de datos invertida:

```
snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>  
-destination-path <hostip:>/lun/<name> -policy <policy>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo elimina la relación inversa entre el volumen fuente original, 0005 en la dirección IP 10.0.0.11 y el volumen desde el que está sirviendo datos, volA_dst en svm_backup :

```
cluster_src:> snapmirror delete -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

8. Restablecer la relación original de protección de datos:

```
snapmirror resync -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo restablece la relación entre el volumen fuente original, 0005 en la dirección IP 10.0.0.11 y el volumen de destino original, volA_dst en svm_backup :

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

Después de terminar

Utilice el `snapmirror show` comando para verificar que se creó la relación SnapMirror . Para conocer la sintaxis completa del comando, consulte la página del manual.

Actualizar manualmente una relación de replicación.

Es posible que deba actualizar manualmente una relación de replicación si una actualización falla debido a un error de red.

Acerca de esta tarea

Debe especificar la ruta de origen del elemento en el formulario `<hostip:>/lun/<name>` , donde “lun” es la cadena real “lun” y name es el nombre del volumen de Element.

Pasos

1. Actualizar manualmente una relación de replicación:

```
snapmirror update -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.



El comando falla si no existe una copia de instantánea común en el origen y el destino. Usar `snapmirror initialize` para reiniciar la relación.

El siguiente ejemplo actualiza la relación entre el volumen de origen 0005 en la dirección IP 10.0.0.11 y el volumen de destino volA_dst en svm_backup :

```
cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

Resincronizar una relación de replicación

Es necesario resincronizar una relación de replicación después de hacer que un volumen de destino sea escribible, después de que falle una actualización porque no existe una copia Snapshot común en los volúmenes de origen y destino, o si se desea cambiar la política de replicación para la relación.

Acerca de esta tarea

Aunque la resincronización no requiere una transferencia de referencia, puede llevar mucho tiempo. Quizás te convenga ejecutar la resincronización en horas de menor actividad.

Debe especificar la ruta de origen del elemento en el formulario `<hostip:>/lun/<name>` , donde “lun” es la cadena real “lun” y name es el nombre del volumen de Element.

Paso

1. Resincronizar los volúmenes de origen y destino:

```
snapmirror resync -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume> -type XDP -policy <policy>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo resincroniza la relación entre el volumen de origen 0005 en la dirección IP 10.0.0.11 y el volumen de destino volA_dst en svm_backup :

```
cluster_dst:> snapmirror resync -source-path 10.0.0.11:/lun/0005  
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

Copia de seguridad y restauración de volúmenes

Copia de seguridad y restauración de volúmenes

Puede realizar copias de seguridad y restaurar volúmenes en otros almacenamientos SolidFire , así como en almacenes de objetos secundarios compatibles con Amazon S3 u OpenStack Swift.

Al restaurar volúmenes desde OpenStack Swift o Amazon S3, se necesita la información del manifiesto del proceso de copia de seguridad original. Si está restaurando un volumen del que se realizó una copia de seguridad en un sistema de almacenamiento SolidFire , no se requiere información de manifiesto.

Encuentra más información

- [Realizar una copia de seguridad de un volumen en un almacenamiento de objetos de Amazon S3](#)
- [Realizar una copia de seguridad de un volumen en un almacén de objetos Swift de OpenStack](#)
- [Realizar una copia de seguridad de un volumen en un clúster de almacenamiento SolidFire](#)
- [Restaurar un volumen desde una copia de seguridad en un almacenamiento de objetos de Amazon S3](#)
- [Restaurar un volumen desde una copia de seguridad en un almacén de objetos OpenStack Swift](#)
- [Restaurar un volumen desde una copia de seguridad en un clúster de almacenamiento SolidFire](#)

Realizar una copia de seguridad de un volumen en un almacenamiento de objetos de Amazon S3

Puede realizar copias de seguridad de volúmenes en almacenes de objetos externos que sean compatibles con Amazon S3.

1. Haz clic en **Administración > Volúmenes**.

2. Haz clic en el icono Acciones del volumen que deseas respaldar.
3. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
4. En el cuadro de diálogo **Copia de seguridad integrada**, en **Realizar copia de seguridad en**, seleccione **S3**.
5. Seleccione una opción en **Formato de datos**:
 - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
 - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Introduzca un nombre de host para acceder al almacén de objetos en el campo **Nombre de host**.
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 bucket de S3 en el que se almacenará la copia de seguridad en el campo **Bucket de S3**.
10. Introduzca una etiqueta de identificación para añadir al prefijo en el campo **Etiqueta de identificación**.
11. Haz clic en **Iniciar lectura**.

Realizar una copia de seguridad de un volumen en un almacén de objetos Swift de OpenStack

Puede realizar copias de seguridad de volúmenes en almacenes de objetos externos que sean compatibles con OpenStack Swift.

1. Haz clic en **Administración > Volúmenes**.
2. Haz clic en el icono de Acciones del volumen que deseas respaldar.
3. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
4. En el cuadro de diálogo **Copia de seguridad integrada**, en **Realizar copia de seguridad en**, seleccione **Swift**.
5. Seleccione un formato de datos en **Formato de datos**:
 - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
 - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Introduzca una 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 **Contenedor**.
10. **Opcional**: Introduzca una etiqueta de nombre para añadir al prefijo en el campo **Etiqueta de nombre**.
11. Haz clic en **Iniciar lectura**.

Realizar una copia de seguridad de un volumen en un clúster de almacenamiento SolidFire

Puede realizar copias de seguridad de los volúmenes que residen en un clúster en un clúster remoto para clústeres de almacenamiento que ejecutan el software Element.

Asegúrese de que los clústeres de origen y destino estén emparejados.

Ver "[Agrupaciones de pares para replicación](#)".

Al realizar copias de seguridad o restauraciones de un clúster a otro, el sistema genera una clave que se utilizará para la autenticación entre los clústeres. Esta clave de escritura de volumen masivo permite que el clúster de origen se autentique con el clúster de destino, proporcionando un nivel de seguridad al escribir en el volumen de destino. Como parte del proceso de copia de seguridad o restauración, debe generar una clave de escritura de volumen masivo desde el volumen de destino antes de iniciar la operación.

1. En el clúster de destino, **Administración > Volúmenes**.
2. Haz clic en el icono Acciones del volumen de destino.
3. En el menú que aparece, haga clic en **Restaurar desde**.
4. En el cuadro de diálogo **Restauración integrada**, en **Restaurar desde**, seleccione * SolidFire*.
5. Seleccione una opción en **Formato de datos**:
 - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
 - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Haz clic en **Generar clave**.
7. Copie la clave del cuadro **Clave de escritura de volumen masivo** al portapapeles.
8. En el clúster de origen, vaya a **Administración > Volúmenes**.
9. Haz clic en el icono de Acciones del volumen que deseas respaldar.
10. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
11. En el cuadro de diálogo **Copia de seguridad integrada**, en **Realizar copia de seguridad en**, seleccione * SolidFire*.
12. Seleccione la misma opción que seleccionó anteriormente en el campo **Formato de datos**.
13. Introduzca la dirección IP virtual de gestión del clúster del volumen de destino en el campo **MVIP de clúster remoto**.
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 **Contraseña del clúster remoto**.
16. En el campo **Clave de escritura de volumen masivo**, pegue la clave que generó anteriormente en el clúster de destino.
17. Haz clic en **Iniciar lectura**.

Restaurar un volumen desde una copia de seguridad en un almacenamiento de objetos de Amazon S3

Puede restaurar un volumen desde una copia de seguridad en un almacenamiento de objetos de Amazon S3.

1. Haz clic en **Informes > Registro de eventos**.
2. Localice el evento de copia de seguridad que creó la copia de seguridad que necesita restaurar.
3. En la columna **Detalles** del evento, haga clic en **Mostrar detalles**.
4. Copie la información del manifiesto al portapapeles.
5. Haz clic en **Administración > Volúmenes**.
6. Haz clic en el icono Acciones del volumen que deseas restaurar.
7. En el menú que aparece, haga clic en **Restaurar desde**.
8. En el cuadro de diálogo **Restauración integrada**, en **Restaurar desde**, seleccione **S3**.

9. Seleccione la opción que coincida con la copia de seguridad en **Formato de datos**:
 - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
 - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
10. Introduzca un nombre de host para acceder al almacén de objetos en el campo **Nombre de host**.
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 bucket de S3 en el que se almacenará la copia de seguridad en el campo **Bucket de S3**.
14. Pegue la información del manifiesto en el campo **Manifiesto**.
15. Haz clic en **Comenzar a escribir**.

Restaurar un volumen desde una copia de seguridad en un almacén de objetos OpenStack Swift

Puede restaurar un volumen desde una copia de seguridad en un almacén de objetos OpenStack Swift.

1. Haz clic en **Informes > Registro de eventos**.
2. Localice el evento de copia de seguridad que creó la copia de seguridad que necesita restaurar.
3. En la columna **Detalles** del evento, haga clic en **Mostrar detalles**.
4. Copie la información del manifiesto al portapapeles.
5. Haz clic en **Administración > Volúmenes**.
6. Haz clic en el icono Acciones del volumen que deseas restaurar.
7. En el menú que aparece, haga clic en **Restaurar desde**.
8. En el cuadro de diálogo **Restauración integrada**, en **Restaurar desde**, seleccione **Swift**.
9. Seleccione la opción que coincida con la copia de seguridad en **Formato de datos**:
 - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
 - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
10. Introduzca una 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 **Contenedor**.
14. Pegue la información del manifiesto en el campo **Manifiesto**.
15. Haz clic en **Comenzar a escribir**.

Restaurar un volumen desde una copia de seguridad en un clúster de almacenamiento SolidFire

Puede restaurar un volumen desde una copia de seguridad en un clúster de almacenamiento SolidFire .

Al realizar copias de seguridad o restauraciones de un clúster a otro, el sistema genera una clave que se utilizará para la autenticación entre los clústeres. Esta clave de escritura de volumen masivo permite que el clúster de origen se autentique con el clúster de destino, proporcionando un nivel de seguridad al escribir en el

volumen de destino. Como parte del proceso de copia de seguridad o restauración, debe generar una clave de escritura de volumen masivo desde el volumen de destino antes de iniciar la operación.

1. En el clúster de destino, haga clic en **Administración > Volúmenes**.
2. Haz clic en el icono Acciones del volumen que deseas restaurar.
3. En el menú que aparece, haga clic en **Restaurar desde**.
4. En el cuadro de diálogo **Restauración integrada**, en **Restaurar desde**, seleccione * SolidFire*.
5. Seleccione la opción que coincida con la copia de seguridad en **Formato de datos**:
 - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
 - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Haz clic en **Generar clave**.
7. Copie la información de la **Clave de escritura de volumen masivo** al portapapeles.
8. En el clúster de origen, haga clic en **Administración > Volúmenes**.
9. Haz clic en el icono Acciones del volumen que deseas usar para la restauración.
10. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
11. En el cuadro de diálogo **Copia de seguridad integrada**, seleccione * SolidFire* en **Realizar copia de seguridad en**.
12. Seleccione la opción que coincida con la copia de seguridad en **Formato de datos**.
13. Introduzca la dirección IP virtual de gestión del clúster del volumen de destino en el campo **MVIP de clúster remoto**.
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 **Contraseña del clúster remoto**.
16. Pegue la clave desde su portapapeles en el campo **Clave de escritura de volumen masivo**.
17. Haz clic en **Iniciar lectura**.

Configurar dominios de protección personalizados

Para los clústeres de Element que contienen más de dos nodos de almacenamiento, puede configurar dominios de protección personalizados para cada nodo. Cuando configure dominios de protección personalizados, deberá asignar todos los nodos del clúster a un dominio.



Cuando se asignan dominios de protección, se inicia una sincronización de datos entre nodos y algunas operaciones del clúster no están disponibles hasta que se complete la sincronización de datos. Después de configurar un dominio de protección personalizado para un clúster, cuando agregue un nuevo nodo de almacenamiento, no podrá agregar unidades para el nuevo nodo hasta que le asigne un dominio de protección y permita que se complete la sincronización de datos. Visita el "[Documentación de dominios de protección](#)" Para obtener más información sobre los dominios de protección.



Para que un esquema de dominio de protección personalizado sea útil para un clúster, todos los nodos de almacenamiento dentro de cada chasis deben estar asignados al mismo dominio de protección personalizado. Debe crear tantos dominios de protección personalizados como sean necesarios para que esto ocurra (el esquema de dominio de protección personalizado más pequeño posible es de tres dominios). Como práctica recomendada, configure el mismo número de nodos por dominio y procure que cada nodo asignado a un dominio en particular sea del mismo tipo.

Pasos

1. Haz clic en **Clúster > Nodos**.
2. Haga clic en **Configurar dominios de protección**.

En la ventana **Configurar dominios de protección personalizados**, puede ver los dominios de protección configurados actualmente (si los hay), así como las asignaciones de dominios de protección para nodos individuales.

3. Introduzca un nombre para el nuevo dominio de protección personalizado y haga clic en **Crear**.

Repita este paso para todos los nuevos dominios de protección que necesite crear.

4. Para cada nodo de la lista **Asignar nodos**, haga clic en el menú desplegable de la columna **Dominio de protección** y seleccione un dominio de protección para asignar a ese nodo.



Asegúrese de comprender la disposición de su nodo y chasis, el esquema de dominio de protección personalizado que ha configurado y los efectos del esquema en la protección de datos antes de aplicar los cambios. Si aplica un esquema de dominio de protección e inmediatamente necesita realizar cambios, podría pasar algún tiempo antes de que pueda hacerlo debido a la sincronización de datos que se produce una vez que se aplica una configuración.

5. Haga clic en **Configurar dominios de protección**.

Resultado

Dependiendo del tamaño de su clúster, la sincronización de datos entre dominios podría tardar algún tiempo. Una vez completada la sincronización de datos, puede ver las asignaciones de dominio de protección personalizadas en la página **Clúster > Nodos**, y el panel de la interfaz de usuario web de Element muestra el estado de protección del clúster en el panel **Estado del dominio de protección personalizado**.

Posibles errores

Aquí tienes algunos errores que podrías ver después de aplicar una configuración de dominio de protección personalizada:

Error	Descripción	Resolución
Falló SetProtectionDomainLayout: ProtectionDomainLayout dejaría el NodeID {9} inutilizable. No se pueden usar nombres predeterminados y no predeterminados al mismo tiempo.	Un nodo no tiene asignado un dominio de protección.	Asigne un dominio de protección al nodo.

Error al establecer el diseño del dominio de protección: el tipo de dominio de protección 'custom' divide el tipo de dominio de protección 'chassis'.	A un nodo en un chasis multinodo se le asigna un Dominio de Protección diferente al de los demás nodos del chasis.	Asegúrese de que todos los nodos del chasis tengan asignado el mismo dominio de protección.

Encuentra más información

- ["Dominios de protección personalizados"](#)
- ["Gestiona el almacenamiento con la API de Element"](#)

Soluciona los problemas de tu sistema

Eventos del sistema

Ver información sobre eventos del sistema

Puedes ver información sobre diversos eventos detectados en el sistema. El sistema actualiza los mensajes de eventos cada 30 segundos. El registro de eventos muestra los eventos clave del clúster.

1. En la interfaz de usuario de Element, seleccione **Informes > Registro de eventos**.

Para cada evento, verá la siguiente información:

Artículo	Descripción
IDENTIFICACIÓN	Identificador único asociado a cada evento.
Tipo de evento	El tipo de evento que se registra, por ejemplo, eventos de API o eventos de clonación.
Mensaje	Mensaje asociado al evento.
Detalles	Información que ayuda a identificar por qué ocurrió el suceso.
Service ID	El servicio que informó del suceso (si procede).
Node	El nodo que informó del evento (si corresponde).
ID de unidad	La unidad que informó del evento (si corresponde).
Hora del evento	La hora en que ocurrió el suceso.

Tipos de eventos

El sistema informa de múltiples tipos de eventos; cada evento es una operación que el sistema ha completado. Los eventos pueden ser rutinarios, normales o que requieran la atención del administrador. La columna "Tipos de evento" en la página del registro de eventos indica en qué parte del sistema ocurrió el evento.



El sistema no registra los comandos de API de solo lectura en el registro de eventos.

La siguiente lista describe los tipos de eventos que aparecen en el registro de eventos:

- **apiEvent**

Eventos iniciados por un usuario a través de una API o interfaz web que modifican la configuración.

- **binAssignmentsEvent**

Eventos relacionados con la asignación de intervalos de datos. Los bins son esencialmente contenedores que almacenan datos y se distribuyen por todo el clúster.

- **binSyncEvent**

Eventos del sistema relacionados con una reasignación de datos entre servicios de bloques.

- **bsCheckEvent**

Eventos del sistema relacionados con comprobaciones de servicio de bloqueo.

- **bsKillEvent**

Eventos del sistema relacionados con la finalización del servicio de bloqueo.

- **Evento de operación masiva**

Eventos relacionados con operaciones realizadas en un volumen completo, como una copia de seguridad, restauración, instantánea o clonación.

- **clonación de evento**

Eventos relacionados con la clonación de volúmenes.

- **Evento maestro de clúster**

Eventos que aparecen al inicializar el clúster o al realizar cambios en su configuración, como agregar o eliminar nodos.

- **cSumEvent**

Eventos relacionados con la detección de una discrepancia en la suma de comprobación durante la validación de la suma de comprobación de extremo a extremo.

Los servicios que detectan una discrepancia en la suma de comprobación se detienen automáticamente y no se reinician después de generar este evento.

- **evento de datos**

Eventos relacionados con la lectura y escritura de datos.

- **Evento de base de datos**

Eventos relacionados con la base de datos global mantenida por los nodos del conjunto en el clúster.

- **driveEvent**

Eventos relacionados con las operaciones de conducción.

- **Evento de cifrado en reposo**

Eventos relacionados con el proceso de cifrado en un clúster.

- **evento de conjunto**

Eventos relacionados con el aumento o la disminución del número de nodos en un conjunto.

- **Evento del canal de fibra**

Eventos relacionados con la configuración y las conexiones a los nodos.

- **gcEvento**

Los eventos relacionados con los procesos se ejecutan cada 60 minutos para recuperar espacio de almacenamiento en las unidades de bloque. Este proceso también se conoce como recogida de basura.

- **ieEvento**

Error interno del sistema.

- **Evento de instalación**

Eventos de instalación automática de software. El software se está instalando automáticamente en un nodo pendiente.

- **Evento iSCSIE**

Eventos relacionados con problemas de iSCSI en el sistema.

- **limitEvento**

Eventos relacionados con el número de volúmenes o volúmenes virtuales en una cuenta o en el clúster que se acercan al máximo permitido.

- **Evento de modo de mantenimiento**

Eventos relacionados con el modo de mantenimiento del nodo, como la desactivación del nodo.

- **evento_de_red**

Eventos relacionados con el informe de errores de red para cada interfaz de tarjeta de interfaz de red (NIC) física.

Estos eventos se activan cuando cualquier recuento de errores para una interfaz supera un umbral predeterminado de 1000 durante un intervalo de monitoreo de 10 minutos. Estos eventos se aplican a errores de red como fallos de recepción, errores de comprobación de redundancia cíclica (CRC), errores de longitud, errores de desbordamiento y errores de trama.

- **Evento de hardware de plataforma**

Eventos relacionados con problemas detectados en dispositivos de hardware.

- **evento de clúster remoto**

Eventos relacionados con el emparejamiento de clústeres remotos.

- **evento del planificador**

Eventos relacionados con instantáneas programadas.

- **evento de servicio**

Eventos relacionados con el estado del servicio del sistema.

- **sliceEvent**

Eventos relacionados con el servidor Slice, como la eliminación de una unidad o volumen de metadatos.

Existen tres tipos de eventos de reasignación de segmentos, que incluyen información sobre el servicio al que se asigna un volumen:

- cambio: modificar el servicio principal a un nuevo servicio principal.

```
sliceID oldPrimaryServiceID->newPrimaryServiceID
```

- traslado: cambio del servicio secundario a un nuevo servicio secundario

```
sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
```

- poda: eliminar un volumen de un conjunto de servicios

```
sliceID {oldSecondaryServiceID(s)}
```

- **snmpTrapEvent**

Eventos relacionados con las trampas SNMP.

- **estadoEvento**

Eventos relacionados con las estadísticas del sistema.

- **tsEvento**

Eventos relacionados con el servicio de transporte del sistema.

- **Excepción inesperada**

Eventos relacionados con excepciones inesperadas del sistema.

- **ureEvento**

Eventos relacionados con errores de lectura irreversibles que ocurren durante la lectura desde el dispositivo de almacenamiento.

- **Evento del proveedor vasa**

Eventos relacionados con un proveedor VASA (vSphere APIs for Storage Awareness).

Ver el estado de las tareas en ejecución

En la interfaz web, puede consultar el progreso y el estado de finalización de las tareas en ejecución que se reportan mediante los métodos API ListSyncJobs y ListBulkVolumeJobs. Puedes acceder a la página Tareas en ejecución desde la pestaña Informes de la interfaz de usuario de Element.

Si hay una gran cantidad de tareas, el sistema podría ponerlas en cola y ejecutarlas por lotes. La página Tareas en ejecución muestra los servicios que se están sincronizando actualmente. Cuando una tarea finaliza, se reemplaza por la siguiente tarea de sincronización en cola. Es posible que las tareas de sincronización sigan apareciendo en la página de Tareas en ejecución hasta que no haya más tareas por completar.



Puedes ver los datos de sincronización de replicación para los volúmenes que se están replicando en la página Tareas en ejecución del clúster que contiene el volumen de destino.

Alertas del sistema

Ver alertas del sistema

Puede consultar las alertas para obtener información sobre fallos del clúster o errores en el sistema. Las alertas pueden ser informativas, de advertencia o de error, y son un buen indicador del buen funcionamiento del clúster. La mayoría de los errores se resuelven automáticamente.

Puede utilizar el método de la API ListClusterFaults para automatizar la supervisión de alertas. Esto le permite recibir notificaciones sobre todas las alertas que se produzcan.

1. En la interfaz de usuario de Element, seleccione **Informes > Alertas**.

El sistema actualiza las alertas en la página cada 30 segundos.

Para cada evento, verá la siguiente información:

Artículo	Descripción

IDENTIFICACIÓN	Identificador único asociado a una alerta de clúster.
Gravedad	El grado de importancia de la alerta. Valores posibles: • Advertencia: Un problema menor que podría requerir atención pronto. Todavía se permiten las actualizaciones del sistema. • error: Un fallo que podría causar una degradación del rendimiento o la pérdida de alta disponibilidad (HA). En general, los errores no deberían afectar al servicio. • crítico: Una falla grave que afecta el servicio. El sistema no puede atender solicitudes de API o de E/S de cliente. Operar en este estado podría conllevar una posible pérdida de datos. • bestPractice: No se está utilizando una práctica recomendada de configuración del sistema.
Tipo	El componente afectado por la falla. Puede ser un nodo, una unidad, un clúster, un servicio o un volumen.
Node	Identificador del nodo al que se refiere este fallo. Incluido para fallos de nodo y unidad, de lo contrario establecido en - (guion).
ID de unidad	Identificación de la unidad a la que se refiere este fallo. Incluido en caso de fallos de la unidad, de lo contrario establecido en - (guion).
Código de error	Un código descriptivo que indica la causa del fallo.
Detalles	Descripción de la avería con detalles adicionales.
Fecha	Fecha y hora en que se registró la falla.

2. Haz clic en **Mostrar detalles** para ver información sobre una alerta individual.
3. Para ver los detalles de todas las alertas en la página, haga clic en la columna Detalles.

Una vez que el sistema resuelve una alerta, toda la información sobre la misma, incluida la fecha en que se resolvió, se traslada al área de Resueltas.

Encuentra más información

- [Códigos de falla del clúster](#)
- ["Gestiona el almacenamiento con la API de Element"](#)

Códigos de falla del clúster

El sistema informa de un error o un estado que podría ser de interés mediante la generación de un código de fallo, que aparece en la página de Alertas. Estos códigos le ayudan a determinar qué componente del sistema experimentó la alerta y por qué se generó.

La siguiente lista describe los diferentes tipos de códigos:

- **Fallo del servicio de autenticación**

El servicio de autenticación en uno o más nodos del clúster no funciona como se esperaba.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Direcciones IP de red virtual disponibles bajas**

El número de direcciones de red virtuales en el bloque de direcciones IP es bajo.

Para resolver este fallo, agregue más direcciones IP al bloque de direcciones de red virtual.

- **bloqueoClústerCompleto**

No hay suficiente espacio de almacenamiento de bloques libre para soportar la pérdida de un solo nodo. Consulte el método de la API `GetClusterFullThreshold` para obtener detalles sobre los niveles de plenitud del clúster. Este fallo en clúster indica una de las siguientes condiciones:

- `etapa3Baja` (Advertencia): Se superó el umbral definido por el usuario. Ajuste la configuración de Cluster Full o agregue más nodos.
- `etapa4Crítica` (Error): No hay suficiente espacio para recuperarse de una falla de 1 nodo. No se permite la creación de volúmenes, instantáneas ni clones.
- `etapa5CompletamenteConsumido` (Crítico)¹: No se permiten escrituras ni nuevas conexiones iSCSI. Las conexiones iSCSI actuales se mantendrán. Las escrituras fallarán hasta que se agregue más capacidad al clúster.

Para resolver este fallo, purgue o elimine volúmenes o agregue otro nodo de almacenamiento al clúster de almacenamiento.

- **bloquesDegradados**

Los datos del bloque ya no se replican completamente debido a una falla.

Gravedad	Descripción
Advertencia	Solo se puede acceder a dos copias completas de los datos del bloque.
Error	Solo se puede acceder a una única copia completa de los datos del bloque.
Crítico	No se puede acceder a copias completas de los datos del bloque.

Nota: El estado de advertencia solo puede ocurrir en un sistema Triple Helix.

Para resolver este fallo, restaure los nodos o servicios fuera de línea o bloquee los servicios, o póngase en contacto con el soporte de NetApp para obtener ayuda.

- **bloqueoServicioDemasiadoLleno**

Un servicio de bloques está utilizando demasiado espacio.

Para resolver este fallo, añada más capacidad aprovisionada.

- **bloquear servicio no saludable**

Se ha detectado que un servicio de bloqueo no funciona correctamente:

- Gravedad = Advertencia: No se toma ninguna medida. Este período de advertencia expirará en `cTimeUntilBSIsKilledMSec=330000` milisegundos.
- Gravedad = Error: El sistema está desactivando automáticamente los datos y replicándolos en otras unidades en buen estado.
- Gravedad = Crítica: Hay servicios de bloque fallidos en varios nodos mayores o iguales al recuento de replicación (2 para doble hélice). Los datos no están disponibles y la sincronización del contenedor no finalizará.

Compruebe si hay problemas de conectividad de red y errores de hardware. Si fallan componentes de hardware específicos, se producirán otras averías. La avería desaparecerá cuando se pueda acceder al servicio de bloqueo o cuando el servicio haya sido desactivado.

- **Error en la autocomprobación de Bmc**

El controlador de gestión de la placa base (BMC) falló una autocomprobación.

Póngase en contacto con el soporte técnico de NetApp para obtener ayuda.

Durante una actualización a Element 12.5 o posterior, `BmcSelfTestFailed` No se genera ningún fallo para un nodo que tenga un BMC defectuoso preexistente, o cuando el BMC de un nodo falla durante la actualización. Los BMC que no superen las autocomprobaciones durante la actualización emitirán un `BmcSelfTestFailed` Se produce un fallo de advertencia después de que todo el clúster complete la actualización.

- **La asimetría del reloj supera el umbral de fallos**

La diferencia horaria entre el nodo maestro del clúster y el nodo que presenta un token supera el umbral recomendado. El clúster de almacenamiento no puede corregir automáticamente la diferencia horaria entre los nodos.

Para resolver este problema, utilice servidores NTP internos de su red, en lugar de los servidores predeterminados de la instalación. Si está utilizando un servidor NTP interno, póngase en contacto con el soporte de NetApp para obtener ayuda.

- **clusterCannotSync**

Existe una condición de falta de espacio y los datos de las unidades de almacenamiento en bloque fuera de línea no se pueden sincronizar con las unidades que aún están activas.

Para solucionar este problema, agregue más almacenamiento.

- **clusterFull**

No hay más espacio de almacenamiento libre en el clúster de almacenamiento.

Para solucionar este problema, agregue más almacenamiento.

- **El clúster tiene sobreaprovisionamiento**

Las IOPS del clúster están sobreaprovisionadas. La suma de todas las IOPS mínimas de QoS es mayor que las IOPS esperadas del clúster. No se puede mantener un nivel mínimo de QoS para todos los volúmenes simultáneamente.

Para resolver este problema, reduzca la configuración mínima de IOPS de QoS para los volúmenes.

- **Umbral de evento térmico de la CPU**

El número de eventos térmicos de la CPU en una o más CPU supera el umbral configurado.

Si no se detectan nuevos eventos térmicos de la CPU en diez minutos, la advertencia desaparecerá automáticamente.

- **Error al deshabilitar la seguridad de la unidad**

El clúster no está configurado para habilitar la seguridad de la unidad (cifrado en reposo), pero al menos una unidad tiene habilitada la seguridad de la unidad, lo que significa que deshabilitar la seguridad de la unidad en esas unidades falló. Este fallo se registra con gravedad "Advertencia".

Para resolver este fallo, compruebe los detalles del fallo para conocer el motivo por el cual no se pudo desactivar la seguridad de la unidad. Las posibles razones son:

- No se pudo obtener la clave de cifrado; investigue el problema de acceso a la clave o al servidor de claves externo.
- La operación de desactivación falló en la unidad; determine si posiblemente se adquirió una clave incorrecta.

Si ninguna de estas es la causa de la avería, es posible que haya que sustituir la unidad.

Puede intentar recuperar una unidad que no logra deshabilitar la seguridad incluso cuando se proporciona la clave de autenticación correcta. Para realizar esta operación, retire la(s) unidad(es) del sistema moviéndola(s) a Disponible, realice un borrado seguro en la unidad y vuelva a moverla(s) a Activo.

- **Par de clústeres desconectado**

Un par de clústeres está desconectado o configurado incorrectamente.

Comprobar la conectividad de red entre los clústeres.

- **nodo remoto desconectado**

Un nodo remoto está desconectado o configurado incorrectamente.

Comprobar la conectividad de red entre los nodos.

- **punto final SnapMirror desconectado**

Un punto final remoto de SnapMirror está desconectado o configurado incorrectamente.

Compruebe la conectividad de red entre el clúster y el SnapMirrorEndpoint remoto.

- **Conductor disponible**

En el clúster hay disponible una o más unidades. En general, todos los clústeres deberían tener todas las unidades agregadas y ninguna en estado disponible. Si este fallo aparece de forma inesperada, póngase en contacto con el soporte de NetApp .

Para resolver este fallo, agregue las unidades disponibles al clúster de almacenamiento.

- **fallo de la unidad**

El clúster devuelve este fallo cuando una o más unidades han fallado, lo que indica una de las siguientes condiciones:

- El administrador de la unidad no puede acceder a la unidad.
- El servicio de segmentación o bloque ha fallado demasiadas veces, presumiblemente debido a fallos de lectura o escritura en la unidad, y no puede reiniciarse.
- Falta la unidad.
- El servicio maestro del nodo es inaccesible (todas las unidades del nodo se consideran faltantes/fallidas).
- La unidad está bloqueada y no se puede obtener la clave de autenticación.
- La unidad está bloqueada y la operación de desbloqueo falla.

Para resolver este problema:

- Compruebe la conectividad de red del nodo.
- Reemplace la unidad.
- Asegúrese de que la clave de autenticación esté disponible.

- **fallo de estado de la unidad**

La unidad no ha superado la comprobación de estado SMART y, como resultado, sus funciones se han visto reducidas. Existe un nivel de gravedad crítico para esta falla:

- La unidad con número de serie: <número de serie> en la ranura: <ranura del nodo><ranura de la unidad> no ha superado la comprobación general de estado SMART.

Para solucionar este problema, sustituya la unidad.

- **Fallo de desgaste de la unidad**

La vida útil restante de la unidad ha caído por debajo de los umbrales establecidos, pero aún funciona. Existen dos posibles niveles de gravedad para esta falla: Crítica y Advertencia.

- La unidad con número de serie: <número de serie> en la ranura: <ranura del nodo><ranura de la unidad> tiene niveles de desgaste críticos.
- La unidad con número de serie: <número de serie> en la ranura: <ranura del nodo><ranura de la unidad> tiene bajas reservas de desgaste.

Para solucionar este problema, sustituya la unidad lo antes posible.

- **candidatos duplicados de maestro de clúster**

Se ha detectado más de un candidato a maestro de clúster de almacenamiento.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Error al habilitar la seguridad de la unidad**

El clúster está configurado para requerir seguridad de la unidad (cifrado en reposo), pero no se pudo habilitar la seguridad de la unidad en al menos una unidad. Este fallo se registra con gravedad "Advertencia".

Para resolver este fallo, compruebe los detalles del fallo para conocer el motivo por el que no se pudo habilitar la seguridad de la unidad. Las posibles razones son:

- No se pudo obtener la clave de cifrado; investigue el problema de acceso a la clave o al servidor de claves externo.
- La operación de habilitación falló en la unidad; determine si posiblemente se adquirió la clave incorrecta. Si ninguna de estas es la causa de la avería, es posible que haya que sustituir la unidad.

Puede intentar recuperar una unidad que no habilita correctamente la seguridad incluso cuando se proporciona la clave de autenticación correcta. Para realizar esta operación, retire la(s) unidad(es) del sistema moviéndola(s) a Disponible, realice un borrado seguro en la unidad y vuelva a moverla(s) a Activo.

- **conjunto degradado**

Se ha perdido la conectividad de red o el suministro eléctrico en uno o más de los nodos del conjunto.

Para resolver esta falla, restablezca la conectividad de red o la alimentación eléctrica.

- **excepción**

Se ha reportado una avería que no es una avería rutinaria. Estas fallas no se borran automáticamente de la cola de fallas.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **fallóEspacioDemasiadoLleno**

Un servicio de bloques no responde a las solicitudes de escritura de datos. Esto provoca que el servicio de segmentación se quede sin espacio para almacenar las escrituras fallidas.

Para resolver este fallo, restaure la funcionalidad de los servicios de bloques para permitir que las escrituras continúen normalmente y que el espacio fallido se elimine del servicio de segmentación.

- **sensor de ventilador**

Un sensor del ventilador ha fallado o falta.

Para solucionar este problema, sustituya cualquier componente de hardware defectuoso.

- **Acceso Fibre Channel degradado**

Un nodo Fibre Channel no responde a otros nodos del clúster de almacenamiento a través de su IP de almacenamiento durante un período de tiempo. En este estado, el nodo se considerará no responsivo y generará un fallo de clúster.

Comprobar la conectividad de red.

- **Acceso a Fibre Channel no disponible**

Todos los nodos Fibre Channel no responden. Se muestran los identificadores de los nodos.

Comprobar la conectividad de red.

- **fibreChannelActiveIxl**

El recuento de Ixl Nexus se está acercando al límite admitido de 8000 sesiones activas por nodo Fibre Channel.

- El límite recomendado es de 5500.
- El límite de advertencia es de 7500.
- El límite máximo (no aplicado) es 8192.

Para resolver este fallo, reduzca el recuento de Ixl Nexus por debajo del límite de mejores prácticas de 5500.

- **Configuración de canal de fibra**

Este fallo en clúster indica una de las siguientes condiciones:

- Hay un puerto Fibre Channel inesperado en una ranura PCI.
- Existe un modelo de HBA de canal de fibra inesperado.
- Existe un problema con el firmware de un HBA de canal de fibra.
- Un puerto Fibre Channel no está en línea.
- Existe un problema persistente al configurar el paso de Fibre Channel.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **IOPS de canal de fibra**

El recuento total de IOPS se está acercando al límite de IOPS para los nodos Fibre Channel en el clúster. Los límites son:

- FC0025: Límite de 450K IOPS con un tamaño de bloque de 4K por nodo Fibre Channel.
- FCN001: Límite de 625K OPS con un tamaño de bloque de 4K por nodo Fibre Channel.

Para resolver este fallo, equilibre la carga entre todos los nodos Fibre Channel disponibles.

- **fibreChannelStaticIxl**

El recuento de Ixl Nexus se está acercando al límite admitido de 16000 sesiones estáticas por nodo Fibre Channel.

- El límite recomendado es de 11000.
- El límite de advertencia es de 15000.
- El límite máximo (aplicable) es 16384.

Para resolver este fallo, reduzca el recuento de Ixl Nexus por debajo del límite de mejores prácticas de 11000.

- **Capacidad del sistema de archivos baja**

No hay suficiente espacio en uno de los sistemas de archivos.

Para resolver este fallo, añada más capacidad al sistema de archivos.

- **El sistema de archivos es de solo lectura**

El sistema de archivos ha entrado en modo de solo lectura.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **FipsDrivesMismatch**

Se ha insertado físicamente una unidad no FIPS en un nodo de almacenamiento compatible con FIPS o se ha insertado físicamente una unidad FIPS en un nodo de almacenamiento no FIPS. Se genera un único fallo por nodo y se enumeran todas las unidades afectadas.

Para solucionar este problema, retire o sustituya la unidad o unidades incompatibles en cuestión.

- **fipsDrivesOutOfCompliance**

El sistema ha detectado que el cifrado en reposo se desactivó después de que se habilitara la función de unidades FIPS. Este fallo también se genera cuando la función de unidades FIPS está habilitada y hay una unidad o nodo que no sea FIPS en el clúster de almacenamiento.

Para resolver este fallo, habilite el cifrado en reposo o retire el hardware no FIPS del clúster de almacenamiento.

- **fallo en la autocomprobación de fips**

El subsistema FIPS ha detectado un fallo durante la autocomprobación.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Desajuste de configuración de hardware**

Este fallo en clúster indica una de las siguientes condiciones:

- La configuración no coincide con la definición del nodo.
- El tamaño de la unidad es incorrecto para este tipo de nodo.
- Se ha detectado una unidad no compatible. Una posible razón es que la versión de Element instalada no reconoce esta unidad. Se recomienda actualizar el software Element en este nodo.
- Existe una incompatibilidad en el firmware del controlador.
- El estado de capacidad de cifrado de la unidad no coincide con el nodo.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Fecha de vencimiento del certificado idPC**

El certificado SSL del proveedor de servicios del clúster para su uso con un proveedor de identidad (IdP) de terceros está próximo a caducar o ya ha caducado. Esta falla utiliza los siguientes niveles de gravedad según su urgencia:

Gravedad	Descripción
Advertencia	El certificado caduca en 30 días.
Error	El certificado caduca en 7 días.
Crítico	El certificado caduca en 3 días o ya ha caducado.

Para solucionar este problema, actualice el certificado SSL antes de que caduque. Utilice el método de la API `UpdateDpConfiguration` con `refreshCertificateExpirationTime=true` para proporcionar el certificado SSL actualizado.

- **modos de enlace inconsistentes**

Faltan los modos de enlace en el dispositivo VLAN. Este fallo mostrará el modo de enlace esperado y el modo de enlace que se está utilizando actualmente.

- **Mtus inconsistente**

Este fallo en clúster indica una de las siguientes condiciones:

- Desajuste en Bond1G: Se han detectado MTU inconsistentes en las interfaces Bond1G.
- Desajuste de Bond10G: Se han detectado MTU inconsistentes en las interfaces Bond10G.

Este error muestra el nodo o nodos en cuestión junto con el valor MTU asociado.

- **reglas de enrutamiento inconsistentes**

Las reglas de enrutamiento para esta interfaz son inconsistentes.

- **máscaras de subred inconsistentes**

La máscara de red del dispositivo VLAN no coincide con la máscara de red registrada internamente para la VLAN. Este error muestra la máscara de red esperada y la máscara de red que se está utilizando actualmente.

- **recuento incorrecto de puertos de enlace**

El número de puertos de enlace es incorrecto.

- **Recuento de nodos de canal de fibra configurado no válido**

Una de las dos conexiones de nodo Fibre Channel previstas está degradada. Este fallo aparece cuando solo está conectado un nodo Fibre Channel.

Para resolver esta falla, verifique la conectividad de la red del clúster y el cableado de red, y compruebe si hay servicios que hayan fallado. Si no hay problemas de red o de servicio, póngase en contacto con el soporte de NetApp para solicitar un reemplazo del nodo Fibre Channel.

- **Error de balanceo de interrupciones**

Se produjo una excepción al intentar equilibrar las interrupciones.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **kmipCertificateFault**

- El certificado de la Autoridad de Certificación (CA) raíz está próximo a caducar.

Para resolver este fallo, adquiera un nuevo certificado de la CA raíz con una fecha de vencimiento de al menos 30 días y utilice `ModifyKeyServerKmp` para proporcionar el certificado actualizado de la CA raíz.

- El certificado del cliente está próximo a caducar.

Para resolver este problema, cree una nueva CSR utilizando `GetClientCertificateSigningRequest`, fírmela asegurándose de que la nueva fecha de vencimiento sea al menos 30 días posterior, y utilice `ModifyKeyServerKmp` para reemplazar el certificado de cliente KMIP que vence con el nuevo certificado.

- El certificado de la Autoridad de Certificación (CA) raíz ha caducado.

Para resolver este fallo, adquiera un nuevo certificado de la CA raíz con una fecha de vencimiento de al menos 30 días y utilice `ModifyKeyServerKmp` para proporcionar el certificado actualizado de la CA raíz.

- El certificado del cliente ha caducado.

Para resolver este problema, cree una nueva CSR utilizando `GetClientCertificateSigningRequest`, fírmela asegurándose de que la nueva fecha de vencimiento sea al menos 30 días posterior y utilice `ModifyKeyServerKmp` para reemplazar el certificado de cliente KMIP vencido con el nuevo certificado.

- Error en el certificado de la Autoridad de Certificación (CA) raíz.

Para resolver este fallo, compruebe que se ha proporcionado el certificado correcto y, si es necesario, vuelva a adquirir el certificado de la CA raíz. Utilice `ModifyKeyServerKmp` para instalar el certificado de cliente KMIP correcto.

- Error en el certificado del cliente.

Para resolver este fallo, compruebe que esté instalado el certificado de cliente KMIP correcto. La CA raíz del certificado del cliente debe estar instalada en el EKS. Utilice `ModifyKeyServerKmp` para instalar el certificado de cliente KMIP correcto.

- **kmipServerFault**

- Fallo de conexión

Para resolver este fallo, compruebe que el servidor de claves externo está activo y accesible a través de la red. Utilice `TestKeyServerKimp` y `TestKeyProviderKmp` para probar su conexión.

- Fallo de autenticación

Para resolver este fallo, compruebe que se están utilizando los certificados de CA raíz y de cliente KMIP correctos, y que la clave privada y el certificado de cliente KMIP coinciden.

- Error del servidor

Para resolver este fallo, compruebe los detalles del error. Es posible que sea necesario solucionar problemas en el servidor de claves externo según el error devuelto.

- **umbral de error de memoria**

Se ha detectado un gran número de errores ECC corregibles e incorregibles. Esta falla utiliza los siguientes niveles de gravedad según su urgencia:

Evento	Gravedad	Descripción
Un único DIMM cErrorCount alcanza cDimmCorrectableErrWarnThreshold.	Advertencia	Errores de memoria ECC corregibles por encima del umbral en DIMM: <Procesador> <Ranura DIMM>
Un único valor de cErrorCount de DIMM permanece por encima de cDimmCorrectableErrWarnThreshold hasta que expire cErrorFaultTimer para el DIMM.	Error	Errores de memoria ECC corregibles por encima del umbral en DIMM: <Procesador> <DIMM>
Un controlador de memoria informa que cErrorCount supera cMemCtrlrCorrectableErrWarnThreshold, y se especifica cMemCtrlrCorrectableErrWarnDuration.	Advertencia	Errores de memoria ECC corregibles por encima del umbral en el controlador de memoria: <Procesador> <Controlador de memoria>
Un controlador de memoria informa que cErrorCount está por encima de cMemCtrlrCorrectableErrWarnThreshold hasta que expire cErrorFaultTimer para el controlador de memoria.	Error	Errores de memoria ECC corregibles por encima del umbral en DIMM: <Procesador> <DIMM>
Un único DIMM informa un uErrorCount superior a cero, pero inferior a cDimmUncorrectableErrFaultThreshold.	Advertencia	Se han detectado errores de memoria ECC no corregibles en el módulo DIMM: <Procesador> <Ranura DIMM>
Un único DIMM informa un uErrorCount de al menos cDimmUncorrectableErrFaultThreshold.	Error	Se han detectado errores de memoria ECC no corregibles en el módulo DIMM: <Procesador> <Ranura DIMM>
Un controlador de memoria informa un uErrorCount superior a cero, pero inferior a cMemCtrlrUncorrectableErrFaultThreshold.	Advertencia	Se han detectado errores de memoria ECC no corregibles en el controlador de memoria: <Procesador> <Controlador de memoria>

Un controlador de memoria informa un uErrorCount de al menos cMemCtrlrUncorrectableErrFaultThreshold.	Error	Se han detectado errores de memoria ECC no corregibles en el controlador de memoria: <Procesador> <Controlador de memoria>

Para resolver este problema, póngase en contacto con el soporte técnico de NetApp para obtener ayuda.

• umbral de uso de memoria

El uso de memoria es superior a lo normal. Esta falla utiliza los siguientes niveles de gravedad según su urgencia:



Consulte el apartado **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 está completamente agotada.

Para resolver este problema, póngase en contacto con el soporte técnico de NetApp para obtener ayuda.

• metadataClusterFull

No hay suficiente espacio libre de almacenamiento de metadatos para soportar la pérdida de un solo nodo. Consulte el método de la API GetClusterFullThreshold para obtener detalles sobre los niveles de plenitud del clúster. Este fallo en clúster indica una de las siguientes condiciones:

- etapa3Baja (Advertencia): Se superó el umbral definido por el usuario. Ajuste la configuración de Cluster Full o agregue más nodos.
- etapa4Crítica (Error): No hay suficiente espacio para recuperarse de una falla de 1 nodo. No se permite la creación de volúmenes, instantáneas ni clones.
- etapa5CompletamenteConsumido (Crítico)¹: No se permiten escrituras ni nuevas conexiones iSCSI. Las conexiones iSCSI actuales se mantendrán. Las escrituras fallarán hasta que se agregue más capacidad al clúster. Elimine o borre datos o agregue más nodos.

Para resolver este fallo, purgue o elimine volúmenes o agregue otro nodo de almacenamiento al clúster de almacenamiento.

• Fallo en la comprobación de mtu

Un dispositivo de red no está configurado con el tamaño MTU adecuado.

Para resolver este fallo, asegúrese de que todas las interfaces de red y los puertos del conmutador estén configurados para tramas jumbo (MTU de hasta 9000 bytes).

- **Configuración de red**

Este fallo en clúster indica una de las siguientes condiciones:

- No se encuentra presente la interfaz esperada.
- Existe una interfaz duplicada.
- Una interfaz configurada está inactiva.
- Es necesario reiniciar la red.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **noHayDireccionesIPdeRedVirtualDisponibles**

No hay direcciones de red virtual disponibles en el bloque de direcciones IP.

- virtualNetworkID # TAG(###) no tiene direcciones IP de almacenamiento disponibles. No se pueden agregar nodos adicionales al clúster.

Para resolver este fallo, agregue más direcciones IP al bloque de direcciones de red virtual.

- **fallo de hardware del nodo (la interfaz de red <nombre> está inactiva o el cable está desconectado)**

La interfaz de red está inactiva o el cable está desconectado.

Para resolver este fallo, compruebe la conectividad de red del nodo o nodos.

- **Fallo de hardware del nodo (El estado de capacidad de cifrado de la unidad no coincide con el estado de capacidad de cifrado del nodo para la unidad en la ranura <ranura del nodo><ranura de la unidad>)**

Una unidad no tiene las capacidades de cifrado compatibles con el nodo de almacenamiento en el que está instalada.

- **Fallo de hardware del nodo (Tamaño incorrecto de la unidad <tipo de unidad> <tamaño real> para la unidad en la ranura <ranura del nodo><ranura de la unidad> para este tipo de nodo - se esperaba <tamaño esperado>)**

Un nodo de almacenamiento contiene una unidad de almacenamiento cuyo tamaño no es el adecuado para este nodo.

- **Fallo de hardware del nodo (Se ha detectado una unidad no compatible en la ranura <ranura del nodo><ranura de la unidad>; las estadísticas y la información de estado de la unidad no estarán disponibles)**

Un nodo de almacenamiento contiene una unidad que no admite.

- **fallo de hardware del nodo (La unidad en la ranura <ranura del nodo><ranura de la unidad> debería estar usando la versión de firmware <versión esperada>, pero está usando una versión no compatible <versión actual>)**

Un nodo de almacenamiento contiene una unidad que ejecuta una versión de firmware no compatible.

- **modo de mantenimiento del nodo**

Un nodo ha sido puesto en modo de mantenimiento. Esta falla utiliza los siguientes niveles de gravedad

según su urgencia:

Gravedad	Descripción
Advertencia	Indica que el nodo aún está en modo de mantenimiento.
Error	Indica que el modo de mantenimiento no se ha podido desactivar, muy probablemente debido a fallos o sistemas en espera activos.

Para solucionar este problema, desactive el modo de mantenimiento una vez finalizado el mantenimiento. Si el fallo de nivel de error persiste, póngase en contacto con el soporte de NetApp para obtener ayuda.

- **nodo fuera de línea**

El software Element no puede comunicarse con el nodo especificado. Comprobar la conectividad de red.

- **no se usa el modo de puente LACP**

El modo de enlace LACP no está configurado.

Para resolver este problema, utilice el enlace LACP al implementar nodos de almacenamiento; los clientes podrían experimentar problemas de rendimiento si LACP no está habilitado y configurado correctamente.

- **Servidor ntp inaccesible**

El clúster de almacenamiento no puede comunicarse con el servidor o servidores NTP especificados.

Para resolver este fallo, compruebe la configuración del servidor NTP, la red y el cortafuegos.

- **ntpTimeNoEstáSincronizado**

La diferencia entre la hora del clúster de almacenamiento y la hora del servidor NTP especificado es demasiado grande. El clúster de almacenamiento no puede corregir la diferencia automáticamente.

Para resolver este problema, utilice servidores NTP internos de su red, en lugar de los servidores predeterminados de la instalación. Si está utilizando servidores NTP internos y el problema persiste, póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Estado del dispositivo nvram**

Un dispositivo NVRAM tiene un error, está fallando o ha fallado. Esta falla presenta las siguientes severidades:

Gravedad	Descripción

Advertencia	El hardware ha detectado una advertencia. Esta condición puede ser transitoria, como por ejemplo una alerta de temperatura. • nvmlLifetimeError • nvmlLifetimeStatus • Estado de la vida útil de la fuente de energía • Estado de la temperatura de la fuente de energía • Se superó el umbral de advertencia
Error	El hardware ha detectado un error o un estado crítico. El maestro del clúster intenta retirar la unidad de partición de funcionamiento (esto genera un evento de extracción de unidad). Si no están disponibles los servicios de partición secundaria, la unidad no se extraerá. Errores devueltos además de los errores de nivel de advertencia: • No existe un punto de montaje para el dispositivo NVRAM . • La partición del dispositivo NVRAM no existe. • La partición del dispositivo NVRAM existe, pero no está montada.
Crítico	El hardware ha detectado un error o un estado crítico. El maestro del clúster intenta retirar la unidad de partición de funcionamiento (esto genera un evento de extracción de unidad). Si no están disponibles los servicios de partición secundaria, la unidad no se extraerá. • persistencia perdida • estado del brazo GuardarN Armado • Error de estado de csave

Reemplace cualquier componente de hardware defectuoso en el nodo. Si esto no resuelve el problema, póngase en contacto con el soporte técnico de NetApp para obtener ayuda.

• Error de fuente de alimentación

Este fallo en clúster indica una de las siguientes condiciones:

- No hay fuente de alimentación.
- Se ha producido un fallo en la fuente de alimentación.
- Falta una entrada de alimentación o está fuera de rango.

Para resolver esta falla, verifique que se suministre alimentación redundante a todos los nodos. Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **espacio aprovisionado demasiado lleno**

La capacidad total aprovisionada del clúster está demasiado llena.

Para resolver este fallo, agregue más espacio aprovisionado o elimine y purgue volúmenes.

- **remoteRepAsyncDelayExceeded**

Se ha superado el retardo asíncrono configurado para la replicación. Comprobar la conectividad de red entre clústeres.

- **remoteRepClusterFull**

Los volúmenes han pausado la replicación remota porque el clúster de almacenamiento de destino está demasiado lleno.

Para resolver este fallo, libere algo de espacio en el clúster de almacenamiento de destino.

- **remoteRepSnapshotClusterFull**

Los volúmenes han pausado la replicación remota de instantáneas porque el clúster de almacenamiento de destino está demasiado lleno.

Para resolver este fallo, libere algo de espacio en el clúster de almacenamiento de destino.

- **Se ha superado el límite de instantáneas de representantes remotos**

Los volúmenes han pausado la replicación remota de instantáneas porque el volumen del clúster de almacenamiento de destino ha superado su límite de instantáneas.

Para resolver este fallo, aumente el límite de instantáneas en el clúster de almacenamiento de destino.

- **Error de acción programada**

Una o más de las actividades programadas se ejecutaron, pero fallaron.

El fallo se soluciona si la actividad programada se ejecuta de nuevo y tiene éxito, si se elimina la actividad programada o si se pausa y se reanuda.

- **Error al leer el sensor**

Un sensor no pudo comunicarse con el controlador de gestión de la placa base (BMC).

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **servicio no en ejecución**

Un servicio necesario no está en funcionamiento.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **sliceServiceTooFull**

Un servicio de segmentación tiene asignada muy poca capacidad aprovisionada.

Para resolver este fallo, añada más capacidad aprovisionada.

- **sliceServicePoco saludable**

El sistema ha detectado que un servicio de segmentación no funciona correctamente y lo está desactivando automáticamente.

- Gravedad = Advertencia: No se toma ninguna medida. Este periodo de advertencia expirará en 6 minutos.
- Gravedad = Error: El sistema está desactivando automáticamente los datos y replicándolos en otras unidades en buen estado.

Compruebe si hay problemas de conectividad de red y errores de hardware. Si fallan componentes de hardware específicos, se producirán otras averías. El fallo se solucionará cuando el servicio de segmentación esté accesible o cuando el servicio haya sido desactivado.

- **ssh habilitado**

El servicio SSH está habilitado en uno o más nodos del clúster de almacenamiento.

Para resolver este fallo, deshabilite el servicio SSH en el nodo o nodos correspondientes o póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Caducidad del certificado SSL**

El certificado SSL asociado a este nodo está próximo a caducar o ya ha caducado. Esta falla utiliza los siguientes niveles de gravedad según su urgencia:

Gravedad	Descripción
Advertencia	El certificado caduca en 30 días.
Error	El certificado caduca en 7 días.
Crítico	El certificado caduca en 3 días o ya ha caducado.

Para solucionar este problema, renueve el certificado SSL. Si necesita ayuda, póngase en contacto con el soporte técnico de NetApp .

- **capacidad varada**

Un solo nodo representa más de la mitad de la capacidad del clúster de almacenamiento.

Para mantener la redundancia de datos, el sistema reduce la capacidad del nodo más grande, de modo que parte de su capacidad de bloque queda inactiva (sin utilizar).

Para resolver este fallo, agregue más unidades a los nodos de almacenamiento existentes o agregue nodos de almacenamiento al clúster.

- **sensor de temperatura**

Un sensor de temperatura está registrando temperaturas superiores a lo normal. Esta falla puede producirse junto con fallas de powerSupplyError o fanSensor.

Para resolver este fallo, compruebe si hay obstrucciones en el flujo de aire cerca del clúster de almacenamiento. Si es necesario, póngase en contacto con el soporte de NetApp para obtener ayuda.

- **mejora**

La actualización lleva en curso más de 24 horas.

Para resolver este problema, reanude la actualización o póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Servicio que no responde**

Un servicio ha dejado de responder.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Configuración de red virtual**

Este fallo en clúster indica una de las siguientes condiciones:

- No hay ninguna interfaz presente.
- Existe un espacio de nombres incorrecto en una interfaz.
- Existe una máscara de red incorrecta.
- Existe una dirección IP incorrecta.
- Una interfaz no está operativa.
- Existe una interfaz superflua en un nodo.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **volúmenes degradados**

Los volúmenes secundarios no han terminado de replicarse y sincronizarse. El mensaje se borra cuando finaliza la sincronización.

- **volúmenesDesconectados**

Uno o más volúmenes del clúster de almacenamiento están fuera de línea. También estará presente el fallo **volumeDegraded**.

Póngase en contacto con el soporte de NetApp para obtener ayuda.

Ver actividad de rendimiento del nodo

Puede visualizar la actividad de rendimiento de cada nodo en formato gráfico. Esta información proporciona estadísticas en tiempo real sobre la CPU y las operaciones de E/S de lectura/escritura por segundo (IOPS) para cada unidad del nodo. El gráfico de utilización se actualiza cada cinco segundos, y el gráfico de estadísticas de la unidad se actualiza cada diez segundos.

1. Haz clic en **Clúster > Nodos**.
2. Haz clic en **Acciones** para el nodo que deseas ver.
3. Haga clic en **Ver detalles**.



Puedes ver puntos específicos en el tiempo en los gráficos de líneas y barras colocando el cursor sobre la línea o la barra.

Rendimiento de volumen

Rendimiento del volumen de visualización

Puede consultar información detallada sobre el 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 puedes filtrar la información según ciertos criterios.

Puedes 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 selecciona el valor Nunca, la actualización automática de la página se desactiva.

Puedes volver a habilitar la actualización automática haciendo clic en **Activar actualización automática**.

1. En la interfaz de usuario de Element, seleccione **Informes > Rendimiento de volumen**.
2. En la lista de volúmenes, haga clic en el icono Acciones de un volumen.
3. Haga clic en **Ver detalles**.

En la parte inferior de la página se muestra una bandeja 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, así como gráficos de rendimiento del volumen.

Encuentra más información

[Detalles del rendimiento del volumen](#)

Detalles del rendimiento del volumen

Puede consultar las estadísticas de rendimiento de los volúmenes en la página Rendimiento del volumen de la pestaña Informes en la interfaz de usuario de Element.

La siguiente lista describe los detalles que están a su disposición:

- **IDENTIFICACIÓN**

El identificador generado por el sistema para el volumen.

- **Nombre**

El nombre que se le dio al volumen cuando fue creado.

- **Cuenta**

El nombre de la cuenta asignada al volumen.

- **Grupos de acceso**

El nombre del grupo o grupos de acceso al volumen al que pertenece el volumen.

- **Utilización del volumen**

Un valor porcentual que describe cuánto volumen está utilizando el cliente.

Valores posibles:

- 0 = El cliente no usa el volumen
- 100 = El cliente está utilizando el máximo
- >100 = El cliente está utilizando la ráfaga.

- **Total de IOPS**

El número total de IOPS (lectura y escritura) que se están ejecutando actualmente en el volumen.

- **Leer IOPS**

El número total de IOPS de lectura que se están ejecutando actualmente en el volumen.

- **Escribir IOPS**

El número total de IOPS de escritura que se están ejecutando actualmente en el volumen.

- **Rendimiento total**

Cantidad total de operaciones de lectura y escritura que se están ejecutando actualmente en el volumen.

- **Rendimiento de lectura**

Cantidad total de operaciones de lectura que se están ejecutando actualmente en el volumen.

- **Rendimiento de escritura**

Cantidad total de operaciones de escritura que se están ejecutando actualmente en el volumen.

- **Latencia total**

El tiempo promedio, en microsegundos, para completar las operaciones de lectura y escritura en un volumen.

- **Latencia de lectura**

Tiempo promedio, en microsegundos, para completar las operaciones de lectura del volumen en los últimos 500 milisegundos.

- **Latencia de escritura**

Tiempo promedio, en microsegundos, para completar las operaciones de escritura en un volumen en los últimos 500 milisegundos.

- **Profundidad de la cola**

Número de operaciones de lectura y escritura pendientes en el volumen.

- **Tamaño promedio de E/S**

Tamaño promedio en bytes de las operaciones de E/S recientes en el volumen en los últimos 500 milisegundos.

Sesiones iSCSI

Ver sesiones iSCSI

Puede ver las sesiones iSCSI que están conectadas al clúster. Puedes filtrar la información para incluir solo las sesiones deseadas.

1. En la interfaz de usuario de Element, seleccione **Informes > Sesiones iSCSI**.
2. Para ver los campos de criterios de filtro, haga clic en **Filtrar**.

Encuentra más información

[Detalles de la sesión iSCSI](#)

Detalles de la sesión iSCSI

Puede ver información sobre las sesiones iSCSI que están conectadas al clúster.

La siguiente lista describe la información que puede encontrar sobre las sesiones iSCSI:

- **Nodo**

El nodo que aloja la partición de metadatos principal del volumen.

- **Cuenta**

El nombre de la cuenta propietaria del volumen. Si el valor está en blanco, se muestra un guion (-).

- **Volumen**

El nombre del volumen identificado en el nodo.

- **ID de volumen**

Identificación del volumen asociado con el IQN objetivo.

- **ID del iniciador**

Un identificador generado por el sistema para el iniciador.

- **Alias del iniciador**

Un nombre opcional para el iniciador que facilita su búsqueda en una lista larga.

- **Dirección IP del iniciador**

La dirección IP del punto final que inicia la sesión.

- **Iniciador IQN**

El IQN del punto final que inicia la sesión.

- **IP de destino**

La dirección IP del nodo que aloja el volumen.

- **IQN objetivo**

El IQN del volumen.

- **CAP**

El algoritmo CHAP para una sesión iSCSI. Si no se está utilizando un algoritmo CHAP, se muestra un guion (-). Disponible a partir del Elemento 12.8.

- **Creado el**

Fecha en que se estableció la sesión.

Sesiones de Fibre Channel

Ver sesiones de Fibre Channel

Puede ver las sesiones de Fibre Channel (FC) que están conectadas al clúster. Puede filtrar la información para incluir solo las conexiones que desea que se muestren en la ventana.

1. En la interfaz de usuario de Element, seleccione **Informes > Sesiones FC**.
2. Para ver los campos de criterios de filtro, haga clic en **Filtrar**.

Encuentra más información

[Detalles de la sesión de Fibre Channel](#)

Detalles de la sesión de Fibre Channel

Puede encontrar información sobre las sesiones Fibre Channel (FC) activas que están conectadas al clúster.

La siguiente lista describe la información que puede encontrar sobre las sesiones FC conectadas al clúster:

- **ID del nodo**

El nodo que aloja la sesión para la conexión.

- **Nombre del nodo**

Nombre del nodo generado por el sistema.

- **ID del iniciador**

Un identificador generado por el sistema para el iniciador.

- **Iniciador WWPN**

El nombre del puerto mundial inicial.

- **Alias del iniciador**

Un nombre opcional para el iniciador que facilita su búsqueda en una lista larga.

- **WWPN objetivo**

Nombre del puerto mundial de destino.

- **Grupo de acceso por volumen**

Nombre del grupo de acceso al volumen al que pertenece la sesión.

- **ID de grupo de acceso por volumen**

ID generado por el sistema para el grupo de acceso.

Solucionar problemas de las unidades

Solucionar problemas de las unidades

Puedes reemplazar una unidad de estado sólido (SSD) defectuosa por una unidad de reemplazo. Las unidades SSD para nodos de almacenamiento SolidFire son intercambiables en caliente. Si sospecha que una unidad SSD ha fallado, póngase en contacto con el soporte de NetApp para verificar la falla y que le guíen a través del procedimiento de resolución adecuado. El soporte de NetApp también trabaja con usted para obtener una unidad de reemplazo de acuerdo con su acuerdo de nivel de servicio.

En este caso, "intercambiable" significa que puede extraer una unidad defectuosa de un nodo activo y reemplazarla con una nueva unidad SSD de NetApp. No se recomienda extraer unidades que no hayan fallado en un clúster activo.

Debe mantener repuestos in situ sugeridos por el soporte de NetApp para permitir el reemplazo inmediato de la unidad en caso de falla.



Para fines de prueba, si está simulando una falla de la unidad extrayendo una unidad de un nodo, debe esperar 30 segundos antes de volver a insertar la unidad en la ranura de la unidad.

Si falla una unidad, Double Helix redistribuye los datos de la unidad entre los nodos restantes del clúster. Las fallas en múltiples unidades en el mismo nodo no representan un problema, ya que el software Element protege contra la existencia de dos copias de datos en el mismo nodo. Un fallo en el disco duro provoca los siguientes eventos:

- Los datos se migran fuera de la unidad.
- La capacidad total del clúster se reduce en la capacidad de la unidad.
- La protección de datos Double Helix garantiza que existan dos copias válidas de los datos.



Los sistemas de almacenamiento SolidFire no admiten la extracción de una unidad si esto resulta en una cantidad de almacenamiento insuficiente para migrar los datos.

Para más información

- [Retire las unidades defectuosas del clúster.](#)
- [Solución de problemas básicos de la unidad MDSS](#)
- [Retire las unidades MDSS](#)
- ["Sustitución de unidades para nodos de almacenamiento SolidFire"](#)
- ["Sustitución de unidades para nodos de almacenamiento de la serie H600S"](#)
- ["Información de hardware H410S y H610S"](#)
- ["Información sobre el hardware de la serie SF"](#)

Retire las unidades defectuosas del clúster.

El sistema SolidFire marca una unidad como averiada si su autodiagnóstico indica al nodo que ha fallado o si la comunicación con la unidad se interrumpe durante cinco minutos y medio o más. El sistema muestra una lista de las unidades que han fallado. Debe eliminar una unidad defectuosa de la lista de unidades defectuosas en el software NetApp Element .

Las unidades en la lista **Alertas** se muestran como **blockServiceUnhealthy** cuando un nodo está fuera de línea. Al reiniciar 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 continúan como unidades activas en el clúster.

1. En la interfaz de usuario de Element, seleccione **Clúster > Unidades**.
2. Haz clic en **Error** para ver la lista de unidades que han fallado.
3. Anote el número de ranura de la unidad averiada.

Necesitas esta información para localizar la unidad averiada en el chasis.

4. Retire las unidades defectuosas utilizando uno de los siguientes métodos:

Opción	Pasos
Para extraer unidades individuales	a. Haz clic en Acciones para la unidad que deseas eliminar. b. Haga clic en Eliminar.
Para extraer varias unidades	a. Seleccione todas las unidades que desea eliminar y haga clic en Acciones en lote. b. Haga clic en Eliminar.

Solución de problemas básicos de la unidad MDSS

Puede recuperar las unidades de metadatos (o particiones) volviéndolas a agregar al

clúster en caso de que falle una o ambas unidades de metadatos. Puede realizar la operación de recuperación en la interfaz de usuario de NetApp Element si la función MDSS ya está habilitada en el nodo.

Si una o ambas unidades de metadatos de un nodo experimentan una falla, el servicio de segmentación se apagará y los datos de ambas unidades se respaldarán en unidades diferentes del nodo.

Los siguientes escenarios describen posibles situaciones de fallo y proporcionan recomendaciones básicas para corregir el problema:

La unidad de partición del sistema falla

- En este escenario, se verifica la ranura 2 y se devuelve a un estado disponible.
- Es necesario volver a llenar la unidad de partición del sistema antes de que se pueda volver a poner en línea el servicio de partición.
- Debes reemplazar la unidad de partición del sistema; cuando esté disponible, agrega esta unidad y la unidad de la ranura 2 al mismo tiempo.



No se puede agregar la unidad en la ranura 2 por sí sola como unidad de metadatos. Debes volver a agregar ambas unidades al nodo al mismo tiempo.

La ranura 2 falla

- En este escenario, se verifica la unidad de partición del sistema y se devuelve a un estado disponible.
- Debes reemplazar la ranura 2 con una de repuesto; cuando la ranura 2 esté disponible, agrega la unidad de partición del sistema y la unidad de la ranura 2 al mismo tiempo.

La unidad de partición del sistema y la ranura 2 fallan

- Debes reemplazar tanto la unidad de partición del sistema como la ranura 2 con una unidad de repuesto. Cuando ambas unidades estén disponibles, agregue la unidad de partición del sistema y la unidad de la ranura 2 al mismo tiempo.

Orden de operaciones

- Reemplace la unidad de hardware defectuosa con una unidad de repuesto (reemplace ambas unidades si ambas han fallado).
- Vuelva a agregar las unidades al clúster cuando se hayan repoblado y estén disponibles.

Verificar operaciones

- Verifique que las unidades en la ranura 0 (o interna) y la ranura 2 se identifiquen como unidades de metadatos en la lista de Unidades Activas.
- Verifique que se haya completado todo el balanceo de segmentos (no debe haber más mensajes de movimiento de segmentos en el registro de eventos durante al menos 30 minutos).

Para más información

[Agregar unidades MDSS](#)

Agregar unidades MDSS

Puede agregar una segunda unidad de metadatos en un nodo SolidFire convirtiendo la unidad de bloques en la ranura 2 en una unidad de partición. Esto se logra habilitando la función de servicio de segmentación de múltiples unidades (MDSS). Para habilitar esta función, debe ponerse en contacto con el soporte de NetApp .

Para que una unidad de partición esté disponible, puede ser necesario reemplazar una unidad averiada por una unidad nueva o de repuesto. Debe agregar la unidad de partición del sistema al mismo tiempo que agrega la unidad para la ranura 2. Si intenta agregar la unidad de partición de la ranura 2 sola o antes de agregar la unidad de partición del sistema, el sistema generará un error.

1. Haz clic en **Clúster > Unidades**.
2. Haz clic en **Disponible** para ver la lista de unidades disponibles.
3. Seleccione las unidades de partición que desea agregar.
4. Haz clic en **Acciones en lote**.
5. Haga clic en **Agregar**.
6. Confirme en la pestaña **Unidades activas** que las unidades se han agregado.

Retire las unidades MDSS

Puede extraer las unidades del servicio de segmentación de unidades múltiples (MDSS). Este procedimiento se aplica únicamente si el nodo tiene varias unidades de partición.



Si fallan la unidad de partición del sistema y la unidad de la ranura 2, el sistema apagará los servicios de partición y extraerá las unidades. Si no se produce ningún fallo y se extraen las unidades, ambas deben extraerse al mismo tiempo.

1. Haz clic en **Clúster > Unidades**.
2. Desde la pestaña **Unidades disponibles**, haga clic en la casilla de verificación de las unidades de partición que se van a eliminar.
3. Haz clic en **Acciones en lote**.
4. Haga clic en **Eliminar**.
5. Confirma la acción.

Solucionar problemas de nodos

Eliminar nodos de un clúster

Puedes eliminar nodos de un clúster para realizar mantenimiento o reemplazo. Debe utilizar la interfaz de usuario o la API de NetApp Element para eliminar nodos antes de desconectarlos.

A continuación se ofrece una descripción general del procedimiento para eliminar nodos de almacenamiento:

- Asegúrese de que el clúster tenga capacidad suficiente para crear una copia de los datos en el nodo.
- Elimine las unidades del clúster utilizando la interfaz de usuario o el método API RemoveDrives.

Esto provoca que el sistema migre datos desde las unidades del nodo a otras unidades del clúster. El tiempo que tarda este proceso depende de la cantidad de datos que deban migrarse.

- Elimine el nodo del clúster.

Tenga en cuenta las siguientes consideraciones antes de apagar o encender un nodo:

- Apagar nodos y clústeres conlleva riesgos si no se realiza correctamente.

El apagado de un nodo debe realizarse bajo la dirección del soporte de NetApp .

- Si un nodo ha estado inactivo durante más de 5,5 minutos bajo cualquier tipo de condición de apagado, la protección de datos Double Helix comienza la tarea de escribir bloques replicados individuales 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 que ha fallado.
- Para reiniciar o apagar un nodo de forma segura, puede utilizar el comando de la API Shutdown.
- Si un nodo está inactivo o apagado, debe ponerse en contacto con el soporte de NetApp antes de volver a conectarlo.
- Una vez que un nodo vuelve a estar en línea, debe volver a agregar las unidades al clúster, dependiendo del tiempo que haya estado fuera de servicio.

Para más información

["Sustitución de un chasis SolidFire averiado"](#)

["Sustitución de un nodo de la serie H600S averiado"](#)

Apagar un grupo

Realice el siguiente procedimiento para apagar un clúster completo.

Pasos

1. (Opcional) Comuníquese con el soporte de NetApp para obtener ayuda para completar los pasos preliminares.
2. Verifique que todas las operaciones de E/S se hayan detenido.
3. Desconectar todas las sesiones iSCSI:
 - a. Navegue hasta la dirección IP virtual de administración (MVIP) en el clúster para abrir la interfaz de usuario de Element.
 - b. Observe los nodos que aparecen en la lista de nodos.
 - c. Ejecute el método de la API Shutdown con la opción de detención especificada en cada ID de nodo del clúster.

Al reiniciar el clúster, debe seguir ciertos pasos para verificar que todos los nodos se conecten:



1. Verifique que toda la gravedad crítica y `volumesOffline` Se han resuelto los fallos del clúster.
2. Espere de 10 a 15 minutos para que el grupo se asiente.
3. Comience a iniciar los hosts para acceder a los datos.

Si desea disponer de más tiempo al encender los nodos y verificar que estén en buen estado después del mantenimiento, póngase en contacto con el soporte técnico para obtener ayuda para retrasar la sincronización de datos y evitar la sincronización innecesaria de contenedores.

Encuentra más información

["Cómo apagar y encender correctamente un clúster de almacenamiento NetApp Solidfire/HCI"](#)

Trabajar con utilidades por nodo para nodos de almacenamiento

Trabajar con utilidades por nodo para nodos de almacenamiento

Puede utilizar 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 le proporcionan suficiente información para la resolución de problemas. Las utilidades por nodo proporcionan información y herramientas específicas que pueden ayudarle a solucionar problemas de red entre nodos o con el nodo de administración.

Encuentra más información

- [Acceda a la configuración de cada nodo mediante la interfaz de usuario correspondiente.](#)
- [Detalles de la configuración de red desde la interfaz de usuario de cada nodo.](#)
- [Detalles de configuración del clúster desde la interfaz de usuario por nodo](#)
- [Ejecute pruebas del sistema utilizando la interfaz de usuario por nodo.](#)
- [Ejecute las utilidades del sistema mediante la interfaz de usuario de cada nodo.](#)

Acceda a la configuración de cada nodo mediante la interfaz de usuario correspondiente.

Puede acceder a la configuración de red, la configuración del clúster y las pruebas y utilidades del sistema en la interfaz de usuario por nodo después de ingresar la IP del nodo de administración y autenticarse.

Si desea modificar la configuración de un nodo en estado Activo que forma parte de un clúster, debe iniciar sesión como usuario administrador del clúster.



Debe configurar o modificar un nodo a la vez. Debe asegurarse de que la configuración de red especificada tenga el efecto esperado y de que la red sea estable y funcione correctamente antes de realizar modificaciones en otro nodo.

1. Abra la interfaz de usuario por nodo utilizando uno de los siguientes métodos:

- Ingrese la dirección IP de administración seguida de :442 en una ventana del navegador e inicie sesión con un nombre de usuario y contraseña de administrador.
- En la interfaz de usuario de Element, seleccione **Clúster** > **Nodos** y haga clic en el enlace de la dirección IP de administración del nodo que desea configurar o modificar. En la ventana del navegador que se abre, puede editar la configuración del nodo.

NetApp
Hybrid Cloud Control

Node01

NETWORK SETTINGS CLUSTER SETTINGS SYSTEM TESTS SYSTEM UTILITIES

Network Settings

Bond1G Bond10G [Reset Changes](#)

Method Link Speed

static 1000

IPv4 Address IPv4 Subnet Mask

255.255.255.0

IPv4 Gateway Address IPv6 Address

IPv6 Gateway Address MTU

1500

DNS Servers

Search Domains

Bond Mode Status

Detalles de la configuración de red desde la interfaz de usuario de cada nodo.

Puede cambiar la configuración de red del nodo de almacenamiento para asignarle un nuevo conjunto de atributos de red.

Puedes ver la configuración de red de un nodo de almacenamiento en la página **Configuración de red** cuando inicies sesión en el nodo. (https://<node_IP>:442/hcc/node/network-settings). Puede

seleccionar la configuración **Bond1G** (gestión) o **Bond10G** (almacenamiento). La siguiente lista describe la configuración que puede modificar cuando un nodo de almacenamiento se encuentra en estado Disponible, Pendiente o Activo:

- **Método**

El método utilizado para configurar la interfaz. Métodos posibles:

- loopback: Se utiliza para definir la interfaz loopback IPv4.
- manual: Se utiliza para definir interfaces para las que no se realiza ninguna configuración por defecto.
- dhcp: Se utiliza para obtener una dirección IP mediante DHCP.
- estático: Se utiliza para definir interfaces Ethernet con direcciones IPv4 asignadas estáticamente.

- **Velocidad de enlace**

La velocidad negociada por la NIC virtual.

- **Dirección IPv4**

La dirección IPv4 para la red eth0.

- **Máscara de subred IPv4**

Subdivisiones de direcciones de la red IPv4.

- **Dirección de puerta de enlace IPv4**

Dirección de red del router para enviar paquetes fuera de la red local.

- **Dirección IPv6**

La dirección IPv6 para la red eth0.

- **Dirección de puerta de enlace IPv6**

Dirección de red del router para enviar paquetes fuera de la red local.

- **MTU**

Tamaño máximo de paquete que un protocolo de red puede transmitir. Debe ser mayor o igual a 1500. Si agrega una segunda NIC de almacenamiento, el valor debería ser 9000.

- **Servidores DNS**

Interfaz de red utilizada para la comunicación del clúster.

- **Dominios de búsqueda**

Busque direcciones MAC adicionales disponibles para el sistema.

- **Modo de vínculo**

Puede ser uno de los siguientes modos:

- ActivoPasivo (predeterminado)

- ALBA
- LACP

- **Estado**

Valores posibles:

- En funcionamiento
- Abajo
- Arriba

- **Etiqueta de red virtual**

Etiqueta asignada al crear la red virtual.

- **Rutas**

Rutas estáticas a hosts o redes específicas a través de la interfaz asociada que las rutas están configuradas para usar.

Detalles de configuración del clúster desde 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.

La siguiente lista describe la configuración del clúster para un nodo de almacenamiento indicado en la página **Configuración del clúster** de la interfaz de usuario por nodo. (https://<node_IP>:442/hcc/node/cluster-settings).

- **Role**

Función que desempeña el nodo en el clúster. Valores posibles:

- Almacenamiento: Nodo de almacenamiento o de canal de fibra.
- Gestión: Nodo es un nodo de gestión.

- **Nombre de host**

Nombre del nodo.

- **Grupo**

Nombre del clúster.

- **Membresía de grupo**

Estado del nodo. Valores posibles:

- Disponible: El nodo no tiene un nombre de clúster asociado y aún no forma parte de un clúster.
- Pendiente: El nodo está configurado y se puede agregar a un clúster designado. No se requiere autenticación para acceder al nodo.
- PendienteActivo: El sistema está en proceso de instalar software compatible en el nodo. Una vez completado, el nodo pasará al estado Activo.

- Activo: El nodo participa en un clúster. Se requiere autenticación para modificar el nodo.

- **Versión**

Versión del software Element que se ejecuta en el nodo.

- **Conjunto**

Nodos que forman parte del conjunto de la base de datos.

- **ID del nodo**

Se asigna un ID cuando se agrega un nodo al clúster.

- **Interfaz de clúster**

Interfaz de red utilizada para la comunicación del clúster.

- **Interfaz de gestión**

Interfaz de red de gestión. Por defecto se utiliza Bond1G, pero también se puede usar Bond10G.

- **Interfaz de almacenamiento**

Interfaz de red de almacenamiento mediante Bond10G.

- **Capacidad de cifrado**

Indica si el nodo admite o no el cifrado de unidades.

Ejecute pruebas del sistema utilizando la interfaz de usuario por nodo.

Puedes probar los cambios en la configuración de red después de confirmarlos en la configuración de red. Puedes ejecutar las pruebas para asegurarte de que el nodo de almacenamiento es estable y se puede poner en línea sin problemas.

Has iniciado sesión en la interfaz de usuario por nodo para el nodo de almacenamiento.

1. Haz clic en **Pruebas del sistema**.
2. Haz clic en **Ejecutar prueba** junto a la prueba que desees ejecutar o selecciona **Ejecutar todas las pruebas**.



La ejecución de todas las operaciones de prueba puede consumir mucho tiempo y solo debe realizarse bajo la dirección del Soporte de NetApp .

- **Prueba de conjunto conectado**

Prueba y verifica la conectividad a un conjunto de bases de datos. Por defecto, la prueba utiliza el conjunto para el clúster con el que está asociado el nodo. Alternativamente, puede proporcionar un conjunto diferente para probar la conectividad.

- **Prueba Connect Mvip**

Hace ping a la dirección IP virtual de administración (MVIP) especificada y luego ejecuta una llamada

API simple a la MVIP para verificar la conectividad. Por defecto, la prueba utiliza el MVIP para el clúster con el que está asociado el nodo.

- **Prueba Connect Svip**

Hace ping a la dirección IP virtual de almacenamiento (SVIP) especificada utilizando paquetes del Protocolo de mensajes de control de Internet (ICMP) que coinciden con el tamaño de la Unidad de transmisión máxima (MTU) configurado en el adaptador de red. Luego se conecta al SVIP como un iniciador iSCSI. Por defecto, la prueba utiliza la SVIP del clúster con el que está asociado el nodo.

- **Configuración de hardware de prueba**

Comprueba 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 funcionando correctamente. Esto es lo mismo que las pruebas de fábrica.



Esta prueba consume muchos recursos y solo debe ejecutarse si lo solicita el soporte de NetApp .

- **Prueba de conectividad local**

Prueba la conectividad con todos los demás nodos del clúster haciendo ping a la IP del clúster (CIP) en cada nodo. Esta prueba solo se mostrará en un nodo si este forma parte de un clúster activo.

- **Prueba de localización de clúster**

Valida que el nodo pueda localizar el clúster especificado en la configuración del clúster.

- **Configuración de red de prueba**

Verifica que la configuración de red configurada coincida con la configuración de red que se está utilizando en el sistema. Esta prueba no está diseñada para detectar fallos de hardware cuando un nodo participa activamente en un clúster.

- **Prueba de ping**

Envía un ping a una lista específica de hosts o, si no se especifica ninguna, crea dinámicamente una lista de todos los nodos registrados en el clúster y envía un ping a cada uno para comprobar la conectividad simple.

- **Prueba de conectividad remota**

Prueba la conectividad a todos los nodos en clústeres emparejados remotamente haciendo ping a la IP del clúster (CIP) en cada nodo. Esta prueba solo se mostrará en un nodo si este forma parte de un clúster activo.

Ejecute las utilidades del sistema mediante la interfaz de usuario de cada nodo.

Puede utilizar la interfaz de usuario por nodo para el nodo de almacenamiento para crear o eliminar paquetes de soporte, restablecer la configuración de las unidades y reiniciar los servicios de red o de clúster.

Has iniciado sesión en la interfaz de usuario por nodo para el nodo de almacenamiento.

1. Haz clic en **Utilidades del sistema**.
2. Haz clic en el botón de la utilidad del sistema que deseas ejecutar.

- **Control de potencia**

Reinicia, apaga o desconecta el nodo.



Esta operación provoca una pérdida temporal de la conectividad de red.

Especifique los siguientes parámetros:

- Acción: Las opciones incluyen Reiniciar y Detener (apagar).
- Retardo de activación: Cualquier tiempo adicional antes de que el nodo vuelva a estar en línea.

- **Recopilar registros de nodos**

Crea un paquete de soporte en el directorio /tmp/bundles del nodo.

Especifique los siguientes parámetros:

- Nombre del paquete: Nombre único para cada paquete de soporte creado. Si no se proporciona ningún nombre, se utilizará "supportbundle" y el nombre del nodo como nombre de archivo.
- Argumentos adicionales: Este parámetro se pasa al script sf_make_support_bundle. Este parámetro solo debe utilizarse a petición del soporte de NetApp .
- Tiempo de espera (seg.): Especifique el número de segundos que se esperarán para cada respuesta de ping individual.

- **Eliminar registros del nodo**

Elimina cualquier paquete de soporte actual en el nodo que se haya creado utilizando **Create Cluster Support Bundle** o el método de API CreateSupportBundle.

- **Restablecer unidades**

Inicializa las unidades y elimina todos los datos que residen actualmente en la unidad. Puedes reutilizar la unidad en un nodo existente o en un nodo actualizado.

Especifique el siguiente parámetro:

- Unidades: Lista de nombres de dispositivos (no identificadores de unidad) para 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.

- **Reiniciar nodo**

Restablece un nodo a la configuración de fábrica. Durante esta operación se eliminan todos los datos, pero se conservan los ajustes de red del nodo. Los nodos solo se pueden reiniciar si no están asignados a un clúster y se encuentran en estado Disponible.



Al utilizar esta opción, se eliminan del nodo todos los datos, paquetes (actualizaciones de software), configuraciones y archivos de registro.

◦ Reiniciar la conexión de red

Reinicia todos los servicios de red en un nodo.



Esta operación puede provocar una pérdida temporal de la conectividad de la red.

◦ Reiniciar servicios

Reinicia los servicios de software Element en un nodo.



Esta operación puede provocar una interrupción temporal del servicio del nodo. Esta operación solo debe realizarse bajo la dirección del soporte de NetApp .

Especifique los siguientes parámetros:

- Servicio: Nombre del servicio que se reiniciará.
- Acción: Acción a realizar en el servicio. Las opciones incluyen iniciar, detener y reiniciar.

Trabajar con el nodo de gestión

Puede utilizar el nodo de administración (mNode) para actualizar los servicios del sistema, administrar 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 resolución de problemas.



Como práctica recomendada, asocie solo un nodo de administración con una instancia de VMware vCenter y evite definir los mismos recursos de almacenamiento y computación o instancias de vCenter en varios nodos de administración.

Ver "[Documentación del nodo de gestión](#)" Para más información.

Comprender los niveles de plenitud del clúster

El clúster que ejecuta el software Element genera fallos de clúster para advertir al administrador de almacenamiento cuando el clúster se está quedando sin capacidad. Existen tres niveles de llenado del clúster, todos los cuales se muestran en la interfaz de usuario de NetApp Element : advertencia, error y crítico.

El sistema utiliza el código de error BlockClusterFull para advertir sobre la saturación del almacenamiento de bloques del clúster. Puede consultar los niveles de gravedad de la ocupación del clúster en la pestaña Alertas 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 configurable por el cliente que aparece cuando la capacidad de bloques del clúster se acerca al nivel de gravedad del error. Por defecto, este nivel está establecido en un tres por ciento por debajo del nivel de error y se puede ajustar a través de la interfaz de usuario y la API de Element. Debes añadir más capacidad o liberar capacidad lo antes posible.

- **Error**

Cuando el clúster se encuentra en este estado, si se pierde un nodo, no habrá suficiente capacidad en el clúster para reconstruir la protección de datos Double Helix. La creación de nuevos volúmenes, clones y snapshots está bloqueada mientras el clúster se encuentra en este estado. Este no es un estado seguro ni recomendable para ningún clúster. Debe agregar más capacidad o liberar capacidad de inmediato.

- **Crítico**

Este error crítico se ha producido porque el clúster está consumido al 100 por ciento. Se encuentra en estado de solo lectura y no se pueden establecer nuevas conexiones iSCSI al clúster. Cuando se llega a esta etapa, debe liberar o agregar más capacidad de inmediato.

El sistema utiliza el código de error MetadataClusterFull para advertir sobre la falta de espacio de almacenamiento para los metadatos del clúster. Puede consultar el nivel de almacenamiento de metadatos del clúster en la sección Capacidad del clúster de la página Resumen de la pestaña Informes en la interfaz de usuario de Element.

La siguiente lista incluye información sobre los niveles de gravedad de MetadataClusterFull:

- **Advertencia**

Se trata de una advertencia configurable por el cliente que aparece cuando la capacidad de metadatos del clúster se acerca al nivel de gravedad del error. Por defecto, este nivel está establecido en un tres por ciento por debajo del nivel de error y se puede ajustar a través de la API de Element. Debes añadir más capacidad o liberar capacidad lo antes posible.

- **Error**

Cuando el clúster se encuentra en este estado, si se pierde un nodo, no habrá suficiente capacidad en el clúster para reconstruir la protección de datos Double Helix. La creación de nuevos volúmenes, clones y snapshots está bloqueada mientras el clúster se encuentra en este estado. Este no es un estado seguro ni recomendable para ningún clúster. Debe agregar más capacidad o liberar capacidad de inmediato.

- **Crítico**

Este error crítico se ha producido porque el clúster está consumido al 100 por ciento. Se encuentra en estado de solo lectura y no se pueden establecer nuevas conexiones iSCSI al clúster. Cuando se llega a esta etapa, debe liberar o agregar más capacidad de inmediato.



Lo siguiente se aplica a los umbrales de clústeres de dos nodos:

- El error de integridad de metadatos es un 20% inferior al crítico.
- El error de llenado de bloque se produce cuando 1 bloque de capacidad (incluida la capacidad no utilizada) está por debajo del nivel crítico; es decir, cuando la capacidad equivale a dos bloques de capacidad por debajo del nivel crítico.

Administre y supervise el almacenamiento con NetApp Hybrid Cloud Control.

Agregue y administre clústeres de almacenamiento mediante NetApp Hybrid Cloud Control.

Puede agregar clústeres de almacenamiento al inventario de activos del nodo de administración para que puedan administrarse mediante NetApp Hybrid Cloud Control (HCC). El primer clúster de almacenamiento que se agrega durante la configuración del sistema es el predeterminado. ["clúster de almacenamiento autorizado"](#) , pero se pueden agregar clústeres adicionales mediante la interfaz de usuario de HCC.

Después de agregar un clúster de almacenamiento, puede supervisar el rendimiento del clúster, cambiar las credenciales del clúster de almacenamiento para el activo administrado o eliminar un clúster de almacenamiento del inventario de activos del nodo de administración si ya no es necesario administrarlo mediante HCC.

Lo que necesitarás

- **Permisos de administrador del clúster:** Usted tiene permisos como administrador en el clúster. ["clúster de almacenamiento autorizado"](#) . El clúster autoritativo es el primer clúster que se agrega al inventario de nodos de administración durante la configuración del sistema.
- **Software Element:** Su versión de clúster de almacenamiento ejecuta el software NetApp Element 11.3 o posterior.
- **Nodo de administración:** Ha implementado un nodo de administración que ejecuta la versión 11.3 o posterior.
- **Servicios de gestión:** Ha actualizado su paquete de servicios de gestión a la versión 2.17 o posterior.

Opciones

- [Agregar un clúster de almacenamiento](#)
- [Confirmar el estado del clúster de almacenamiento](#)
- [Editar credenciales del clúster de almacenamiento](#)
- [Eliminar un clúster de almacenamiento](#)
- [Activar y desactivar el modo de mantenimiento](#)

Agregar un clúster de almacenamiento

Puede agregar un clúster de almacenamiento al inventario de activos del nodo de administración mediante NetApp Hybrid Cloud Control. Esto le permite administrar y monitorear el clúster utilizando la interfaz de usuario de HCC.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador autorizado del clúster de almacenamiento.
2. Desde el Panel de control, seleccione el menú de opciones en 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 administración de clúster de almacenamiento



Solo se pueden agregar clústeres de almacenamiento remoto que actualmente no estén administrados por un nodo de administración.

- Nombre de usuario y contraseña del clúster de almacenamiento

6. Seleccione **Agregar**.



Después de agregar el clúster de almacenamiento, el inventario del clúster puede tardar hasta 2 minutos en actualizarse y mostrar la nueva incorporación. Es posible que necesites actualizar la página en tu navegador para ver los cambios.

Confirmar el estado del clúster de almacenamiento

Puede supervisar el estado de conexión de los recursos de los clústeres de almacenamiento mediante la interfaz de usuario de NetApp Hybrid Cloud Control.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador autorizado del clúster de almacenamiento.
2. Desde el Panel de control, seleccione el menú de opciones en la parte superior derecha y seleccione **Configurar**.
3. Revisa el estado de los clústeres de almacenamiento en el inventario.
4. Desde el panel **Clústeres de almacenamiento**, seleccione **Detalles del clúster de almacenamiento** para obtener información adicional.

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 NetApp Hybrid Cloud Control proporcionando las credenciales de administrador autorizado del clúster de almacenamiento.
2. Desde el Panel de control, seleccione el menú de opciones en 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 del clúster**.
5. Actualice el nombre de usuario y la contraseña del clúster de almacenamiento.
6. Seleccione **Guardar**.

Eliminar un clúster de almacenamiento

Al eliminar un clúster de almacenamiento de NetApp Hybrid Cloud Control, el clúster se elimina del inventario de nodos de administración. Después de eliminar un clúster de almacenamiento, HCC ya no podrá administrarlo y solo podrá acceder a él navegando directamente a su dirección IP de administración.



No se puede eliminar el clúster autoritativo del inventario. Para determinar el clúster autorizado, vaya a **Administración de usuarios > Usuarios**. El grupo autorizado se encuentra junto al encabezado **Usuarios**.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador autorizado del clúster de almacenamiento.
2. Desde el Panel de control, seleccione el menú de opciones en 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 **Eliminar clúster de almacenamiento**.



Seleccionar **Sí** a continuación elimina el clúster de la instalación.

5. Seleccione **Sí**.

Activar y desactivar el modo de mantenimiento

Si necesita desconectar un nodo de almacenamiento para realizar tareas de mantenimiento, como actualizaciones de software o reparaciones del host, puede minimizar el impacto de E/S en el resto del clúster de almacenamiento mediante [habilitación](#) Modo de mantenimiento para ese nodo. Cuando tú [desactivar](#) En el modo de mantenimiento, el nodo se supervisa para garantizar que se cumplan ciertos criterios antes de que el nodo pueda salir del modo de mantenimiento.

Lo que necesitarás

- **Software Element:** Su versión de clúster de almacenamiento ejecuta el software NetApp Element 12.2 o posterior.
- **Nodo de administración:** Ha implementado un nodo de administración que ejecuta la versión 12.2 o posterior.
- **Servicios de gestión:** Ha actualizado su paquete de servicios de gestión a la versión 2.19 o posterior.
- Tienes acceso para iniciar sesión a nivel de administrador.

Activar 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 administración 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 la función de modo de mantenimiento están deshabilitadas en el nivel de solo lectura.

3. En el cuadro azul de navegación izquierdo, seleccione la instalación SolidFire all-flash.
4. En el panel de navegación izquierdo, seleccione **Nodos**.
5. Para ver la información del inventario de almacenamiento, seleccione **Almacenamiento**.
6. Habilitar el modo de mantenimiento en un nodo de almacenamiento:

La tabla de nodos de almacenamiento se actualiza automáticamente cada dos minutos para las acciones no iniciadas por el usuario. Antes de realizar cualquier acción, para asegurarse de tener el estado más actualizado, puede actualizar la tabla de nodos utilizando el icono de actualización situado en la parte superior derecha de la tabla de nodos.



- a. En **Acciones**, seleccione **Habilitar modo de mantenimiento**.

Mientras el **Modo de mantenimiento** está habilitado, las acciones del modo de mantenimiento no están disponibles para el nodo seleccionado ni para los demás nodos del mismo clúster.

Una vez completado el **Modo de mantenimiento**, la columna **Estado del nodo** muestra un icono de llave inglesa y el texto "**Modo de mantenimiento**" para el nodo que se encuentra en modo de mantenimiento.

Desactivar modo de mantenimiento

Una vez que un nodo se ha puesto correctamente en modo de mantenimiento, la acción **Deshabilitar modo de mantenimiento** estará disponible para este nodo. Las acciones en los demás nodos no estarán disponibles hasta que el modo de mantenimiento se desactive correctamente en el nodo que se está sometiendo a mantenimiento.

Pasos

1. Para el nodo en modo de mantenimiento, en **Acciones**, seleccione **Desactivar modo de mantenimiento**.

Mientras el **Modo de mantenimiento** esté desactivado, las acciones del modo de mantenimiento no

estarán disponibles para el nodo seleccionado ni para los demás nodos del mismo clúster.

Una vez finalizado el **Modo de mantenimiento desactivado**, la columna **Estado del nodo** muestra **Activo**.



Cuando un nodo está en modo de mantenimiento, no acepta nuevos datos. Como resultado, puede llevar más tiempo desactivar el modo de mantenimiento porque el nodo debe sincronizar sus datos antes de poder salir del modo de mantenimiento. Cuanto más tiempo permanezca en modo de mantenimiento, más tiempo puede tardar en desactivarse dicho modo.

Solución de problemas

Si se producen errores al activar o desactivar el modo de mantenimiento, aparecerá un mensaje de error en la parte superior de la tabla de nodos. Para obtener más información sobre el error, puede seleccionar el enlace **Mostrar detalles** que se proporciona en el banner para ver qué devuelve la API.

Encuentra más información

- ["Crear y administrar activos de clúster de almacenamiento"](#)
- ["Documentación del software SolidFire y Element"](#)

Configurar el acceso a la interfaz web del nombre de dominio completo

El almacenamiento totalmente flash SolidFire con el software NetApp Element 12.2 o posterior le permite acceder a las interfaces web del clúster de almacenamiento utilizando el nombre de dominio totalmente calificado (FQDN). Si desea utilizar el FQDN para acceder a interfaces de usuario web como la interfaz web de Element, la interfaz de usuario por nodo o la interfaz de usuario del nodo de administración, primero debe agregar una configuración de clúster de almacenamiento para identificar el FQDN utilizado por el clúster.

Este proceso permite que el clúster redirija correctamente una sesión de inicio de sesión y mejora la integración con servicios externos como gestores de claves y proveedores de identidad para la autenticación multifactor.

Lo que necesitarás

- Esta función requiere Element 12.2 o posterior.
- La configuración de esta función mediante las API REST de NetApp Hybrid Cloud Control requiere los servicios de administración 2.15 o posterior.
- La configuración de esta función mediante la interfaz de usuario de NetApp Hybrid Cloud Control requiere los servicios de administración 2.19 o posterior.
- Para utilizar las API REST, debe haber implementado un nodo de administración que ejecute la versión 11.5 o posterior.
- Necesita nombres de dominio completos para el nodo de administración y cada clúster de almacenamiento que se resuelvan correctamente a la dirección IP del nodo de administración y a la dirección IP de cada clúster de almacenamiento.

Puede configurar o eliminar el acceso a la interfaz web FQDN mediante NetApp Hybrid Cloud Control y la API REST. También puede solucionar problemas relacionados con FQDN configurados incorrectamente.

- [Configure el acceso a la interfaz web de FQDN mediante NetApp Hybrid Cloud Control.](#)
- [Configure el acceso a la interfaz web mediante FQDN utilizando la API REST.](#)
- [Eliminar el acceso a la interfaz web de FQDN mediante NetApp Hybrid Cloud Control](#)
- [Eliminar el acceso a la interfaz web de FQDN mediante la API REST](#)
- [Solución de problemas](#)

Configure el acceso a la interfaz web de FQDN mediante NetApp Hybrid Cloud Control.

Pasos

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

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

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione el icono de menú situado en la parte superior derecha de la página.
4. Seleccione **Configurar**.
5. En el panel **Nombres de dominio totalmente calificados**, seleccione **Configurar**.
6. En la ventana resultante, ingrese los FQDN para el nodo de administración y cada clúster de almacenamiento.
7. Seleccione **Guardar**.

El panel **Nombres de dominio totalmente calificados** muestra cada clúster de almacenamiento con su MVIP y FQDN asociados.



En el panel **Nombres de dominio totalmente calificados** solo se muestran los clústeres de almacenamiento conectados con el FQDN configurado.

Configure el acceso a la interfaz web mediante FQDN utilizando la API REST.

Pasos

1. Asegúrese de que los nodos de almacenamiento de Element y el mNode tengan el DNS configurado correctamente para el entorno de red, de modo que se puedan resolver los FQDN del entorno. Para configurar el DNS, vaya a la interfaz de usuario de cada nodo de almacenamiento y al nodo de administración, luego seleccione **Configuración de red > Red de administración**.
 - a. Interfaz de usuario por nodo para nodos de almacenamiento:
https://<storage_node_management_IP>:442
 - b. Interfaz de usuario por nodo para el nodo de administración:
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 de clúster utilizando "CrearPreferenciaDeInterfazDeClúster" Método API, insertando el FQDN 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 administración mediante la API REST en el nodo de administración:

- a. Acceda a la interfaz de usuario de la API REST para el nodo de administración introduciendo la dirección IP del nodo de administración seguida de `/mnode/2/`

Por ejemplo:

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

- a. Haga clic en **Autorizar** o en cualquier icono de candado e introduzca el nombre de usuario y la contraseña del clúster.
- b. Introduzca el ID del cliente como `mnode-client`.
- c. Haz clic en **Autorizar** para comenzar la sesión y luego cierra la ventana.
- d. Desde la lista de servidores, seleccione `mnode2`.
- e. Haz clic en **GET /settings**.
- f. Haz clic en **Pruébalo**.
- g. Haz clic en **Ejecutar**.
- h. Registre cualquier configuración de proxy que se indique en el cuerpo de la respuesta.
 - i. Haz clic en **PUT/settings**.
 - j. Haz clic en **Pruébalo**.
- k. En el área del cuerpo de la solicitud, introduzca el FQDN del nodo de administración como valor para el `mnode_fqdn` parámetro.
- l. Introduzca los valores de configuración del proxy que registró 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 eliminarán los ajustes del proxy existentes.
- m. Haz clic en **Ejecutar**.

Eliminar el acceso a la interfaz web de FQDN mediante NetApp Hybrid Cloud Control

Puede utilizar este procedimiento para eliminar el acceso web FQDN para el nodo de administración y los clústeres de almacenamiento.

Pasos

1. En el panel **Nombres de dominio totalmente calificados**, seleccione **Editar**.
2. En la ventana resultante, borre el contenido del campo de texto **FQDN**.
3. Seleccione **Guardar**.

La ventana se cierra y el FQDN ya no aparece en el panel **Nombres de dominio totalmente calificados**.

Eliminar el acceso a la interfaz web de FQDN mediante la API 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 `DeleteClusterInterfacePreference` Método de la 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 administración mediante la API REST en el nodo de administración:
 - a. Acceda a la interfaz de usuario de la API REST para el nodo de administración introduciendo la dirección IP del nodo de administración seguida de `/mnode/2/` . Por ejemplo:

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

- b. Seleccione **Autorizar** o cualquier icono de candado e introduzca el nombre de usuario y la contraseña del clúster de Element.
- c. Introduzca el ID del cliente como `mnode-client` .
- d. Seleccione **Autorizar** para iniciar una sesión.
- e. Cerrar la ventana.
- f. Seleccione **PUT /settings**.
- g. Seleccione **Probarlo**.
- h. En el área del cuerpo de la solicitud, no introduzca ningún valor para el `mnode_fqdn` parámetro. Especifique también si se debe utilizar el proxy.(`true` o `false`) para el `use_proxy` parámetro.

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

- i. Seleccione **Ejecutar**.

Solución de problemas

Si los FQDN están configurados incorrectamente, podría tener problemas para acceder al nodo de administración, a un clúster de almacenamiento o a ambos. Utilice la siguiente información para ayudarle a solucionar el problema.

Asunto	Causa	Resolución
- Se produce un error del navegador al intentar acceder al nodo de administración o al clúster de almacenamiento utilizando el FQDN. - No se puede iniciar sesión ni en el nodo de administración ni en el clúster de almacenamiento utilizando una dirección IP.	Tanto el FQDN del nodo de administración como el FQDN del clúster de almacenamiento están configurados incorrectamente.	Utilice las instrucciones de la API REST de esta página para eliminar la configuración del nodo de administración y del FQDN del clúster de almacenamiento y configurarlos de nuevo.
- Se produce un error del navegador al intentar acceder al FQDN del clúster de almacenamiento. - No se puede iniciar sesión ni en el nodo de administración ni en el clúster de almacenamiento utilizando una dirección IP.	El nombre de dominio completo (FQDN) del nodo de administración está configurado correctamente, pero el FQDN del clúster de almacenamiento está configurado incorrectamente.	Siga las instrucciones de la API REST en esta página para eliminar la configuración del FQDN del clúster de almacenamiento y volver a configurarla.
- Se produce un error del navegador al intentar acceder al FQDN del nodo de administración. - Puede iniciar sesión en el nodo de administración y en el clúster de almacenamiento utilizando una dirección IP.	El nombre de dominio completo (FQDN) del nodo de administración está configurado incorrectamente, pero el FQDN del clúster de almacenamiento está configurado correctamente.	Inicie sesión en NetApp Hybrid Cloud Control para corregir la configuración FQDN del nodo de administración en la interfaz de usuario, o utilice las instrucciones de la API REST en esta página para corregir la configuración.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Cree y gestione cuentas de usuario mediante NetApp Hybrid Cloud Control.

En los sistemas de almacenamiento basados en elementos, se pueden crear usuarios de

clúster autorizados para habilitar el acceso de inicio de sesión a NetApp Hybrid Cloud Control según los permisos que desee otorgar a los usuarios "Administrador" o "Solo lectura". Además de los usuarios del clúster, también existen cuentas de volumen, que permiten a los clientes conectarse a volúmenes en un nodo de almacenamiento.

Gestiona los siguientes tipos de cuentas:

- [Gestionar cuentas de clúster autorizadas](#)
- [Gestionar cuentas de volumen](#)

Habilitar LDAP

Para utilizar LDAP para 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 Element.
2. Desde el Panel de control, seleccione el icono de Opciones en la parte superior derecha y seleccione **Administración de usuarios**.
3. Desde la página Usuarios, seleccione **Configurar LDAP**.
4. Define tu configuración LDAP.
5. Seleccione el tipo de autenticación: Búsqueda y enlace o Enlace directo.
6. Antes de guardar los cambios, seleccione **Probar inicio de sesión LDAP** en la parte superior de la página, ingrese el nombre de usuario y la contraseña de un usuario que sepa que existe y seleccione **Probar**.
7. Seleccione **Guardar**.

Gestionar cuentas de clúster autorizadas

"[cuentas de usuario autorizadas](#)" Se gestionan desde la opción Administración de usuarios del menú superior derecho en NetApp Hybrid Cloud Control. Este tipo de cuentas le permiten autenticarse en cualquier recurso de almacenamiento asociado con una instancia de nodos y clústeres de NetApp Hybrid Cloud Control. Con esta cuenta, puede administrar volúmenes, cuentas, grupos de acceso y más en todos los clústeres.

Crea una cuenta de clúster autorizada

Puede crear una cuenta utilizando NetApp Hybrid Cloud Control.

Esta cuenta se puede utilizar para iniciar sesión en Hybrid Cloud Control, la interfaz de usuario por nodo para el 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 Element.
2. Desde el Panel de control, seleccione el icono de Opciones en la parte superior derecha y seleccione **Administración de usuarios**.
3. Seleccione **Crear usuario**.
4. Seleccione el tipo de autenticación: clúster o LDAP.

5. Complete una de las siguientes opciones:

- Si seleccionaste LDAP, introduce el DN.



Para usar LDAP, primero debe habilitar LDAP o LDAPS. Ver [Habilitar LDAP](#).

- Si seleccionaste Cluster como tipo de autenticación, introduce 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 asignarán permisos de solo lectura. Si selecciona todos los permisos heredados, a la cuenta se le asignarán permisos de administrador.



Para garantizar que todos los elementos secundarios de un grupo hereden los permisos, cree un grupo administrador de organización DN en el servidor LDAP. Todas las cuentas secundarias de ese grupo heredarán esos permisos.

7. Marque la casilla que indica que "He leído y acepto el Acuerdo de licencia de usuario final de NetApp".

8. Seleccione **Crear usuario**.

Editar 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 Element.
2. Desde el Panel de control, seleccione el icono de la esquina superior derecha y seleccione **Administración de usuarios**.
3. Opcionalmente, filtre la lista de cuentas de usuario seleccionando **Cluster**, **LDAP** o **Idp**.

Si configuró usuarios en el clúster de almacenamiento con LDAP, esas cuentas mostrarán un Tipo de usuario "LDAP". Si configuró usuarios en el clúster de almacenamiento con Idp, esas cuentas mostrarán 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 sesión en NetApp Hybrid Cloud Control.



La interfaz de usuario de NetApp Hybrid Cloud Control puede tardar 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 REST. `https://[management node IP]/inventory/1/` y correr `GET /installations/{id}` para el clúster.

8. Inicie sesión en NetApp Hybrid Cloud Control.

Eliminar una cuenta de usuario autorizada

Puedes eliminar una o más cuentas cuando ya no sean necesarias. Puedes eliminar una cuenta de usuario LDAP.

No se puede eliminar la cuenta de usuario administrador principal del clúster autoritativo.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el Panel de control, seleccione el icono de la esquina superior derecha y seleccione **Administración de usuarios**.
3. En la columna **Acciones** de la tabla Usuarios, expanda el menú de la cuenta y seleccione **Eliminar**.
4. Confirme la eliminación seleccionando **Sí**.

Gestionar cuentas de volumen

"Cuentas de volumen" se gestionan dentro de la tabla de volúmenes de control de la nube híbrida de NetApp . Estas cuentas son específicas únicamente del clúster de almacenamiento en el que fueron creadas. Este tipo de cuentas permite establecer permisos en volúmenes de toda la red, pero no tienen efecto fuera de esos volúmenes.

Una cuenta de volumen contiene la autenticación CHAP necesaria para acceder a los volúmenes que le han sido asignados.

Crea 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 Element.
2. Desde el Panel de control, seleccione **Almacenamiento > Volúmenes**.
3. Seleccione la pestaña **Cuentas**.
4. Seleccione el botón **Crear cuenta**.
5. Introduce un nombre para la nueva cuenta.
6. En la sección Configuración de CHAP, introduzca la siguiente información:
 - Secreto de iniciador para la autenticación de sesión de nodo CHAP
 - Secreto de destino para la autenticación de sesión de nodo CHAP



Para generar automáticamente cualquiera de las contraseñas, deje los campos de credenciales en blanco.

7. Seleccione **Crear cuenta**.

Editar una cuenta de volumen

Puedes modificar la información CHAP y cambiar si una cuenta está activa o bloqueada.



Eliminar o bloquear una cuenta asociada al nodo de administración da como resultado un nodo de administración inaccesible.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el Panel de control, seleccione **Almacenamiento > Volúmenes**.
3. Seleccione la pestaña **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

Elimina una cuenta que ya no necesites.

Antes de eliminar una cuenta de volumen, elimine y purgue primero todos los volúmenes asociados a la cuenta.



Eliminar o bloquear una cuenta asociada al nodo de administración da como resultado un nodo de administración inaccesible.



Los volúmenes persistentes asociados a los servicios de gestión se asignan a una nueva cuenta durante la instalación o actualización. Si utiliza volúmenes persistentes, no modifique ni elimine los volúmenes ni la cuenta asociada. Si eliminás estas cuentas, podrías dejar tu nodo de administración inutilizable.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el Panel de control, seleccione **Almacenamiento > Volúmenes**.
3. Seleccione la pestaña **Cuentas**.
4. En la columna **Acciones** de la tabla, expanda el menú de la cuenta y seleccione **Eliminar**.
5. Confirme la eliminación seleccionando **Sí**.

Encuentra más información

- ["Obtén más información sobre las cuentas."](#)
- ["Trabajar con cuentas que utilizan CHAP"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Cree y gestione volúmenes mediante NetApp Hybrid Cloud Control.

Puede crear un volumen y asociar ese volumen a una cuenta determinada. Al asociar un volumen con una cuenta, la cuenta obtiene acceso al volumen a través de los iniciadores iSCSI y las credenciales CHAP.

Puede especificar la configuración de QoS para un volumen durante su creación.

Puede administrar los volúmenes en NetApp Hybrid Cloud Control de las siguientes maneras:

- [Crear un volumen](#)
- [Aplicar una política de QoS a un volumen](#)
- [Editar un volumen](#)
- [Volúmenes de clonación](#)
- [Agregar volúmenes a un grupo de acceso a volúmenes](#)
- [Eliminar un volumen](#)
- [Restaurar un volumen eliminado](#)
- [Eliminar un volumen borrado](#)

Crear un volumen

Puede crear un volumen de almacenamiento utilizando NetApp Hybrid Cloud Control.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione la pestaña **Volúmenes > Resumen**.

OVERVIEW

ACCESS GROUPS

ACCOUNTS

INITIATORS

QOS POLICIES

VOLUMES

Overview

Active

Deleted

Create Volume

Actions

ID ↑

Name

Account

Access Groups

Access

Used

Size

Snapshots

QoS Policy

Min IOPS

Max IOPS

Burst IOPS

ISCSI Sessions

Actions

1

NetApp-HCI-Datastore-01

NetApp-HCI

NetApp-HCI-6ee7b8e7...

Read/Write

4%

2.15 TB

0

50

15000

15000

2

2

NetApp-HCI-Datastore-02

NetApp-HCI

NetApp-HCI-6ee7b8e7...

Read/Write

0%

2.15 TB

0

50

15000

15000

2

3

NetApp-HCI-credential...

Read/Write

0%

5.37 GB

0

1000

2000

4000

1

4

NetApp-HCI-mnode-api

Read/Write

0%

53.69 GB

0

1000

2000

4000

1

5

NetApp-HCI-hci-monitor

Read/Write

0%

1.07 GB

0

1000

2000

4000

1

</

4. Seleccione **Crear volumen**.
5. Introduzca un nombre para el nuevo volumen.
6. Introduzca el tamaño total del volumen.



La selección de tamaño de volumen predeterminada está en GB. Puedes crear volúmenes utilizando tamaños medidos 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. De la lista **Cuenta**, seleccione la cuenta que debería tener acceso al volumen.

Si no existe una cuenta, seleccione **Crear nueva cuenta**, ingrese 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, la lista no aparece. Empieza a escribir y la función de autocompletar te mostrará valores para que elijas.

9. Para configurar la calidad de servicio para el 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 QoS predeterminados.
- Seleccione una política QoS existente habilitando el interruptor **Asignar política de calidad de servicio** y eligiendo una política QoS existente de la lista resultante.
- Cree y asigne una nueva política de QoS habilitando el interruptor **Asignar política de calidad de servicio** y seleccionando **Crear nueva política de QoS**. En la ventana resultante, introduzca un nombre para la política QoS y, a continuación, introduzca los valores QoS. Cuando haya terminado, seleccione **Crear política de calidad de servicio**.

Los volúmenes que tienen un valor de IOPS máximo o de ráfaga superior a 20 000 IOPS podrían requerir una gran profundidad de cola o varias sesiones para alcanzar este nivel de IOPS en un solo volumen.

10. Seleccione **Crear volumen**.

Aplicar una política de QoS a un volumen

Puede aplicar una política de QoS a los volúmenes de almacenamiento existentes mediante NetApp Hybrid Cloud Control. Si, en cambio, necesita establecer valores QoS personalizados para un volumen, puede hacerlo. [Editar un volumen](#) . Para crear una nueva política de QoS, consulte "[Crear y gestionar políticas de QoS de volumen](#)".

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **Volúmenes > Resumen**.
4. Seleccione uno o más volúmenes para asociarlos con una política de QoS.
5. Seleccione la lista desplegable **Acciones** en la parte superior de la tabla de volúmenes y seleccione **Aplicar política de QoS**.
6. En la ventana resultante, seleccione una política QoS de la lista y seleccione **Aplicar política QoS**.



Si está utilizando políticas de QoS en un volumen, puede configurar una QoS personalizada para eliminar la asociación de la política de QoS con el volumen. Los valores QoS personalizados anulan los valores de la política QoS para la configuración QoS de volumen.

Editar un volumen

Con NetApp Hybrid Cloud Control, puede editar atributos de volumen como valores QoS, tamaño de volumen y la unidad de medida con la que se calculan los valores de bytes. También puede modificar el acceso a la cuenta para el uso de replicación o para restringir el acceso al volumen.

Acerca de esta tarea

Puede cambiar el tamaño de un volumen cuando haya suficiente espacio en el clúster bajo las siguientes condiciones:

- Condiciones normales de funcionamiento.
- Se están reportando errores o fallos de volumen.
- Se está clonando el volumen.
- El volumen se está resincronizando.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **Volúmenes > Resumen**.
4. En la columna **Acciones** de la tabla de volúmenes, expanda el menú del volumen y seleccione **Editar**.
5. Realice los cambios necesarios:
 - a. Cambiar el tamaño total del volumen.



Puedes aumentar, pero no disminuir, el tamaño del volumen. Solo se puede cambiar el tamaño de un volumen en una sola operación de cambio de tamaño. Las operaciones de recolección de basura y las actualizaciones de software no interrumpen la operación de cambio de tamaño.



Si está ajustando el tamaño del volumen para la replicación, primero aumente el tamaño del volumen asignado como destino de la replicación. Luego puedes cambiar el tamaño del volumen de origen. El volumen objetivo puede ser mayor o igual en tamaño que el volumen de origen, pero no puede ser menor.



La selección de tamaño de volumen predeterminada está en GB. Puedes crear volúmenes utilizando tamaños medidos en GB o GiB: 1 GB = 1 000 000 000 bytes 1 GiB = 1 073 741 824 bytes

- b. Seleccione un nivel de acceso a la cuenta diferente:

- Solo lectura
- Leer/Escribir

- Bloqueado
 - Destino de replicación
- c. Seleccione la cuenta que debería tener acceso al volumen.
- Empieza a escribir y la función de autocompletar te mostrará los valores posibles para que elijas.
- Si no existe una cuenta, seleccione **Crear nueva cuenta**, ingrese un nuevo nombre de cuenta y seleccione **Crear**. La cuenta se crea y se asocia con el volumen existente.
- d. Mejore la calidad del servicio realizando una de las siguientes acciones:
- i. Seleccione una póliza existente.
 - ii. En Configuración personalizada, establezca los valores mínimo, máximo y de ráfaga para IOPS o utilice los valores predeterminados.



Si está utilizando políticas de QoS en un volumen, puede configurar una QoS personalizada para eliminar la asociación de la política de QoS con el volumen. La QoS personalizada anulará los valores de la política de QoS para la configuración de QoS de volumen.



Cuando cambie los valores de IOPS, debe incrementarlos en decenas o centenas. Los valores de entrada deben ser números enteros válidos. Configure volúmenes con un valor de ráfaga extremadamente alto. Esto permite que el sistema procese cargas de trabajo secuenciales y de bloques grandes ocasionales más rápidamente, al tiempo que limita las IOPS sostenidas para un volumen.

6. Seleccione **Guardar**.

Volúmenes de clonación

Puede crear un clon de un único volumen de almacenamiento o clonar un grupo de volúmenes para realizar una copia puntual de los datos. Cuando se clona un volumen, el sistema crea una instantánea del volumen y luego crea una copia de los datos a los que hace referencia la instantánea.

Antes de empezar

- Debe añadirse y estar en funcionamiento al menos un clúster.
- Se ha creado al menos un volumen.
- Se ha creado una cuenta de usuario.
- El espacio disponible sin aprovisionar debe ser igual o superior al tamaño del volumen.

Acerca de esta tarea

El clúster admite hasta dos solicitudes de clonación en ejecución por volumen a la vez y hasta 8 operaciones de clonación de volumen activas a la vez. Las solicitudes que superen estos límites se pondrán en cola para su posterior procesamiento.

La clonación de volúmenes es un proceso asíncrono, y el tiempo que requiere depende del tamaño del volumen que se está clonando y de la carga actual del clúster.



Los volúmenes clonados no heredan la pertenencia al grupo de acceso al volumen del volumen de origen.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione la pestaña **Volúmenes > Resumen**.
4. Seleccione cada volumen que desee clonar.
5. Seleccione la lista desplegable **Acciones** en la parte superior de la tabla de volúmenes y seleccione **Clonar**.
6. En la ventana resultante, haga lo siguiente:
 - a. Introduzca un prefijo para el nombre del volumen (esto es opcional).
 - b. Elija el tipo de acceso de la lista **Acceso**.
 - c. Elija una cuenta para asociarla con el nuevo clon de volumen (de forma predeterminada, está seleccionada **Copiar desde volumen**, que utilizará la misma cuenta que utiliza el volumen original).
 - d. Si no existe una cuenta, seleccione **Crear nueva cuenta**, ingrese un nuevo nombre de cuenta y seleccione **Crear cuenta**. La cuenta se crea y se asocia al volumen.



Utilice las mejores prácticas de nomenclatura descriptiva. Esto es especialmente importante si se utilizan varios clústeres o servidores vCenter en su entorno.



Al aumentar el tamaño del volumen de un clon, se obtiene un nuevo volumen con espacio libre adicional al final del volumen. Dependiendo del uso que le des al volumen, es posible que necesites extender particiones o crear nuevas particiones en el espacio libre para poder utilizarlo.

- a. Seleccione **Volúmenes de clonación**.



El tiempo necesario 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.

Agregar volúmenes a un grupo de acceso a volúmenes

Puede agregar un solo volumen o un grupo de volúmenes a un grupo de acceso a volúmenes.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **Volúmenes > Resumen**.
4. Seleccione uno o más volúmenes para asociarlos con un grupo de acceso a volúmenes.
5. Seleccione la lista desplegable **Acciones** en la parte superior de la tabla de volúmenes y seleccione **Agregar al grupo de acceso**.

6. En la ventana resultante, seleccione un grupo de acceso a volúmenes de la lista **Grupo de acceso a volúmenes**.
7. Seleccione **Agregar volumen**.

Eliminar un volumen

Puede eliminar uno o más volúmenes de un clúster de almacenamiento Element.

Acerca de esta tarea

El sistema no elimina inmediatamente los volúmenes borrados; permanecen disponibles durante aproximadamente ocho horas. Tras ocho horas, se eliminan y ya no están disponibles. Si restaura un volumen antes de que el sistema lo elimine, el volumen vuelve a estar en línea y se restablecen las conexiones iSCSI.

Si se elimina un volumen utilizado para crear una instantánea, sus instantáneas asociadas quedan inactivas. Cuando se eliminan los volúmenes de origen borrados, las instantáneas inactivas asociadas también se eliminan del sistema.



Los volúmenes persistentes asociados a los servicios de gestión se crean y se asignan a una nueva cuenta durante la instalación o actualización. Si utiliza volúmenes persistentes, no modifique ni elimine los volúmenes ni la cuenta asociada. Si borras estos volúmenes, podrías dejar tu nodo de administración inutilizable.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **Volúmenes > Resumen**.
4. Seleccione uno o más volúmenes para eliminar.
5. Seleccione la lista desplegable **Acciones** en la parte superior de la tabla de volúmenes y seleccione **Eliminar**.
6. En la ventana resultante, confirme la acción seleccionando **Sí**.

Restaurar un volumen eliminado

Después de eliminar un volumen de almacenamiento, aún puede restaurarlo si lo hace antes de que transcurran ocho horas desde su eliminación.

El sistema no elimina inmediatamente los volúmenes borrados; permanecen disponibles durante aproximadamente ocho horas. Tras ocho horas, se eliminan y ya no están disponibles. Si restaura un volumen antes de que el sistema lo elimine, el volumen vuelve a estar en línea y se restablecen las conexiones iSCSI.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **Volúmenes > Resumen**.

4. Seleccione **Eliminado**.
5. En la columna **Acciones** de la tabla Volúmenes, expanda el menú del volumen y seleccione **Restaurar**.
6. Confirme el proceso seleccionando **Sí**.

Eliminar un volumen borrado

Después de eliminar los volúmenes de almacenamiento, permanecen disponibles durante aproximadamente ocho horas. Después de ocho horas, se eliminan automáticamente y ya no están disponibles. Si no quieres esperar las ocho horas, puedes eliminar

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **Volúmenes > Resumen**.
4. Seleccione **Eliminado**.
5. Seleccione uno o más volúmenes para purgar.
6. Debe realizar una de las siguientes acciones:
 - Si ha seleccionado varios volúmenes, seleccione el filtro rápido **Purgar** en la parte superior de la tabla.
 - Si seleccionó un solo volumen, en la columna **Acciones** de la tabla Volúmenes, expanda el menú del volumen y seleccione **Purgar**.
7. En la columna **Acciones** de la tabla Volúmenes, expanda el menú del volumen y seleccione **Eliminar**.
8. Confirme el proceso seleccionando **Sí**.

Encuentra más información

- ["Aprende sobre volúmenes"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Crear y administrar grupos de acceso por volumen

Puede crear nuevos grupos de acceso a volúmenes, modificar el nombre, los iniciadores asociados o los volúmenes asociados de los grupos de acceso, o eliminar los grupos de acceso a volúmenes existentes mediante NetApp Hybrid Cloud Control.

Lo que necesitarás

- Usted dispone de credenciales de administrador para este sistema de almacenamiento all-flash SolidFire .
- Has actualizado tus servicios de gestión al menos a la versión 2.15.28. La gestión del almacenamiento de NetApp Hybrid Cloud Control no está disponible en versiones anteriores del paquete de servicios.
- Asegúrese de tener un esquema de nomenclatura lógico para los grupos de acceso a volúmenes.

Agregar un grupo de acceso por volumen

Puede agregar un grupo de acceso a 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 Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **Volúmenes**.
4. Seleccione la pestaña **Grupos de acceso**.
5. Seleccione el botón **Crear grupo de acceso**.
6. En el cuadro de diálogo resultante, introduzca un nombre para el nuevo grupo de acceso al volumen.
7. (Opcional) En la sección **Iniciadores**, seleccione uno o más iniciadores para asociar con el nuevo grupo de acceso al volumen.

Si asocia un iniciador con el grupo de acceso a volúmenes, ese iniciador podrá acceder a cada volumen del grupo sin necesidad de autenticación.

8. (Opcional) En la sección **Volúmenes**, seleccione uno o más volúmenes para incluir en este grupo de acceso a volúmenes.
9. Seleccione **Crear grupo de acceso**.

Editar un grupo de acceso a volumen

Puede editar las propiedades de un grupo de acceso a volúmenes existente mediante NetApp Hybrid Cloud Control. Puede 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 Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **Volúmenes**.
4. Seleccione la pestaña **Grupos de acceso**.
5. En la columna **Acciones** de la tabla de grupos de acceso, expanda el menú de opciones del 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. Confirma los cambios seleccionando **Guardar**.
9. En la tabla **Grupos de acceso**, verifique que el grupo de acceso refleje sus cambios.

Eliminar un grupo de acceso a volumen

Puede eliminar un grupo de acceso a volúmenes mediante NetApp Hybrid Cloud Control y, al mismo tiempo, eliminar del sistema los iniciadores asociados a este grupo de acceso.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **Volúmenes**.
4. Seleccione la pestaña **Grupos de acceso**.
5. En la columna **Acciones** de la tabla de grupos de acceso, expanda el menú de opciones del grupo de acceso que desea eliminar.
6. En el menú de opciones, seleccione **Eliminar**.
7. Si no desea eliminar los iniciadores asociados al grupo de acceso, desmarque la casilla de verificación **Eliminar iniciadores en este grupo de acceso**.
8. Confirme la operación de eliminación seleccionando **Sí**.

Encuentra más información

- ["Obtenga información sobre los grupos de acceso por volumen."](#)
- ["Agregar iniciador a un grupo de acceso a volumen"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Crear y gestionar iniciadores

Puedes usar ["iniciadores"](#) para el acceso a volúmenes basado en CHAP en lugar de en cuentas. Puede crear y eliminar iniciadores, y asignarles alias descriptivos para simplificar la administración y el acceso por volumen. Cuando se agrega un iniciador a un grupo de acceso a volúmenes, ese iniciador habilita el acceso a todos los volúmenes del grupo.

Lo que necesitarás

- Usted dispone de credenciales de administrador de clúster.
- Has actualizado tus servicios de gestión al menos a la versión 2.17. La gestión del iniciador de NetApp Hybrid Cloud Control no está disponible en versiones anteriores del paquete de servicios.

Opciones

- [Crear un iniciador](#)
- [Agregar iniciadores a un grupo de acceso por volumen](#)
- [Cambiar un alias de iniciador](#)
- [Eliminar iniciadores](#)

Crear un iniciador

Puede crear iniciadores iSCSI o Fibre Channel y, opcionalmente, asignarles alias.

Acerca de esta tarea

El formato aceptado para un IQN iniciador es `iqn. yyyy-mm` donde `y` y `m` son dígitos seguidos de texto que solo debe contener dígitos, caracteres alfabéticos en minúscula y un punto(.), colon(:) o guion(-). Un ejemplo del formato es el siguiente:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

El formato aceptado para un WWPN de iniciador de Fibre Channel es `:Aa:bB:CC:dd:11:22:33:44` o `AabBCCdd11223344` . Un ejemplo del formato es el siguiente:

```
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 Element.
- 2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
- 3. Seleccione **Volúmenes**.
- 4. Seleccione la pestaña **Iniciadores**.
- 5. Seleccione el botón **Crear iniciadores**.

Opción	Pasos
Crea uno o más iniciadores	a. Introduzca el IQN o WWPN del iniciador en el campo IQN/WWPN. b. Introduzca un nombre amigable para el iniciador en el campo Alias. c. (Opcional) Seleccione Agregar iniciador para abrir nuevos campos de iniciador o utilice la opción de creación masiva. d. Seleccione Crear iniciadores.

Opción	Pasos
Iniciadores de creación masiva	- Seleccione Agregar IQN/WWPN en bloque. - Introduzca una lista de IQN o WWPN en el cuadro de texto. Cada IQN o WWPN debe estar separado por comas o espacios o en su propia línea. - Seleccione Agregar IQN/WWPN. (Opcional) Agregue alias únicos a cada iniciador. - Elimine de la lista cualquier iniciador que ya exista en la instalación. - Seleccione Crear iniciadores.

Agregar iniciadores a un grupo de acceso por volumen

Puede agregar iniciadores a un grupo de acceso a volumen. Cuando se agrega un iniciador a un grupo de acceso a volúmenes, el iniciador habilita el acceso a todos los volúmenes de ese grupo de acceso a volúmenes.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **Volúmenes**.
4. Seleccione la pestaña **Iniciadores**.
5. Seleccione uno o más iniciadores que desee agregar.
6. Seleccione **Acciones > Agregar al grupo de acceso**.
7. Seleccione el grupo de acceso.
8. Confirma los cambios seleccionando **Añadir iniciador**.

Cambiar un alias de iniciador

Puedes cambiar el alias de un iniciador existente o agregar un alias si aún no existe.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **Volúmenes**.
4. Seleccione la pestaña **Iniciadores**.
5. En la columna **Acciones**, expanda el menú de opciones para el iniciador.

6. Seleccione **Editar**.
7. Realiza los cambios necesarios en el alias o añade un nuevo alias.
8. Seleccione **Guardar**.

Eliminar iniciadores

Puedes eliminar uno o más iniciadores. Cuando se elimina un iniciador, el sistema lo quita de cualquier grupo de acceso a volúmenes asociado. Las conexiones que utilizan el iniciador permanecen 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 Element.
2. Desde el panel de control, expanda el nombre de su clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **Volúmenes**.
4. Seleccione la pestaña **Iniciadores**.
5. Eliminar uno o más iniciadores:
 - a. Seleccione uno o más iniciadores que desee eliminar.
 - b. Seleccione **Acciones > Eliminar**.
 - c. Confirme la operación de eliminación y seleccione **Sí**.

Encuentra más información

- ["Aprende sobre los iniciadores"](#)
- ["Obtenga información sobre los grupos de acceso por volumen."](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Crear y gestionar políticas de QoS de volumen

Una política de QoS (Calidad de Servicio) le permite crear y guardar una configuración de calidad de servicio estandarizada que se puede aplicar a muchos volúmenes. El clúster seleccionado debe ser Element 10.0 o posterior para utilizar las políticas de QoS; de lo contrario, las funciones de política de QoS no estarán disponibles.



Consulte el contenido de Conceptos de almacenamiento all-flash de SolidFire para obtener más información sobre su uso. ["Políticas de QoS"](#) en lugar de volumen individual ["Calidad de servicio"](#)

Con NetApp Hybrid Cloud Control, puede crear y administrar políticas de QoS realizando las siguientes tareas:

- [Crea una política de QoS](#)
- [Aplicar una política de QoS a un volumen](#)
- [Cambiar la asignación de política QoS de un volumen](#)

- [Editar una política de QoS](#)
- [Eliminar una política de QoS](#)

Crea una política de QoS

Puede crear políticas de QoS y aplicarlas a volúmenes que deban tener un rendimiento equivalente.



Si está utilizando políticas de QoS, no utilice QoS personalizada en un volumen. La QoS personalizada anulará y ajustará los valores de la política de QoS para la configuración de QoS de volumen.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el menú de su clúster de almacenamiento.
3. Seleccione **Almacenamiento > Volúmenes**.
4. Seleccione la pestaña **Políticas de QoS**.
5. Seleccione **Crear política**.
6. Ingrese el **Nombre de la política**.



Utilice las mejores prácticas de nomenclatura descriptiva. Esto es especialmente importante si se utilizan varios clústeres o servidores vCenter en su entorno.

7. Introduzca los valores mínimos de IOPS, máximos de IOPS y de ráfaga de IOPS.
8. Seleccione **Crear política QoS**.

Se genera un ID de sistema para la política y esta aparece en la página de Políticas QoS con sus valores QoS asignados.

Aplicar una política de QoS a un volumen

Puede asignar una política QoS existente a un volumen utilizando NetApp Hybrid Cloud Control.

Lo que necesitarás

La política de QoS que desea asignar ha sido [creado](#).

Acerca de esta tarea

Esta tarea describe cómo asignar una política QoS a un volumen individual cambiando su configuración. La última versión de NetApp Hybrid Cloud Control no dispone de una opción de asignación masiva para más de un volumen. Hasta que se incluya la funcionalidad de asignación masiva en una versión futura, puede utilizar la interfaz web de Element o la interfaz de usuario del complemento de vCenter para asignar políticas de QoS de forma masiva.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el menú de 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 aparece, seleccione **Editar**.
6. En el cuadro de diálogo, habilite **Asignar política QoS** y seleccione la política QoS de la lista desplegable que desea aplicar al volumen seleccionado.



La asignación de QoS anulará cualquier valor de QoS de volumen individual que se haya aplicado previamente.

7. Seleccione **Guardar**.

Cambiar la asignación de política QoS de un volumen

Puede eliminar la asignación de una política QoS de un volumen o seleccionar una política QoS diferente o una QoS personalizada.

Lo que necesitarás

El volumen que desea modificar es **asignado** una política de QoS.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el menú de 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 aparece, seleccione **Editar**.
6. En el cuadro de diálogo, realice una de las siguientes acciones:
 - Deshabilite **Asignar política de QoS** y modifique los valores de **IOPS mínimas**, **IOPS máximas** e **IOPS de ráfaga** para la QoS de volumen individual.



Cuando las políticas de QoS están deshabilitadas, el volumen utiliza los valores de IOPS de QoS predeterminados a menos que se modifiquen de otro modo.

- Seleccione una política QoS diferente de la lista desplegable para aplicarla al volumen seleccionado.

7. Seleccione **Guardar**.

Editar una política de QoS

Puede cambiar el nombre de una política QoS existente o editar los valores asociados a la política. Modificar los valores de rendimiento de la política de QoS afecta a la QoS de todos los volúmenes asociados a dicha política.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el menú de su clúster de almacenamiento.
3. Seleccione **Almacenamiento > Volúmenes**.

4. Seleccione la pestaña **Políticas de QoS**.
5. Seleccione el menú **Acciones** situado junto a la política de QoS que desea modificar.
6. Seleccione **Editar**.
7. En el cuadro de diálogo **Editar política de QoS**, cambie uno o más de los siguientes elementos:
 - **Nombre**: El nombre definido por el usuario para la política de QoS.
 - **IOPS mínimas**: El número mínimo de IOPS garantizado para el volumen. Valor predeterminado = 50.
 - **IOPS máx.**: El número máximo de IOPS permitido para el volumen. Valor predeterminado = 15.000.
 - **IOPS de ráfaga**: El número máximo de IOPS permitidos durante un corto período de tiempo para el volumen. Valor predeterminado = 15.000.
8. Seleccione **Guardar**.



Puede seleccionar el enlace en la columna **Volúmenes activos** de una póliza para mostrar una lista filtrada de los volúmenes asignados a esa póliza.

Eliminar una política de QoS

Puede eliminar una política QoS si ya no es necesaria. Cuando se elimina una política de QoS, todos los volúmenes asignados a dicha política mantienen los valores de QoS definidos previamente por la política, pero como QoS de volumen individual. Se elimina cualquier asociación con la política QoS eliminada.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. Desde el panel de control, expanda el menú de su clúster de almacenamiento.
3. Seleccione **Almacenamiento > Volúmenes**.
4. Seleccione la pestaña **Políticas de QoS**.
5. Seleccione el menú **Acciones** situado junto a la política de QoS que desea modificar.
6. Seleccione **Eliminar**.
7. Confirma la acción.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Supervise su sistema SolidFire con NetApp Hybrid Cloud Control.

Supervise los recursos de almacenamiento en el panel de control de la nube híbrida.

Con el panel de control de la nube híbrida de NetApp , puede ver todos sus recursos de almacenamiento de un vistazo. Además, puede supervisar la capacidad de

almacenamiento y el rendimiento del almacenamiento.



Al iniciar una nueva sesión de NetApp Hybrid Cloud Control por primera vez, puede haber una demora en la carga de la vista del panel de control de NetApp Hybrid Cloud Control cuando el nodo de administración está gestionando muchos clústeres. El tiempo de carga varía dependiendo del número de clústeres que estén siendo gestionados activamente por el nodo de gestión. En los siguientes lanzamientos, experimentará tiempos de carga más rápidos.

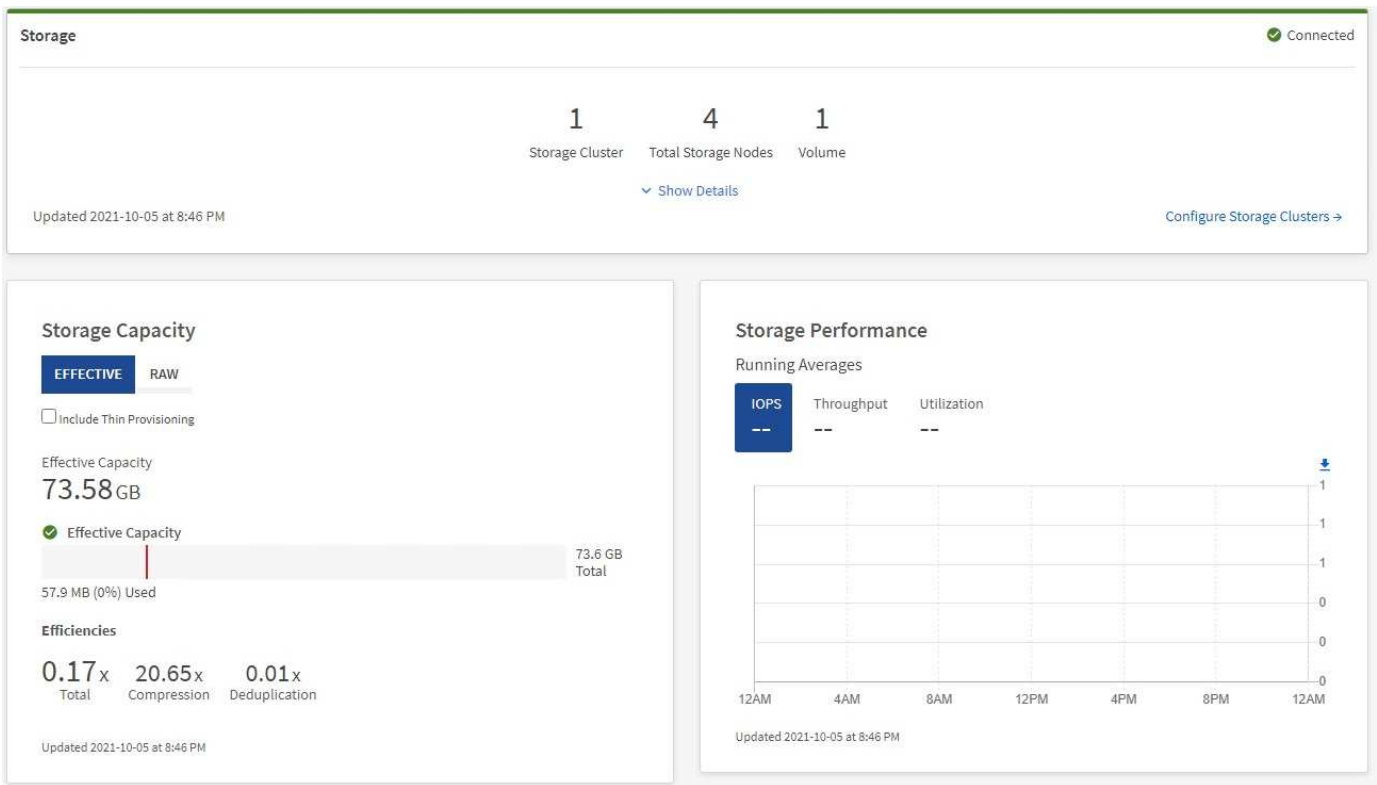
- [Acceda al panel de control de NetApp HCC.](#)
- [Recursos de almacenamiento de monitorización](#)
- [Supervisar la capacidad de almacenamiento](#)
- [Rendimiento del almacenamiento de monitorización](#)

Acceda al panel de control de NetApp HCC.

1. Abra la dirección IP del nodo de administración 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. Vea el panel de control de la nube híbrida.



Recursos de almacenamiento de monitorización

Utilice el panel **Almacenamiento** para ver su entorno de almacenamiento total. Puede supervisar el número de clústeres de almacenamiento, nodos de almacenamiento y volúmenes totales.

Para ver los detalles, en el panel Almacenamiento, seleccione **Mostrar detalles**.

Storage

Connected

1

2

16

Storage Cluster

Total Storage Nodes

Total Volumes

^ Hide Details

Cluster Name ↑	Nodes	Volumes	Connection Status
hci-tt-test8-cluster	4	16	Connected

Updated 2021-10-04 at 4:52 PM

Configure Storage Clusters →



El número total de nodos de almacenamiento no incluye los nodos testigo de los clústeres de almacenamiento de dos nodos. Los nodos testigo están incluidos en el número de nodos en la sección de detalles de ese clúster.



Para ver los datos más recientes del clúster de almacenamiento, utilice la página Clústeres de almacenamiento, donde la consulta se realiza con mayor frecuencia que en el Panel de control.

Supervisar la capacidad de almacenamiento

Es fundamental controlar la capacidad de almacenamiento de su entorno. Mediante el panel Capacidad de almacenamiento, puede determinar las mejoras en la eficiencia de su capacidad de almacenamiento con o sin las funciones de compresión, deduplicación y aprovisionamiento ligero habilitadas.

Puedes ver el espacio de almacenamiento físico total disponible en tu clúster en la pestaña **RAW**, y la información sobre el almacenamiento aprovisionado en la pestaña **EFFECTIVE**.



Pasos

1. Seleccione la pestaña **RAW** para ver el espacio de almacenamiento físico total utilizado y disponible en su clúster.

Fíjese en las líneas verticales para determinar si su capacidad utilizada es inferior al total o inferior a los umbrales de Advertencia, Error o Crítico. Pase el cursor sobre las líneas para ver los detalles.



Puedes configurar el umbral de Advertencia, que por defecto es un 3% inferior al umbral de Error. Los umbrales de error y crítico están preestablecidos y no son configurables por diseño. El umbral de error indica que queda menos de un nodo de capacidad en el clúster. Para conocer los pasos para configurar el umbral, consulte ["Configurando el umbral de clúster completo"](#).



Para obtener detalles sobre los umbrales de clúster relacionados con la API de elementos, consulte ["obtenerUmbralCompletoDelClúster"](#) en la *documentación de la API del software Element*. Para ver detalles sobre la capacidad de bloques y metadatos, consulte ["Comprensión de los niveles de plenitud del clúster"](#) en la *documentación del software Element*.

2. Seleccione la pestaña **EFFECTIVO** para ver información sobre el almacenamiento total aprovisionado a los hosts conectados y para ver las calificaciones de eficiencia.
 - a. Opcionalmente, marque **Incluir aprovisionamiento ligero** para ver las tasas de eficiencia del aprovisionamiento ligero en el gráfico de barras de capacidad efectiva.
 - b. **Gráfico de barras de capacidad efectiva:** Observe las líneas verticales para determinar si su capacidad utilizada es inferior al total o inferior a los umbrales de advertencia, error o crítico. Al igual que en la pestaña Raw, puedes pasar el cursor sobre las líneas verticales para ver los detalles.
 - c. **Eficiencia:** Consulte estas calificaciones para determinar las mejoras en la eficiencia de su capacidad de almacenamiento con las funciones de compresión, deduplicación y aprovisionamiento ligero habilitadas. Por ejemplo, si la compresión se muestra como "1.3x", esto significa que la eficiencia del almacenamiento con la compresión habilitada es 1.3 veces más eficiente que sin ella.



La eficiencia total es igual a (espacio máximo utilizado * factor de eficiencia) / 2, donde factor de eficiencia = (factor de aprovisionamiento ligero * factor de deduplicación * factor de compresión). Cuando la opción de aprovisionamiento ligero está desactivada, 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 detallado y un contexto histórico, consulte: ["Detalles de NetApp SolidFire Active IQ"](#) .

Rendimiento del almacenamiento de monitorización

Puedes consultar cuántas IOPS o rendimiento puedes obtener de un clúster sin superar el rendimiento útil de ese recurso utilizando el panel Rendimiento de almacenamiento. El rendimiento del almacenamiento es el punto en el que se obtiene la máxima utilización antes de que la latencia se convierta en un problema.

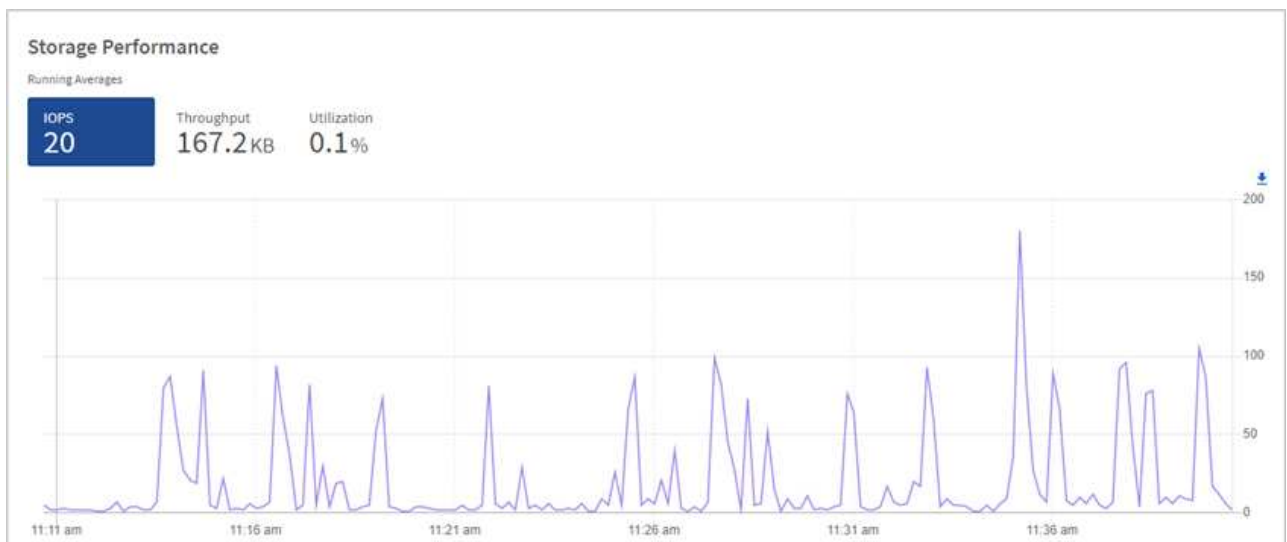
El panel Rendimiento de almacenamiento le ayuda a identificar si el rendimiento está llegando al punto en que podría degradarse si aumentan las cargas de trabajo.

La información de este panel se actualiza cada 10 segundos y muestra un promedio de todos los puntos del gráfico.

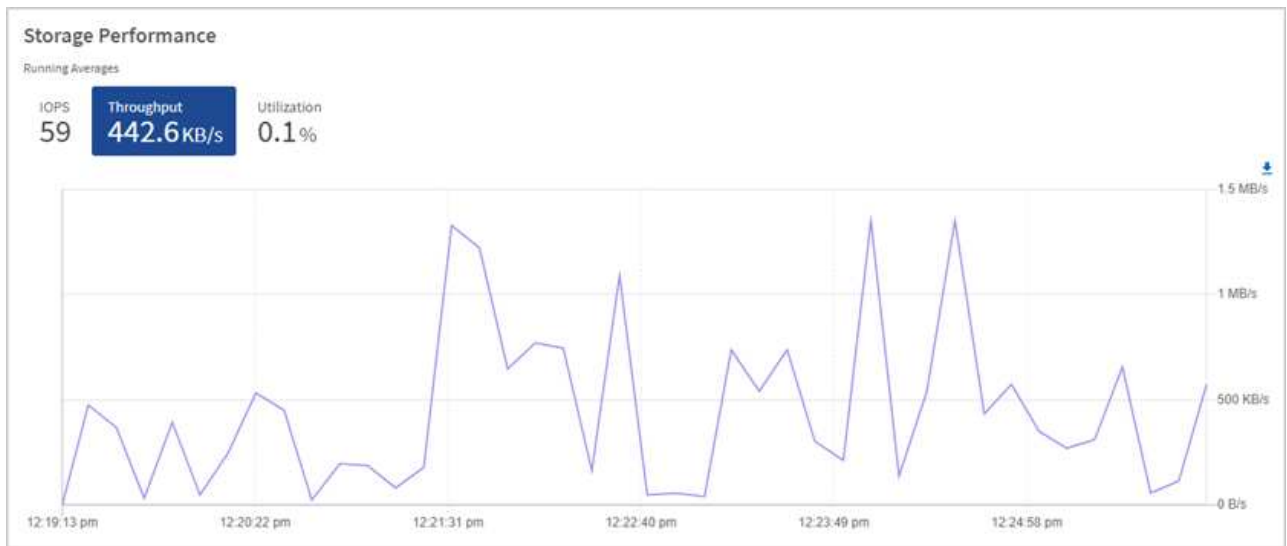
Para obtener más detalles sobre el método de la API de elementos asociado, consulte la ["Obtener estadísticas del clúster"](#) método en la *documentación de la API del software Element*.

Pasos

1. Consulte el panel Rendimiento de almacenamiento. Para obtener más detalles, coloque el cursor sobre los puntos del gráfico.
 - a. Pestaña **IOPS**: Consulte las operaciones por segundo actuales. Busque tendencias o picos en los datos. Por ejemplo, si ve que el IOPS máximo es de 160K y de ese total, 100K son IOPS libres o disponibles, podría considerar agregar más cargas de trabajo a este clúster. Por otro lado, si ve que solo hay 140K disponibles, podría considerar descargar cargas de trabajo o ampliar su sistema.



- b. Pestaña **Rendimiento**: Monitoree patrones o picos en el rendimiento. También conviene controlar si se mantienen altos los valores de rendimiento, ya que esto podría indicar que se está acercando al rendimiento máximo útil del recurso.



- c. Pestaña **Utilización**: Monitorea la utilización de IOPS en relación con el total de IOPS disponibles sumadas a nivel de clúster.



2. Para un análisis más detallado, examine el rendimiento del almacenamiento utilizando el complemento NetApp Element para vCenter Server.

["Rendimiento mostrado en el complemento NetApp Element para vCenter Server"](#).

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Consulta tu inventario en la página de Nodos.

Puedes ver tus recursos de almacenamiento en tu sistema y determinar sus direcciones IP, nombres y versiones de software.

Puede consultar la información de almacenamiento de sus sistemas de múltiples nodos. Si ["dominios de protección personalizados"](#) Una vez asignados, puede ver qué dominios de protección están asignados a

nodos específicos.

Pasos

- 1. Abra la dirección IP del nodo de administración 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 menú de navegación izquierdo, seleccione **Nodos**.

Nodos

Only NetApp HCI Nodes are displayed on this page.

STORAGE

COMPUTE

Cluster1

1 of 1

Two-node

▼

☰

⬇

Hostname	Node Model	Element Version	Management IP Address
stg01	H410S-0	12.0.0.318	- VLAN 1184
stg02	H410S-0	12.0.0.318	- VLAN 1184

1 - 2 of 2 results

1

30

Witness Nodes

Hostname	Management IP Address	Storage (iSCSI) IP Address
wit01		
wit02		



Al iniciar una nueva sesión de NetApp Hybrid Cloud Control por primera vez, puede haber una demora en la carga de la página de nodos de NetApp Hybrid Cloud Control cuando el nodo de administración esté gestionando muchos clústeres. El tiempo de carga varía dependiendo del número de clústeres que estén siendo gestionados activamente por el nodo de gestión. En los siguientes lanzamientos, experimentará tiempos de carga más rápidos.

- 4. En la pestaña **Almacenamiento** de la página Nodos, revise la siguiente información:
 - a. Clústeres de dos nodos: Aparece una etiqueta de “dos nodos” en la pestaña Almacenamiento y se enumeran los nodos testigo 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 desplegado en espera para mantener una alta disponibilidad en caso de fallo de un nodo.
 - c. Clusters con cuatro nodos o más: Aparece información para clusters con cuatro o más nodos. Los nodos testigo no aplican. Si comenzaste con dos o tres nodos de almacenamiento y agregaste más nodos, los nodos testigo seguirán apareciendo. De lo contrario, no aparecerá la tabla de nodos testigo.
 - d. Versión del paquete de firmware: A partir de la versión 2.14 de los servicios de administración, si tiene clústeres que ejecutan Element 12.0 o posterior, puede ver la versión del paquete de firmware para

estos clústeres. Si los nodos de un clúster tienen diferentes versiones de firmware, puede ver **Múltiple** en la columna **Versión del paquete de firmware**.

- e. Dominios de protección personalizados: Si se utilizan dominios de protección personalizados en el clúster, puede ver las asignaciones de dominios de protección personalizados para cada nodo del clúster. Si los dominios de protección personalizados no están habilitados, esta columna no aparece.

5. Puedes manipular la información de estas páginas de varias maneras:

- a. Para filtrar la lista de elementos en los resultados, seleccione el icono **Filtrar** y seleccione los filtros. También puedes 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 la cantidad de almacenamiento, consulte el panel de control de NetApp Hybrid Cloud Control (HCC). Ver ["Supervise los recursos de almacenamiento con el panel de control de HCC."](#)

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Supervise los volúmenes en su clúster de almacenamiento.

El sistema SolidFire aprovisiona almacenamiento mediante volúmenes. Los volúmenes son dispositivos de bloque a los que acceden a través de la red los clientes iSCSI o Fibre Channel. Puede supervisar los 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 (QoS) asociada al volumen.

También puedes ver detalles sobre los volúmenes activos y eliminados.

Con esta vista, es posible que primero desee supervisar la columna de capacidad utilizada.

Solo puede acceder a esta información si tiene privilegios administrativos de NetApp Hybrid Cloud Control.

Pasos

1. Abra la dirección IP del nodo de administración 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 izquierdo, seleccione la instalación de almacenamiento totalmente flash SolidFire .
4. En el panel de navegación izquierdo, seleccione el clúster y luego **Almacenamiento > Volúmenes**.

OVERVIEW ACCESS GROUPS ACCOUNTS INITIATORS QOS POLICIES													
VOLUMES Overview													
Active Deleted Create Volume Actions													
	ID ↑	Name	Account	Access Groups	Access	Used	Size	Snapshots	QoS Policy	Min IOPS	Max IOPS	Burst IOPS	iSCSI Sessions
☐	1	NetApp-HCI-Datastore-01	NetApp-HCI	NetApp-HCI-6ee7b8e7...	Read/Write	4%	2.15 TB	0		50	15000	15000	2
☐	2	NetApp-HCI-Datastore-02	NetApp-HCI	NetApp-HCI-6ee7b8e7...	Read/Write	0%	2.15 TB	0		50	15000	15000	2
☐	3	NetApp-HCI-credential...			Read/Write	0%	5.37 GB	0		1000	2000	4000	1
☐	4	NetApp-HCI-mnode-api			Read/Write	0%	53.69 GB	0		1000	2000	4000	1
☐	5	NetApp-HCI-hci-monitor			Read/Write	0%	1.07 GB	0		1000	2000	4000	1

5. En la página Volúmenes, utilice las siguientes opciones:



- a. Filtra los resultados seleccionando el icono **Filtrar**.
 - b. Oculte o muestre columnas seleccionando el icono **Ocultar/Mostrar**.
 - c. Actualice los datos seleccionando el icono **Actualizar**.
 - d. Descarga un archivo CSV seleccionando el icono **Descargar**.
6. Supervise la columna de capacidad utilizada. Si se alcanzan los umbrales de Advertencia, Error o Crítico, el color representa el estado de la capacidad utilizada:
- a. Advertencia - Amarillo
 - b. Error - Naranja
 - c. Crítico - Rojo

7. Desde la vista Volúmenes, seleccione las pestañas para ver detalles adicionales sobre los volúmenes:

- a. **Grupos de acceso:** Puede ver los grupos de acceso a volúmenes que están asignados desde los iniciadores a una colección de volúmenes para un acceso seguro.

Ver información sobre ["grupos de acceso por volumen"](#).

- b. **Cuentas:** Aquí puede ver las cuentas de usuario, que permiten a los clientes conectarse a volúmenes en un nodo. Cuando se crea un volumen, este se asigna a una cuenta de usuario específica.

Ver información sobre ["cuentas de usuario del sistema de almacenamiento totalmente flash SolidFire"](#).

- c. **Iniciadores:** Puede ver el IQN del iniciador iSCSI o los WWPN de Fibre Channel para el volumen. Cada IQN añadido a un grupo de acceso puede acceder a cada volumen del grupo sin necesidad de autenticación CHAP. Cada WWPN agregado a un grupo de acceso habilita el acceso a la red 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 QoS aplica configuraciones estandarizadas para IOPS mínimas, IOPS máximas e IOPS de ráfaga a múltiples volúmenes.

Ver información sobre ["Políticas de rendimiento y calidad de servicio"](#).

Encuentra más información

- ["Documentación de SolidFire y Element"](#)

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Recopilar registros para la resolución de problemas

Si tiene problemas con la instalación de su almacenamiento all-flash SolidFire , puede recopilar registros para enviarlos al soporte de NetApp para ayudar con el diagnóstico. Puede utilizar NetApp Hybrid Cloud Control o la API REST para recopilar registros en un sistema Element.

Lo que necesitarás

- Asegúrese de que la versión de su clúster de almacenamiento esté ejecutando el software NetApp Element 11.3 o posterior.
- Asegúrese de haber implementado un nodo de administración que ejecute la versión 11.3 o posterior.

Opciones de recopilación de registros

Elige una de las siguientes opciones:

- [Utilice NetApp Hybrid Cloud Control para recopilar registros.](#)
- [Utilice la API REST para recopilar registros.](#)

Utilice NetApp Hybrid Cloud Control para recopilar registros.

Puede acceder al área de recopilación de registros desde el panel de control de NetApp Hybrid Cloud.

Pasos

1. Abra la dirección IP del nodo de administración 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 Element.
3. Desde el Panel de control, seleccione el menú en la parte superior derecha.
4. Seleccione **Recopilar registros**.

Si ya ha recopilado registros anteriormente, puede descargar el paquete de registros existente o iniciar una nueva recopilación de registros.

5. Seleccione un rango de fechas en el menú desplegable **Rango de fechas** para especificar qué fechas deben incluir los registros.

Si especifica una fecha de inicio personalizada, puede seleccionar la fecha con la que comenzará el rango de fechas. Se recopilarán los registros desde esa fecha hasta la actualidad.

6. En la sección **Recopilación de registros**, seleccione los tipos de archivos de registro que debe incluir el paquete de registros.

Para los registros de almacenamiento, puede expandir la lista de nodos de almacenamiento y seleccionar nodos individuales de los que recopilar registros (o todos los nodos de la lista).

7. Seleccione **Recopilar registros** para iniciar la recopilación de registros.

La recopilación de registros se ejecuta en segundo plano y la página muestra el progreso.



Dependiendo de los registros que recopiles, la barra de progreso podría permanecer en un porcentaje determinado durante varios minutos, o avanzar muy lentamente en algunos puntos.

8. Seleccione **Descargar registros** para descargar el paquete de registros.

El paquete de registros está en formato de archivo .tgz comprimido de UNIX.

Utilice la API REST para recopilar registros.

Puedes utilizar la API REST para recopilar los registros de Element.

Pasos

1. Localice el ID del clúster de almacenamiento:
 - a. Abra la interfaz de usuario de la API REST del nodo de administración en el nodo de administración:

```
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 del cliente como `mnode-client` si el valor no está ya asignado.
 - iii. Seleccione **Autorizar** para iniciar una sesión.
2. Recopilar registros de Element:
 - a. Seleccione **POST /bundle**.
 - b. Seleccione **Probarlo**.
 - c. Modifique los valores de los siguientes parámetros en el campo **Cuerpo de la solicitud** según el tipo de registros que necesite recopilar y el intervalo de tiempo correspondiente:

Parámetro	Tipo	Descripción
modifiedSince	Cadena de fecha	Incluir únicamente 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	Establezca este parámetro en <code>true</code> para incluir los registros del nodo de administración.

Parámetro	Tipo	Descripción
storageCrashDumps	Booleano	Establezca este parámetro en <code>true</code> para incluir registros de depuración de fallos de nodos de almacenamiento.
storageLogs	Booleano	Establezca este parámetro en <code>true</code> para incluir los registros de los nodos de almacenamiento.
storageNodeIds	matriz UUID	Si <code>storageLogs</code> está configurado para <code>true</code> , complete este parámetro con los ID de los nodos del clúster de almacenamiento para limitar la recopilación de registros a esos nodos de almacenamiento específicos. Utilice el GET <code>https://[management node IP]/logs/1/bundle/options</code> como punto de acceso para ver todos los ID de nodo posibles que puede usar.

- d. Seleccione **Ejecutar** para comenzar la recopilación de registros. La respuesta debería ser 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. Comprobar el estado de la tarea de recopilación de registros:

- Seleccione **GET /bundle**.
- Seleccione **Probarlo**.
- Seleccione **Ejecutar** para obtener el estado de la tarea de recopilación.
- Desplácese hasta el final del cuerpo de la respuesta.

Deberías ver un `percentComplete` atributo que detalla el progreso de la colección. Si la colección está completa, `downloadLink` El atributo contiene el enlace de descarga completo, incluido el nombre del archivo del paquete de registro.

- Copia el nombre del archivo al final del `downloadLink` atributo.

4. Descargue el paquete de registros recopilados:

- Seleccione **GET /bundle/{filename}**.

- b. Seleccione **Probarlo**.
- c. Pegue el nombre del archivo que copió anteriormente en el `filename` Campo de texto del parámetro.
- d. Seleccione **Ejecutar**.

Tras la ejecución, aparece un enlace de descarga en el cuerpo de la respuesta.

- e. Seleccione **Descargar archivo** y guarde el archivo resultante en su ordenador.

El paquete de registros está en formato de archivo `.tgz` comprimido de UNIX.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Gestiona el almacenamiento con la API de Element

Software Element API

Aprenda a administrar el almacenamiento con la API de Element.

La API de Element se basa en el protocolo JSON-RPC sobre HTTPS. JSON-RPC es un protocolo RPC simple basado en texto que utiliza el formato ligero de intercambio de datos JSON. Existen bibliotecas cliente disponibles para todos los principales lenguajes de programación.

Puedes realizar solicitudes a la API mediante solicitudes HTTPS POST al punto final 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 solicitud POST). Al enviar solicitudes a la API, debe utilizar "application/json-rpc" como tipo de contenido de la solicitud y asegurarse de que el cuerpo no esté codificado en formato de formulario.



La interfaz web de Element utiliza los métodos de la API descritos en este documento. Puedes supervisar las operaciones de la API en la interfaz de usuario habilitando el registro de la API; esto te permite ver los métodos que se están enviando al sistema. Puedes habilitar tanto las solicitudes como las respuestas para ver cómo responde el sistema a los métodos que se emiten.

A menos que se indique lo contrario, todas las cadenas de fecha en las respuestas de la API están en formato UTC+0.



Cuando el clúster de almacenamiento está muy cargado o se envían muchas solicitudes API consecutivas sin demora intermedia, un método podría fallar y devolver el error "xDBVersionMismatch". Si esto ocurre, vuelva a intentar la llamada al método.

objetos comunes

La API del software Element utiliza objetos JSON para representar conceptos de datos organizados. Muchos de estos métodos de la API utilizan estos objetos para la entrada y salida de datos. Esta sección documenta los objetos de uso común; los objetos que solo se utilizan dentro de un único método se documentan con ese método en lugar de en esta sección.

["Aprende sobre objetos comunes"](#)

Métodos comunes

Los métodos comunes son aquellos utilizados para recuperar información sobre el clúster de almacenamiento, la propia API o las operaciones de API en curso.

["Aprenda sobre los métodos comunes"](#)

Métodos de la API de cuentas

Los métodos de cuenta le permiten agregar, eliminar, ver y modificar la información de la cuenta y la

seguridad.

["Obtenga información sobre los métodos de la API de cuentas"](#)

Métodos de la API de administrador

Puede utilizar los métodos de la API de administrador para crear, modificar, ver y eliminar administradores de clústeres de almacenamiento y asignar niveles de acceso y privilegios a quienes tengan acceso a un clúster de almacenamiento.

["Obtenga información sobre los métodos de la API de administrador."](#)

Métodos de la API de clúster

Los métodos de la API del clúster de software Element le permiten gestionar la configuración y la topología del clúster de almacenamiento y los nodos que pertenecen a un clúster de almacenamiento.

Algunos métodos de la API de clúster operan en nodos que forman parte de un clúster o que han sido configurados para unirse a un clúster. Puedes agregar nodos a un clúster nuevo o a un clúster existente. Los nodos que están listos para ser agregados a un clúster se encuentran en estado "pendiente", lo que significa que han sido configurados pero aún no se han agregado al clúster.

["Aprenda sobre los métodos de la API de clúster"](#)

Métodos de la API de creación de clústeres

Puedes utilizar estos métodos de la API para crear un clúster de almacenamiento. Todos estos métodos deben utilizarse contra el punto final de la API en un único nodo.

["Aprenda sobre los métodos de la API de creación de clústeres."](#)

Métodos de la API de Drive

Puede utilizar los métodos de la API de unidades para agregar y administrar unidades que estén disponibles para un clúster de almacenamiento. Cuando se agrega un nodo de almacenamiento al clúster de almacenamiento o se instalan nuevas unidades en un nodo de almacenamiento existente, las unidades están disponibles para ser agregadas al clúster de almacenamiento.

["Aprenda sobre los métodos de la API de Drive"](#)

Métodos de la API de Fibre Channel

Puede utilizar los métodos de la API de Fibre Channel para agregar, modificar o eliminar miembros de nodo Fibre Channel de un clúster de almacenamiento.

["Aprenda sobre los métodos de la API de Fibre Channel"](#)

Métodos de la API del iniciador

Los métodos de iniciador le permiten agregar, eliminar, ver y modificar objetos de iniciador iSCSI, que gestionan la comunicación entre el sistema de almacenamiento y los clientes de almacenamiento externos.

["Aprenda sobre los métodos de la API de iniciación"](#)

Métodos de la API LDAP

Puede utilizar el Protocolo Ligero de Acceso a Directorios (LDAP) para autenticar el acceso al almacenamiento de Element. Los métodos de la API LDAP descritos en esta sección le permiten configurar el acceso LDAP al clúster de almacenamiento.

["Aprenda sobre los métodos de la API de LDAP"](#)

Métodos de la API de autenticación multifactor

Puede utilizar la autenticación multifactor (MFA) para gestionar las sesiones de usuario utilizando un proveedor de identidad (IdP) de terceros a través del lenguaje de marcado de aserción de seguridad (SAML).

["Aprenda sobre los métodos de la API de autenticación multifactor."](#)

Métodos de la API de autenticación de sesión

Puedes utilizar la autenticación basada en sesiones para gestionar las sesiones de usuario.

["Aprenda sobre los métodos de la API de autenticación de sesión"](#)

Métodos de la API de Node

Puedes utilizar los métodos de la API de nodos para configurar nodos individuales. Estos métodos operan en nodos individuales que necesitan ser configurados, están configurados pero aún no participan en un clúster, o participan activamente en un clúster. Los métodos de la API de nodos le permiten ver y modificar la configuración de nodos individuales y de la red del clúster utilizada para comunicarse con el nodo. Debe ejecutar estos métodos en nodos individuales; no puede ejecutar métodos de API por nodo en la dirección del clúster.

["Aprende sobre los métodos de la API de Node."](#)

Métodos de la API de replicación

Los métodos de la API de replicación le permiten conectar dos clústeres para la protección continua de datos (CDP). Al conectar dos clústeres, los volúmenes activos dentro de un clúster se pueden replicar continuamente en un segundo clúster para proporcionar recuperación de datos. Al emparejar volúmenes para la replicación, puede proteger sus datos de eventos que podrían hacerlos inaccesibles.

["Aprenda sobre los métodos de la API de replicación"](#)

Métodos de la API de seguridad

Puede integrar el software Element con servicios externos relacionados con la seguridad, como un servidor externo de gestión de claves. Estos métodos relacionados con la seguridad le permiten configurar las funciones de seguridad de Element, como la administración de claves externas para el cifrado en reposo.

["Aprenda sobre los métodos de la API de seguridad"](#)

Métodos de la API de SnapMirror

Los métodos de la API SnapMirror son utilizados por la interfaz web de Element para administrar las instantáneas replicadas con sistemas ONTAP remotos. Estos métodos están destinados únicamente para su uso por la interfaz web de Element. Si necesita acceso a la API de la funcionalidad de SnapMirror, utilice las API de ONTAP. No se proporcionan ejemplos de solicitud y retorno para los métodos de la API de SnapMirror

["Aprenda sobre los métodos de la API de SnapMirror"](#)

Métodos de la API de configuración del sistema

Los métodos de la API de configuración del sistema le permiten obtener y establecer valores de configuración que se aplican a todos los nodos del clúster.

["Aprenda sobre los métodos de la API de configuración del sistema."](#)

Métodos de API de redes multiinquilino

Las redes multiinquilino en los clústeres de almacenamiento Element permiten que el tráfico entre múltiples clientes que se encuentran en redes lógicas separadas se conecte a un clúster de almacenamiento Element sin enrutamiento de capa 3.

Las conexiones al clúster de almacenamiento están segregadas en la pila de red mediante el uso de etiquetado VLAN.

Requisitos previos para configurar una red virtual multiinquilino

- Debe haber identificado el bloque de direcciones IP de red del cliente que se asignarán a las redes virtuales en los nodos de almacenamiento.
- Debe haber identificado una dirección IP de red de almacenamiento del cliente (SVIP) que se utilizará como punto final para todo el tráfico de almacenamiento.

orden de operaciones de redes virtuales

1. Utilice el método AddVirtualNetwork para aprovisionar en bloque las direcciones IP que introduzca.

Después de agregar una red virtual, el clúster realiza automáticamente los siguientes pasos:

- Cada nodo de almacenamiento crea una interfaz de red virtual.
 - A cada nodo de almacenamiento se le asigna una dirección VLAN a la que se puede enrutar utilizando la SVIP virtual.
 - Las direcciones IP de VLAN persisten en cada nodo en caso de reinicio del mismo.
2. Una vez asignadas la interfaz de red virtual y las direcciones VLAN, puede asignar el tráfico de red del cliente a la SVIP virtual.

["Aprenda sobre los métodos de la API de redes multiinquilino"](#)

Métodos de la API de volumen

Los métodos de la API de volúmenes del software Element le permiten administrar volúmenes que residen en un nodo de almacenamiento. Con estos métodos puede crear, modificar, clonar y eliminar volúmenes. También puede utilizar los métodos de la API de volumen para recopilar y mostrar mediciones de datos para un volumen.

["Aprenda sobre los métodos de la API de volumen"](#)

Métodos de la API de grupos de acceso por volumen

Los métodos de grupo de acceso a volúmenes le permiten agregar, eliminar, ver y modificar grupos de acceso a volúmenes, que son conjuntos de volúmenes a los que los usuarios pueden acceder mediante iniciadores iSCSI o Fibre Channel.

["Obtenga información sobre los métodos de la API de grupos de acceso por volumen."](#)

Métodos de la API de instantáneas de volumen

Los métodos de la API de instantáneas de volumen del software Element le permiten administrar instantáneas de volumen. Puede crear, modificar, clonar y eliminar instantáneas de volumen utilizando los métodos de la API de instantáneas de volumen.

["Aprenda sobre los métodos de la API de instantáneas de volumen"](#)

Métodos de la API de volumen virtual

Los métodos de la API de volúmenes virtuales del software Element le permiten administrar volúmenes virtuales (VVols). Con estos métodos de la API, puede ver los VVols existentes, así como crear, modificar y eliminar contenedores de almacenamiento de volúmenes virtuales. Aunque no puede utilizar estos métodos para operar con volúmenes normales, puede utilizar los métodos de la API de volúmenes normales para listar información sobre VVols.

["Aprenda sobre los métodos de la API de volumen virtual"](#)

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

miembros del objeto de solicitud

Cada solicitud a la API del software Element tiene las siguientes partes básicas:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
método	Nombre del método a invocar.	cadena	Ninguno	Sí
parámetros	Objeto que contiene los parámetros del método que se está invocando. Los parámetros con nombre son obligatorios. No se permiten parámetros posicionales (pasados como un array).	Objeto JSON	{}	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
identificación	Identificador utilizado para relacionar la solicitud con la respuesta, devuelto en el resultado.	cadena o entero	{}	No

miembros del objeto de respuesta

Cada cuerpo de respuesta de la API del software Element tiene las siguientes partes básicas:

Nombre	Descripción	Tipo
resultado	El objeto devuelto por el método. El sistema devuelve un objeto con miembros nombrados que corresponden al valor de retorno documentado para el método. Este miembro no está presente si se ha producido un error.	Objeto JSON
error	El objeto que se devuelve cuando se produce un error. Este miembro solo está presente si se ha producido un error.	Objeto
identificación	Un identificador utilizado para relacionar la solicitud con la respuesta, tal como se proporciona en la solicitud.	cadena o entero
parámetros no utilizados	Un mensaje de advertencia que indica que se ha pasado al menos un parámetro incorrecto al método de la API y que este no se ha utilizado.	Objeto

puntos de conexión de solicitud

En la API se utilizan tres tipos de puntos de conexión de solicitud (clúster de almacenamiento, creación de clúster de almacenamiento y por nodo). Siempre debes utilizar el punto de conexión más reciente compatible con tu versión del software Element.

Los tres puntos de conexión de solicitud en la API se designan de las siguientes maneras:

Métodos de la API de clúster

El punto de conexión HTTPS para las solicitudes de API de todo el clúster de almacenamiento es `https://<mvip>/json-rpc/<api-version>`, donde:

- `<mvip>` es la dirección IP virtual de gestión para el clúster de almacenamiento.
- `<api-version>` es la versión de la API que estás utilizando.

Métodos de la API para la creación y arranque de clústeres

El punto de conexión HTTPS para crear un clúster de almacenamiento y acceder a las solicitudes de la API de arranque es `https://<nodeIP>/json-rpc/<api-version>`, donde:

- `<nodeIP>` es la dirección IP del nodo que está agregando al clúster.
- `<api-version>` es la versión de la API que estás utilizando.

Métodos de API por nodo

El punto de conexión HTTPS para las solicitudes de API de nodos de almacenamiento individuales es `https://<nodeIP>:442/json-rpc/<api-version>`, donde:

- `<nodeIP>` es la dirección IP de administración 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 estás utilizando.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Autenticación API

Puede autenticarse con el sistema al usar la API incluyendo un encabezado de autenticación HTTP Basic en todas las solicitudes a la API. Si omite la información de autenticación, el sistema rechaza la solicitud no autenticada con una respuesta HTTP 401. El sistema admite la autenticación básica HTTP sobre TLS.

Utilice la cuenta de administrador del clúster para la autenticación de la API.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Métodos asíncronos

Algunos métodos de la API son asíncronos, lo que significa que la operación que realizan podría no estar completa cuando el método devuelve un valor. Los métodos asíncronos devuelven un identificador que se puede consultar para ver el estado de la operación; la información de estado de algunas operaciones puede incluir un porcentaje

de finalización.

Cuando se consulta una operación asíncrona, su resultado puede ser de uno de los siguientes tipos:

- ``DriveAdd`` El sistema está añadiendo una unidad al clúster.
- ``BulkVolume`` El sistema está realizando una operación de copia entre volúmenes, como una copia de seguridad o una restauración.
- ``Clone`` El sistema está clonando un volumen.
- ``DriveRemoval`` El sistema está copiando datos de una unidad como preparación para eliminarla del clúster.
- ``RtfsPendingNode`` El sistema está instalando software compatible en un nodo antes de agregarlo al clúster.

Tenga en cuenta los siguientes puntos al utilizar métodos asíncronos o al obtener el estado de una operación asíncrona en ejecución:

- Los métodos asíncronos se indican en la documentación de cada método.
- Los métodos asíncronos devuelven un "asyncHandle", que es un identificador conocido por el método API que lo emite. Puede utilizar el identificador para consultar el estado o el resultado de la operación asíncrona.
- Puedes obtener el resultado de métodos asíncronos individuales con el método `GetAsyncResult`. Cuando se utiliza `GetAsyncResult` para consultar una operación completada, el sistema devuelve el resultado y lo elimina automáticamente del sistema. Cuando se utiliza `GetAsyncResult` para consultar una operación incompleta, el sistema devuelve el resultado pero no lo elimina.
- 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 elimina los resultados de las operaciones completadas.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Atributos

Muchas de las solicitudes y respuestas de la API utilizan objetos, además de 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 nombre-valor personalizados que el usuario puede establecer en objetos JSON. Algunos métodos permiten agregar atributos al crear o modificar objetos.

Existe un límite de 1000 bytes en los objetos de atributos codificados.

miembro del objeto

Este objeto contiene el siguiente miembro:

Nombre	Descripción	Tipo
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON

Ejemplo de solicitud

El siguiente ejemplo de solicitud utiliza el método AddClusterAdmin:

```
{
  "method": "AddClusterAdmin",
  "params": {
    "username": "joeadmin",
    "password": "68!5Aru268)$",
    "access": [
      "volume",
      "reporting"
    ],
    "attributes": {
      "name1": "value1",
      "name2": "value2",
      "name3": "value3"
    }
  }
}
```

objetos comunes

cuenta

El `account` El objeto contiene información sobre una cuenta. Este objeto incluye únicamente información "configurada" sobre la cuenta, no información de tiempo de ejecución ni de uso.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
accountID	El identificador único de la cuenta.	entero
attributes	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON

Nombre	Descripción	Tipo
enableChap	Especifica si las credenciales de la cuenta CHAP pueden ser utilizadas por un iniciador para acceder a los volúmenes.	booleano
initiatorSecret	El secreto del iniciador CHAP.	cadena
status	Estado actual de la cuenta. Valores posibles: • activa: Una cuenta activa. • bloqueado: Una cuenta bloqueada. • Eliminada: Una cuenta que ha sido borrada y purgada.	cadena
storageContainerID	El identificador único del contenedor de almacenamiento de volumen virtual asociado a esta cuenta.	UUID
targetSecret	El secreto CHAP objetivo.	cadena
username	El nombre de usuario de la cuenta.	cadena
volumes	Lista de identificadores de volumen para los volúmenes que pertenecen a esta cuenta.	matriz de enteros

Encuentra más información

- [Agregar cuenta](#)
- [ObtenerCuentaPorID](#)
- [ObtenerCuentaPorNombre](#)
- [Lista de cuentas](#)

información de sesión de autenticación

El `authSessionInfo` El objeto contiene información sobre una sesión de autenticación.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
<code>accessGroupList</code>	Lista de grupos de acceso para el usuario.	matriz de cadenas
<code>authMethod</code>	El tipo de autorización que tiene el usuario administrador del clúster. Valores posibles: • LDAP - autenticado mediante LDAP. • Clúster: autenticación mediante un nombre de usuario y una contraseña almacenados en la base de datos del clúster. • IdP - autenticado a través de un proveedor de identidad de terceros.	cadena
<code>clusterAdminIDs</code>	Lista de AdminID de clúster asociados con esta sesión. Para las sesiones relacionadas con LDAP o un proveedor de identidad (IdP) de terceros, esta será una lista agregada de los AdminID de clúster coincidentes asociados con esta sesión.	matriz de enteros
<code>finalTimeout</code>	Hora en la que la sesión deja de ser válida. Esto se establece cuando se crea la sesión y no se puede cambiar.	cadena
<code>idpConfigVersion</code>	Versión de configuración del IdP cuando se creó la sesión.	entero
<code>lastAccessTimeout</code>	Tiempo en el que la sesión se vuelve inválida por inactividad. Se establece un nuevo valor cuando se accede a la sesión para su uso, hasta el momento en que la sesión se vuelve inválida debido a que se alcanza el tiempo de espera final.	cadena
<code>sessionCreationTime</code>	Hora en que se crea la sesión.	cadena
<code>sessionID</code>	UUID para esta sesión.	UUID

Nombre	Descripción	Tipo
username	Nombre de usuario asociado a esta sesión. Para las sesiones relacionadas con LDAP, este será el DN LDAP del usuario. Para las sesiones relacionadas con un IdP de terceros, se utilizará un par nombre-valor arbitrario para auditar las operaciones dentro de la sesión. No necesariamente coincidirá con el nombre de un administrador del clúster. Por ejemplo, un ID de sujeto SAML, pero esto vendrá determinado por la configuración del IdP y el contenido resultante de la aserción SAML.	cadena

Trabajo de gran volumen

El `bulkVolumeJob` El objeto contiene información sobre operaciones de lectura o escritura de volúmenes masivos, como la clonación o la creación de instantáneas.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
attributes	Atributo JSON del trabajo de volumen masivo.	Objeto JSON
bulkVolumeID	El ID del trabajo de volumen masivo interno.	entero
createTime	Marca de tiempo creada para el trabajo de volumen masivo en formato UTC+0.	cadena de fecha ISO 8601
elapsedTime	El número de segundos transcurridos desde que comenzó el trabajo.	cadena
format	El formato de la operación de volumen masivo. Valores posibles: • nativo • sin comprimir	cadena

Nombre	Descripción	Tipo
key	La clave única creada por la sesión de volumen masivo.	cadena
percentComplete	Porcentaje completado reportado por la operación.	entero
remainingTime	Tiempo restante estimado en segundos.	entero
srcVolumeID	El ID del volumen de origen.	entero
status	Estado de la operación. Valores posibles: • preparante • correr • completo • fallido	cadena
script	El nombre del script, si se proporciona alguno.	cadena
snapshotID	El ID de la instantánea si existe una instantánea en el origen del trabajo de volumen masivo.	entero
type	El tipo de operación a granel. Valores posibles: • leer • escribir	cadena

enlace (volúmenes virtuales)

El objeto de enlace contiene información sobre el enlace para un volumen virtual. Puede recuperar una lista de esta información para todos los volúmenes virtuales utilizando el `ListVirtualVolumeBindings` Método API.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
protocolEndpointID	El identificador único del punto final del protocolo.	UUID
protocolEndpointInBandID	El scsiNAADeviceID del punto final del protocolo.	cadena
protocolEndpointType	El tipo de punto final del protocolo. SCSI es el único valor devuelto para el tipo de extremo del protocolo.	cadena
virtualVolumeBindingID	El identificador único del objeto de enlace de volumen virtual.	entero
virtualVolumeHostID	El identificador único del host del volumen virtual.	UUID
virtualVolumeID	El identificador único del volumen virtual.	UUID
virtualVolumeSecondaryID	El identificador secundario del volumen virtual.	cadena

Encuentra más información

- [ListVirtualVolumeBindings](#)
- [punto final del protocolo](#)

Detalles del certificado

El `certificateDetails` El objeto contiene la información decodificada sobre un certificado de seguridad.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
issuer	El nombre del emisor.	cadena
modulus	El módulo de la clave pública.	cadena
notAfter	La fecha de vencimiento del certificado.	Cadena ISO 8601

Nombre	Descripción	Tipo
notBefore	La fecha de inicio del certificado.	Cadena ISO 8601
serial	El número de serie del certificado.	cadena
sha1Fingerprint	Resumen de la versión del certificado codificada en DER.	cadena
subject	El nombre del sujeto.	cadena

clúster

El objeto de clúster contiene información que el nodo utiliza para comunicarse con el clúster. Puede recuperar esta información con el método de la API GetClusterConfig.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
cipi	Interfaz de red utilizada para la comunicación del clúster.	cadena
clúster	Nombre de clúster único.	cadena
Capaz de cifrado	Indica si el nodo admite el cifrado de unidades.	booleano
conjunto	Los nodos que participan en el clúster.	matriz de cadenas
Configuración de la unidad fips	Indica si el nodo admite unidades con certificación FIPS 140-2.	booleano
mipi	La interfaz de red utilizada para la gestión de nodos.	cadena
nombre	El nombre del clúster.	cadena
ID de nodo	El ID del nodo en el clúster.	cadena
ID de nodo pendiente	El ID del nodo pendiente en el clúster.	entero

Nombre	Descripción	Tipo
role	Identifica la función del nodo.	entero
sipi	La interfaz de red utilizada para el tráfico de almacenamiento.	cadena
estado	Estado actual del nodo. Valores posibles: • Disponible: El nodo no ha sido configurado con un nombre de clúster. • Pendiente: El nodo está pendiente para un clúster con nombre específico y se puede agregar. • Activo: El nodo es un miembro activo de un clúster y no se puede agregar a otro clúster. • PendienteActivo: El nodo actualmente está siendo restaurado a la imagen de software de fábrica y aún no es un miembro activo de un clúster. Una vez completado, pasará al estado Activo.	cadena
versión	La versión del software que se ejecuta en el nodo.	cadena

Modificabilidad de los miembros y estados de los nodos

Esta tabla indica si los parámetros del objeto pueden modificarse o no en cada estado posible del nodo.

Nombre del parámetro	Estado disponible	Estado pendiente	Estado activo
cipi	No	No	No
clúster	Sí	Sí	No
Capaz de cifrado	No	No	No
conjunto	No	No	No
mipi	Sí	Sí	No
nombre	Sí	Sí	Sí

ID de nodo	No	No	No
ID de nodo pendiente	No	No	No
role	No	No	No
sipi	No	No	No
estado	No	No	No
versión	No	No	No

Encuentra más información

[Obtener configuración de clúster](#)

administrador del clúster

El objeto `clusterAdmin` contiene información sobre el usuario administrador del clúster actual. Puede recuperar información de usuario administrador con el método API `GetCurrentClusterAdmin`.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
acceso	Los métodos que puede utilizar este administrador de clúster.	matriz de cadenas
método de autenticación	El tipo de autorización que tiene el usuario administrador del clúster. Valores posibles: • LDAP • Grupo • Local	cadena
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON
ID de administrador del clúster	El ID del administrador del clúster para este usuario administrador del clúster.	entero

Nombre	Descripción	Tipo
nombre de usuario	Nombre de usuario para este administrador de clúster.	cadena

Encuentra más información

[ObtenerAdministradorDeClústerActual](#)

capacidad del clúster

El objeto `clusterCapacity` contiene mediciones de capacidad de alto nivel para el clúster. Puede obtener información sobre la capacidad del clúster con el método de la API `GetClusterCapacity`. Las medidas de espacio en los miembros del objeto se calculan en bytes.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Espacio de bloque activo	La cantidad de espacio en el bloque de unidades. Esto incluye información adicional como entradas de metadatos y espacio que se puede eliminar.	entero
sesiones activas	El número de sesiones iSCSI activas que se comunican con el clúster.	entero
promedio de IOPS	El promedio de IOPS para el clúster desde la medianoche, hora universal coordinada (UTC).	entero
<code>clusterRecentIOSize</code>	El tamaño promedio de IOPS para todos los volúmenes del clúster.	entero
IOPS actuales	El promedio de IOPS para todos los volúmenes del clúster durante los últimos 5 segundos.	entero
IOPS máximas	La capacidad máxima estimada de IOPS del clúster actual.	entero

Nombre	Descripción	Tipo
espacio máximo sobreaprovisionable	La cantidad máxima de espacio disponible. Este es un valor calculado. No se pueden crear nuevos volúmenes si el espacio provisionado actual más el tamaño del nuevo volumen supera este número. El valor se calcula de la siguiente manera: $\text{maxOverProvisionableSpace} = \text{maxProvisionedSpace} * \text{maxMetadataOverProvisionFactor}$	entero
espacio máximo provisionado	La cantidad total de espacio provisionable si todos los volúmenes están llenos al 100% (sin metadatos de provisionamiento ligero).	entero
espacio de metadatos usado máximo	Número de bytes en unidades de volumen utilizados para almacenar metadatos.	entero
espacio máximo utilizado	Cantidad total de espacio en todas las unidades de bloque activas.	entero
nonZeroBlock	El número total de bloques de 4 KiB que contienen datos después de que se haya completado la última operación de recolección de basura.	entero
sesiones activas máximas	El número máximo de conexiones iSCSI desde la medianoche UTC.	entero
pico de IOPS	El valor más alto para currentIOPS desde la medianoche UTC.	entero
espacio provisionado	La cantidad total de espacio provisionado en todos los volúmenes del clúster.	entero
marca de tiempo	La fecha y hora, en formato UTC+0, en que se tomó esta muestra de capacidad del clúster.	Cadena ISO 8601

Nombre	Descripción	Tipo
operaciones totales	El número total de operaciones de E/S realizadas durante la vida útil del clúster.	entero
bloques únicos	El número total de bloques almacenados en las unidades de bloques. El valor incluye bloques replicados.	entero
Espacio utilizado de bloques únicos	La cantidad total de datos que ocupan los uniqueBlocks en las unidades de bloque. Consulte el método GetclusterCapacity para obtener información sobre cómo se relaciona este número con el valor de uniqueBlocks.	entero
useMetadataSpace	El número total de bytes en las unidades de volumen utilizados para almacenar metadatos.	entero
useMetadataSpaceInSnapshots	Número de bytes en unidades de volumen utilizados para almacenar datos únicos en instantáneas. Esta cifra proporciona una estimación de cuánto espacio de metadatos se recuperaría al eliminar todas las instantáneas del sistema.	entero
espacio usado	Cantidad total de espacio utilizado por todas las unidades de bloque del sistema.	entero
bloques cero	Número total de bloques vacíos de 4 KiB sin datos después de que se haya completado la última ronda de operación de recolección de basura.	entero

Encuentra más información

[Obtener capacidad del clúster](#)

configuración del clúster

El `clusterConfig` El objeto devuelve información que el nodo utiliza para comunicarse con el clúster.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
<code>cipi</code>	Interfaz de red utilizada para la comunicación del clúster.	cadena
<code>cluster</code>	Nombre único del clúster.	cadena
<code>encryptionCapable</code>	Especifica si el nodo admite cifrado.	booleano
<code>ensemble</code>	Nodos que participan en el clúster.	matriz de cadenas
<code>fipsDriveConfiguration</code>	Especifica si el nodo admite unidades con certificación FIPS 140-2.	booleano
<code>hasLocalAdmin</code>	Especifica si el clúster tiene un administrador local.	booleano
<code>mipi</code>	Interfaz de red utilizada para la gestión de nodos.	cadena
<code>name</code>	Identificador único del clúster.	cadena
<code>nodeID</code>	Identificador único del nodo.	entero
<code>pendingNodeID</code>	Identificador único para el nodo pendiente.	entero
<code>role</code>	Identifica la función del nodo.	cadena
<code>sipi</code>	Interfaz de red utilizada para el almacenamiento.	cadena
<code>state</code>	Indica el estado del nodo.	cadena
<code>version</code>	Indica la versión del nodo.	cadena

Información del clúster

El objeto `clusterInfo` contiene información que el nodo utiliza para comunicarse con el clúster. Puedes obtener esta información con el método API `GetClusterInfo`.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON
esquema de protección predeterminado	El esquema de protección utilizado por defecto para los nuevos volúmenes, a menos que se proporcione un esquema de protección con el Crear volumen Llamada al método. Este esquema de protección siempre debe estar incluido en el conjunto de esquemas de protección habilitados.	cadena
esquemas de protección habilitados	Una lista de todos los esquemas de protección que se han habilitado en este clúster de almacenamiento.	matriz de cadenas
cifradoEnEstadoDeReposo	Estado de la función de cifrado en reposo. Valores posibles: • Habilitación: Se está habilitando el cifrado en reposo. • Habilitado: El cifrado en reposo está habilitado. • Deshabilitando: Se está deshabilitando el cifrado en reposo. • Deshabilitado: El cifrado en reposo está deshabilitado.	cadena
conjunto	Los nodos que participan en el clúster.	matriz de cadenas
MVIP	La dirección IP flotante (virtual) del clúster en la red de administración.	cadena
Interfaz mvip	La interfaz física asociada a la dirección MVIP.	cadena
ID de nodo mvip	El nodo que contiene la dirección MVIP maestra.	entero

Nombre	Descripción	Tipo
Etiqueta VLAN mvip	El identificador VLAN para la dirección MVIP.	cadena
nombre	El nombre único del clúster.	cadena
recuento de repeticiones	El número de réplicas de cada dato que se almacenarán en el clúster. El valor válido es "2".	entero
Cifrado de software en estado de reposo	Estado de cifrado en reposo basado en software.	cadena
esquemas de protección admitidos	Una lista de todos los esquemas de protección compatibles con este clúster de almacenamiento.	matriz de cadenas
svip	La dirección IP flotante (virtual) para el clúster en la red de almacenamiento (iSCSI).	cadena
Interfaz svip	La interfaz física asociada con la dirección SVIP maestra.	cadena
svipNodeID	El nodo que contiene la dirección SVIP maestra.	entero
Etiqueta VLAN svip	El identificador VLAN para la dirección SVIP maestra.	cadena
ID único	El identificador único del clúster.	cadena
UUID	El identificador único del clúster.	UUID
balanceo de carga de volumen en el estado de lops reales	El estado del equilibrio de segmentos se basa en las IOPS reales en lugar de la función de IOPS mínimas. Disponible a partir del Elemento 12.8.	cadena

Encuentra más información

- ["Obtener información del clúster"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

clusterPair

El objeto clusterPair contiene información sobre los clústeres emparejados con el clúster local. Puede recuperar una lista de objetos clusterPair para el clúster local con el método ListClusterPairs.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
nombre del clúster	El nombre del otro grupo del par.	cadena
clusterPairID	Se asigna un identificador único a cada clúster del par.	entero
clusterPairUUID	El identificador único universal para el par de clústeres.	cadena
UUID	Identificador único para el clúster remoto en el par de clústeres.	entero
latencia	La latencia, en milisegundos, entre clústeres.	entero
MVIP	La dirección IP de la conexión de gestión para clústeres emparejados.	cadena
estado	El estado de la conexión entre los grupos emparejados. Valores posibles: • Sin configurar • Conectado • Mal configurado • Desconectado	cadena
versión	La versión Element del otro clúster del par.	cadena

Encuentra más información

[ListClusterPairs](#)

estadísticas del clúster

El objeto `clusterStats` contiene datos estadísticos para un clúster. Muchas de las estadísticas relacionadas con el volumen que contiene el objeto son promedios de todos los volúmenes del clúster. Puede utilizar el método `GetClusterStats` para recuperar esta información para un clúster.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Cálculo	Tipo
IOPS reales	IOPS reales actuales para todo el clúster en los últimos 500 milisegundos.	Punto en el tiempo	entero
Tamaño promedio de IOPS	Tamaño promedio en bytes de las operaciones de E/S recientes en el clúster en los últimos 500 milisegundos.	Punto en el tiempo	entero
profundidad de la cola de clientes	Número de operaciones de lectura y escritura pendientes en el clúster.	N/A	entero
Utilización del clúster	Porcentaje de IOPS máximas del clúster que se están utilizando actualmente. Esto se calcula como $\text{clusterUtilization} = \text{normalizedIOPS} / \text{maxIOPS}$ (de <code>GetClusterCapacity</code>).	N/A	flotar
latenciaUSeg	Tiempo promedio, en microsegundos, para completar operaciones en un clúster en los últimos 500 milisegundos.	Punto en el tiempo	entero
IOPS normalizadas	Número promedio de IOPS para todo el clúster en los últimos 500 milisegundos.	Punto en el tiempo	entero

Nombre	Descripción	Cálculo	Tipo
bytes leídos	El total acumulado de bytes leídos del clúster desde su creación.	Aumento monótono	entero
readBytesLastSample	Número total de bytes leídos del clúster durante el último período de muestreo.	Punto en el tiempo	entero
Latencia de lectura (segundos)	Tiempo promedio, en microsegundos, para completar las operaciones de lectura al clúster en los últimos 500 milisegundos.	Punto en el tiempo	entero
Latencia de lectura (USec) Total	El tiempo total empleado en realizar operaciones de lectura desde la creación del clúster.	Aumento monótono	entero
operaciones de lectura	El total acumulado de operaciones de lectura en el clúster desde su creación.	Aumento monótono	entero
readOpsLastSample	El número total de operaciones de lectura durante el último período de muestra.	Punto en el tiempo	entero
período de muestra MSeg	Duración del período de muestreo, en milisegundos.	N/A	entero
serviciosCount	El número de servicios que se ejecutan en el clúster. Si es igual a servicesTotal, esto indica que se recopilaron estadísticas válidas de todos los nodos.	Punto en el tiempo	entero
Servicios Total	El número total de servicios que se espera que se ejecuten en el clúster.	N/A	entero

Nombre	Descripción	Cálculo	Tipo
marca de tiempo	La hora actual en formato UTC+0.	N/A	cadena de fecha ISO 8601
lecturas no alineadas	El total acumulado de operaciones de lectura no alineadas en un clúster desde la creación del clúster.	Aumento monótono	entero
escrituras no alineadas	El total acumulado de operaciones de escritura no alineadas en un clúster desde la creación del clúster.	Aumento monótono	entero
escribirBytes	El total acumulado de bytes escritos en el clúster desde su creación.	Aumento monótono	entero
writeBytesLastSample	El número total de bytes escritos en el clúster durante el último período de muestreo.	Aumento monótono	entero
Latencia de escritura (segundos)	Tiempo promedio, en microsegundos, para completar las operaciones de escritura en un clúster en los últimos 500 milisegundos.	Punto en el tiempo	entero
Latencia de escritura (Usec) total	El tiempo total empleado en realizar operaciones de escritura desde la creación del clúster.	Aumento monótono	entero
operaciones de escritura	El total acumulado de operaciones de escritura en el clúster desde su creación.	Aumento monótono	entero
writeOpsLastSample	El número total de operaciones de escritura durante el último período de muestra.	Punto en el tiempo	entero

Encuentra más información

[Obtener estadísticas del clúster](#)

Estructura del clúster

El objeto `clusterStructure` contiene información de copia de seguridad de la configuración del clúster creada por el método `GetClusterStructure`. Puede utilizar el método `SetClusterStructure` para restaurar esta información en un clúster de almacenamiento que esté reconstruyendo.

miembros del objeto

Este objeto contiene la información de retorno combinada de los siguientes métodos:

- [Obtener información del clúster](#)
- [Lista de cuentas](#)
- [Iniciadores de listas](#)
- [Lista de volúmenes](#)(con `includeVirtualVolumes=false`)
- [Listar grupos de acceso de volumen](#)
- [Listar contenedores de almacenamiento](#)
- [Lista de políticas de QoS](#)
- [Obtener información SNMP](#)
- [Obtener información NTP](#)
- [Lista de redes virtuales](#)
- [Lista de administradores de clúster](#)
- [Listas de horarios](#)
- [ListSnapMirrorEndpoints](#)
- [Obtener estado de la función](#)
- [Obtener configuración LDAP](#)
- [Obtener hosts de registro remoto](#)
- [Obtener QoS predeterminado](#)
- [Obtener asignaciones de LUN de acceso al volumen](#)

Encuentra más información

- [ObtenerEstructuraDeClúster](#)
- [Establecer estructura de clúster](#)

conducir

El objeto de unidad contiene información sobre las unidades individuales en los nodos activos del clúster. Este objeto contiene detalles sobre las unidades que se han agregado como metadatos de volumen o unidades de bloque, así como sobre las unidades que

aún no se han agregado y están disponibles. Puedes recuperar esta información con el `ListDrives` Método API.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	Lista de pares nombre-valor en formato de objeto JSON. Este objeto siempre es nulo y no se puede modificar.	Objeto JSON
capacidad	La capacidad total de la unidad, en bytes.	entero
ranura del chasis	Para las plataformas HCI, este valor es la letra del nodo y el número de ranura en el chasis del servidor donde se encuentra esta unidad. Para las plataformas de almacenamiento, el número de ranura es una representación en cadena del entero "ranura".	cadena
Detalle de fallo de la unidad	Si el estado de una unidad es "Fallo", este campo proporciona más detalles sobre por qué se marcó la unidad como fallida.	cadena
driveID	El ID de esta unidad.	entero
motivo de fallo de seguridad de la unidad	Si la activación o desactivación de la seguridad de la unidad falló, indique el motivo del fallo. Si el valor es "ninguno", no hubo ningún fallo.	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
ID del proveedor de clave	Identifica al proveedor de la clave de autenticación para desbloquear esta unidad.	entero
ID de nodo	El ID del nodo que contiene esta unidad.	entero

Nombre	Descripción	Tipo
tamaño del archivo del segmento	Tamaño del archivo de segmento de la unidad, en bytes.	entero
de serie	El número de serie de la unidad.	cadena
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	Estado de la unidad. Valores posibles: • disponible: Una unidad disponible. • activo: Una unidad activa. • Borrando: Se está realizando un borrado seguro de la unidad. Cualquier dato que contenga esa unidad se eliminará permanentemente. • Falló: Una unidad que ha fallado. Los datos que anteriormente se encontraban en la unidad se han migrado a otras unidades del clúster. • Extracción: Se está procediendo a extraer una unidad. Los datos que anteriormente se encontraban en la unidad se están migrando a otras unidades del clúster.	cadena
tipo	El tipo de transmisión. Valores posibles: • volumen: Almacena metadatos de volumen. • bloque: Almacena datos de bloque. • Desconocido: El tipo de unidad aún no está activo y está por determinar.	cadena
capacidad utilizable	La capacidad utilizable de la unidad, en bytes.	entero

Encuentra más información

[ListDrives](#)

Estadísticas de la unidad

El objeto `driveStats` contiene mediciones de actividad de alto nivel para una sola unidad. Puede recuperar información de medición con el método API. `GetDriveStats`.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
sesiones activas	Número de sesiones iSCSI que utilizan actualmente esta unidad (solo se muestra para unidades de metadatos).	entero
driveID	Identificador único de la unidad en el clúster.	entero
recuento de datos fallidos	Número de elementos de hardware de la unidad que fallaron.	entero
iosEnProgreso	Número de operaciones de entrada/salida en curso en esta unidad.	entero
porcentaje de vida restante	Indicador de desgaste del disco duro.	entero
bytes leídos de por vida	Total de bytes leídos de esta unidad durante su vida útil.	entero
escritura de bytes de por vida	Total de bytes escritos en esta unidad durante su vida útil.	entero
horas de encendido	Número de horas que esta unidad ha estado encendida.	entero
lecturas	Número de llamadas a <code>read()</code> por segundo a esta unidad.	entero
bytes leídos	Total de bytes leídos de la unidad debido a operaciones del cliente.	entero

Nombre	Descripción	Tipo
lecturasCombinadas	El número de llamadas read() a sectores adyacentes que podrían combinarse en una lectura mayor.	entero
leer Msec	El número de milisegundos empleados en la lectura.	entero
operaciones de lectura	Total de operaciones de lectura en la unidad debido a operaciones del cliente.	entero
sectores reasignados	Número de sectores defectuosos reemplazados en esta unidad.	entero
porcentaje de capacidad de reserva	La capacidad de reserva disponible del variador.	entero
marca de tiempo	La hora actual en formato UTC+0.	cadena de fecha ISO 8601
capacidad total	Capacidad total de la unidad, en bytes.	entero
Errores incorregibles	Valor de Errores Incorregibles Reportados del sistema de monitoreo SMART (Tecnología de Automonitoreo, Análisis e Informe) en la unidad.	entero
capacidad utilizada	Capacidad utilizada de la unidad, en bytes.	entero
memoria utilizada	Cantidad de memoria utilizada actualmente por el nodo que aloja esta unidad.	entero
escribe	Número de llamadas a write() por segundo a esta unidad.	entero
escribirBytes	Total de bytes escritos en la unidad debido a la actividad del cliente.	entero
escribeCombinado	El número de llamadas write() a sectores adyacentes que podrían combinarse en una escritura mayor.	entero

Nombre	Descripción	Tipo
Escribir Msec	El número de milisegundos empleados en la escritura.	entero
operaciones de escritura	Operaciones de escritura totales en la unidad debido a la actividad del cliente.	entero

Encuentra más información

[GetDriveStats](#)

error

El objeto de error contiene un código y un mensaje de error si se produce un error durante una llamada a un método. Todos los errores generados por el sistema tienen un código de error 500.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
código	El código numérico utilizado para identificar el error. Todos los errores generados por el sistema devuelven un código 500.	entero
nombre	El identificador único del error específico que se produjo. Cada método devuelve un conjunto documentado de errores, aunque también debes estar preparado para manejar errores no reconocidos.	cadena
mensaje	Una descripción del error, posiblemente con detalles adicionales.	cadena

evento

El objeto de evento contiene detalles de los eventos que ocurren durante una llamada a un método de la API o mientras el sistema está realizando una operación.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
detalles	Información adicional sobre el evento.	Objeto JSON
driveID	El identificador de la unidad que informa del fallo. 0 si no corresponde.	entero
ID de unidad	Una lista de los identificadores de las unidades que informan del fallo. Una lista vacía si no corresponde.	matriz de enteros
ID de evento	Identificador único asociado a cada evento.	entero
eventInfoType	El tipo de avería.	cadena
mensaje	Una breve descripción del evento ocurrido.	cadena
ID de nodo	El nodo ID del nodo que informa del fallo. 0 si no corresponde.	entero
ID de servicio	El ID del servicio que informa del fallo. 0 si no corresponde.	entero
gravedad	Gravedad del evento que se está reportando.	entero
horaDePublicación	La hora en que el registro de eventos del clúster recibió el evento, en formato UTC+0.	cadena de fecha ISO 8601
tiempoDelInforme	La hora en 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 ocurrió y no pudo publicarse inmediatamente.

Tipos de eventos

La siguiente lista describe los posibles tipos de eventos que puede contener el miembro eventInfoType:

- apiEvent: Eventos iniciados a través de la API o la interfaz de usuario web que modifican la configuración.

- binAssignmentsEvent: 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 las comprobaciones del servicio de bloqueo.
- bsKillEvent: Eventos relacionados con la finalización del servicio de bloqueo.
- bulkOpEvent: Eventos que operan en un volumen completo, como una copia de seguridad, restauración, instantánea o clonación de volumen.
- cloneEvent: Eventos relacionados con la clonación de volúmenes.
- clusterMasterEvent: Eventos de cambio de configuración del clúster, como agregar o eliminar nodos.
- dataEvent: Eventos relacionados con la lectura y escritura de datos.
- dbEvent: Eventos relacionados con la base de datos del nodo del conjunto.
- driveEvent: Eventos relacionados con las operaciones de conducción.
- 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 las conexiones de nodos de Fibre Channel.
- gcEvent: Eventos relacionados con la recolección de basura. Estos procesos se ejecutan cada 60 minutos para recuperar espacio de almacenamiento en las unidades de bloque.
- ieEvent: Eventos relacionados con errores internos del sistema.
- installEvent: Eventos relacionados con la instalación automática de software en nodos de almacenamiento pendientes.
- iSCSIEvent: Eventos relacionados con problemas de conexión o configuración de iSCSI.
- limitEvent: Eventos relacionados con el número de volúmenes o volúmenes virtuales en una cuenta o en el clúster que se acerca al máximo permitido.
- networkEvent: Eventos relacionados con redes virtuales.
- platformHardwareEvent: Eventos relacionados con problemas detectados en dispositivos de hardware.
- remoteClusterEvent: Eventos relacionados con el emparejamiento de clústeres remotos.
- schedulerEvent: Eventos relacionados con instantáneas 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 trampas SNMP.
- tsEvent: Eventos del servicio de transporte del sistema.
- unexpectedException: Eventos relacionados con errores inesperados.
- vasaProviderEvent: Eventos relacionados con un proveedor VASA de VMware.

Encuentra más información

[Lista de eventos](#)

falla

El objeto de fallo contiene información sobre los fallos detectados en el clúster. El `ListClusterFaults` El método devuelve información sobre fallos del clúster.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Actualizar bloques	El fallo impide la actualización. Valores posibles: • Verdadero: El fallo impide la actualización. • Falso: El fallo no impide una actualización.	booleano
clusterFaultID	El identificador único asociado a cada fallo del clúster.	entero
código	El código de error correspondiente al fallo específico detectado. Para obtener más detalles, consulte Códigos de falla del clúster.	cadena
data	Información adicional específica sobre la falla.	Objeto JSON
fecha	La hora actual en formato UTC+0.	Cadena ISO 8601
detalles	Descripción de la avería con detalles adicionales.	cadena
driveID	El primer identificador de unidad en la lista de identificadores de unidad. Si la lista driveIDs está vacía (lo que significa que no se devolvieron fallas relacionadas con las unidades), este valor es 0.	entero
ID de unidad	Una lista de valores driveID para las unidades a las que se refiere este fallo. Incluido para fallos relacionados con las unidades. Si no hay ninguno, se trata de una matriz vacía.	matriz de enteros

Nombre	Descripción	Tipo
nodoHardwareFaultID	El identificador asignado a una falla de hardware en el clúster.	entero
ID de nodo	El ID del nodo al que se refiere este fallo. Incluido para fallos de nodo y unidad, de lo contrario se establece en 0.	entero
resuelto	Estado resuelto de la avería. Valores posibles: • Verdadero: Ya no se detecta la falla. • Falso: La falla aún está presente.	booleano
fecha resuelta	Fecha y hora en que se solucionó la avería.	Cadena ISO 8601
ID de servicio	El servicio asociado a la avería. Este valor es "0" (cero) si la falla no está asociada con un servicio.	entero

Nombre	Descripción	Tipo
gravedad	La gravedad de la falla. Valores posibles: • Advertencia: Un problema menor. El clúster está funcionando y se permiten actualizaciones en este nivel de gravedad. • error: Un fallo que generalmente no debería afectar al servicio (excepto una posible degradación del rendimiento o pérdida de alta disponibilidad). Algunas funciones podrían estar desactivadas. • crítico: Una falla grave que está afectando el servicio. El sistema no puede atender las solicitudes de la API ni las operaciones de entrada/salida del cliente y corre el riesgo de sufrir pérdida de datos. • Buenas prácticas: Fallos provocados por una configuración del sistema subóptima.	cadena
tipo	El tipo de avería. Valores posibles: • nodo: Un fallo que afecta a todo un nodo. • unidad: Un fallo que afecta a una unidad individual. • clúster: Un fallo que afecta a todo el clúster. • servicio: Un fallo que afecta a un servicio del clúster. • volumen: Un fallo que afecta a un volumen individual.	cadena

Encuentra más información

- [ListClusterFaults](#)
- ["Códigos de falla del clúster"](#)

Puerto de canal de fibra

El objeto `fiberChannelPort` contiene información sobre puertos individuales en un nodo, o para un nodo completo en el clúster. Puedes recuperar esta información utilizando el `ListNodeFibreChannelPortInfo` método.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
firmware	La versión del firmware instalada en el puerto Fibre Channel.	entero
Puerto hba	El identificador del puerto del adaptador de bus de host (HBA) individual.	entero
modelo	Modelo del HBA en el puerto.	cadena
nPortID	El identificador único del nodo del puerto.	cadena
ranura PCI	La ranura que contiene la tarjeta PCI en el chasis del nodo Fibre Channel.	entero
de serie	El número de serie del puerto Fibre Channel.	cadena
velocidad	La velocidad del HBA en el puerto.	cadena

Nombre	Descripción	Tipo
estado	Valores posibles: • Desconocido • No presente • En línea • Sin conexión • Obstruido • Eludido • Diagnóstico • Enlace descendente • Error • Bucle de retorno • Eliminado	cadena
interruptorWwn	Nombre mundial del puerto del conmutador Fibre Channel.	cadena
wwnn	Nombre del nodo HBA a nivel mundial.	cadena
wwwpn	Nombre de puerto mundial asignado al puerto físico del HBA.	cadena

Encuentra más información

[Información del puerto del canal de fibra del nodo de lista](#)

Informe de nodo de error de fips

El objeto `fipsErrorNodeReport` contiene información de error para cada nodo que no responde con información sobre la compatibilidad con FIPS 140-2 cuando se le consulta con el `GetFipsReport` método.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de nodo	El ID del nodo que no respondió.	entero
error	Un objeto JSON que contiene información de error.	Objeto JSON

Informe de nodo fips

El objeto `fipsNodeReport` contiene información sobre la compatibilidad con FIPS 140-2 para un único nodo en el clúster de almacenamiento. Puedes recuperar esta información utilizando el `GetFipsReport` método.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de nodo	El ID del nodo que reporta la información.	entero
Unidades fips	Si el cifrado de unidad FIPS 140-2 está habilitado o no para este nodo. Valores posibles: • Ninguno: Este nodo no es capaz de realizar el cifrado de unidades FIPS. • Parcial: El nodo es capaz de realizar el cifrado de unidades FIPS, pero no todas las unidades presentes son compatibles con FIPS. • Listo: El nodo es capaz de realizar el cifrado de unidades FIPS y o bien todas las unidades presentes son compatibles con FIPS, o bien no hay ninguna unidad presente.	Tipo de estado de FipsDrives
httpsHabilitado	Si el cifrado HTTPS FIPS 140-2 está habilitado o no para este nodo. Valores posibles: • verdadero: habilitado • falso: deshabilitado	booleano

Informe fips

El objeto `fipsReport` contiene información sobre la compatibilidad con FIPS 140-2 para todos los nodos del clúster de almacenamiento. Puedes recuperar esta información utilizando el `GetFipsReport` método.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
nodos	Un informe sobre el estado de compatibilidad con FIPS 140-2 para cada nodo del clúster de almacenamiento.	Informe de nodo fips
nodos de error	Información de error para cada nodo que no respondió con el estado de soporte FIPS 140-2.	Informe de nodo de error de fips

Instantánea de grupo

El objeto groupSnapshot contiene información sobre una instantánea para un grupo de volúmenes. Puedes usar el `ListGroupSnapshots` Método API para recuperar información de instantáneas de grupo.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON
crearTiempo	Fecha y hora en formato UTC+0 en las que se creó la instantánea del grupo.	cadena de fecha ISO 8601
habilitar la replicación remota	Identifica si la instantánea está habilitada para la replicación remota.	booleano
ID de instantánea del grupo	El identificador único de la instantánea del grupo.	entero
ID de instantánea de grupo	El UUID de la instantánea del grupo.	cadena
miembros	Una matriz de objetos que contiene información sobre cada miembro de la instantánea del grupo.	instantánea información

Nombre	Descripción	Tipo
nombre	El nombre de la instantánea del grupo o, si no se proporcionó ninguna, la fecha y hora en formato UTC en que se creó la instantánea.	cadena de texto o cadena de fecha ISO 8601
estados remotos	Una matriz que contiene el identificador universal y el estado de replicación de cada instantánea remota en el clúster de destino, tal como se ve desde el clúster de origen.	Estado de instantánea del clúster remoto formación
estado	Estado actual de la instantánea. Valores posibles: • Desconocido: Se produjo un error al obtener el estado de la instantánea. • Preparando: Esta instantánea se está preparando para su uso y aún no se puede escribir en ella. • Sincronización remota: Esta instantánea se está replicando desde un clúster remoto. • Listo: Esta instantánea ha finalizado su preparación o replicación y ahora se puede utilizar. • Activa: Esta instantánea corresponde a la rama activa. • Clonación: Esta instantánea está involucrada en una operación CopyVolume.	cadena

Encuentra más información

[Lista de instantáneas de grupo](#)

Información de hardware

El objeto `hardwareInfo` contiene información detallada sobre el hardware y el estado de cada nodo del clúster. Puedes recuperar esta información con el `GetHardwareInfo` Método API.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Serie de la placa	El número de serie de la placa DMI.	cadena
autobús	Información del bus multimedia de la placa base.	Objeto JSON
chasisSerial	El número de serie del chasis.	cadena
Hardware de la unidad	Una lista de información para cada unidad en el nodo.	matriz de objetos JSON
Puertos de canal de fibra	Lista de puertos Fibre Channel en el nodo.	matriz de enteros
configuración de hardware	Información de configuración periférica de la placa base.	Objeto JSON
estado de volcado de memoria del kernel	La configuración del volcado de memoria del núcleo del sistema operativo.	cadena
memoria	Información sobre el firmware y el hardware de la memoria del sistema.	Objeto JSON
red	Descripción 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
nodoSlot	Para las plataformas HCI, la letra correspondiente a la ranura del chasis en la que se encuentra este nodo ("A", "B", "C" o "D"). Para las plataformas de almacenamiento, este valor es nulo.	cadena
NVRAM	Estadísticas NVRAM para el nodo.	Objeto JSON
origen	El proveedor de la placa base.	cadena

Nombre	Descripción	Tipo
plataforma	Descripción de la plataforma del chasis.	Objeto JSON
de serie	El número de serie del producto.	cadena
almacenamiento	Información del controlador de almacenamiento.	Objeto JSON
Memoria del sistema	Información sobre el uso de memoria y el rendimiento del sistema operativo.	Objeto JSON
sistema	El tipo de chasis del nodo.	Objeto JSON
UUID	El identificador único del nodo.	UUID

Encuentra más información

[Obtener información de hardware](#)

host (volúmenes virtuales)

El objeto host contiene información sobre un host de volumen virtual. Puedes usar el `ListVirtualVolumeHosts` Método para obtener esta información para todos los hosts de volúmenes virtuales.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
uniones	Una lista de objetos que describen los enlaces para el host del volumen virtual.	matriz de enteros
ID de clúster	El identificador único del clúster con el que está asociado este host.	UUID
Dirección del host	La dirección IP o el nombre DNS del host del volumen virtual.	cadena
nombres de iniciadores	Una lista de IQN iniciadores para el host de volumen virtual.	matriz de cadenas

Nombre	Descripción	Tipo
ID de host de volumen virtual	El identificador único de este host de volumen virtual.	UUID
IDs de punto final de protocolo visibles	Una lista de identificadores de los puntos finales del protocolo visibles en este host.	matriz UUID

Encuentra más información

[Listar hosts de volumen virtual](#)

idpConfigInfo

El objeto idpConfigInfo contiene detalles de configuración e integración relativos a un proveedor de identidad (IdP) de terceros.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
activado	Especifica si esta configuración de ID de terceros está habilitada.	booleano
idpConfigurationID	UUID para la configuración del IdP de terceros.	UUID
idpMetadata	Metadatos para detalles de configuración e integración para el inicio de sesión único SAML 2.0.	cadena
idpName	Nombre para recuperar el proveedor de identidad (IdP) para el inicio de sesión único SAML 2.0.	cadena
Certificado del proveedor de servicios	Un certificado X.509 PKCS#10 codificado en Base64 en formato PEM que se utilizará para la comunicación con este IdP.	cadena
spMetadataUrl	URL para recuperar los metadatos del proveedor de servicios (SP) del clúster para proporcionárselos al IdP para establecer una relación de confianza.	cadena

iniciador

El objeto iniciador contiene información sobre un iniciador iSCSI o Fibre Channel. Un objeto iniciador puede contener identificadores IQN o WWPN. Puedes usar 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 a través de grupos de acceso a volúmenes. Un iniciador solo puede ser miembro de un grupo de acceso a volumen a la vez. Puede restringir el acceso del iniciador a una o más VLAN especificando uno o más ID de red virtual mediante el `CreateInitiators` y `ModifyInitiators` métodos. Si no se especifica ninguna red virtual, el iniciador puede acceder a todas las redes.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
alias	El nombre de pila asignado al iniciador, si lo hubiere.	cadena
atributos	Un conjunto de atributos JSON asignados a este iniciador. Vacía si no se han asignado atributos.	Objeto JSON
chapNombre de usuario	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
iniciadorSecreto	La clave secreta CHAP utilizada para autenticar al iniciador.	cadena
requerirCapítulo	Verdadero si se requiere CHAP para este iniciador.	booleano
secreto del objetivo	El secreto CHAP utilizado para autenticar el objetivo (cuando se utiliza la autenticación CHAP mutua).	cadena

Nombre	Descripción	Tipo
IDs de red virtuales	La lista de identificadores de red virtual asociados a este iniciador. Si se define una o más redes virtuales, este iniciador solo podrá iniciar sesión en las redes virtuales especificadas. Si no se definen redes virtuales, este iniciador puede iniciar sesión en todas las redes.	entero
grupos de acceso de volumen	Una lista de los identificadores de grupo de acceso a volumen a los que pertenece este iniciador.	matriz de enteros

Encuentra más información

[Iniciadores de listas](#)

Autenticación iSCSI

El objeto `ISCSIAuthentication` contiene información de autenticación sobre una sesión iSCSI.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
método de autenticación	El método de autenticación utilizado durante el inicio de sesión de sesión iSCSI, por ejemplo, CHAP o Ninguno.	cadena
Algoritmo de capítulo	El algoritmo CHAP que se utiliza, por ejemplo, MD5, SHA1*, SHA-256* o SHA3-256*.	cadena
chapNombre de usuario	El nombre de usuario CHAP especificado por el iniciador durante un inicio de sesión de sesión iSCSI.	cadena
dirección	La dirección de la autenticación, por ejemplo, unidireccional (solo el iniciador) o bidireccional (tanto el iniciador como el destino).	cadena

- Disponible a partir del Elemento 12.7.

proveedor de clavesKmip

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 para su uso con funciones de clúster como el cifrado en reposo.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID del proveedor de clave	El identificador del proveedor de claves KMIP. Este es un valor único asignado por el clúster durante la creación del proveedor de claves que no se puede cambiar.	entero
<code>keyProviderIsActive</code>	Verdadero si el proveedor de claves KMIP está activo. Un proveedor se considera activo si existen claves pendientes que fueron creadas pero aún no eliminadas y, por lo tanto, se asume que todavía están en uso.	booleano
nombre del proveedor de clave	El nombre del proveedor de claves KMIP.	cadena
IDs de servidor de claves	Un identificador de servidor clave asociado a este proveedor. El servidor debe añadirse antes de que este proveedor pueda activarse. El servidor no se puede eliminar mientras este proveedor esté activo. Solo se admite un ID de servidor por proveedor.	matriz de enteros
Capacidades de kmip	Las capacidades de este proveedor de claves KMIP incluyen detalles sobre la biblioteca subyacente, el cumplimiento de FIPS, el proveedor SSL, etc.	cadena

servidor de clavesKmip

El objeto `keyServerKmip` describe un servidor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP), que es una ubicación para recuperar claves de autenticación para su uso con funciones de clúster como el cifrado en reposo.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID del proveedor de clave	Si este servidor de claves KMIP está asignado 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
ID del servidor de claves	El identificador del servidor de claves KMIP. Este es un valor único asignado por el clúster durante la creación del servidor de claves. Este valor no se puede cambiar.	entero
<code>kmipAssignedProviderIsActive</code>	Si este servidor de claves KMIP está asignado a un proveedor (<code>keyProviderID</code> no es nulo), este miembro indica si ese proveedor está activo (proporcionando claves que están actualmente en uso). De lo contrario, este miembro es nulo.	booleano
Certificado <code>kmipCa</code>	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 clave donde los servidores individuales utilizan diferentes CA, este miembro contiene una cadena concatenada de los certificados raíz de todas las CA.	cadena
Certificado de cliente <code>kmip</code>	Un certificado X.509 PKCS#10 codificado en Base64 en formato PEM utilizado por el cliente KMIP de almacenamiento Element.	cadena

Nombre	Descripción	Tipo
Nombres de host del servidor de claves kmip	Los nombres de host o direcciones IP asociados con este servidor de claves KMIP.	matriz de cadenas
kmipKeyServerName	El nombre del servidor de claves KMIP. Este nombre se utiliza únicamente con fines ilustrativos y no necesita ser único.	cadena
kmipKeyServerPort	El número de puerto asociado con este servidor de claves KMIP (normalmente 5696).	entero

Configuración LDAP

El objeto `LdapConfiguration` contiene información sobre la configuración LDAP en el sistema de almacenamiento. Puedes recuperar información LDAP con el `GetLdapConfiguration` Método API.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
tipo de autenticación	Identifica qué método de autenticación de usuario se debe utilizar. Valores posibles: • DirectBind • Buscar y enlazar	cadena
activado	Identifica si el sistema está configurado o no para LDAP. Valores posibles: • verdadero • FALSO	booleano
groupSearchBaseDN	El DN base del árbol para iniciar la búsqueda de grupo (el sistema realizará una búsqueda de subárbol desde aquí).	cadena
groupSearchCustomFilter	El filtro de búsqueda personalizado utilizado.	cadena

Nombre	Descripción	Tipo
tipo de búsqueda de grupo	Controla el filtro de búsqueda de grupo predeterminado utilizado. Valores posibles: • NoGroups: No hay soporte para grupos. • Active Directory: Membresía anidada de todos los grupos de AD de un usuario. • MemberDN: Grupos de estilo MemberDN (de un solo nivel).	cadena
searchBindDN	Un DN completo para iniciar sesión y realizar una búsqueda LDAP del usuario (necesita acceso de lectura al directorio LDAP).	cadena
URI del servidor	Una lista de URI de servidores LDAP separadas por comas (por ejemplo, ldap://1.2.3.4 y ldaps://1.2.3.4:123.)	cadena
plantilla de DN de usuario	Una cadena que se utiliza para formar un DN de usuario completo.	cadena
userSearchBaseDN	El DN base del árbol utilizado para iniciar la búsqueda (desde aquí se realizará una búsqueda en un subárbol).	cadena
filtro de búsqueda de usuarios	El filtro LDAP utilizado.	cadena

Encuentra más información

[Obtener configuración LDAP](#)

servidor de registro

El objeto `loggingServer` contiene información sobre cualquier host de registro configurado para el clúster de almacenamiento. Puedes usar `GetRemoteLoggingHosts` para determinar cuáles son los hosts de registro actuales y luego usar `SetRemoteLoggingHosts` para establecer la lista deseada de hosts de registro actuales y nuevos.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
anfitrión	Dirección IP del servidor de registro.	cadena
puerto	Número de puerto utilizado para comunicarse con el servidor de registro.	entero

red (interfaces enlazadas)

El objeto de red (interfaces enlazadas) contiene información de configuración para las interfaces de red enlazadas en un nodo de almacenamiento. Puedes usar el `GetConfig` y `GetNetworkConfig` Métodos para obtener esta información para un nodo de almacenamiento.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
DIRECCIÓN	La dirección IPv4 asignada a esta interfaz en el nodo.	cadena
addressV6	La dirección de gestión IPv6 asignada a la interfaz Bond1G en el nodo.	cadena
retraso en la bajada de bonos	Tiempo de espera, en milisegundos, antes de deshabilitar un esclavo después de que se haya 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, con la que se inspecciona el estado del enlace MII para detectar fallos en el enlace.	cadena

modo de enlace	El modo de unión. Valores posibles: • ActivoPasivo (Predeterminado) • ALBA • LACP (Recomendado)	cadena
reselección de bono primario	Especifica cuándo se elige al esclavo de enlace primario como esclavo activo. Valores posibles: • Siempre • Mejor • Falla	cadena
esclavos	La lista de interfaces esclavas para el enlace.	cadena
tasa de lap de bonos	Cuando el modo de enlace es LACP, la tasa puede cambiar a una de las siguientes: • LACP Rápido (Predeterminado) • LACP lento	cadena
retraso de fianza	El tiempo, en milisegundos, que se debe esperar antes de habilitar un esclavo después de que se detecte un enlace.	cadena
servidores de nombres dns	Una lista de direcciones utilizadas para los servicios de nombres de dominio, separadas por comas o espacios.	cadena
búsqueda de DNS	Una lista de dominios de búsqueda DNS separados por espacios o comas.	cadena
familia	Familia de direcciones que la interfaz está configurada para usar. Actualmente se admite "inet" para IPv4.	cadena
puerta	La dirección de red del router 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 local Bond1G.	cadena
ipV6PrefixLength	Longitud del prefijo de subred para rutas estáticas de tipo "net" para tráfico IPv6 en la red Bond1G.	cadena
dirección MAC	La dirección MAC real asignada a la interfaz y observada por la red.	cadena
Dirección MAC permanente	La dirección MAC inmutable asignada por el fabricante a la interfaz.	cadena
método	El método utilizado para configurar la interfaz. Valores posibles: • Loopback: Se utiliza para definir la interfaz de loopback IPv4. • manual: Se utiliza para definir interfaces que no se configuran automáticamente. • dhcp: Se puede utilizar para obtener una dirección IP mediante DHCP. • estático: Se utiliza para definir interfaces Ethernet con direcciones IPv4 asignadas estáticamente.	cadena
mtu	El tamaño máximo de paquete (en bytes) que la interfaz puede transmitir. Debe ser mayor o igual a 1500; se admite hasta 9000.	cadena
máscara de red	La máscara de bits que especifica la subred para la interfaz.	cadena
red	Indica dónde comienza el rango de direcciones IP en función de la máscara de red.	cadena
rutas	Matriz de cadenas de ruta separadas por comas para aplicar a la tabla de enrutamiento.	matriz de cadenas

estado	El estado de la interfaz. Valores posibles: • Abajo: La interfaz está inactiva. • Arriba: La interfaz está lista, pero no tiene enlace. • En funcionamiento: La interfaz está lista y se ha establecido una conexión.	cadena
Reglas de ruta simétricas	Las reglas de enrutamiento simétrico configuradas en el nodo.	matriz de cadenas
En funcionamiento	Indica si la interfaz está lista y tiene un enlace.	booleano
etiqueta de red virtual	El identificador de red virtual de la interfaz (etiqueta VLAN).	cadena

Modificabilidad de los miembros y estados de los nodos

Esta tabla indica si los parámetros del objeto pueden modificarse o no en cada estado posible del nodo.

Nombre del miembro	Estado disponible	Estado pendiente	Estado activo
DIRECCIÓN	Sí	Sí	No
addressV6	Sí	Sí	No
retraso en la bajada de bonos	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
modo de enlace	Sí	Sí	Sí
reselección de bono primario	Configurado por el sistema	N/A	N/A
esclavos	Configurado por el sistema	N/A	N/A
tasa de lap de bonos	Sí	Sí	Sí

retraso de fianza	Configurado por el sistema	N/A	N/A
servidores de nombres dns	Sí	Sí	Sí
búsqueda de DNS	Sí	Sí	Sí
familia	No	No	No
puerta	Sí	Sí	Sí
gatewayV6	Sí	Sí	Sí
ipV6PrefixLength	Sí	Sí	Sí
dirección MAC	Configurado por el sistema	N/A	N/A
Dirección MAC permanente	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
Reglas de ruta simétricas	Configurado por el sistema	N/A	N/A
En funcionamiento	Configurado por el sistema	N/A	N/A
etiqueta de red virtual	Sí	Sí	Sí

Encuentra más información

- [Obtener configuración](#)
- [Obtener configuración de red](#)

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. Puedes usar el `GetConfig` y `GetNetworkConfig` Métodos para obtener esta información para un nodo de almacenamiento.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Bond10G	Información de configuración para la interfaz enlazada Bond10G.	red (interfaces enlazadas)
Bond1G	Información de configuración para la interfaz de enlace Bond1G.	red (interfaces enlazadas)
eth0-5	Un objeto para cada interfaz Ethernet en el nodo de almacenamiento, que 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 para la interfaz de bucle invertido.	red (interfaces locales)

Encuentra más información

- [Obtener configuración](#)
- [Obtener configuración de red](#)

red (interfaces Ethernet)

El objeto de red (interfaces Ethernet) contiene información de configuración para interfaces Ethernet individuales. Puedes usar el `GetConfig` y `GetNetworkConfig` Métodos para obtener esta información para un nodo de almacenamiento.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo

maestro de fianzas	Especifica a qué interfaz vinculada se ha unido esta interfaz física como esclava vinculada.	cadena
familia	Familia de direcciones que la interfaz está configurada para usar. Actualmente se admite "inet" para IPv4.	cadena
dirección MAC	La dirección MAC real asignada a la interfaz y observada por la red.	cadena
Dirección MAC permanente	La dirección MAC inmutable asignada por el fabricante a la interfaz.	cadena
método	El método utilizado para configurar la interfaz. Valores posibles: • loopback: Se utiliza para definir la interfaz loopback IPv4. • manual: Se utiliza para definir interfaces que no se configuran automáticamente. • dhcp: Se puede utilizar para obtener una dirección IP mediante DHCP. • estático: Se utiliza para definir interfaces Ethernet con direcciones IPv4 asignadas estáticamente.	cadena
estado	El estado de la interfaz. Valores posibles: • Abajo: La interfaz está inactiva. • Arriba: La interfaz está lista, pero no tiene enlace. • En funcionamiento: La interfaz está lista y se ha establecido una conexión.	cadena
En funcionamiento	Indica si la interfaz está lista y tiene un enlace.	booleano

Modificabilidad de los miembros y estados de los nodos

Esta tabla indica si los parámetros del objeto pueden modificarse o no en cada estado posible del nodo.

Nombre del parámetro	Estado disponible	Estado pendiente	Estado activo
maestro de fianzas	No	No	No
familia	No	No	No
dirección MAC	Configurado por el sistema	N/A	N/A
Dirección MAC permanente	Configurado por el sistema	N/A	N/A
método	No	No	No
estado	Sí	Sí	Sí
En funcionamiento	Configurado por el sistema	N/A	N/A

Encuentra más información

- [Obtener configuración](#)
- [Obtener configuración de red](#)

red (interfaces locales)

El objeto de red (interfaces locales) contiene información de configuración para las interfaces de red locales, como la interfaz de bucle invertido, en un nodo de almacenamiento. Puedes usar el `GetConfig` y `GetNetworkConfig` Métodos para obtener esta información para un nodo de almacenamiento.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
familia	Familia de direcciones que la interfaz está configurada para usar. Actualmente se admite "inet" para IPv4.	cadena
dirección MAC	La dirección MAC real asignada a la interfaz y observada por la red.	cadena
Dirección MAC permanente	La dirección MAC inmutable asignada por el fabricante a la interfaz.	cadena

método	El método utilizado para configurar la interfaz. Valores posibles: • loopback: Se utiliza para definir la interfaz loopback IPv4. • manual: Se utiliza para definir interfaces que no se configuran automáticamente. • dhcp: Se puede utilizar para obtener una dirección IP mediante DHCP. • estático: Se utiliza para definir interfaces Ethernet con direcciones IPv4 asignadas estáticamente.	cadena
estado	El estado de la interfaz. Valores posibles: • Abajo: La interfaz está inactiva. • Arriba: La interfaz está lista, pero no tiene enlace. • En funcionamiento: La interfaz está lista y se ha establecido una conexión.	cadena
En funcionamiento	Indica si la interfaz está lista y tiene un enlace.	booleano

Modificabilidad de los miembros y estados de los nodos

Esta tabla indica si los parámetros del objeto pueden modificarse o no en cada estado posible del nodo.

Nombre del parámetro	Estado disponible	Estado pendiente	Estado activo
familia	No	No	No
dirección MAC	Configurado por el sistema	N/A	N/A
Dirección MAC permanente	Configurado por el sistema	N/A	N/A
método	No	No	No
estado	Sí	Sí	Sí

En funcionamiento	Configurado por el sistema	N/A	N/A

Encuentra más información

- [Obtener configuración](#)
- [Obtener configuración de red](#)

red (SNMP)

El objeto de red SNMP contiene información sobre la configuración SNMP v3 para los nodos del clúster.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
acceso	El tipo de acceso permitido para las solicitudes de información SNMP. Valores posibles: • ro: Acceso de solo lectura. • rw: Acceso de lectura y escritura. • rosys: Acceso de solo lectura a un conjunto restringido de información del sistema.	cadena
sidra	Máscara de red CIDR. Esta máscara de red debe ser un número entero mayor o igual que 0 y menor o igual que 32. Tampoco debe ser igual a 31.	entero
comunidad	La cadena de comunidad SNMP.	cadena
red	Este miembro, junto con el miembro CIDR, controla a qué red se aplican la cadena de 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 "default".	cadena

Encuentra más información

[Obtener información SNMP](#)

Interfaz de red

El objeto `networkInterface` contiene información de configuración para interfaces de red individuales en un nodo de almacenamiento.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
DIRECCIÓN	La dirección de gestión IPv4 de la interfaz.	cadena
addressV6	La dirección de gestión IPv6 de la interfaz.	cadena
transmisión	La dirección de difusión de la interfaz.	cadena
dirección MAC	La dirección MAC de la interfaz.	cadena
mtu	La Unidad Máxima de Transferencia, en bytes, de la interfaz.	entero
nombre	El nombre de la interfaz.	cadena
espacio de nombres	Independientemente de si a esta interfaz se le asigna o no un espacio de nombres de red virtual.	booleano
máscara de red	La máscara de subred de la interfaz.	cadena
estado	Estado operativo de la interfaz.	cadena
tipo	El tipo de interfaz (maestro de enlace, esclavo de enlace, etc.).	cadena
etiqueta de red virtual	El ID de VLAN asignado a la interfaz en la red virtual.	entero

Estadísticas de interfaz de red

El objeto `networkInterfaceStats` contiene estadísticas de red, el número total de paquetes transmitidos y recibidos, e información de errores para interfaces de red individuales en un nodo de almacenamiento. Puedes usar el `ListNetworkInterfaceStats` Método API para listar esta información para las interfaces de red en un nodo de almacenamiento.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
colisiones	Número de colisiones detectadas.	entero
nombre	Nombre de la interfaz de red.	cadena
rxBytes	El número total de bytes recibidos.	entero
rxCrcErrors	Número de paquetes recibidos que presentaban un error CRC.	entero
rxDropped	Número de paquetes recibidos que fueron descartados.	entero
Errores de recepción	Número de paquetes defectuosos o malformados recibidos.	entero
rxFifoErrores	Número de errores de desbordamiento FIFO en los datos recibidos.	entero
rxFrameErrors	Número de paquetes recibidos con errores de alineación de trama.	entero
rxLengthErrors	Número de paquetes recibidos con un error de longitud.	entero
rxMissedErrors	Número de paquetes que el receptor no logró entregar.	entero
rxOverErrors	Número de errores de desbordamiento del búfer de anillo del receptor para esta interfaz.	entero
Paquetes rx	El número total de paquetes recibidos.	entero
txBytes	El número total de bytes transmitidos.	entero
Errores de portadora de transmisión	Número de errores de portadora en el lado de transmisión.	entero
Errores de transacción	El número de errores de transmisión de paquetes.	entero

Nombre	Descripción	Tipo
txFifoErrores	Número de errores de desbordamiento FIFO en el lado de transmisión.	entero
Paquetes de transmisión	El número total de paquetes transmitidos.	entero

nodo

El objeto nodo contiene información sobre cada nodo del clúster. Puedes recuperar esta información utilizando el `ListActiveNodes` y `ListAllNodes` métodos.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de servicio asociado	El ID del servicio Fibre Channel para el nodo. "0" si el nodo no es un nodo Fibre Channel.	entero
ID de servicio maestro asociado	ID de servicio maestro para el nodo.	entero
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON
nombre del chasis	Identifica de forma única un chasis; idéntico para todos los nodos en un mismo chasis.	cadena
cip	La dirección IP del clúster asignada al nodo.	cadena
cipi	Interfaz de red utilizada para la comunicación del clúster.	cadena
nombre de dominio de protección personalizado	Identifica de forma única un dominio de protección personalizado. Este nombre es idéntico para todos los nodos de almacenamiento dentro de todos los chasis en un dominio de protección personalizado determinado.	cadena

Nombre	Descripción	Tipo
Grupo de puertos de destino de canal de fibra	El grupo objetivo asociado a este nodo. "nulo" si el nodo no es un nodo Fibre Channel.	entero
Modo de mantenimiento	Indica en qué modo se encuentra un nodo para su 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	Nombre de host del nodo.	cadena
ID de nodo	NodeID para este nodo.	entero
nodoSlot	Para las plataformas HCI, la letra correspondiente a la ranura del chasis en la que se encuentra este nodo ("A", "B", "C" o "D"). Para las plataformas de almacenamiento, este valor es nulo.	cadena
Información de la plataforma	Información de hardware del nodo. Miembros: • Tipo de chasis: La plataforma de hardware del nodo. • cpuModel: El modelo de CPU de la plataforma de hardware. • nodeMemoryGB: Cantidad de memoria instalada en la plataforma física en GB. • nodeType: El nombre del modelo de nodo. • platformConfigVersion: La versión del software configurada para el hardware de este nodo.	Objeto JSON

Nombre	Descripción	Tipo
role	El rol del nodo en el clúster. Valores posibles: • Gestión • Almacenamiento • Calcular • Testigo	
sorbo	La dirección IP de almacenamiento asignada al nodo.	cadena
sipi	La interfaz de red utilizada para el tráfico de almacenamiento.	cadena
Versión del software	Devuelve la versión actual del software Element que se ejecuta en el nodo.	cadena
UUID	El identificador único universal asociado a este nodo.	cadena
redes virtuales	Objeto que contiene direcciones IP e identificadores de red virtual.	red virtual formación

Encuentra más información

- [Lista de nodos activos](#)
- [Lista todos los nodos](#)

Dominios de protección de nodos

El objeto nodeProtectionDomains contiene información sobre la identidad de un nodo y los dominios de protección asociados a ese nodo.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de nodo	Identificador único del nodo.	entero
dominios de protección	Lista de dominios de protección a los que pertenece el nodo.	"dominio de protección"

estadísticas del nodo

El objeto `nodeStats` contiene mediciones de actividad de alto nivel para un nodo. Puedes usar el `getNodeStats` y `ListNodeStats` Métodos de la API para obtener algunos o todos los objetos `nodeStats`.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
contar	El número total de muestras en el objeto <code>nodeStats</code> .	entero
UPC	Uso de CPU, en %.	entero
CPU total	Valor de utilización de la CPU que aumenta de forma monótona.	entero
cBytesEn	Bytes de entrada en la interfaz del clúster.	entero
cBytesOut	Salida de bytes en la interfaz del clúster.	entero
sBytesEn	Bytes de entrada en la interfaz de almacenamiento.	entero
sBytesOut	Bytes de salida en la interfaz de almacenamiento.	entero
mBytesEn	Bytes de entrada en la interfaz de gestión.	entero
mBytesOut	Salida de bytes en la interfaz de gestión.	entero
Clúster de utilización de red	Utilización de la interfaz de red (en %) para la interfaz de red del clúster.	entero
Utilización de la red Almacenamiento	Utilización de la interfaz de red (en %) para la interfaz de red de almacenamiento.	entero

Nombre	Descripción	Tipo
nodoCalor	Información sobre la utilización del nodo. Disponible a partir del Elemento 12.8. Miembros: • primaryTotalHeat: IOPS totales del nodo primario / IOPS configuradas del nodo, promediadas durante 24 horas • recentPrimaryTotalHeat: IOPS totales del nodo primario / IOPS configuradas del nodo, promediadas durante una hora. • recentTotalHeat: IOPS totales del nodo / IOPS configuradas del nodo, promedio durante una hora. • totalHeat: IOPS totales del nodo / IOPS configuradas del nodo, promedio durante 24 horas	Objeto JSON
Latencia de lectura (Usec) Total	Valor creciente de forma monótona del tiempo total empleado en realizar operaciones de lectura en el nodo.	entero
operaciones de lectura	Valor creciente de forma monótona del total de operaciones de lectura en un nodo.	entero
ssLoadHistogram	Datos del histograma que ilustran la carga del servicio de segmentación a lo largo del tiempo.	Objeto JSON
marca de tiempo	La hora actual en formato UTC+0.	cadena de fecha ISO 8601
memoria utilizada	Uso total de memoria en bytes.	entero
Latencia de escritura (Usec) total	Valor creciente de forma monótona del tiempo total empleado en realizar operaciones de escritura en el nodo.	entero
operaciones de escritura	Valor creciente de forma monótona del total de operaciones de escritura en un nodo.	entero

Encuentra más información

- [Obtener estadísticas del nodo](#)
- [Estadísticas de nodo de lista](#)

ontapVersionInfo

El objeto `ontapVersionInfo` contiene información sobre la versión de la API del clúster ONTAP en una relación `SnapMirror`. La interfaz web de Element utiliza `GetOntapVersionInfo` Método API para obtener esta información.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de punto final de <code>SnapMirror</code>	El identificador del sistema ONTAP de destino.	entero
<code>clienteAPIMajorVersión</code>	La versión principal de la API de ONTAP que utiliza el cliente de la API de Element.	cadena
<code>clientAPIMinorVesion</code>	La versión menor de la API de ONTAP que utiliza el cliente de la API de Element.	cadena
<code>ontapAPIMajorVersion</code>	La versión principal actual de la API compatible con el sistema ONTAP.	cadena
<code>ontapAPIMinorVesion</code>	La versión menor actual de la API compatible con el sistema ONTAP.	cadena
<code>ontapVersion</code>	La versión actual del software que se ejecuta en el clúster ONTAP.	cadena

nodo activo pendiente

El objeto `pendingActiveNode` contiene información sobre un nodo que actualmente se encuentra en el estado `pendingActive`, entre los estados pendiente y activo. Estos son nodos que actualmente se están devolviendo a la imagen de software de fábrica. Utilice el `ListPendingActiveNodes` Método API para devolver una lista de esta información para todos los nodos `pendingActive`.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
clave de nodo activo	Una clave única que permite que el nodo se una al clúster automáticamente después de una instalación exitosa del software.	cadena
ID de nodo asignado	El ID de nodo asignado al nodo.	cadena
manejador asíncrono	El identificador del 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
nodoSlot	Para las plataformas HCI, la letra correspondiente a la ranura del chasis en la que se encuentra este nodo ("A", "B", "C" o "D"). Para las plataformas de almacenamiento, este valor es nulo.	cadena
ID de nodo activo pendiente	El ID del nodo pendiente.	entero
Información de la plataforma	Información de hardware del nodo. Miembros: • Tipo de chasis: La plataforma de hardware del nodo. • cpuModel: El modelo de CPU de la plataforma de hardware. • nodeMemoryGB: Cantidad de memoria instalada en la plataforma física en GB. • nodeType: El nombre del modelo de nodo. • platformConfigVersion: La versión del software configurada para el hardware de este nodo.	Objeto JSON

Nombre	Descripción	Tipo
role	El rol del nodo en el clúster. Valores posibles: • Gestión • Almacenamiento • Calcular • Testigo	
sorbo	La dirección IP de almacenamiento (iSCSI) asignada al nodo.	cadena
Versión del software	La versión actual del software Element que se ejecuta en el nodo.	cadena

Encuentra más información

[Lista de nodos activos pendientes](#)

nodo pendiente

El objeto `pendingNode` contiene información sobre un nodo que se puede agregar a un clúster. Utilice el `ListPendingNodes` Método API para devolver una lista de esta información para todos los nodos pendientes. Puedes agregar cualquiera de los nodos enumerados a un clúster usando el `AddNodes` Método API.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
cipi	La dirección IP del clúster asignada al nodo.	cadena
clave de nodo activo	Una clave única que permite que el nodo se una al clúster automáticamente después de una instalación exitosa del software.	cadena
ID de nodo asignado	El ID de nodo asignado al nodo.	cadena
manejador asíncrono	El identificador del método asíncrono que puede utilizar para consultar el estado de la operación.	entero

Nombre	Descripción	Tipo
nombre del chasis	Identifica de forma única un chasis; idéntico para todos los nodos en un mismo chasis.	cadena
cip	La dirección IP del clúster asignada al nodo.	cadena
mip	La dirección IP de gestión asignada al nodo.	cadena
nodoSlot	Para las plataformas HCI, la letra correspondiente a la ranura del chasis en la que se encuentra este nodo ("A", "B", "C" o "D"). Para las plataformas de almacenamiento, este valor es nulo.	cadena
ID de nodo activo pendiente	El ID del nodo pendiente.	entero
Información de la plataforma	Información de hardware del nodo. Miembros: • Tipo de chasis: La plataforma de hardware del nodo. • cpuModel: El modelo de CPU de la plataforma de hardware. • nodeMemoryGB: Cantidad de memoria instalada en la plataforma física en GB. • nodeType: El nombre del modelo de nodo. • platformConfigVersion: La versión del software configurada para el hardware de este nodo.	Objeto JSON
role	El rol del nodo en el clúster. Valores posibles: • Gestión • Almacenamiento • Calcular • Testigo	

Nombre	Descripción	Tipo
sorbo	La dirección IP de almacenamiento (iSCSI) asignada al nodo.	cadena
Versión del software	La versión actual del software Element que se ejecuta en el nodo.	cadena

Encuentra más información

- [Agregar nodos](#)
- [Lista de nodos pendientes](#)

dominio de protección

El objeto protectionDomain contiene el nombre y los detalles del tipo de un dominio de protección.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
nombre de dominio de protección	El nombre del dominio de protección.	cadena
Tipo de dominio de protección	El tipo de dominio de protección. Valores posibles: • Chasis: Todos los nodos de almacenamiento en un único chasis. • personalizado: Todos los nodos de almacenamiento en un único dominio de protección definido por el cliente.	cadena

Nivel de dominio de protección

El objeto protectionDomainLevel contiene información sobre los niveles actuales de tolerancia y resiliencia del clúster de almacenamiento. Los niveles de tolerancia indican la capacidad del clúster para continuar leyendo y escribiendo datos en caso de una falla, y los niveles de resiliencia indican la capacidad del clúster para recuperarse automáticamente de una o más fallas dentro de su dominio de protección asociado.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Tipo de dominio de protección	El tipo de dominio de protección que presenta la tolerancia y la resiliencia asociadas. Valores posibles: • nodo: Cualquier nodo individual. • chasis: Cualquier nodo individual o todos los nodos de almacenamiento en un solo chasis. • personalizado: Todos los nodos de almacenamiento en un único dominio de protección definido por el cliente.	cadena
resistencia	La resiliencia actual de este grupo desde la perspectiva de este tipo de dominio de protección.	Resiliencia del dominio de protección
tolerancia	La tolerancia actual de este clúster desde la perspectiva de este tipo de dominio de protección.	protecciónDominioTolerancia

Resiliencia del dominio de protección

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 una o más fallas dentro de un único dominio de protección de su tipo de dominio de protección asociado. Se considera que un clúster de almacenamiento se ha recuperado cuando puede seguir leyendo y escribiendo datos a pesar del fallo de cualquier nodo de almacenamiento individual (un estado conocido como tolerancia de nodo).

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Resiliencias del esquema de protección	Una lista de objetos (uno por cada esquema de protección) que contiene información sobre la resiliencia ante fallos para el tipo de dominio de protección asociado.	Resiliencia del esquema de protección formación
singleFailureThresholdBytesForBlockData	El número máximo de bytes que se pueden almacenar en el clúster de almacenamiento antes de perder la capacidad de recuperarse automáticamente a un estado de tolerancia del nodo.	entero
Fracasos sostenibles para el conjunto	El número previsto de fallos simultáneos que pueden ocurrir sin perder la capacidad de recuperarse automáticamente hasta alcanzar un estado de tolerancia de nodos para el quórum del conjunto.	entero

protecciónDominioTolerancia

El objeto `protectionDomainTolerance` contiene información sobre la capacidad del clúster de almacenamiento para continuar leyendo y escribiendo datos en caso de una o más fallas dentro de un único dominio de protección de su tipo de dominio de protección asociado.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Tolerancias del esquema de protección	Una lista de objetos (uno por cada esquema de protección) que contiene información sobre la tolerancia a fallos para el tipo de dominio de protección asociado.	Tolerancia del esquema de protección formación
Fracasos sostenibles para el conjunto	El número de fallos simultáneos dentro del dominio de protección de tipo asociado que pueden ocurrir sin perder el quórum del conjunto.	entero

Resiliencia del esquema de protección

El objeto `protectionSchemeResiliency` contiene información sobre si un clúster de almacenamiento, para un esquema de protección específico, puede recuperarse automáticamente de una o más fallas dentro de su `protectionDomainType` asociado. Se considera que un clúster de almacenamiento se ha recuperado cuando puede seguir leyendo y escribiendo datos a pesar del fallo de cualquier nodo de almacenamiento individual (un estado conocido como tolerancia de nodo).

miembros del 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 <code>doubleHelix</code> .	cadena
Fracasos sostenibles para BlockData	El número previsto de fallos simultáneos que pueden ocurrir sin perder la capacidad de recuperarse automáticamente hasta alcanzar un estado de tolerancia de nodos para los datos.	entero
fallos sostenibles para los metadatos	El número previsto de fallos simultáneos que pueden ocurrir sin perder la capacidad de recuperarse automáticamente hasta un estado de tolerancia del nodo para los metadatos.	entero

Tolerancia del esquema de protección

El objeto `protectionSchemeTolerance` contiene información sobre si un clúster de almacenamiento, para un esquema de protección específico, puede continuar leyendo y escribiendo datos después de fallos.

miembros del 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
Fracasos sostenibles para BlockData	El número actual de fallos simultáneos que pueden producirse sin perder la disponibilidad de datos de bloque para el esquema de protección asociado.	entero
fallos sostenibles para los metadatos	El número actual de fallos simultáneos que pueden producirse sin perder la disponibilidad de metadatos para el esquema de protección asociado.	entero

punto final del protocolo

El objeto `protocolEndpoint` contiene los atributos de un punto final de protocolo. Puede recuperar esta información para todos los puntos finales del protocolo en el clúster utilizando `ListProtocolEndpoints` Método API.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de proveedor principal	El ID del objeto proveedor del punto final del protocolo principal para el punto final del protocolo.	entero
ID de punto final del protocolo	El identificador único del punto final del protocolo.	UUID

Nombre	Descripción	Tipo
estado del punto final del protocolo	Estado del punto final del protocolo. Valores posibles: • Activo: El punto final del protocolo está en uso. • Inicio: El punto final del protocolo se está iniciando. • Conmutación por error: El extremo del protocolo ha conmutado por error. • Reservado: El punto final del protocolo está reservado.	cadena
Tipo de proveedor	El tipo de proveedor del punto final del protocolo. Valores posibles: • Primario • Secundario	cadena
scsiNAADeviceID	El identificador de dispositivo SCSI único a nivel mundial para el punto final del protocolo en formato extendido registrado IEEE NAA.	cadena
ID de proveedor secundario	El ID del objeto proveedor del punto final del protocolo secundario para el punto final del protocolo.	entero

Encuentra más información

[ListProtocolEndpoints](#)

Calidad de servicio

El objeto QoS contiene información sobre la configuración de Calidad de Servicio (QoS) para los volúmenes. Los volúmenes creados sin valores QoS especificados se crean utilizando los valores predeterminados. Puedes encontrar los valores predeterminados usando el `GetDefaultQoS` método.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ráfaga IOPS	Se permite un máximo de IOPS de 4 KB durante períodos cortos de tiempo. Permite ráfagas de actividad de E/S por encima del valor maxIOPS normal.	entero
tiempo de ráfaga	Duración permitida de burstIOPS. El valor devuelto se representa en segundos. Este valor lo calcula el sistema en función de las IOPS establecidas para QoS.	entero
curva	La curva es un conjunto de pares clave-valor. Las claves son tamaños de E/S en bytes. Los valores representan el costo de realizar una IOP con un tamaño I/O específico. La curva se calcula en relación con una operación de 4096 bytes configurada a 100 IOPS.	Objeto JSON
IOPS máximas	El máximo deseado de IOPS de 4 KB permitido durante un período de tiempo prolongado.	entero
minIOPS	Se requiere un mínimo de 4 KB de IOPS para garantizarlo. El número de IOPS permitidas solo descenderá por debajo de este nivel si todos los volúmenes han alcanzado su valor mínimo de IOPS y aún existe una capacidad de rendimiento insuficiente.	entero

Encuentra más información

[Obtener QoS predeterminado](#)

Política de QoS

El objeto QoSPolicy contiene información sobre una política QoS en un clúster de almacenamiento que ejecuta el software Element.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de política de qos	Un identificador entero único para la QoSPolicy asignado automáticamente por el clúster de almacenamiento.	entero
nombre	El nombre de la política de QoS. Por ejemplo: oro, platino o plata.	cadena
QoS	La configuración de QoS que representa esta política.	Calidad de servicio
IDs de volumen	Lista de volúmenes asociados a esta póliza.	matriz de enteros

Encuentra más información

[Obtener política de QoS](#)

Estado de instantánea del clúster remoto

El `remoteClusterSnapshotStatus` El objeto contiene el UUID y el estado de una instantánea almacenada en un clúster de almacenamiento remoto. Puedes obtener esta información con el `ListSnapshots` o `ListGroupSnapshots` Métodos de la API.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
estado remoto	Estado de replicación de la instantánea remota en el clúster de destino, tal como se ve desde el clúster de origen. Valores posibles: • Presente: La instantánea existe en un clúster remoto. • NotPresent: La instantánea no existe en un clúster remoto. • Sincronizando: Este es un clúster de destino y actualmente está replicando la instantánea. • Eliminado: Este es un clúster de destino. La instantánea se ha eliminado, pero aún existe en la fuente.	cadena

Nombre	Descripción	Tipo
volumenPairUUID	El identificador universal del par de volúmenes.	UUID

cronograma

El objeto de programación contiene información sobre una programación creada para realizar de forma autónoma una instantánea de un volumen. Puedes recuperar información de horarios para todos los horarios con el `ListSchedules` Método API.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	Indica la frecuencia con la que se produce el evento programado. Valores posibles: • Día de la semana • Día del mes • Intervalo de tiempo	Objeto JSON
tieneError	Indica si el cronograma tiene errores o no. Valores posibles: • verdadero • FALSO	booleano
horas	Muestra las horas que transcurrirán antes de que se cree la siguiente instantánea. Los valores posibles son de 0 a 24.	entero
último estado de ejecución	Indica el estado de la última instantánea programada. Valores posibles: • Éxito • Con errores	cadena
último tiempo de ejecución	Indica la última hora de inicio del horario.	cadena de fecha ISO 8601

Nombre	Descripción	Tipo
minutos	Muestra los minutos que transcurrirán antes de que se cree la siguiente instantánea. Los valores posibles son de 0 a 59.	entero
días del mes	Indica los días del mes en que se tomará la instantánea.	formación
pausa	Indica si la programación está en pausa o no. Valores posibles: • verdadero • FALSO	booleano
periódico	Indica si la programación es recurrente o no. Valores posibles: • verdadero • FALSO	booleano
ejecutarSiguienteIntervalo	Indica si la programación se ejecutará o no la próxima vez que el programador esté activo. Cuando es verdadero, la programación se ejecutará la próxima vez que el programador esté activo y luego este valor se restablecerá a falso. Valores posibles: • verdadero • FALSO	booleano
ID de programación	El identificador único del horario.	entero

Nombre	Descripción	Tipo
Información del horario	Incluye el nombre único asignado a la programación, el período de retención de la instantánea creada y el ID del volumen desde el cual se creó la instantánea. Valores válidos: • <code>`enableRemoteReplication`</code> Indica si la instantánea debe incluirse en la replicación remota. (booleano) • <code>ensureSerialCreation</code>: Especifica si se debe permitir la creación de una nueva instantánea si hay una replicación de instantánea anterior en curso. (booleano) • <code>`name`</code> Nombre de la instantánea que se utilizará. (cadena) • <code>retention</code>: El tiempo durante el cual se conserva la instantánea. Dependiendo de la hora, se muestra en uno de los siguientes formatos: ◦ <code>`fifo`</code> La instantánea se conserva según el principio de primero en entrar, primero en salir (FIFO). Si está vacía, la instantánea se conserva indefinidamente. (cadena) ◦ <code>HH:mm:ss</code> • <code>volumeID</code>: El identificador del volumen que se incluirá en la instantánea. (entero) • <code>volumes</code>: Una lista de identificadores de volumen que se incluirán en la instantánea del grupo. (matriz de enteros)	Objeto JSON
nombre del horario	El nombre único asignado al horario.	cadena

Nombre	Descripción	Tipo
Tipo de horario	Por el momento, solo se admiten los tipos de instantáneas programadas.	cadena
snapMirrorLabel	La etiqueta snapMirrorLabel que se aplicará a la instantánea o instantánea de grupo creada, contenida en scheduleInfo. Si no se establece, este valor es nulo.	cadena
fecha de inicio	Indica la fecha en que comenzó o comenzará el horario por primera vez; con formato de hora UTC.	cadena de fecha ISO 8601
para ser eliminado	Indica si la programación está marcada para su eliminación. Valores posibles: • verdadero • FALSO	booleano
días laborables	Indica los días de la semana en que se tomará la instantánea.	formación

Encuentra más información

[Listas de horarios](#)

sesión (Canal de fibra)

El objeto de sesión contiene información sobre cada sesión de Fibre Channel que es visible para el clúster y en qué puertos de destino es visible. Puedes recuperar esta información con el `ListFibreChannelSessions` Método API.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
iniciadorWWPN	El nombre de puerto mundial (WWPN) del iniciador que está conectado al puerto de destino.	cadena
ID de nodo	El nodo propietario de la sesión Fibre Channel.	entero

Nombre	Descripción	Tipo
iniciador	Información sobre el servidor iniciador de esta sesión de Fibre Channel. Miembros: • alias: El nombre descriptivo asignado al iniciador. • atributos: Los atributos de este iniciador. • initiatorID: El ID de este iniciador. • nombreIniciador: El nombre de este iniciador. • volumeAccessGroups: Una lista de los grupos de acceso a volúmenes asociados con este iniciador.	Objeto JSON
ID de servicio	El ID de servicio del puerto de destino involucrado en esta sesión.	entero
targetWWPN	El WWPN del puerto de destino involucrado en esta sesión.	cadena
ID de grupo de acceso al volumen	El ID del grupo de acceso al volumen al que pertenece el initiatorWWPN. Si no se encuentra en un grupo de acceso a volúmenes, este valor es nulo.	entero

Encuentra más información

[Lista de sesiones de FibreChannel](#)

sesión (iSCSI)

El objeto de sesión (iSCSI) contiene información detallada sobre la sesión iSCSI de cada volumen. Puede recuperar la información de la sesión iSCSI con el `ListISCSISessions` Método API.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de cuenta	El identificador de la cuenta utilizada para la autenticación CHAP, si la hubiera.	entero
nombre de cuenta	El nombre de la cuenta utilizada para la autenticación CHAP, si la hubiere.	cadena
autenticación	Información de autenticación para esta sesión iSCSI.	Autenticación iSCSI
crearTiempo	Hora de creación de la sesión iSCSI, en formato UTC+0.	cadena de fecha ISO 8601
driveID	El driveID asociado al servicio de transporte que aloja la sesión.	entero
ID de unidad	Una lista de los identificadores de las unidades que informan del fallo. Una lista vacía si no corresponde.	matriz de enteros
iniciador	Información sobre el servidor iniciador de esta sesión iSCSI. Miembros: • alias: El nombre descriptivo asignado al iniciador. • atributos: Los atributos de este iniciador. • initiatorID: El ID de este iniciador. • nombreIniciador: El nombre de este iniciador. • volumeAccessGroups: Una lista de los grupos de acceso a volúmenes asociados con este iniciador.	Objeto JSON
IP iniciadora	La dirección IP y el número de puerto del iniciador del servidor iSCSI.	cadena
nombre del iniciador	El nombre calificado iSCSI (IQN) del iniciador del servidor iSCSI.	cadena

Nombre	Descripción	Tipo
nombre de puerto del iniciador	El nombre del iniciador, combinado con el ID de sesión del iniciador, identifica el puerto del iniciador.	cadena
ID de sesión del iniciador	Un identificador de 48 bits proporcionado por el iniciador que identifica la sesión iSCSI como perteneciente a ese iniciador.	entero
msDesdeLaÚltimalscsiPDU	El tiempo, en milisegundos, transcurrido desde que se recibió la última PDU iSCSI para esta sesión.	entero
msDesdeElÚltimoComandoScsi	El tiempo, en milisegundos, transcurrido desde que se recibió el último comando SCSI para esta sesión.	entero
ID de nodo	El nodeID asociado al servicio de transporte que aloja la sesión.	entero
ID de servicio	El ID del servicio de transporte que aloja la sesión.	entero
ID de sesión	El ID de sesión iSCSI.	entero
targetIP	La dirección IP y el número de puerto del destino de almacenamiento iSCSI.	cadena
nombre de destino	El IQN del destino iSCSI.	cadena
nombre de puerto de destino	El nombre del destino, combinado con la etiqueta del grupo del portal de destino, identifica el puerto de destino.	cadena
ID de red virtual	El identificador de red virtual asociado a la sesión.	entero
ID de volumen	El ID del volumen asociado a la sesión, si lo hubiera.	entero
instancia de volumen	Identifica el objeto de volumen asociado con la sesión iSCSI, si existe.	entero

Encuentra más información

[Lista de sesiones iSCSI](#)

snapMirrorAggregate

El objeto snapMirrorAggregate contiene información sobre los agregados ONTAP disponibles, que son conjuntos de discos puestos a disposición de los volúmenes como almacenamiento. Puede obtener esta información utilizando el método API ListSnapMirrorAggregates.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de punto final de SnapMirror	El identificador del sistema ONTAP de destino.	entero
nombre agregado	El nombre del agregado.	cadena
nombre del nodo	El nombre del nodo ONTAP propietario de este agregado.	cadena
Tallas disponibles	El número de bytes disponibles restantes en el total.	entero
tamañoTotal	El tamaño total (en bytes) del agregado.	entero
porcentaje de capacidad utilizada	Porcentaje de espacio en disco actualmente en uso.	entero
recuento de volumen	El número de volúmenes en total.	entero

snapMirrorClusterIdentity

El objeto snapMirrorClusterIdentity contiene información de identificación sobre el clúster ONTAP remoto en una relación SnapMirror .

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de punto final de SnapMirror	El identificador del sistema ONTAP de destino.	entero
nombre del clúster	El nombre del clúster ONTAP de destino.	cadena
clusterUUID	El identificador único universal de 128 bits del clúster ONTAP de destino.	cadena
número de serie del clúster	El número de serie del clúster 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 Element. Puede recuperar esta información con el método API ListSnapMirrorEndpoints.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de punto final de SnapMirror	El identificador único del objeto en el clúster local.	entero
gestión de la propiedad intelectual	La dirección IP de gestión del clúster del punto final.	cadena
nombre del clúster	El nombre del clúster ONTAP . Este valor se completa automáticamente con el valor de "clusterName" del objeto snapMirrorClusterIdentity.	cadena
nombre de usuario	El nombre de usuario de administración para el sistema ONTAP .	cadena

Nombre	Descripción	Tipo
direcciones ip	Lista de las direcciones IP de almacenamiento entre clústeres para todos los nodos del clúster. Puedes obtener estas direcciones IP con el método ListSnapMirrorNetworkInterfaces.	matriz de cadenas
está conectado	Estado de conectividad del enlace de control al clúster ONTAP .	booleano

snapMirrorJobScheduleCronInfo

El objeto snapMirrorJobScheduleCronInfo contiene información sobre la programación de una tarea cron en el sistema ONTAP .

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de punto final de SnapMirror	El identificador del sistema ONTAP de destino.	entero
nombreDeHorarioDeTrabajo	El nombre del horario de trabajo.	cadena
Descripción del horario de trabajo	Un resumen del horario generado automáticamente y legible para humanos.	cadena

snapMirrorLunInfo

El objeto snapMirrorLunInfo contiene información sobre el objeto LUN de ONTAP .

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de punto final de SnapMirror	El identificador del sistema ONTAP de destino.	entero
marca de tiempo de creación	El tiempo de creación del LUN.	cadena de fecha ISO 8601
nombre de lun	El nombre del LUN.	cadena

Nombre	Descripción	Tipo
camino	La trayectoria del LUN.	cadena
tamaño	Tamaño de la LUN en bytes.	entero
tamañoUsado	Número de bytes utilizados por la LUN.	entero
estado	Estado de acceso actual de la LUN. Valores posibles: • en línea • desconectado • error_lun_extranjero • nvfail • error_espacio	cadena
volume	El nombre del volumen que contiene el LUN.	cadena
vserver	El servidor virtual que contiene la LUN.	cadena

snapMirrorInterfazDeRed

El objeto snapMirrorNetworkInterface contiene información sobre las interfaces lógicas (LIF) entre clústeres.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
Estado administrativo	Si la interfaz lógica (LIF) está habilitada o deshabilitada administrativamente. Valores posibles: • arriba • abajo	cadena
ID de punto final de SnapMirror	El identificador del sistema ONTAP de destino.	entero
nombre de interfaz	El nombre LIF.	cadena

Nombre	Descripción	Tipo
dirección de red	La dirección IP del LIF.	cadena
máscara de red	La máscara de red del LIF.	cadena
rol de interfaz	El papel del LIF. Valores posibles: • indefinido • clúster • data • gestión de nodos • intercluster • gestión de clústeres	cadena
Estado operativo	El estado operativo del LIF (si ha establecido o no una conexión exitosa). Este estado puede diferir del estado administrativo si existe un problema de red que impide el funcionamiento de la interfaz. Valores posibles: • arriba • abajo	cadena
vserverName	El nombre del servidor virtual.	cadena

snapMirrorNode

El objeto snapMirrorNode contiene información sobre los nodos del clúster ONTAP de destino en una relación SnapMirror .

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de punto final de SnapMirror	El identificador del sistema ONTAP de destino.	entero
nombre	El nombre del nodo ONTAP .	cadena
modelo	Modelo del nodo ONTAP .	cadena

Nombre	Descripción	Tipo
número de serie	El número de serie del nodo ONTAP .	cadena
Versión del producto	La versión del producto ONTAP .	cadena
¿El nodo está sano?	El estado de salud de un nodo en el clúster ONTAP . Valores posibles: • verdadero • FALSO	cadena
esNodoElegible	Si el nodo es elegible o no para participar en un clúster ONTAP . Valores posibles: • verdadero • FALSO	cadena

snapMirrorPolicy

El objeto snapMirrorPolicy contiene información sobre una política SnapMirror que está almacenada en un sistema ONTAP .

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de punto final de SnapMirror	El identificador del sistema ONTAP de destino.	entero
nombre de la política	El nombre único asignado a la póliza.	cadena
tipo de política	El tipo de póliza. Valores posibles: • espejo asíncrono • bóveda_espejo	cadena
comentario	Una descripción legible por humanos asociada con la política de SnapMirror .	cadena

Nombre	Descripción	Tipo
prioridad de transferencia	La prioridad con la que se ejecuta una transferencia de SnapMirror . Valores posibles: • normal: La prioridad predeterminada. Estas transferencias se programan antes que la mayoría de las transferencias de baja prioridad. • baja: Estas transferencias tienen la prioridad más baja y se programan después de la mayoría de las transferencias de prioridad normal.	cadena
reglas de política	Una lista de objetos que describen las reglas de la política.	Regla de política de espejo snapformación
totalKeepCount	El recuento total de retenciones para todas las reglas de la política.	entero
Reglas totales	El número total de reglas en la política.	entero
vserverName	El nombre del servidor virtual para la política SnapMirror .	cadena

Regla de política de espejo snap

El objeto snapMirrorPolicyRule contiene información sobre las reglas de una política de SnapMirror .

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
snapMirrorLabel	La etiqueta de copia de instantánea, utilizada para la selección de copias de instantáneas en relaciones de protección de datos extendidas.	cadena

Nombre	Descripción	Tipo
keepCount	Especifica el número máximo de copias de instantáneas que se conservan en el volumen de destino de SnapMirror para una regla.	entero

snapMirrorRelationship

El objeto snapMirrorRelationship contiene información sobre una relación SnapMirror entre un volumen Element y un volumen ONTAP .

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de punto final de SnapMirror	El identificador del sistema ONTAP de destino.	entero
snapMirrorRelationshipID	El identificador único para cada objeto snapMirrorRelationship en una matriz, tal como se devolvería en ListSnapMirrorRelationships. Este UUID es creado y devuelto por el sistema ONTAP .	cadena
Volumen de origen	Un objeto que describe el volumen de origen.	snapMirrorVolumeInfo
volumen de destino	Un objeto que describe el volumen de destino.	snapMirrorVolumeInfo
tasa de transferencia máxima actual	La tasa de transferencia máxima actual entre los volúmenes de origen y destino, en kilobytes por segundo.	entero

Nombre	Descripción	Tipo
es saludable	Independientemente de si la relación es sana o no. Valores posibles: • Es cierto: la relación es sana. • Falso: La relación no es sana. Esto puede deberse a que una actualización manual o programada falle o se cancele, o a que la última actualización programada se retrase.	booleano
tiempo de retardo	Cantidad de tiempo en segundos en que los datos del volumen de destino se retrasan con respecto a los datos del volumen de origen.	entero
últimaDuraciónDeTransferencia	El tiempo en segundos que tardó en completarse la última transferencia.	entero
último error de transferencia	Un mensaje que describe la causa del último fallo de transferencia.	cadena
últimoTamañoDeTransferencia	El número total de bytes transferidos durante la última transferencia.	entero
marca de tiempo de finalización de la última transferencia	La hora de finalización de la última transferencia.	cadena de fecha ISO 8601
últimoTipo de transferencia	El tipo de transferencia anterior en la relación.	cadena
tasa de transferencia máxima	Especifica la velocidad máxima de transferencia de datos entre los volúmenes en kilobytes por segundo. El valor predeterminado, 0, es ilimitado y permite que la relación SnapMirror utilice completamente el ancho de banda de red disponible.	entero

Nombre	Descripción	Tipo
estado del espejo	El estado espejo de la relación SnapMirror . Valores posibles: • no inicializado: El volumen de destino no se ha inicializado. • snapmirrored: El volumen de destino se ha inicializado y está listo para recibir actualizaciones de SnapMirror . • volumen interrumpido: El volumen de destino es de lectura y escritura y existen instantáneas.	cadena
Instantánea más reciente	El nombre de la copia de instantánea más reciente en el volumen de destino.	cadena
nombre de la política	Especifica el nombre de la política ONTAP SnapMirror para la relación. Se puede obtener una lista de las políticas disponibles con ListSnapMirrorPolicies. Los valores de ejemplo son "MirrorLatest" y "MirrorAndVault".	cadena
tipo de política	El tipo de política ONTAP SnapMirror para la relación. Consulte ListSnapMirrorPolicies. Ejemplos son: "async_mirror" o "mirror_vault".	cadena
Progreso de la relación	El número total de bytes que se han procesado hasta el momento para la actividad actual de la relación, tal como se devuelve en el estado de la relación. Esto se configura solo cuando el miembro "relationshipStatus" indica que hay una actividad en curso.	entero

Nombre	Descripción	Tipo
Estado de la relación	El estado de la relación SnapMirror . Valores posibles: • inactivo • transfiriendo • de cheques • aquiescencia • aquietó • en cola • preparante • finalizando • abortar • rotura	cadena
tipo de relación	El tipo de relación SnapMirror . En los clústeres de almacenamiento que ejecutan el software Element, este valor siempre es "extended_data_protection".	cadena
nombre del horario	El nombre de la tarea cron preexistente en el sistema ONTAP que se utiliza para actualizar la relación SnapMirror . Se puede obtener una lista de los horarios disponibles con ListSnapMirrorSchedules.	cadena
Razón insalubre	La razón por la que la relación no es sana.	cadena

snapMirrorVolume

El objeto snapMirrorVolume contiene información sobre un volumen ONTAP .

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de punto final de SnapMirror	El identificador del sistema ONTAP de destino.	entero

Nombre	Descripción	Tipo
nombre	El nombre del volumen.	cadena
tipo	El tipo de volumen. Valores posibles: • rw: Volumen de lectura y escritura • ls: Volumen de reparto de carga • dp: Volumen de protección de datos	cadena
vserver	El nombre del servidor virtual (Vserver) propietario de este volumen.	cadena
aggrName	El nombre del agregado contenedor.	cadena
estado	El estado del volumen. Valores posibles: • en línea • restringido • desconectado • mezclado	cadena
tamaño	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 snapMirrorVolumeInfo contiene información sobre la ubicación de un volumen en una relación SnapMirror , como su nombre y tipo.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
tipo	El tipo de volumen. Valores posibles: • solidfire: El volumen reside en un clúster de almacenamiento que ejecuta el software Element. • ontap: El volumen reside en un clúster ONTAP remoto.	cadena
ID de volumen	El identificador del volumen. Solo válido si "type" es solidfire.	entero
vserver	El nombre del servidor virtual (Vserver) propietario de este volumen. Solo válido si "type" está disponible.	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 del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de punto final de SnapMirror	El identificador del sistema ONTAP de destino.	entero
vserverName	El nombre del servidor virtual.	cadena
vserverType	El tipo de Vserver. Valores posibles: • data • administración • sistema • nodo	cadena

Nombre	Descripción	Tipo
vserverSubtype	El subtipo del Vserver. Valores posibles: • por defecto • destino dp • data • fuente_sincronizada • destino_sincronizado	cadena
volumen raíz	El volumen raíz del Vserver.	cadena
Agregado de volumen raíz	El agregado sobre el cual se creará el volumen raíz.	cadena
vserverAggregateInfo	Una matriz de objetos snapMirrorVserverAggregateInfo.	Objeto JSON
Estado administrativo	El estado administrativo detallado del Vserver. Valores posibles: • correr • interrumpido • a partir de • parada • inicialización • eliminación	cadena
estado operativo	El estado operativo básico del Vserver. Valores posibles: • correr • interrumpido	cadena

snapMirrorVserverAggregateInfo

El objeto snapMirrorVserverAggregateInfo contiene información sobre las máquinas virtuales de almacenamiento de datos disponibles (también llamadas Vservers) en el clúster ONTAP de destino.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
aggrName	El nombre del agregado asignado a un Vserver.	cadena
tamaño disponible agregado	Tamaño disponible del agregado asignado.	entero

instantánea

El objeto de instantánea contiene información sobre una instantánea realizada para un volumen. Puedes usar el `ListSnapshots` Método de API para recuperar una lista de información de instantáneas para un volumen o para todos los volúmenes. El objeto incluye información sobre la instantánea activa, así como sobre cada instantánea creada para un volumen.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON
suma de comprobación	Una pequeña representación en cadena de los datos en la instantánea almacenada. Esta suma de comprobación se puede utilizar posteriormente para comparar otras instantáneas y detectar errores en los datos.	cadena
crearTiempo	Hora en formato UTC+0 en la que se creó la instantánea.	cadena de fecha ISO 8601
habilitar la replicación remota	Identifica si la instantánea está habilitada para la replicación remota.	booleano

Nombre	Descripción	Tipo
motivo de expiración	Indica cómo se configura la expiración de la instantánea. Valores posibles: • API: El tiempo de expiración se establece mediante la API. • Ninguno: No se ha establecido ningún tiempo de expiración. • Prueba: El tiempo de expiración se ha establecido para realizar pruebas. • FIFO: La caducidad se produce según el principio de primero en entrar, primero en salir.	cadena
tiempo de expiración	Hora en la que esta instantánea caducará y será eliminada del clúster.	cadena de fecha ISO 8601
ID de grupo	El ID del grupo si la instantánea pertenece a un grupo de instantáneas.	entero
grupo snapshotUUID	Contiene información sobre cada instantánea del grupo. Cada uno de estos miembros tendrá un parámetro UUID para el UUID de la instantánea.	cadena
tiempoDeCreaciónDeInstancia	La hora en que se creó la instantánea en el clúster local.	cadena de fecha ISO 8601
UUID de instantánea de instancia	El identificador único universal de la instantánea en el clúster local. Este ID no se replica en otros clústeres.	cadena
nombre	El nombre único asignado a la instantánea. Si no se especifica ningún nombre, el nombre es la marca de tiempo con formato UTC+0 del momento en que se creó la instantánea.	cadena

Nombre	Descripción	Tipo
estados remotos	Una matriz que contiene el identificador universal y el estado de replicación de cada instantánea remota en el clúster de destino, tal como se ve desde el clúster de origen.	Estado de instantánea del clúster remoto formación
snapMirrorLabel	Etiqueta utilizada por el software SnapMirror para especificar la política de retención de instantáneas en los endpoints de SnapMirror . Si no se establece, este valor es nulo.	cadena
ID de instantánea	El identificador único de una instantánea existente.	cadena
snapshotUUID	El identificador único universal de una instantánea existente. Cuando la instantánea se replica en diferentes clústeres, este ID se replica junto con ella y se utiliza para identificar la instantánea en todos los clústeres.	cadena
estado	Estado actual de la instantánea. Valores posibles: • Desconocido: Se produjo un error al obtener el estado de la instantánea. • Preparando: Esta instantánea se está preparando para su uso y aún no se puede escribir en ella. • Sincronización remota: Esta instantánea se está replicando desde un clúster remoto. • Listo: Esta instantánea ha finalizado su preparación o replicación y ahora se puede utilizar. • Activa: Esta instantánea corresponde a la rama activa. • Clonación: Esta instantánea está involucrada en una operación CopyVolume.	cadena

Nombre	Descripción	Tipo
tamaño total	Tamaño total en bytes de la instantánea.	entero
ID de volumen virtual	El ID del volumen virtual asociado a esta instantánea.	UUID
ID de volumen	El identificador del volumen a partir del cual se creó la instantánea.	entero
nombre del volumen	El nombre del volumen en el momento en que se creó la instantánea.	cadena

Encuentra más información

[Instantáneas de la lista](#)

Destinatario de trampa SNMP

El objeto `snmpTrapRecipient` contiene información sobre un host que está configurado para recibir traps SNMP generados por el clúster de almacenamiento. Puedes usar el `GetSnmpTrapInfo` Método API para obtener una lista de hosts configurados para recibir traps SNMP.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
anfitrión	La dirección IP o el nombre de host del host de destino.	cadena
puerto	El número de puerto UDP en el host al que se debe enviar la trampa. El rango válido es de 1 a 65535. 0 (cero) no es un número de puerto válido. El puerto predeterminado es 162.	entero
comunidad	Cadena de comunidad SNMP.	cadena

contenedor de almacenamiento

El objeto `storageContainer` contiene los atributos de un contenedor de almacenamiento de volumen virtual. Puede recuperar esta información para cada contenedor de

almacenamiento del clúster utilizando ListStorageContainers Método API.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
ID de cuenta	El ID de la cuenta del sistema de almacenamiento asociada al contenedor de almacenamiento.	entero
iniciadorSecreto	La clave secreta de autenticación CHAP para el iniciador asociado con el contenedor de almacenamiento.	cadena
nombre	El nombre del contenedor de almacenamiento.	cadena
tipo de punto final del protocolo	Tipo de punto final del protocolo del contenedor de almacenamiento. SCSI es el único valor válido.	cadena
estado	Estado del contenedor de almacenamiento. Valores posibles: • Activo: El contenedor de almacenamiento está en uso. • Bloqueado: El contenedor de almacenamiento está bloqueado.	cadena
ID del contenedor de almacenamiento	El identificador único del contenedor de almacenamiento.	UUID
secreto del objetivo	La clave secreta de autenticación CHAP para el objetivo asociado al contenedor de almacenamiento.	cadena
volúmenes virtuales	Una lista de los identificadores de los volúmenes virtuales asociados al contenedor de almacenamiento.	matriz UUID

Encuentra más información

[Listar contenedores de almacenamiento](#)

trabajo de sincronización

El objeto `syncJob` contiene información sobre trabajos de clonación, replicación remota o sincronización de segmentos que se están ejecutando en un clúster.

Puedes recuperar información de sincronización con el `ListSyncJobs` Método API.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
<code>bloquesPorSegundo</code>	Número de bloques de datos que se transfieren por segundo desde el clúster de origen al clúster de destino. Presente solo si el miembro de tipo está configurado como remoto.	entero
<code>tipo de rama</code>	Devuelto solo para trabajos de sincronización de replicación remota. Valores posibles: • instantánea • volume	cadena
<code>bytesPorSegundo</code>	Número de bytes que el clon procesa por segundo. Presente solo si el miembro de tipo está configurado como clonar o segmentar.	flotar
<code>ID de clon</code>	El identificador de la operación de clonación que está en curso. Presente solo si el miembro de tipo está configurado como clon.	entero
<code>Bytes actuales</code>	El número de bytes que el clon ha procesado en el volumen de origen. Presente solo si el miembro de tipo está configurado como clonar o segmentar.	entero
<code>ID de servicio de destino</code>	El identificador del servicio que aloja la réplica principal del volumen. Presente solo si el miembro de tipo está configurado como remoto.	entero

Nombre	Descripción	Tipo
ID de volumen de destino	El ID del volumen de destino. Presente solo si el miembro de tipo está configurado como clon o remoto.	entero
tiempo transcurrido	Tiempo transcurrido, en segundos, desde que se inició la tarea de sincronización.	Número de punto flotante o entero, dependiendo del tipo de operación de sincronización.
ID de clon de grupo	El ID de la operación de clonación de grupo que está en curso.	entero
ID de nodo	Especifica el nodo en el que se está realizando la clonación. Presente solo si el miembro de tipo está configurado como clon.	entero
porcentaje completado	Porcentaje de finalización del trabajo de sincronización.	Número de punto flotante o entero, dependiendo del tipo de operación de sincronización.
tiempo restante	Tiempo estimado, en segundos, para completar la operación.	flotar
ID de segmento	El identificador de la unidad de partición que se está sincronizando.	entero
escenario	Presente solo si el miembro de tipo está configurado como remoto o clon. Valores posibles: • Metadatos: La replicación está en proceso de determinar qué datos deben transferirse al clúster remoto. No se informa del estado de esta etapa del proceso de replicación. • Datos: La replicación está en proceso de transferir la mayor parte de los datos al clúster remoto. • Entero: Indica la compatibilidad con versiones anteriores de la porción para trabajos de sincronización de porciones.	cadena

Nombre	Descripción	Tipo
ID de instantánea	El ID de la instantánea a partir de la cual se creó el clon. Presente solo si el miembro de tipo está configurado como clon.	entero
srcServiceID	El ID del servicio de origen.	entero
ID de volumen de origen	El ID del volumen de origen.	entero
totalBytes	El número total de bytes del clon. Presente solo si el miembro de tipo está configurado como clonar o segmentar.	entero
tipo	El tipo de operación de sincronización. Valores posibles: • clon • rebanada • block • remoto	cadena

Encuentra más información

[ListSyncJobs](#)

tarea (volúmenes virtuales)

El objeto de tarea contiene información sobre una tarea de volumen virtual que se está ejecutando actualmente o que ha finalizado en el sistema. Puedes usar el `ListVirtualVolumeTasks` Método para recuperar esta información para todas las tareas de volumen virtual.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
cancelado	Indica si la tarea fue cancelada o no. Valores posibles: • verdadero • FALSO	booleano

Nombre	Descripción	Tipo
cloneVirtualVolumeID	El ID de volumen virtual único del volumen virtual que se está clonando (para tareas de clonación).	UUID
metadatos de padres	Un objeto que contiene metadatos del elemento principal para tareas que clonan o crean instantáneas de un volumen virtual.	Objeto JSON
tamañoTotalPadre	El espacio total disponible (en bytes) en el elemento padre para tareas de clonación o instantánea.	entero
tamaño usado del padre	El espacio utilizado del padre (en bytes) para tareas de clonación o instantánea.	entero
operación	El tipo de operación que realiza la tarea. Valores posibles: • desconocido: Se desconoce la operación de la tarea. • preparación: La tarea consiste en preparar un volumen virtual. • Instantánea: La tarea consiste en crear una instantánea de un volumen virtual. • Reversión: La tarea consiste en revertir un volumen virtual a una instantánea. • clonar: La tarea consiste en crear un clon del volumen virtual. • fastClone: La tarea consiste en crear un clon rápido de un volumen virtual. • copyDiffs: La tarea consiste en copiar bloques diferentes a un volumen virtual.	cadena

Nombre	Descripción	Tipo
estado	Estado actual de la tarea de volumen virtual. Valores posibles: • Error: La tarea ha fallado y ha devuelto un error. • En cola: La tarea está esperando a ser ejecutada. • En ejecución: La tarea se está ejecutando actualmente. • Éxito: La tarea se ha completado correctamente.	cadena
ID de host de volumen virtual	El identificador único del host que inició la tarea.	UUID
ID de volumen virtual	El nuevo ID de volumen virtual único (para tareas que crean un nuevo volumen virtual).	UUID
ID de tarea de volumen virtual	El identificador único de la tarea.	UUID

Encuentra más información

[Listar tareas de volumen virtual](#)

usmUser

Puedes utilizar el objeto SNMP usmUser con el `SetSnmpInfo` Método API para configurar SNMP en el clúster de almacenamiento.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
acceso	El tipo de acceso SNMP para este usuario. Valores posibles: • agitador: Acceso de solo lectura. • rwuser: Acceso de lectura y escritura. Todos los objetos MIB del software Element son de solo lectura.	cadena

Nombre	Descripción	Tipo
nombre	El nombre del usuario.	cadena
contraseña	La contraseña del usuario.	cadena
contraseña	La contraseña del usuario.	cadena
Nivel de seguridad	Tipo de credenciales requeridas para este usuario. Valores posibles: • noauth: No se requiere contraseña ni frase de contraseña. • Autenticación: Se requiere una contraseña para el acceso del usuario. • priv: Se requiere una contraseña y una frase de contraseña para el acceso del usuario.	cadena

Encuentra más información

[SetSnmpInfo](#)

red virtual

El objeto `virtualNetwork` contiene información sobre una red virtual específica. Puedes usar el `ListVirtualNetworks` Método API para recuperar una lista de esta información para todas las redes virtuales del sistema.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
bloques de direcciones	El rango de bloques de direcciones actualmente asignados a la red virtual. Miembros: • disponible: Cadena binaria de "1" y "0". "1" indica que la dirección IP está disponible y "0" indica que la IP no está disponible. La cadena se lee de derecha a izquierda, siendo el dígito situado más a la derecha la primera dirección IP de la lista de bloques de direcciones. • Tamaño: El tamaño de este bloque de direcciones. • inicio: La primera dirección IP del bloque.	matriz de objetos JSON
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON
nombre	El nombre asignado a la red virtual.	cadena
máscara de red	La dirección IP de la máscara de red para la red virtual.	cadena
svip	La dirección IP de almacenamiento para la red virtual.	cadena
puerta	La puerta de enlace utilizada para la red virtual.	cadena
ID de red virtual	El identificador único de una red virtual.	entero
etiqueta de red virtual	El identificador de etiqueta VLAN.	entero

Encuentra más información

[Lista de redes virtuales](#)

volumen virtual

El objeto `virtualVolume` contiene información de configuración sobre un volumen virtual, así como información sobre instantáneas del volumen virtual. No incluye información sobre el tiempo de ejecución ni el uso. Puedes usar el `ListVirtualVolumes` Método para recuperar esta información para un clúster.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
uniones	Una lista de identificadores de enlace para este volumen virtual.	matriz UUID
niños	Una lista de UUID de volúmenes virtuales que son hijos de este volumen virtual.	matriz UUID
descendientes	Cuando se pasa recursive: true al método ListVirtualVolumes, contiene una lista de UUID de volúmenes virtuales que son descendientes de este volumen virtual.	matriz UUID
metadatos	Pares clave-valor de los metadatos del volumen virtual, como el tipo de volumen virtual, el tipo de sistema operativo invitado, etc.	Objeto JSON
ID de volumen virtual principal	El ID del volumen virtual del volumen virtual principal. Si el ID está compuesto solo por ceros, se trata de un volumen virtual independiente sin vínculo con un elemento principal.	UUID
ID de instantánea	El identificador de la instantánea de volumen subyacente. Este valor es "0" si el volumen virtual no representa una instantánea.	entero
snapshotInfo	El objeto de instantánea para la instantánea asociada (nulo si no existe).	instantánea

Nombre	Descripción	Tipo
estado	Estado actual del volumen virtual. Valores posibles: • clonación: El volumen virtual se está procesando en respuesta a una operación de clonación o instantánea. • En espera: El volumen virtual está esperando a que se complete una operación de instantánea. • Listo: El volumen virtual está listo para su uso general.	cadena
contenedor de almacenamiento	Un objeto que describe el contenedor de almacenamiento propietario de este volumen virtual.	contenedor de almacenamiento
ID de volumen virtual	El identificador único del volumen virtual.	UUID
Tipo de volumen virtual	El tipo de volumen virtual.	cadena
ID de volumen	El identificador del volumen subyacente.	entero
información de volumen	Cuando se pasa details: true al método ListVirtualVolumes, este miembro es un objeto que describe el volumen.	volume

Encuentra más información

- [Listar volúmenes virtuales](#)
- [instantánea](#)
- [contenedor de almacenamiento](#)
- [volume](#)

volume

El objeto de volumen contiene información de configuración sobre volúmenes no emparejados o emparejados. No incluye información sobre el tiempo de ejecución o el uso, ni contiene información sobre volúmenes virtuales.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
acceso	El tipo de acceso permitido para el volumen. Valores posibles: • <code>`readOnly`</code> Solo se permiten operaciones de lectura. • <code>`readWrite`</code> Se permiten lecturas y escrituras. • <code>`locked`</code> No se permiten lecturas ni escrituras. • <code>replicationTarget</code>: Designado como volumen objetivo en un par de volúmenes replicados.	cadena
ID de cuenta	El ID de la cuenta que contiene el volumen.	entero
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON
tamaño del bloque	El tamaño de los bloques en el volumen.	entero
crearTiempo	Hora de creación del volumen en formato UTC+0.	Cadena ISO 8601
esquema de protección actual	El esquema de protección que se está utilizando para este volumen. Si un volumen se está convirtiendo de un régimen de protección a otro, este miembro refleja el régimen de protección al que se está convirtiendo el volumen.	cadena
Tiempo de eliminación	Hora en formato UTC+0 en que se eliminó el volumen.	Cadena ISO 8601
enable512e	Si se establece en verdadero, el volumen proporciona emulación de sector de 512 bytes.	booleano

Nombre	Descripción	Tipo
habilitarSnapMirrorReplication	Si el volumen se puede utilizar o no para la replicación con puntos de conexión SnapMirror .	booleano
fifoSize	Especifica el número máximo de instantáneas del volumen que se mantendrán simultáneamente si se utiliza el modo de retención de instantáneas Primero en entrar, primero en salir (FIFO).	entero
iqn	El nombre calificado iSCSI del volumen.	cadena
última hora de acceso	La última vez que se produjo algún acceso (incluida la E/S) al volumen (formateado como UTC+0). Si se desconoce la hora del último acceso, este valor es nulo.	Cadena ISO 8601
últimoAccesoHoralO	La última vez que se produjo alguna operación de E/S en el volumen (formateada como UTC+0). Si se desconoce la hora del último acceso, este valor es nulo.	Cadena ISO 8601
tamaño mínimo de Fifo	Especifica el número mínimo de ranuras de instantáneas First-In-First-Out (FIFO) reservadas simultáneamente por el volumen si se utiliza el modo de retención de instantáneas First-In-First-Out (FIFO).	entero
nombre	El nombre del volumen tal como se proporcionó en el momento de su creación.	cadena
esquema de protección anterior	Si un volumen se está convirtiendo de un régimen de protección a otro, este miembro refleja el régimen de protección del que se está convirtiendo el volumen. Este miembro no cambia hasta que se inicia una conversión. Si un volumen nunca se ha convertido, este miembro es nulo.	cadena

Nombre	Descripción	Tipo
tiempo de purga	Hora en formato UTC+0 en que se eliminó el volumen del sistema.	Cadena ISO 8601
QoS	Configuración de calidad de servicio para este volumen.	Calidad de servicio
ID de política de qos	El ID de la política QoS asociada al volumen. El valor es nulo si el volumen no está asociado a una póliza.	entero
scsiEUIDeviceID	Identificador de dispositivo SCSI único a nivel mundial para el volumen en formato de 16 bytes basado en EUI-64.	cadena
scsiNAADeviceID	Identificador de dispositivo SCSI único a nivel mundial para el volumen en formato NAA IEEE Registered Extended.	cadena
sliceCount	El número de porciones del volumen. Este valor siempre es "1".	entero
estado	Estado actual del volumen. Valores posibles: • init: Un volumen que se está inicializando y no está listo para conexiones. • activo: Un volumen activo listo para conexiones. • eliminado: Un volumen que ha sido marcado para su eliminación, pero que aún no se ha purgado.	cadena
tamaño total	El total de bytes de capacidad aprovisionada.	entero
ID de volumen virtual	El identificador único de volumen virtual asociado al volumen, si lo hubiera.	UUID

Nombre	Descripción	Tipo
grupos de acceso de volumen	Lista de identificadores de los grupos de acceso a volúmenes a los que pertenece un volumen. Este valor es una lista vacía si un volumen no pertenece a ningún grupo de acceso a volúmenes.	matriz de enteros
UUID del grupo de consistencia de volumen	El identificador único universal del grupo de consistencia de volumen al que pertenece el volumen.	UUID
ID de volumen	El ID de volumen único para el volumen.	entero
volúmenesPares	Información sobre un volumen emparejado. Solo visible si hay un volumen emparejado. Este valor es una lista vacía si el volumen no está emparejado.	volumenPar información
UUID del volumen	El identificador único universal del volumen.	UUID

Encuentra más información

- [Listar volúmenes activos](#)
- [Lista de volúmenes eliminados](#)
- [Lista de volúmenes](#)
- [Listar volúmenes para la cuenta](#)
- [Calidad de servicio](#)

volumeAccessGroup

El objeto volumeAccessGroup contiene información sobre un grupo de acceso a volúmenes específico. Puede recuperar una lista de esta información para todos los grupos de acceso con el método API. `ListVolumeAccessGroups` .

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON

Nombre	Descripción	Tipo
volúmenes eliminados	Conjunto de volúmenes que han sido eliminados del grupo de acceso a volúmenes y que aún no han sido purgados del sistema.	matriz de enteros
identificadores de iniciador	Una lista de identificadores de iniciadores que están asignados al grupo de acceso al volumen.	matriz de enteros
iniciadores	Conjunto de iniciadores IQN/WWPN únicos que están asignados al grupo de acceso al volumen.	matriz de cadenas
nombre	Nombre del grupo de acceso al volumen.	cadena
ID de grupo de acceso al volumen	Identificador único VolumeAccessGroupID para el grupo de acceso al volumen.	entero
volúmenes	Una lista de los ID de volumen que pertenecen al grupo de acceso al volumen.	matriz de enteros

Encuentra más información

[Listar grupos de acceso de volumen](#)

volumenPar

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. Puedes usar el `ListActivePairedVolumes` y `ListActiveVolumes` Métodos de la API para devolver información sobre volúmenes emparejados.

miembros del objeto

Este objeto contiene los siguientes miembros:

Nombre	Descripción	Tipo
clusterPairID	El clúster en el que se encuentra emparejado el volumen.	entero

Nombre	Descripción	Tipo
Replicación remota	Detalles sobre la replicación de volúmenes. Miembros: • modo: (cadena) Uno de "Async", "Sync" o "SnapshotsOnly". • pauseLimit: (entero) Solo para uso interno. • remoteServiceID: (entero) El ID del servicio de segmento remoto. • resumeDetails: (cadena) Reservado para uso futuro. • Replicación de instantánea (objeto JSON) ◦ estado: (cadena) El estado de la replicación de instantánea en curso, si hay alguna en progreso. ◦ stateDetails: (cadena) Reservado para uso futuro. • estado: (cadena) El estado de la replicación del volumen. • stateDetails: (cadena) Reservado para uso futuro.	Objeto JSON
ID de segmento remoto	El ID de segmento definido por el clúster en el clúster remoto.	entero
ID de volumen remoto	El identificador del volumen en el clúster remoto con el que está emparejado el volumen local.	entero
nombreVolumenRemoto	El nombre del volumen remoto.	cadena
volumenPairUUID	Un identificador único y universal, definido por el clúster, para este emparejamiento en formato canónico.	cadena

Encuentra más información

- [Lista de volúmenes emparejados activos](#)
- [Listar volúmenes activos](#)

estadísticas de volumen

El objeto volumeStats contiene datos estadísticos para un volumen individual.

miembros del objeto

Puede utilizar los siguientes métodos para obtener objetos volumeStats para algunos o todos los volúmenes:

- [Obtener estadísticas de volumen](#)
- [ListVolumeStatsByAccount](#)
- [Listar estadísticas de volumen por volumen](#)
- [Lista de estadísticas de volumen por grupo de acceso de volumen](#)

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
IOPS reales	Las IOPS reales actuales del volumen en los últimos 500 milisegundos.	Punto en el tiempo	entero
retardo asíncrono	El tiempo transcurrido desde la última sincronización del volumen con el clúster remoto. Si el volumen no está emparejado, este valor es nulo. Nota: Un volumen de destino en un estado de replicación activo siempre tiene un asyncDelay de 0 (cero). Los volúmenes de destino tienen en cuenta el sistema durante la replicación y asumen que asyncDelay es preciso en todo momento.	N/A	Cadena de duración ISO 8601 o nulo
Tamaño promedio de IOPS	Tamaño promedio en bytes de las operaciones de E/S recientes en el volumen en los últimos 500 milisegundos.	Punto en el tiempo	entero
crédito de IOPS de explosión	El número total de créditos IOP disponibles para el usuario. Cuando los volúmenes no utilizan el máximo de IOPS configurado, se acumulan créditos.	N/A	entero
profundidad de la cola de clientes	Número de operaciones de lectura y escritura pendientes en el volumen.	N/A	entero
Hosts de metadatos deseados	Los servicios de metadatos (segmentos) a los que se migran si los metadatos del volumen se migran entre servicios de metadatos. Un valor "nulo" significa que el volumen no se está migrando.	N/A	Objeto JSON

Nombre	Descripción	Cálculo	Tipo
latenciaUSeg	El tiempo promedio, en microsegundos, para completar las operaciones al volumen en los últimos 500 milisegundos. Un valor "0" (cero) significa que no hay E/S en el volumen.	Punto en el tiempo	entero
metadatosHosts	Los servicios de metadatos (segmentos) en los que residen los metadatos del volumen. Valores posibles: • primario: Los servicios de metadatos primarios que alojan el volumen. • liveSecondaries: Servicios de metadatos secundarios que actualmente se encuentran en estado "activo". • deadSecondaries: Servicios de metadatos secundarios que se encuentran en estado inactivo.	N/A	Objeto JSON
IOPS normalizadas	Número promedio de IOPS para todo el clúster en los últimos 500 milisegundos.	Punto en el tiempo	entero
bloques no cero	El número total de bloques de 4 KiB que contienen datos después de que se haya completado la última operación de recolección de basura.	N/A	entero
bytes leídos	El total acumulado de bytes leídos del volumen desde su creación.	Aumento monótono	entero
readBytesLastSample	Número total de bytes leídos del volumen durante el último período de muestreo.	Punto en el tiempo	entero
Latencia de lectura (segundos)	Tiempo promedio, en microsegundos, para completar las operaciones de lectura del volumen en los últimos 500 milisegundos.	Punto en el tiempo	entero
Latencia de lectura (USec) Total	El tiempo total empleado en realizar operaciones de lectura del volumen.	Aumento monótono	entero
operaciones de lectura	El total de operaciones de lectura realizadas en el volumen desde su creación.	Aumento monótono	entero
readOpsLastSample	El número total de operaciones de lectura durante el último período de muestra.	Punto en el tiempo	entero
período de muestra MSeg	Duración del período de muestreo, en milisegundos.	N/A	entero

Nombre	Descripción	Cálculo	Tipo
slicelopsStats	Estadísticas de uso de E/S para un volumen. Disponible a partir del Elemento 12.8. Valores posibles para slicelopsStats: • largeStatistics: Las estadísticas de E/S para el volumen medido durante un período de tiempo más largo, típicamente las últimas 24 horas. • smallStatistics: Las estadísticas de E/S para el volumen medido durante un período de tiempo más corto, normalmente la última hora. Valores posibles para largeStatistics y smallStatistics: • averageReadlops: El promedio de IOPS de lectura para el volumen. • averageTotallops: El promedio total de IOPS (lectura + escritura) para el volumen. • averageWritelops: El promedio de IOPS de escritura para el volumen. • nMuestras: El número de muestras incluidas en el cálculo estadístico. • peakReadlops: El número máximo de IOPS de lectura observado durante un intervalo estadístico. • peakTotallops: El total máximo de IOPS observado durante un intervalo estadístico. • peakWritelops: El número máximo de IOPS de escritura observado durante un intervalo estadístico. • ID de corte: ID de volumen o ID de corte	Punto en el tiempo	Objeto JSON
acelerador	Un valor flotante entre 0 y 1 que representa cuánto está limitando el sistema a los clientes por debajo de su maxIOPS debido a la replicación de datos, errores transitorios y instantáneas tomadas.	N/A	flotar
marca de tiempo	La hora actual en formato UTC+0.	N/A	cadena de fecha ISO 8601
lecturas no alineadas	El total acumulado de operaciones de lectura no alineadas en un volumen desde la creación del volumen.	Aumento monótono	entero

Nombre	Descripción	Cálculo	Tipo
escrituras no alineadas	El total acumulado de operaciones de escritura no alineadas en un volumen desde la creación del volumen.	Aumento monótono	entero
grupos de acceso de volumen	La lista de identificadores de los grupos de acceso a volúmenes a los que pertenece un volumen.	N/A	matriz de enteros
ID de volumen	El identificador del volumen.	N/A	entero
tamaño del volumen	Capacidad total aprovisionada en bytes.	N/A	entero
utilización del volumen	Un valor de punto flotante que describe en qué medida el cliente está utilizando las capacidades de entrada/salida del volumen en comparación con la configuración QoS maxIOPS para ese volumen. Valores posibles: • 0: El cliente no está utilizando el volumen. • 0,01 a 0,99: El cliente no está utilizando completamente las capacidades de IOPS del volumen. • 1.00: El cliente está utilizando completamente el volumen hasta el límite de IOPS establecido por la configuración maxIOPS. • > 1.00: El cliente está utilizando más del límite establecido por maxIOPS. Esto es posible cuando la configuración QoS burstIOPS está establecida en un valor superior a maxIOPS. Por ejemplo, si maxIOPS se establece en 1000 y burstIOPS en 2000, <code>volumeUtilization</code> El valor sería de 2,00 si el cliente utiliza completamente el volumen.	N/A	flotar
escribirBytes	El total acumulado de bytes escritos en el volumen desde su creación.	Aumento monótono	entero
writeBytesLastSample	El número total de bytes escritos en el volumen durante el último período de muestreo.	Aumento monótono	entero
Latencia de escritura (segundos)	Tiempo promedio, en microsegundos, para completar las operaciones de escritura en un volumen en los últimos 500 milisegundos.	Punto en el tiempo	entero
Latencia de escritura (USec) total	El tiempo total empleado en realizar operaciones de escritura en el volumen.	Aumento monótono	entero

Nombre	Descripción	Cálculo	Tipo
operaciones de escritura	El total acumulado de operaciones de escritura en el volumen desde su creación.	Aumento monótono	entero
writeOpsLastSample	El número total de operaciones de escritura durante el último período de muestra.	Punto en el tiempo	entero
bloques cero	Número total de bloques vacíos de 4 KiB sin datos después de que se haya completado la última ronda de operación de recolección de basura.	Punto en el tiempo	entero

Métodos comunes

Obtener API

Puedes usar el `GetAPI` Método para obtener una lista de todos los métodos de la API y los endpoints de la API compatibles que se pueden utilizar en el sistema.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
<versión>	Una lista de todos los métodos API compatibles con esta versión de software, donde <versión> es la versión de software actual que ejecuta este sistema.	matriz de cadenas
versión actual	La versión actual del software del clúster de almacenamiento.	cadena
Versiones compatibles	Una lista de todos los endpoints de la API compatibles con el sistema.	matriz de cadenas

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:


```
{
  "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",
"GetKeyProviderKmp",
"GetKeyServerKmp",
"GetLdapConfiguration",
"GetLimits",
"GetLldpInfo",
"GetLoginBanner",
"GetLoginSessionInfo",
"GetNetworkConfig",
"GetNetworkInterface",
"GetNodeFipsDrivesReport",
"GetNodeHardwareInfo",
"GetNodeStats",
"GetNtpInfo",
```

```
"GetNvramInfo",
"GetOntapVersionInfo",
"GetOrigin",
"GetPendingOperation",
"GetProtectionDomainLayout",
"GetQoSPolicy",
"GetRawStats",
"GetRemoteLoggingHosts",
"GetSSLCertificate",
"GetSchedule",
"GetSnapMirrorClusterIdentity",
"GetSnmpACL",
"GetSnmpInfo",
"GetSnmpState",
"GetSnmpTrapInfo",
"GetStorageContainerEfficiency",
"GetSupportedTlsCiphers",
"GetSystemStatus",
"GetVirtualVolumeCount",
"GetVolumeAccessGroupEfficiency",
"GetVolumeAccessGroupLunAssignments",
"GetVolumeCount",
"GetVolumeEfficiency",
"GetVolumeStats",
"InitializeSnapMirrorRelationship",
"ListAccounts",
"ListActiveAuthSessions",
"ListActiveNodes",
"ListActivePairedVolumes",
"ListActiveVolumes",
"ListAllNodes",
"ListAsyncResults",
"ListAuthSessionsByClusterAdmin",
"ListAuthSessionsByUsername",
"ListBackupTargets",
"ListBulkVolumeJobs",
"ListClusterAdmins",
"ListClusterFaults",
"ListClusterInterfacePreferences",
"ListClusterPairs",
"ListDeletedVolumes",
"ListDriveHardware",
"ListDriveStats",
"ListDrives",
"ListEvents",
"ListFibreChannelPortInfo",
```

```
"ListFibreChannelSessions",
"ListGroupSnapshots",
"ListISCSISessions",
"ListIdpConfigurations",
"ListInitiators",
"ListKeyProvidersKmip",
"ListKeyServersKmip",
"ListNetworkInterfaces",
"ListNodeFibreChannelPortInfo",
"ListNodeStats",
"ListPendingActiveNodes",
"ListPendingNodes",
"ListProtectionDomainLevels",
"ListProtocolEndpoints",
"ListQoS Policies",
"ListSchedules",
"ListServices",
"ListSnapMirrorAggregates",
"ListSnapMirrorEndpoints",
"ListSnapMirrorLuns",
"ListSnapMirrorNetworkInterfaces",
"ListSnapMirrorNodes",
"ListSnapMirrorPolicies",
"ListSnapMirrorRelationships",
"ListSnapMirrorSchedules",
"ListSnapMirrorVolumes",
"ListSnapMirrorVservers",
"ListSnapshots",
"ListStorageContainers",
"ListSyncJobs",
"ListTests",
"ListUtilities",
"ListVirtualNetworks",
"ListVirtualVolumeBindings",
"ListVirtualVolumeHosts",
"ListVirtualVolumeTasks",
"ListVirtualVolumes",
"ListVolumeAccessGroups",
"ListVolumeStats",
"ListVolumeStatsByAccount",
"ListVolumeStatsByVirtualVolume",
"ListVolumeStatsByVolume",
"ListVolumeStatsByVolumeAccessGroup",
"ListVolumes",
"ListVolumesForAccount",
"ModifyAccount",
```

```
"ModifyBackupTarget",
"ModifyClusterAdmin",
"ModifyClusterFullThreshold",
"ModifyClusterInterfacePreference",
"ModifyGroupSnapshot",
"ModifyInitiators",
"ModifyKeyServerKmip",
"ModifyQoSPolicy",
"ModifySchedule",
"ModifySnapMirrorEndpoint",
"ModifySnapMirrorEndpointUnmanaged",
"ModifySnapMirrorRelationship",
"ModifySnapshot",
"ModifyStorageContainer",
"ModifyVirtualNetwork",
"ModifyVolume",
"ModifyVolumeAccessGroup",
"ModifyVolumeAccessGroupLunAssignments",
"ModifyVolumePair",
"ModifyVolumes",
"PurgeDeletedVolume",
"PurgeDeletedVolumes",
"QuiesceSnapMirrorRelationship",
"RemoveAccount",
"RemoveBackupTarget",
"RemoveClusterAdmin",
"RemoveClusterPair",
"RemoveDrives",
"RemoveInitiatorsFromVolumeAccessGroup",
"RemoveKeyServerFromProviderKmip",
"RemoveNodes",
"RemoveSSLCertificate",
"RemoveVirtualNetwork",
"RemoveVolumePair",
"RemoveVolumesFromVolumeAccessGroup",
"ResetDrives",
"ResetNetworkConfig",
"ResetNode",
"ResetSupplementalTlsCiphers",
"RestartNetworking",
"RestartServices",
"RestoreDeletedVolume",
"ResumeSnapMirrorRelationship",
"ResyncSnapMirrorRelationship",
"RollbackToGroupSnapshot",
"RollbackToSnapshot",
```

```

    "SecureEraseDrives",
    "SetClusterConfig",
    "SetClusterStructure",
    "SetConfig",
    "SetDefaultQoS",
    "SetLoginBanner",
    "SetLoginSessionInfo",
    "SetNetworkConfig",
    "SetNtpInfo",
    "SetProtectionDomainLayout",
    "SetRemoteLoggingHosts",
    "SetSSLCertificate",
    "SetSnmpACL",
    "SetSnmpInfo",
    "SetSnmpTrapInfo",
    "SetSupplementalTlsCiphers",
    "Shutdown",
    "SnmpSendTestTraps",
    "StartBulkVolumeRead",
    "StartBulkVolumeWrite",
    "StartClusterPairing",
    "StartVolumePairing",
    "TestAddressAvailability",
    "TestConnectEnsemble",
    "TestConnectMvip",
    "TestConnectSvip",
    "TestDrives",
    "TestHardwareConfig",
    "TestKeyProviderKmip",
    "TestKeyServerKmip",
    "TestLdapAuthentication",
    "TestLocalConnectivity",
    "TestLocateCluster",
    "TestNetworkConfig",
    "TestPing",
    "TestRemoteConnectivity",
    "UpdateBulkVolumeStatus",
    "UpdateIdpConfiguration",
    "UpdateSnapMirrorRelationship"
],
"currentVersion": "12.0",
"supportedVersions": [
    "1.0",
    "2.0",
    "3.0",
    "4.0",

```

```
        "5.0",  
        "5.1",  
        "6.0",  
        "7.0",  
        "7.1",  
        "7.2",  
        "7.3",  
        "7.4",  
        "8.0",  
        "8.1",  
        "8.2",  
        "8.3",  
        "8.4",  
        "8.5",  
        "8.6",  
        "8.7",  
        "9.0",  
        "9.1",  
        "9.2",  
        "9.3",  
        "9.4",  
        "9.5",  
        "9.6",  
        "10.0",  
        "10.1",  
        "10.2",  
        "10.3",  
        "10.4",  
        "10.5",  
        "10.6",  
        "10.7",  
        "11.0",  
        "11.1",  
        "11.3",  
        "11.5",  
        "11.7",  
        "11.8",  
        "12.0"  
    ]  
}  
}
```

ObtenerResultadoAsíncrono

Puedes usar `GetAsyncResult` para recuperar el resultado de las llamadas a métodos asíncronos. Algunas llamadas a métodos requieren cierto tiempo para ejecutarse y es

posible que no hayan finalizado cuando el sistema envíe la respuesta inicial. Para obtener el estado o el resultado de la llamada al método, utilice `GetAsyncResult` para consultar el valor `asyncHandle` devuelto por el método.

`GetAsyncResult` Devuelve el estado general de la operación (en curso, completada o con 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 el parámetro `keepResult` no existe o es falso, el `asyncHandle` se vuelve inactivo cuando se devuelve el resultado, y los intentos posteriores de consultar ese `asyncHandle` devuelven un error. Puedes mantener activo el `asyncHandle` para futuras consultas configurando el parámetro `keepResult` en verdadero.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
manejador asíncrono	Un valor que fue devuelto por la llamada al método asíncrono original.	entero	Ninguno	Sí
mantenerResultado	Si es cierto, <code>GetAsyncResult</code> no elimina el resultado asíncrono al devolverlo, lo que permite realizar consultas futuras a ese <code>asyncHandle</code> .	booleano	FALSO	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
estado	Estado de la llamada al método asíncrono. Valores posibles: • En ejecución: El método aún se está ejecutando. • completo: El método ha finalizado y el resultado o error está disponible.	cadena

Nombre	Descripción	Tipo
resultado	Si el método asíncrono se completó correctamente, este es el resultado de la operación asíncrona. Si la operación asíncrona falló, este miembro no está presente.	cadena
error	Si el estado es completo y el método asíncrono falló, este miembro incluye los detalles del error. Si la operación asíncrona tuvo éxito, este miembro no está presente.	cadena
tipo de resultado	El tipo de operación que realiza o realizaba la llamada al método asíncrono.	cadena
detalles	Si el estado es "en ejecución", este miembro incluye información relevante para el funcionamiento actual del método. Si el método asíncrono no se está ejecutando, este miembro no está presente.	Objeto JSON
crearTiempo	La hora en que se llamó al método asíncrono, en formato UTC+0.	cadena de fecha ISO 8601
última actualización	La hora en que se actualizó por última vez el estado del método asíncrono, en formato UTC+0.	cadena de fecha ISO 8601

Nota: El valor de retorno de `GetAsyncResult` es esencialmente una versión anidada de la respuesta JSON estándar con un campo de estado adicional.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
[/asyncrests/1]",
    "name": "xDBNoSuchPath"
  },
  "id": 1
}
```

Si "response" fuera el objeto de respuesta JSON de la llamada a GetAsyncResult, entonces "response.error" correspondería a un error con el propio método GetAsyncResult (como consultar un asyncHandle inexistente).

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 "response.result.error" correspondería a un resultado de error de la llamada al método original.

Ejemplo de respuesta: éxito de la tarea asíncrona

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"
  }
}
```

El valor “response.result.result” es el valor devuelto por la llamada al método original si la llamada se completó correctamente.

Nueva versión

9,6

Obtener estadísticas completas

La ingeniería de NetApp utiliza `GetCompleteStats` Método API para probar nuevas funcionalidades. Los datos devueltos de `GetCompleteStats` No está documentado, cambia con frecuencia y no se garantiza su exactitud. No deberías usar `GetCompleteStats` para recopilar datos de rendimiento o cualquier otra integración de gestión con un clúster de almacenamiento que ejecute el software Element.

Utilice los siguientes métodos de API compatibles para recuperar información estadística:

- [Obtener estadísticas de volumen](#)
- [Obtener estadísticas del clúster](#)
- [Obtener estadísticas del nodo](#)
- [GetDriveStats](#)

Nueva versión

9,6

Obtener límites

Puedes usar el `GetLimits` Método para obtener los valores límite establecidos por la API. Estos valores pueden cambiar entre versiones de Element, pero no cambian sin una actualización del sistema. Conocer los valores límite establecidos por la API puede

resultar útil al escribir scripts de API para herramientas orientadas al usuario.



El `GetLimits` El método devuelve los límites para la versión actual del software, independientemente de la versión del punto de conexión de la API utilizada para pasar el método.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método devuelve un objeto JSON con pares nombre-valor que contienen los límites de la API.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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

```

```

}

```

```

}

```

Obtener origen

Puedes usar el `GetOrigin` Método para obtener el certificado de origen del lugar donde se construyó el nodo.

Parámetros



Este método devuelve "null" si no existe un certificado 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 para este método son similares al siguiente ejemplo:

```
{
  "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"
}
]
```

Nueva versión

9,6

GetRawStats

La ingeniería de NetApp utiliza `GetRawStats` Método API para probar nuevas funcionalidades. Los datos devueltos de `GetRawStats` No está documentado, cambia con frecuencia y no se garantiza su exactitud. No deberías usar `GetRawStats` para recopilar datos de rendimiento o cualquier otra integración de gestión con un clúster de almacenamiento que ejecute el software Element.

Utilice los siguientes métodos de API compatibles para recuperar información estadística:

- [Obtener estadísticas de volumen](#)
- [Obtener estadísticas del clúster](#)
- [Obtener estadísticas del nodo](#)
- [GetDriveStats](#)

Nueva versión

9,6

ListAsyncResults

Puedes usar `ListAsyncResults` para listar los resultados de todos los métodos asíncronos que se están ejecutando actualmente y los que han finalizado en el sistema. Consultar resultados asíncronos con `ListAsyncResults` no provoca que caduquen los `asyncHandles` completados; puede usar `GetAsyncResult` para consultar cualquiera de los `asyncHandles` devueltos por `ListAsyncResults` .

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
tipos de resultados asíncronos	Una lista opcional de tipos de resultados. Puedes utilizar esta lista para restringir los resultados únicamente a estos tipos de operaciones. Valores posibles: • DriveAdd: Operaciones que implican que el sistema agregue una unidad al clúster. • BulkVolume: Operaciones de copia entre volúmenes, como copias de seguridad o restauraciones. • Clonar: Operaciones de clonación de volúmenes. • Extracción de unidad: Operaciones que implican que el sistema copie datos de una unidad como preparación para su extracción del clúster. • RtfiPendingNode: Operaciones que implican la instalación por parte del sistema de software compatible en un nodo antes de agregarlo al clúster.	matriz de cadenas	Ninguno	No
504				

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
manejadores asíncronos	Una matriz de resultados de métodos asíncronos serializados.	matriz de objetos JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      },
      ...
    ]
  }
}
```

Nueva versión

9,6

Encuentra más información

[ObtenerResultadoAsíncrono](#)

Métodos de la API de cuentas

Agregar cuenta

Puedes usar `AddAccount` para agregar una nueva cuenta al sistema. También puede utilizar este método para crear nuevos volúmenes en la nueva cuenta a medida que se crea la cuenta. La configuración del protocolo de autenticación por desafío-respuesta (CHAP) que especifique 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	Requerido
<code>attributes</code>	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
<code>enableChap</code>	Especifica si las credenciales de la cuenta CHAP pueden ser utilizadas por un iniciador para acceder a los volúmenes.	booleano	verdadero	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
initiatorSecret	El secreto CHAP que debe usar el iniciador. Este secreto debe tener entre 12 y 16 caracteres de longitud y debe ser impenetrable. La clave secreta CHAP del iniciador debe ser única y no puede ser la misma que la clave secreta CHAP del destino. Si no se especifica, se crea un secreto aleatorio.	cadena	Ninguno	No
targetSecret	La clave secreta CHAP que se utilizará para el objetivo (autenticación CHAP mutua). Este secreto debe tener entre 12 y 16 caracteres de longitud y debe ser impenetrable. La clave secreta CHAP de destino debe ser única y no puede ser la misma que la clave secreta 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 de retorno:

Nombre	Descripción	Tipo
cuenta	Un objeto que contiene información sobre la cuenta recién creada.	cuenta
ID de cuenta	El ID del objeto de cuenta recién creado.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}
```

Nueva versión

9,6

ObtenerCuentaPorID

Puedes usar `GetAccountByID` Para obtener detalles sobre una cuenta específica, dado su ID de cuenta.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de cuenta	El ID de la cuenta de la que se desea obtener información.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
cuenta	Detalles de la cuenta.	cuenta

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

ObtenerCuentaPorNombre

Puedes usar `GetAccountByName` Para obtener detalles sobre una cuenta específica, dado su nombre de usuario.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nombre de usuario	Nombre de usuario de la cuenta.	cadena	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
cuenta	Detalles de la cuenta.	cuenta

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

Obtén la eficiencia de la cuenta

Puedes usar `GetAccountEfficiency` para obtener estadísticas de eficiencia sobre una cuenta de volumen. Este método devuelve información de eficiencia únicamente para la cuenta que se proporciona como parámetro.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de cuenta	Especifica la cuenta de volumen para la que se devuelven las estadísticas de eficiencia.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
compresión	Cantidad de espacio ahorrado mediante la compresión de datos para todos los volúmenes de la cuenta. Se expresa como una relación donde un valor de "1" significa que los datos se han almacenado sin compresión.	flotar
deduplicación	La cantidad de espacio ahorrado al no duplicar los datos de todos los volúmenes de la cuenta. Expresado como una proporción.	flotar
volúmenes faltantes	Los volúmenes de los que no se pudieron obtener datos de eficiencia. La falta de volúmenes puede deberse a que el ciclo de recolección de basura (GC) tenga menos de una hora de antigüedad, a una pérdida temporal de conectividad de red o a servicios reiniciados desde el ciclo de GC.	matriz de enteros

Nombre	Descripción	Tipo
aprovisionamiento ligero	La proporción de espacio utilizado con respecto a la cantidad de espacio asignado para almacenar datos. Expresado como una proporción.	flotar
marca de tiempo	Último momento en que se recopilaban datos de eficiencia después de la recolección de basura (GC), en formato UTC+0.	cadena de fecha ISO 8601

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

Lista de cuentas

Puedes usar `ListAccounts` Para obtener la lista completa de cuentas de inquilinos de almacenamiento, con soporte de paginación opcional. Las cuentas de elementos permiten el acceso a los volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
incluir contenedores de almacenamiento	Los contenedores de almacenamiento de volúmenes virtuales se incluyen en la respuesta de forma predeterminada. Para excluir los contenedores de almacenamiento, establezca el valor en falso.	booleano	verdadero	No
ID de cuenta de inicio	ID de cuenta inicial a devolver. Si no existe ninguna cuenta con este ID de cuenta, se utiliza la siguiente cuenta en orden de ID de cuenta como inicio de la lista. Para navegar por la lista, pase el <code>accountID</code> de la última cuenta en la respuesta anterior + 1.	entero	Ninguno	No
límite	Número máximo de objetos de cuenta a devolver.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo

cuentas	La lista de cuentas.	cuenta formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}
```

Nueva versión

9,6

Modificar cuenta

Puedes usar el `ModifyAccount` Método para modificar una cuenta existente.

Al bloquear una cuenta, se terminan inmediatamente todas las conexiones existentes desde esa cuenta. Cuando se modifican los ajustes CHAP de una cuenta, las conexiones existentes permanecen activas y los nuevos ajustes CHAP se utilizan en las conexiones o reconexiones posteriores. Para borrar los atributos de una cuenta, especifique {} para el parámetro de atributos.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de cuenta	ID de cuenta para la cuenta que se va a modificar.	entero	Ninguno	Sí
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
habilitarCapítulo	Especifica si las credenciales de la cuenta CHAP pueden ser utilizadas por un iniciador para acceder a los volúmenes.	booleano	Ninguno	No
iniciadorSecreto	El secreto CHAP que debe usar el iniciador. Este secreto debe tener entre 12 y 16 caracteres y ser impenetrable. La clave secreta CHAP del iniciador debe ser única y no puede ser la misma que la clave secreta CHAP del destino.	cadena	Ninguno	No
estado	Estado de la cuenta. Valores posibles: • activo: La cuenta está activa y se permiten conexiones. • bloqueado: La cuenta está bloqueada y las conexiones están rechazadas.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
secreto del objetivo	La clave secreta CHAP que se utilizará para el objetivo (autenticación CHAP mutua). Este secreto debe tener entre 12 y 16 caracteres y ser impenetrable. La clave secreta CHAP de destino debe ser única y no puede ser la misma que la clave secreta 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 de retorno:

Nombre	Descripción	Tipo
cuenta	Un objeto que contiene información sobre la cuenta modificada.	cuenta

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo. En este ejemplo, los atributos se borran especificándolos con {}:


```
{
  "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": "rxel23b567890"
  }
}
```

Nueva versión

9,6

Eliminar cuenta

Puedes usar el `RemoveAccount` Método para eliminar una cuenta existente. Debe eliminar y purgar todos los volúmenes asociados a la cuenta mediante `DeleteVolume` antes de que puedas eliminar la cuenta. Si aún hay volúmenes de la cuenta pendientes de eliminación, no podrá utilizarlos. `RemoveAccount` para eliminar la cuenta.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de cuenta	El ID de la cuenta que se va a eliminar.	entero	Ninguno	Sí

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo.

```
{
  "method": "RemoveAccount",
  "params": {
    "accountID" : 25
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : { }
}
```

Nueva versión

9,6

Encuentra más información

[Eliminar volumen](#)

Métodos de la API de administrador

Agregar administrador de clúster

Puedes usar el `AddClusterAdmin` Método para agregar 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 clúster son

completamente independientes y no guardan relación con las cuentas de inquilino estándar.

Cada administrador de clúster puede estar restringido a un subconjunto de la API. Debe utilizar varias cuentas de administrador de clúster para diferentes usuarios y aplicaciones. Como buena práctica, otorgue a cada administrador del clúster los permisos mínimos necesarios; esto reduce el impacto potencial de una vulneración de las credenciales.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
acceso	Controla qué métodos puede usar el administrador del clúster.	matriz de cadenas	Ninguno	Sí
aceptar el EULA	Acepte el Acuerdo de Licencia de Usuario Final. Establézcalo en verdadero para agregar 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	Lista de pares nombre/valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
contraseña	Contraseña utilizada para autenticar al administrador de este clúster.	cadena	Ninguno	Sí
nombre de usuario	Nombre de usuario único para este administrador de clúster. Debe tener entre 1 y 1024 caracteres de longitud.	cadena	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
ID de administrador del clúster	ID de administrador de clúster para el administrador de clúster recién creado.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}
```

Nueva versión

9,6

Encuentra más información

[Control de acceso](#)

ObtenerAdministradorDeClústerActual

Puedes usar el `GetCurrentClusterAdmin` Método para devolver información sobre el administrador de clúster principal actual. El administrador principal del clúster se creó cuando se creó el clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
administrador del clúster	Información sobre el administrador del clúster.	administrador del clúster

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  }
}
```

Nueva versión

10,0

Obtener banner de inicio de sesión

Puedes usar el `GetLoginBanner` Método para obtener el banner de Términos de uso actualmente activo que los usuarios ven cuando inician sesión en la interfaz web de Element.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
bandera	Texto actual del banner de Condiciones de uso. Este valor puede contener texto incluso cuando el banner esté desactivado.	cadena
activado	Estado del banner de Condiciones de uso. Valores posibles: • Verdadero: El banner de Términos de uso se muestra al iniciar sesión en la interfaz web. • Falso: El banner de Condiciones de uso no se muestra al iniciar sesión en la interfaz web.	booleano

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
  }
}
```

Nueva versión

10,0

Lista de administradores de clúster

Puedes usar el `ListClusterAdmins` Método para devolver la lista de todos los administradores 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 principal del clúster es el administrador que se creó cuando se creó el clúster. También se pueden crear administradores LDAP al configurar un sistema LDAP en el clúster.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
mostrar oculto	Muestra los usuarios administradores de clúster ocultos, como el administrador SNMP.	booleano	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo

administradores de clúster	Información sobre todos los administradores de clúster y LDAP que existen para un clúster.	administrador del clúster formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}

```

Nueva versión

9,6

Modificar administrador de clúster

Puedes usar 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 identidad (IdP) de terceros. No se puede cambiar el acceso para la cuenta de administrador del clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
acceso	Controla qué métodos puede usar este administrador de clúster.	matriz de cadenas	Ninguno	No
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
ID de administrador del clúster	ClusterAdminID para que el administrador del clúster, el administrador del clúster LDAP o el administrador del clúster IdP lo modifiquen.	entero	Ninguno	Sí
contraseña	Contraseña utilizada para autenticar al administrador de este clúster. Este parámetro no se aplica a un administrador de clúster LDAP o IdP.	cadena	Ninguno	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ModifyClusterAdmin",
  "params": {
    "clusterAdminID" : 2,
    "password"      : "7925Brc429a"
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1
  "result" : { }
}
```

Nueva versión

9,6

Encuentra más información

[Control de acceso](#)

Eliminar administrador del clúster

Puedes usar el `RemoveClusterAdmin` Método para eliminar un administrador de clúster, un administrador de clúster LDAP o un administrador de clúster de proveedor de identidad (IdP) de terceros. No puedes eliminar la cuenta de administrador del clúster "admin".

Parámetro

Cuando se elimina un administrador de clúster IdP que tiene sesiones autenticadas asociadas con un proveedor de identidad IdP de terceros, esas sesiones se cerrarán 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 eliminado coincidía con alguno de los múltiples administradores del clúster IdP de los atributos SAML de un usuario determinado. El conjunto restante de administradores de clúster IdP coincidentes da como resultado un conjunto reducido de derechos de acceso agregados. Los demás tipos de usuarios administradores del clúster se desconectan cuando se eliminan sus administradores del clúster.

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de administrador del clúster	ID de administrador del clúster para eliminar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "RemoveClusterAdmin",
  "params": {
    "clusterAdminID" : 2
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1
  "result" : { }
}
```

Nueva versión

9,6

Establecer banner de inicio de sesión

Puedes usar el `SetLoginBanner` Método para configurar el banner de Términos de uso que los usuarios ven cuando inician sesión en la interfaz web de Element.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
bandera	El texto deseado para el banner de Términos de Uso. La longitud máxima permitida es de 4.096 caracteres.	cadena	Ninguno	No
activado	Estado del banner de Condiciones de uso. Valores posibles: • `true` El banner de Condiciones de uso se muestra al iniciar sesión en la interfaz web. • `false` El banner de Condiciones de uso no se muestra al iniciar sesión en la interfaz web.	booleano	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
bandera	Texto actual del banner de Condiciones de uso. Este valor puede contener texto incluso cuando el banner esté desactivado.	cadena
activado	Estado del banner de Condiciones de uso. Valores posibles: • Verdadero: El banner de Términos de uso se muestra al iniciar sesión en la interfaz web. • Falso: El banner de Condiciones de uso no se muestra al iniciar sesión en la interfaz web.	booleano

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
  }
}
```

Nueva versión

10,0

Métodos de la API de clúster

Agregar nodos

Puedes usar el `AddNodes` Método para agregar uno o más nodos nuevos a un clúster.

Cuando un nodo que no está configurado se inicia por primera vez, se le solicita que configure el nodo. Una vez configurado el nodo, queda registrado como "nodo pendiente" en el clúster. Los clústeres de almacenamiento que ejecutan el software Element crean automáticamente una imagen de un nodo a la versión del clúster. Cuando agregas un nodo pendiente, la respuesta del método incluye un valor `asyncHandle` que puedes usar con el `GetAsyncResult` Método para consultar el estado del proceso de creación automática de imágenes.

El proceso para agregar un nodo Fibre Channel es el mismo que para agregar nodos de almacenamiento Element iSCSI a un clúster. Los nodos Fibre Channel se registran en el sistema con un `NodeID`. Cuando se vuelven accesibles, se les coloca en estado de "nodo pendiente". El `ListAllNodes` El método devolverá el

pendingNodeID para los nodos iSCSI, así como cualquier nodo Fibre Channel que esté disponible para agregar al clúster.

Cuando se agrega un nodo a un clúster que se ha configurado para redes virtuales, el sistema requiere un número suficiente de direcciones IP de almacenamiento virtual para asignar una IP virtual al nuevo nodo. Si no hay direcciones IP virtuales disponibles para el nuevo nodo, AddNode La operación falla. Utilice el ModifyVirtualNetwork Método para agregar más direcciones IP de almacenamiento a su red virtual.

Una vez que agregue un nodo, todas las unidades del nodo estarán disponibles y podrá agregarlas mediante la opción AddDrives Método para aumentar la capacidad de almacenamiento del clúster.



Pueden pasar varios segundos después de agregar un nuevo nodo para que se inicie y registre sus unidades como disponibles.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
autoinstalación	Si es cierto, se realizará un restablecimiento a la imagen de fábrica (RTFI) en el nodo al agregarlo. El comportamiento predeterminado es realizar RTFI. Si el cEnableAutoInstall La constante de clúster es falsa; tiene prioridad sobre este parámetro. Si hay una actualización en curso, el proceso RTFI no se llevará a cabo independientemente del valor de este parámetro.	booleano	Ninguno	No
nodos pendientes	NodeIDs pendientes para los nodos que se agregarán. Puede listar todos los nodos pendientes utilizando el método ListPendingNodes.	matriz de enteros	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
autoinstalación	Si los nodos añadidos se devuelven o no a la imagen de fábrica.	booleano
nodos	Una matriz de objetos que relaciona el "pendingNodeID" anterior con el "nodeID". Cuando agrega un nodo pendiente que ejecuta una versión de software incompatible, esta matriz incluye un valor asyncHandle que puede usar con el método GetAsyncResult para consultar el estado del proceso de creación automática de imágenes.	matriz de objetos JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}

```

Nueva versión

9,6

Encuentra más información

- [Agregar unidades](#)
- [ObtenerResultadoAsíncrono](#)
- [Lista todos los nodos](#)
- [Modificar red virtual](#)

Borrar fallos de clúster

Puedes usar el `ClearClusterFaults` Método para borrar información sobre fallos actuales y detectados previamente. Se pueden borrar tanto las averías resueltas como las no resueltas.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
Tipos de fallos	Determina los tipos de fallas que se deben corregir. Valores posibles: • actual: Fallos detectados actualmente que aún no se han resuelto. • Resueltos: Fallos que fueron detectados y resueltos previamente. • Todas: Tanto las averías actuales como las resueltas. El estado de la falla se puede determinar mediante el campo “resuelto” del objeto de falla.	cadena	resuelto	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ClearClusterFaults",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nueva versión

9,6

CrearPreferenciaDeInterfazDeClúster

El `CreateClusterInterfacePreference` Este método permite que los sistemas integrados con clústeres de almacenamiento que ejecutan el software Element creen y almacenen 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	Requerido
nombre	El nombre de la preferencia de interfaz del clúster.	cadena	Ninguno	Sí
valor	El valor de la preferencia de interfaz del clúster.	cadena	Ninguno	Sí

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
    "method": "CreateClusterInterfacePreference",
    "params": {
        "name": "prefname",
        "value": "testvalue"
    },
    "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {}
}
```

Nueva versión

11,0

EliminarPreferenciaDeInterfazDeClúster

El `DeleteClusterInterfacePreference` Este método permite a los sistemas integrados con clústeres de almacenamiento que ejecutan el software Element 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	Requerido
nombre	Nombre de la preferencia de interfaz de clúster que se va a eliminar.	cadena	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DeleteClusterInterfacePreference",
  "params": {
    "name": "prefname"
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nueva versión

11,0

Deshabilitar función

Puedes usar el `DisableFeature` método para deshabilitar el `VolumeLoadBalanceOnActualIOPS` característica. `VolumeLoadBalanceOnActualIOPS` está desactivado por defecto.

Si intenta desactivar otra función, como VVols, aparece el siguiente mensaje de error:



```
{"error":{"code":500,"message":"VolumeLoadBalanceOnActualIOPS is
the only feature that can be
disabled","name":"xAPINotPermitted"},"id":null}
```

Parámetro

Este método tiene el siguiente parámetro de entrada.

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
característica	Deshabilitar una función del clúster. Valor posible: • `VolumeLoadBalanceOnActualIOPS` Deshabilitar el balanceo de segmentos en IOPS reales en lugar de IOPS mínimas.	cadena	Ninguno	Sí

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DisableFeature",
  "params": {
    "feature" : "VolumeLoadBalanceOnActualIOPS"
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nueva versión

12,8

Habilitar función

Puedes usar el `EnableFeature` Método para habilitar funciones de clúster como VVols que están deshabilitadas de forma predeterminada.

Parámetro

Este método tiene el siguiente parámetro de entrada.



Para los sistemas que ejecutan el software Element 11.x, habilitar los volúmenes virtuales antes o después de configurar la supervisión del dominio de protección hace que la función de dominios de protección del clúster funcione solo a nivel de nodo.

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
característica	Habilitar una función de clúster. Valores posibles: • `fips` Habilitar el cifrado certificado FIPS 140-2 para las comunicaciones HTTPS. • `FipsDrives`: Habilitar la compatibilidad con unidades FIPS 140-2 para el clúster de almacenamiento. • `SnapMirror` Habilite la función de clúster de replicación SnapMirror . • `VolumeLoadBalanceOnActualIOPS` Habilitar el balanceo de segmentos en función de las IOPS reales en lugar de las IOPS mínimas. Disponible a partir del Elemento 12.8. • `vvols` Habilite la función de clúster VVols del software Element.	cadena	Ninguno	Sí

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "EnableFeature",
  "params": {
    "feature" : "vvols"
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nueva versión

9,6

Obtener capacidad del clúster

Puedes usar el `GetClusterCapacity` para devolver mediciones de capacidad de alto nivel para todo un clúster de almacenamiento. Este método devuelve campos que puede utilizar para calcular los índices de eficiencia que se muestran en la interfaz web de Element. Puedes utilizar los cálculos de eficiencia en scripts para obtener los índices de eficiencia para el aprovisionamiento ligero, la deduplicación, la compresión y la eficiencia general.

Cálculos de eficiencia

Utilice las siguientes ecuaciones para calcular el aprovisionamiento ligero, la deduplicación y la compresión. Estas ecuaciones se aplican al Elemento 8.2 y posteriores.

- Factor de aprovisionamiento delgado = (bloques no nulos + bloques nulos) / bloques no nulos
- Factor de deduplicación = (bloquesnuceros + bloquesnucerosinstantáneos) / bloquesúnicos
- Factor de compresión = (bloques únicos * 4096) / (espacio usado de bloques únicos * 0,93)

Cálculo de la tasa de eficiencia global

Utilice la siguiente ecuación para calcular la eficiencia general del clúster utilizando los resultados de los cálculos de eficiencia de aprovisionamiento ligero, deduplicación y compresión.

- Factor de eficiencia = Factor de aprovisionamiento ligero * Factor de deduplicación * Factor de compresión

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
capacidad del clúster	Medidas de capacidad del clúster de almacenamiento.	capacidad del clúster

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
  }
}
```

Nueva versión

9,6

Umbral completo del clúster

Puedes usar el `GetClusterFullThreshold` Método para visualizar las etapas establecidas para los niveles de plenitud del clúster. Este método devuelve todas las métricas de plenitud del clúster.



Quando un clúster alcanza la etapa de Error por llenado del clúster de bloques, las IOPS máximas en todos los volúmenes se reducen linealmente hasta las IOPS mínimas del volumen a medida que el clúster se acerca a la etapa Crítica. Esto ayuda a evitar que el clúster alcance la etapa crítica de llenado del clúster de bloques.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
plenitud de bloque	El nivel actual calculado de llenado de bloques del clúster. • etapa1Feliz: Sin alertas ni condiciones de error. Corresponde al estado Saludable en la interfaz web. • stage2Aware: Sin alertas ni condiciones de error. Corresponde al estado Saludable en la interfaz web. • Stage3Low: Su sistema no puede proporcionar protección de datos redundante ante dos fallos de nodo no simultáneos. Corresponde al estado Advertencia en la interfaz web. Puede configurar este nivel en la interfaz web (por defecto, el sistema activa esta alerta cuando la capacidad está un 3% por debajo del estado de Error). • Etapa 4 Crítica: El sistema no es capaz de proporcionar protección de datos redundante ante el fallo de un solo nodo. No se pueden crear nuevos volúmenes ni clones. Corresponde al estado Error en la interfaz de usuario de Element. • etapa5CompletamenteConsumido: Completamente consumido. El clúster es de solo lectura y las conexiones iSCSI se mantienen, pero todas las escrituras están suspendidas. Corresponde al estado Crítico en la interfaz de usuario de Element.	cadena

Nombre	Descripción	Tipo
plenitud	Refleja el nivel más alto de plenitud entre "plenitud de bloque" y "plenitud de metadatos".	cadena
factor de sobreaprovisionamiento de metadatos máximo	Un valor representativo del número de veces que se puede sobreaprovisionar el espacio de metadatos en relación con la cantidad de espacio disponible. Por ejemplo, si hubiera suficiente espacio de metadatos para almacenar 100 TiB de volúmenes y este número se estableciera en 5, entonces se podrían crear volúmenes por valor de 500 TiB.	entero

Nombre	Descripción	Tipo
metadataFullness	El nivel actual calculado de integridad de metadatos del clúster. - etapa1Feliz: Sin alertas ni condiciones de error. Corresponde al estado Saludable en la interfaz web. - stage2Aware: Sin alertas ni condiciones de error. Corresponde al estado Saludable en la interfaz web. - Stage3Low: Su sistema no puede proporcionar protección de datos redundante ante dos fallos de nodo no simultáneos. Corresponde al estado Advertencia en la interfaz web. Puede configurar este nivel en la interfaz web (por defecto, el sistema activa esta alerta cuando la capacidad está un 3% por debajo del estado de Error). - Etapas 4 Crítica: El sistema no es capaz de proporcionar protección de datos redundante ante el fallo de un solo nodo. No se pueden crear nuevos volúmenes ni clones. Corresponde al estado Error en la interfaz de usuario de Element. - etapa5CompletamenteConsumido: Completamente consumido. El clúster es de solo lectura y las conexiones iSCSI se mantienen, pero todas las escrituras están suspendidas. Corresponde al estado Crítico en la interfaz de usuario de Element.	cadena
porcentaje de reserva usada de la porción	Condición de error. Se activa una alerta del sistema si la utilización de la porción reservada es mayor que este valor.	entero

Nombre	Descripción	Tipo
stage2AwareThreshold	Estado de conciencia. El valor que se establece para el nivel umbral del clúster de etapa 2.	entero
stage2BlockThresholdBytes	El número de bytes que utiliza el clúster en el que se dará una condición de etapa 2.	entero
stage2MetadataThresholdBytes	El número de bytes de metadatos que utiliza el clúster en el que se alcanzará una condición de llenado de etapa 2.	
stage3BlockThresholdBytes	El número de bytes de almacenamiento que utiliza el clúster en el que se alcanzará una condición de llenado de etapa 3.	entero
stage3BlockThresholdPercent	El valor porcentual establecido para la etapa 3. Al alcanzar este porcentaje de carga, se publica una advertencia en el registro de alertas.	entero
stage3LowThreshold	Condición de error. El umbral en el que se genera una alerta del sistema debido a la baja capacidad de un clúster.	entero
stage3MetadataThresholdBytes	El número de bytes de metadatos utilizados por el clúster en el que existirá una condición de llenado de etapa 3.	entero
stage3MetadataThresholdPercent	Porcentaje establecido para la etapa 3 de integridad de metadatos. Al alcanzar este porcentaje de carga, se publicará una advertencia en el registro de alertas.	entero
stage4BlockThresholdBytes	El número de bytes de almacenamiento que utiliza el clúster en el que se alcanzará una condición de llenado de etapa 4.	entero

Nombre	Descripción	Tipo
stage4CriticalThreshold	Condición de error. El umbral en el que se crea una alerta del sistema para advertir sobre una capacidad críticamente baja en un clúster.	entero
stage4MetadataThresholdBytes	El número de bytes de metadatos utilizados por el clúster en el que existirá una condición de llenado de etapa 4.	entero
stage5BlockThresholdBytes	El número de bytes de almacenamiento utilizados por el clúster en el que existirá una condición de llenado de etapa 5.	entero
stage5MetadataThresholdBytes	El número de bytes de metadatos utilizados por el clúster en el que existirá una condición de llenado de etapa 5.	entero
sumaTotalDeBytesDelClúster	La capacidad física del clúster, medida en bytes.	entero
sumaTotalMetadataClusterBytes	La cantidad total de espacio que se puede utilizar para almacenar metadatos.	entero
suma de bytes del clúster usados	El número de bytes de almacenamiento utilizados en el clúster.	entero
sumaUsedMetadataClusterBytes	La cantidad de espacio utilizado en las unidades de volumen para almacenar metadatos.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}
```

Nueva versión

9,6

Encuentra más información

[Modificar UmbralCompletoDeClúster](#)

Obtener información de hardware del clúster

Puedes usar el `GetClusterHardwareInfo` Método para recuperar el estado del hardware y la información de todos los nodos Fibre Channel, nodos iSCSI y unidades del clúster. Esto generalmente incluye fabricantes, vendedores, versiones y otra información de identificación de hardware asociada.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
tipo	Incluya solo uno de los siguientes tipos de información de hardware en la respuesta. Valores posibles: • unidades: Las listas solo proporcionan información en la respuesta. • nodos: Enumera únicamente la información de los nodos en la respuesta. • todo: Incluye información tanto de la unidad como del nodo en la respuesta. Si se omite este parámetro, se asume el tipo "todos".	cadena	todo	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Información de hardware del clúster	Información de hardware para todos los nodos y unidades del clúster. Cada objeto en esta salida está etiquetado con el nodeID del nodo dado.	Información de hardware

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetClusterHardwareInfo",
  "params": {
    "type": "all"
  },
  "id": 1
}
```

Ejemplo de respuesta

Debido a la extensión de este ejemplo de respuesta, se documenta en un tema complementario.

Nueva versión

9,6

Encuentra más información

[Obtener información de hardware del clúster](#)

Obtener información del clúster

Puedes usar el `GetClusterInfo` Método para devolver información de configuración sobre el clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Información del clúster	Información del clúster.	Información del clúster

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetClusterInfo",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": null,
  "result": {
    "clusterInfo": {
      "attributes": {},
      "defaultProtectionScheme": "doubleHelix",
      "enabledProtectionSchemes": [
        "doubleHelix"
      ],
      "encryptionAtRestState": "disabled",
      "ensemble": [
        "10.10.10.32",
        "10.10.10.33",
        "10.10.10.34",
        "10.10.10.35",
        "10.10.10.36"
      ],
      "mvip": "10.10.11.225",
      "mvipInterface": "Bond1G",
      "mvipNodeID": 1,
      "mvipVlanTag": "0",
      "name": "ClusterName",
      "repCount": 2,
      "softwareEncryptionAtRestState": "disabled",
      "supportedProtectionSchemes": [
        "doubleHelix"
      ],
      "svip": "10.10.10.111",
      "svipInterface": "Bond10G",
      "svipNodeID": 1,
      "svipVlanTag": "0",
      "uniqueID": "ahf7",
      "uuid": "bcfd04b6-9151-4b3a-a6fa-bca22dd145cd",
      "volumeLoadBalanceOnActualIopsState": "enabled"
    }
  }
}
```

Nueva versión

9,6

GetClusterInterfacePreference

El `GetClusterInterfacePreference` Este método permite que los sistemas integrados con clústeres de almacenamiento que ejecutan el software Element obtengan información sobre 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	Requerido
nombre	El nombre de la preferencia de interfaz del clúster.	cadena	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
preferencia	El nombre y el valor de la preferencia de interfaz de clúster solicitada.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  }
}

```

Nueva versión

11,0

Obtener ID de nodo maestro del clúster

Puedes usar el `GetClusterMasterNodeID` Método para recuperar el ID del nodo que realiza tareas de administración en todo el clúster y que contiene la dirección IP virtual de almacenamiento (SVIP) y la dirección IP virtual de administración (MVIP).

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
ID de nodo	Identificador del nodo maestro.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```

{
  "method": "GetClusterMasterNodeID",
  "params": {},
  "id" : 1
}

```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1
  "result": {
    "nodeID": 1
  }
}
```

Nueva versión

9,6

Obtener estadísticas del clúster

Puedes usar el `GetClusterStats` Método para recuperar mediciones de actividad de alto nivel para el clúster. Los valores devueltos son acumulativos desde la creación del clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
estadísticas del clúster	Información sobre la actividad del clúster.	estadísticas del clúster

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
  }
}

```

Nueva versión

9,6

ObtenerInformación de versión del clúster

Puedes usar el `GetClusterVersionInfo` Método para recuperar información sobre la versión del software Element que se ejecuta en cada nodo del clúster. Este método también devuelve información sobre los nodos que actualmente están en proceso de actualización de software.

miembros del objeto de información de versión del clúster

Este método tiene los siguientes miembros de objeto:

Nombre	Descripción	Tipo
ID de nodo	Identificador del nodo.	entero
revisión interna del nodo	Versión de software interna del nodo.	cadena
nodeVersion	Versión de software del nodo.	cadena

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
clusterAPIVersion	La versión actual de la API en el clúster.	cadena
versión del clúster	Versión del software Element que se está ejecutando actualmente en el clúster.	cadena
Información de versión del clúster	Lista de nodos del clúster con información de versión para cada nodo.	matriz de objetos JSON
Versión de clúster pendiente	Si está presente, esta es la versión a la que se está actualizando o revirtiendo el software del clúster.	cadena

Nombre	Descripción	Tipo
Información de la versión del software	El estado de una actualización. Miembros del objeto: • versión actual: La versión actual del software en un nodo. • nodeId: ID del nodo que se está actualizando de currentVersion a pendingVersion. Este campo es 0 (cero) si no hay ninguna actualización en curso. • packageName: Nombre del paquete de software que se está instalando. • pendingVersion: La versión del software que se está instalando. • startTime: La fecha y hora en que se inició la instalación, en formato UTC+0.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": ""
    }
  }
}

```

Nueva versión

9,6

Obtener estado de la función

Puedes usar el `GetFeatureStatus` Método para recuperar el estado de una característica de clúster.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
característica	El estado de una característica del clúster. Si no se proporciona ningún valor, el sistema devuelve un estado de todas las características. Valores posibles: • <code>`Vvols`</code> Recuperar el estado de la función de clúster VVols. • <code>`SnapMirror`</code> Recuperar el estado de la función de clúster de replicación SnapMirror . • <code>`Fips`</code> Recuperar el estado de la función de cifrado FIPS 140-2 para comunicación HTTPS. • <code>`FipsDrives`</code> Recuperar el estado de la función de cifrado de unidad FIPS 140-2. • <code>`VolumeLoadBalanceOnActualIOPS`</code> Recuperar el estado del equilibrio de segmentos en función de las IOPS reales en lugar de la función de IOPS mínimas. Disponible a partir del Elemento 12.8.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
características	Una matriz de objetos de características que indica el nombre de la característica y su estado. Miembros del objeto: • característica: (cadena) El nombre de la característica. • habilitado: (booleano) Indica si la función está habilitada o no.	matriz de objetos JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      },
      {
        "enabled": true,
        "feature": "VolumeLoadBalanceOnActualIOPS"
      }
    ]
  }
}

```

Nueva versión

9,6

Obtener información de sesión de inicio de sesión

Puedes usar el `GetLoginSessionInfo` Método para devolver el período de tiempo durante el cual una sesión de autenticación de inicio de sesión es válida tanto para los shells 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 de retorno:

Nombre	Descripción	Tipo
información de sesión de inicio de sesión	Un objeto que contiene el período de expiración de la autenticación. Objetos posibles devueltos: • se acabó el tiempo: El tiempo, en minutos, en que esta sesión caducará. Formateado en H:mm:ss. Por ejemplo: 1:30:00, 20:00, 5:00. Se eliminan todos los ceros y dos puntos iniciales independientemente del formato en que se haya introducido el tiempo de espera.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetLoginSessionInfo",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result" : {
    "loginSessionInfo" : {
      "timeout" : "30:00"
    }
  }
}
```

Nueva versión

9,6

Información del hardware del nodo

Puedes usar el `GetNodeHardwareInfo` Método para devolver toda la información de hardware y el estado del nodo especificado. Esto generalmente incluye fabricantes, vendedores, versiones y otra información de identificación de hardware asociada.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de nodo	El identificador del nodo para el que se solicita información de hardware. Si se especifica un nodo Fibre Channel, se devuelve información sobre él.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
nodoHardwareInfo	Información de hardware para el <code>nodeID</code> especificado. Cada objeto en esta salida está etiquetado con el <code>nodeID</code> del nodo dado.	Información de hardware

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetNodeHardwareInfo",
  "params": {
    "nodeID": 1
  },
  "id" : 1
}
```

Ejemplo de respuesta

Debido a la extensión de este ejemplo de respuesta, se documenta en un tema complementario.

Nueva versión

9,6

Encuentra más información

[GetNodeHardwareInfo \(salida para nodos Fibre Channel\)](#)

[GetNodeHardwareInfo \(salida para iSCSI\)](#)

Obtener estadísticas del nodo

Puedes usar el `GetNodeStats` Método para recuperar las mediciones de actividad de alto nivel para un solo nodo.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de nodo	Especifica el ID del nodo para el que se devolverán las estadísticas.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
estadísticas del nodo	Información de actividad del nodo.	estadísticas del nodo

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:


```
{  
  "method": "GetNodeStats",  
  "params": {  
    "nodeID": 5  
  },  
  "id": 1  
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```

{
  "id" : 1,
  "result" : {
    "nodeStats": {
      "cBytesIn": 1579657943924,
      "cBytesOut": 1683056745816,
      "count": 119529,
      "cpu": 0,
      "cpuTotal": 56289,
      "mBytesIn": 475476878,
      "mBytesOut": 269270423,
      "networkUtilizationCluster": 0,
      "networkUtilizationStorage": 0,
      "nodeHeat": {
        "primaryTotalHeat": 0.00098,
        "recentPrimaryTotalHeat": 0.00099,
        "recentTotalHeat": 0.00099,
        "totalHeat": 0.00098
      },
      "readLatencyUsecTotal": 10125300382,
      "readOps": 15640075,
      "sBytesIn": 1579657943924,
      "sBytesOut": 1683056745816,
      "ssLoadHistogram": {
        "Bucket0": 4873,
        "Bucket1To19": 6301620,
        "Bucket20To39": 396452,
        "Bucket40To59": 142,
        "Bucket60To79": 0,
        "Bucket80To100": 0
      },
      "timestamp": "2024-03-04T20:13:22.105428Z",
      "usedMemory": 106335510528,
      "writeLatencyUsecTotal": 7314512535,
      "writeOps": 59154830
    }
  }
}

```

Nueva versión

9,6

Lista de nodos activos

Puedes usar el `ListActiveNodes` Método para devolver la lista de nodos actualmente activos que se encuentran en el clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
nodos	Lista de nodos activos en el clúster.	nodo formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ListActiveNodes",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Debido a la extensión de este ejemplo de respuesta, se documenta en un tema complementario.

Nueva versión

9,6

Encuentra más información

[Lista de nodos activos](#)

Lista todos los nodos

Puedes usar el `ListAllNodes` Método para listar los nodos activos y pendientes en el clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
nodos	Lista de objetos que describen los nodos activos en el clúster.	nodo
nodos activos pendientes	Lista de objetos que describen los nodos activos pendientes para el clúster.	nodo activo pendienteformación
nodos pendientes	Lista de objetos que describen los nodos pendientes para el clúster.	nodo pendienteformación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": []
  }
}

```

Nueva versión

9,6

ListClusterFaults

Puedes usar el `ListClusterFaults` Método para listar información sobre cualquier fallo detectado en el clúster. Con este método, puede listar tanto las fallas actuales como las fallas 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	Requerido
mejores prácticas	Incluir fallos provocados por una configuración del sistema subóptima. Valores posibles: • verdadero • FALSO	booleano	Ninguno	No
Tipos de fallos	Determina los tipos de fallos que se devuelven. Valores posibles: • actual: Lista de fallos activos y sin resolver. • Resueltos: Enumere las fallas que se detectaron y resolvieron previamente. • Todos: Enumere tanto las fallas actuales como las resueltas. Puedes ver el estado del fallo en el miembro “resuelto” del objeto de fallo.	cadena	todo	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
fallas	Un objeto que describe los fallos del clúster solicitados.	falla

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": [
      {
        "blocksUpgrade": false,
        "clusterFaultID": 3,
        "code": "driveAvailable",
        "data": null,
        "date": "2024-04-03T22:22:56.660275Z",
        "details": "Node ID 1 has 6 available drive(s).",
        "driveID": 0,
        "driveIDs": [],
        "externalSource": "",
        "networkInterface": "",
        "nodeHardwareFaultID": 0,
        "nodeID": 1,
        "resolved": true,
        "resolvedDate": "2024-04-03T22:24:54.598693Z",
        "serviceID": 0,
        "severity": "warning",
        "type": "drive"
      },
      {
        "clusterFaultID": 9,
        "code": "disconnectedClusterPair",
        "data": null,
        "date": "2016-04-26T20:40:08.736597Z",
        "details": "One of the clusters in a pair may have become
misconfigured or disconnected. Remove the local pairing and retry pairing
the clusters. Disconnected Cluster Pairs: []. Misconfigured Cluster Pairs:
[3]",
        "driveID": 0,
        "driveIDs": [],
        "nodeHardwareFaultID": 0,
        "nodeID": 0,
        "resolved": false,
        "resolvedDate": "",
        "serviceID": 0,
        "severity": "warning",
        "type": "cluster"
      }
    ]
  }
}

```


Nueva versión

9,6

Preferencias de interfaz de clúster de lista

El `ListClusterInterfacePreference` Este método permite que los sistemas integrados con clústeres de almacenamiento que ejecutan el software Element enumeren las preferencias de 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 de retorno:

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.	matriz de objetos JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}

```

Nueva versión

11,0

Lista de eventos

Puedes usar el `ListEvents` Método para listar los eventos detectados en el clúster, ordenados del más antiguo al más reciente.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
driveID	Especifica que solo se devolverán los eventos con este ID de unidad.	entero	0	No
endEventID	Identifica el final de un rango de identificadores de eventos que se devolverán.	entero	(ilimitado)	No
Hora de finalización de publicación	Especifica que solo se devolverán los eventos publicados antes de esta hora.	cadena	0	No
Hora de finalización del informe	Especifica que solo se devolverán los eventos reportados antes de esta hora.	cadena	0	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
tipo de evento	Especifica el tipo de eventos que se devolverán. Verevento para posibles tipos de eventos.	cadena	0	No
eventos máximos	Especifica el número máximo de eventos que se devolverán.	entero	(ilimitado)	No
ID de nodo	Especifica que solo se devolverán los eventos con este ID de nodo.	entero		
ID de servicio	Especifica que solo se devolverán los eventos con este ID de servicio.			
ID de evento de inicio	Identifica el inicio de una serie de eventos que se repetirán.	entero	0	No
hora de inicio de publicación	Especifica que solo se devolverán los eventos publicados después de esta hora.	cadena	0	No
hora de inicio del informe	Especifica que solo se devolverán los eventos reportados después de esta hora.	cadena	0	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
eventos	Lista de eventos.	eventoformación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
]
}
}

```

Nueva versión

9,6

Estadísticas de nodo de lista

Puedes usar el `ListNodeStats` Método para visualizar las mediciones de actividad de alto nivel para todos los nodos de almacenamiento en un clúster de almacenamiento.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
estadísticas del nodo	Información de actividad del nodo de almacenamiento.	estadísticas del nodo

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{  
  "method": "ListNodeStats",  
  "params": {},  
  "id" : 1  
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```

{
  "id": 1,
  "result": {
    "nodeStats": {
      "nodes": [
        {
          "cBytesIn": 223022159806,
          "cBytesOut": 206324217921,
          "count": 17274,
          "cpu": 0,
          "cpuTotal": 9796,
          "mBytesIn": 608219007,
          "mBytesOut": 3487659798,
          "networkUtilizationCluster": 0,
          "networkUtilizationStorage": 0,
          "nodeHeat": {
            "primaryTotalHeat": 0.00028,
            "recentPrimaryTotalHeat": 0.0,
            "recentTotalHeat": 0.00097,
            "totalHeat": 0.00138
          },
          "nodeID": 1,
          "readLatencyUSecTotal": 8964,
          "readOps": 29544,
          "sBytesIn": 223022159806,
          "sBytesOut": 206324217921,
          "ssLoadHistogram": {
            "Bucket0": 5083,
            "Bucket1To19": 5637426,
            "Bucket20To39": 19389,
            "Bucket40To59": 156,
            "Bucket60To79": 0,
            "Bucket80To100": 0
          },
          "timestamp": "2024-02-27T18:21:26.183659Z",
          "usedMemory": 104828780544,
          "writeLatencyUSecTotal": 271773335,
          "writeOps": 23898
        }
      ]
    }
  }
}

```

Nueva versión

9,6

Lista de sesiones iSCSI

Puedes usar el `ListISCSISessions` Método para listar la información de conexión iSCSI para los volúmenes del clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
sesiones	Información sobre cada sesión iSCSI.	sesión

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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",
        "authentication": {
          "authMethod": "CHAP",
          "chapAlgorithm": "SHA3_256",
          "chapUsername": "iqn.1994-05.com."redhat:1cf11f3eed3",
          "direction": "two-way"
        },
        "createTime": "2022-10-03T22:02:49.121723Z",
        "driveID": 23,
        "driveIDs": [23],
        "initiator": null,
        "initiatorIP": "10.1.1.1:37138",
        "initiatorName": "iqn.2010-01.net.solidfire.eng:c",
        "initiatorPortName": "iqn.2010-
01.net.solidfire.eng:c,i,0x23d860000",
        "initiatorSessionID": 9622126592,
        "msSinceLastIscsiPDU": 243,
        "msSinceLastScsiCommand": 141535021,
        "nodeID": 3,
        "serviceID": 6,
        "sessionID": 25769804943,
        "targetIP": "10.1.1.2:3260",
        "targetName": "iqn.2010-01.com.solidfire:a7sd.3",
        "targetPortName": "iqn.2010-01.com.solidfire:a7sd.3,t,0x1",
        "virtualNetworkID": 0,
        "volumeID": 3,
        "volumeInstance": 140327214758656
      }
    ]
  }
}

```

Nueva versión

9,6

Servicios de listas

Puedes usar el `ListServices` Método para listar la información de servicios para nodos, unidades, 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 de retorno:

Nombre	Descripción	Tipo
servicios	Servicios que se ejecutan en unidades y nodos.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  ]
}

```

Nueva versión

9,6

Lista de nodos pendientes

Puedes usar el `ListPendingNodes` Método para listar los nodos de almacenamiento pendientes en el sistema. Los nodos pendientes son nodos de almacenamiento que están en ejecución y configurados para unirse al clúster de almacenamiento, pero que aún no se han agregado mediante el método de la API `AddNodes`.

direcciones de gestión IPv4 e IPv6

Tenga en cuenta que `ListPendingNodes` No enumera los nodos pendientes que tienen diferentes tipos de direcciones para la dirección IP de administración (MIP) y la dirección IP virtual de administración (MVIP). Por ejemplo, si un nodo pendiente tiene una dirección IPv6 multi-IP (MVIP) y una dirección IPv4 multi-IP (MIP), `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 de retorno:

Nombre	Descripción	Tipo
nodos pendientes	Lista de nodos pendientes en el clúster.	nodo pendiente formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}
```

Nueva versión

9,6

Encuentra más información

[Agregar nodos](#)

Lista de nodos activos pendientes

Puedes usar el `ListPendingActiveNodes` Método para listar los nodos del clúster que se encuentran en el estado `PendingActive`, entre los estados pendiente y activo. Los nodos en este estado están siendo devueltos a la imagen de fábrica.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
nodos activos pendientes	Lista de objetos que detalla información sobre todos los nodos PendingActive del sistema.	nodo activo pendiente información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}

```

Nueva versión

9,6

Modificar UmbralCompletoDeClúster

Puedes usar el `ModifyClusterFullThreshold` Método para cambiar el nivel en el que el sistema genera un evento cuando el clúster de almacenamiento se acerca a una determinada utilización de capacidad. Puede utilizar la configuración del umbral para indicar la cantidad aceptable de almacenamiento en bloque 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 nivel de utilización de almacenamiento de bloques "Error", ingrese un valor de "3" para el parámetro `stage3BlockThresholdPercent`. Si se alcanza este nivel, el sistema envía una alerta al registro de eventos en la consola de administración del clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:



Debe seleccionar al menos un parámetro.

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
factor de sobreaprovisionamiento de metadatos máximo	Un valor representativo del número de veces que se puede sobreaprovisionar el espacio de metadatos en relación con la cantidad de espacio disponible. Por ejemplo, si hubiera suficiente espacio de metadatos para almacenar 100 TiB de volúmenes y este número se estableciera en 5, entonces se podrían crear volúmenes por valor de 500 TiB.	entero	5	No
stage2AwareThreshold	Número de nodos de capacidad restantes en el clúster antes de que el sistema active una notificación de capacidad.	entero	Ninguno	No
stage3BlockThresholdPercent	El porcentaje de utilización del almacenamiento en bloque por debajo del umbral de "Error" que provoca que el sistema active una alerta de "Advertencia" del clúster.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
stage3MetadataThresholdPercent	El porcentaje de utilización del almacenamiento de metadatos por debajo del umbral de "Error" que provoca que el sistema active una alerta de "Advertencia" del clúster.	entero	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo

plenitud de bloque	El nivel actual calculado de llenado de bloques del clúster. • etapa1Feliz: Sin alertas ni condiciones de error. Corresponde al estado Saludable en la interfaz web. • stage2Aware: Sin alertas ni condiciones de error. Corresponde al estado Saludable en la interfaz web. • Stage3Low: Su sistema no puede proporcionar protección de datos redundante ante dos fallos de nodo no simultáneos. Corresponde al estado Advertencia en la interfaz web. Puede configurar este nivel en la interfaz web (por defecto, el sistema activa esta alerta cuando la capacidad está un 3% por debajo del estado de Error). • Etapa 4 Crítica: El sistema no es capaz de proporcionar protección de datos redundante ante el fallo de un solo nodo. No se pueden crear nuevos volúmenes ni clones. Corresponde al estado Error en la interfaz de usuario de Element. • etapa5CompletamenteConsumido: Completamente consumido. El clúster es de solo lectura y las conexiones iSCSI se mantienen, pero todas las escrituras están suspendidas. Corresponde al estado Crítico en la interfaz de usuario de Element.	cadena
plenitud	Refleja el nivel más alto de plenitud entre "plenitud de bloque" y "plenitud de metadatos".	cadena

factor de sobreaprovisionamiento de metadatos máximo	Un valor representativo del número de veces que se puede sobreaprovisionar el espacio de metadatos en relación con la cantidad de espacio disponible. Por ejemplo, si hubiera suficiente espacio de metadatos para almacenar 100 TiB de volúmenes y este número se estableciera en 5, entonces se podrían crear volúmenes por valor de 500 TiB.	entero

metadataFullness	El nivel actual calculado de integridad de metadatos del clúster. • etapa1Feliz: Sin alertas ni condiciones de error. Corresponde al estado Saludable en la interfaz web. • stage2Aware: Sin alertas ni condiciones de error. Corresponde al estado Saludable en la interfaz web. • Stage3Low: Su sistema no puede proporcionar protección de datos redundante ante dos fallos de nodo no simultáneos. Corresponde al estado Advertencia en la interfaz web. Puede configurar este nivel en la interfaz web (por defecto, el sistema activa esta alerta cuando la capacidad está un 3% por debajo del estado de Error). • Etapa 4 Crítica: El sistema no es capaz de proporcionar protección de datos redundante ante el fallo de un solo nodo. No se pueden crear nuevos volúmenes ni clones. Corresponde al estado Error en la interfaz de usuario de Element. • etapa5CompletamenteConsumido: Completamente consumido. El clúster es de solo lectura y las conexiones iSCSI se mantienen, pero todas las escrituras están suspendidas. Corresponde al estado Crítico en la interfaz de usuario de Element.	cadena
porcentaje de reserva usada de la porción	Condición de error. Se activa una alerta del sistema si la utilización de la porción reservada es mayor que el valor sliceReserveUsedThresholdPct devuelto.	entero

stage2AwareThreshold	Estado de conciencia. El valor que se establece para el nivel umbral del clúster "Etapa 2".	entero
stage2BlockThresholdBytes	El número de bytes que utiliza el clúster en el que se alcanzará una condición de llenado de etapa 2.	entero
stage2MetadataThresholdBytes	El número de bytes de metadatos que utiliza el clúster en el que se alcanzará una condición de llenado de etapa 2.	
stage3BlockThresholdBytes	El número de bytes de almacenamiento que utiliza el clúster en el que se alcanzará una condición de llenado de etapa 3.	entero
stage3BlockThresholdPercent	El valor porcentual establecido para la etapa 3. Al alcanzar este porcentaje de carga, se publica una advertencia en el registro de alertas.	entero
stage3LowThreshold	Condición de error. El umbral en el que se genera una alerta del sistema debido a la baja capacidad de un clúster.	entero
stage3MetadataThresholdBytes	El número de bytes de metadatos utilizados por el clúster en el que existirá una condición de llenado de etapa 3.	
stage4BlockThresholdBytes	El número de bytes de almacenamiento que utiliza el clúster en el que se alcanzará una condición de llenado de etapa 4.	entero
stage4CriticalThreshold	Condición de error. El umbral en el que se crea una alerta del sistema para advertir sobre una capacidad críticamente baja en un clúster.	entero
stage4MetadataThresholdBytes	El número de bytes de metadatos utilizados por el clúster en el que existirá una condición de llenado de etapa 4.	

stage5BlockThresholdBytes	El número de bytes de almacenamiento utilizados por el clúster en el que existirá una condición de llenado de etapa 5.	entero
stage5MetadataThresholdBytes	El número de bytes de metadatos utilizados por el clúster en el que existirá una condición de llenado de etapa 5.	
sumaTotalDeBytesDelClúster	La capacidad física del clúster, medida en bytes.	entero
sumaTotalMetadataClusterBytes	La cantidad total de espacio que se puede utilizar para almacenar metadatos.	entero
suma de bytes del clúster usados	El número de bytes de almacenamiento utilizados en el clúster.	entero
sumaUsedMetadataClusterBytes	La cantidad de espacio utilizado en las unidades de volumen para almacenar metadatos.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}

```

Nueva versión

9,6

ModificarPreferenciaDeInterfazDeClúster

El `ModifyClusterInterfacePreference` Este método permite que los sistemas integrados con clústeres de almacenamiento que ejecutan el software Element cambien 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	Requerido
nombre	El nombre de la preferencia de interfaz del clúster que se va a modificar.	cadena	Ninguno	Sí

valor	El nuevo valor de la preferencia de interfaz del clúster.	cadena	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ModifyClusterInterfacePreference",
  "params": {
    "name": "testname",
    "value": "newvalue"
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nueva versión

11,0

Eliminar nodos

Puedes usar `RemoveNodes` eliminar uno o más nodos que ya no deberían participar en el clúster.

Antes de eliminar un nodo, debe extraer todas las unidades que contiene utilizando el `RemoveDrives` método. No puedes eliminar un nodo hasta que `RemoveDrives` El proceso ha finalizado y todos los datos se han migrado fuera del nodo. Después de eliminar un nodo, este se registra automáticamente como nodo pendiente. Puedes volver a agregar el nodo o desactivarlo (desactivar el nodo lo elimina de la lista de nodos pendientes).

eliminación del nodo maestro del clúster

Si usted usa `RemoveNodes` Para eliminar el nodo maestro del clúster, el método podría agotar el tiempo de espera antes de devolver una respuesta. Si la llamada al método no logra eliminar el nodo, vuelva a realizar la llamada al método. Tenga en cuenta que si va a eliminar el nodo maestro del clúster junto con otros nodos, deberá utilizar una llamada independiente para eliminar el nodo maestro del clúster por sí solo.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
<code>ignorarEnsembleToleranceChange</code>	Ignorar los cambios en la tolerancia a fallos de nodos del conjunto al eliminar nodos. Si el clúster de almacenamiento utiliza esquemas de protección de datos que toleran fallos de múltiples nodos y la eliminación de nodos disminuiría la tolerancia a fallos de nodos del conjunto, la eliminación del nodo normalmente falla con un error. Puede establecer este parámetro en verdadero para deshabilitar la comprobación de tolerancia del conjunto y así lograr que la eliminación del nodo se realice correctamente.	booleano	FALSO	No
<code>nodos</code>	Lista de <code>NodeIDs</code> para los nodos que se eliminarán.	matriz de enteros	Ninguno	Sí

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "RemoveNodes",
  "params": {
    "nodes" : [3,4,5]
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1
  "result" : {},
}
```

Nueva versión

9,6

SetLoginSessionInfo

Puedes usar el `SetLoginSessionInfo` método para establecer el período de tiempo durante el cual es válida la autenticación de inicio de sesión para una sesión. Una vez transcurrido el período de inicio de sesión sin actividad en el sistema, la autenticación caduca. Se requieren nuevas credenciales de inicio de sesión para continuar accediendo 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	Requerido
se acabó el tiempo	Periodo de expiración de la autenticación del clúster. Formateado en HH:mm:ss. Por ejemplo: 01:30:00, 00:90:00 y 00:00:5400 se pueden usar para igualar un período de tiempo de espera de 90 minutos. El tiempo de espera mínimo es de 1 minuto. Cuando no se proporciona un valor, o se establece en cero, la sesión de inicio de sesión no tiene valor de tiempo de espera.	cadena	30 minutos	No

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "SetLoginSessionInfo",
  "params": {
    "timeout" : "01:30:00"
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nueva versión

9,6

Cerrar

Puedes usar el `Shutdown` Método para reiniciar o apagar los nodos de un clúster. Con este método puede apagar un solo nodo, varios nodos o todos los nodos del clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nodos	Lista de NodeIDs para los nodos que se reiniciarán o apagarán.	matriz de enteros	Ninguno	Sí
opción	Medidas a tomar para el grupo. Valores posibles: • reiniciar: Reinicia el clúster. • detener: Realiza un apagado completo.	cadena	Reanudar	No

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    ]
  }
}
```

Nueva versión

9,6

Métodos de la API de creación de clústeres

VerificarClústerPropuesto

Puedes usar 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 fallos que pudieran producirse al intentarlo, como capacidades de nodos mixtas desequilibradas o tipos de nodos que no son compatibles con clústeres de almacenamiento de dos nodos.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nodos	Una lista de las direcciones IP de almacenamiento del conjunto inicial de nodos de almacenamiento que componen el clúster de almacenamiento.	matriz de cadenas	Ninguno	Sí
fuerza	Establézcalo en verdadero para que se ejecute en todos los nodos de almacenamiento del clúster de almacenamiento.	booleano	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Cluster propuesto válido	Indica si los nodos de almacenamiento propuestos conformarían o no un clúster de almacenamiento válido. Valores posibles: • verdadero • FALSO	booleano
Errores de clúster propuestos	Errores que se producirían si se creara un clúster de almacenamiento utilizando los nodos de almacenamiento propuestos.	matriz de cadenas

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": [ ]
  }
}
```

Nueva versión

11,0

CrearClúster

Puedes usar el `CreateCluster` Método para inicializar el nodo en un clúster que tiene la propiedad de las direcciones "mvip" y "svip". Cada nuevo clúster se inicializa utilizando la IP de gestión (MIP) del primer nodo del clúster. Este método también agrega automáticamente todos los nodos que se están configurando al clúster. Solo necesitas usar este método una vez cada vez que se inicialice un nuevo clúster.



Después de iniciar sesión en el nodo maestro del clúster y ejecutar el [Obtener configuración de Bootstrap](#) Para obtener las direcciones IP del resto de los nodos que desea incluir en el clúster, puede ejecutar el método `CreateCluster` en el nodo maestro del clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
aceptar el EULA	Indique su aceptación del Acuerdo de Licencia de Usuario Final al crear este clúster. Para aceptar el CLUF, configure este parámetro en verdadero.	booleano	Ninguno	Sí
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
habilitar el cifrado de software en reposo	Habilite este parámetro para utilizar el cifrado basado en software en reposo. Valor predeterminado: falso en todos los clústeres. Una vez habilitada la encriptación de software en reposo, no se puede deshabilitar en el clúster.	booleano	verdadero	No
MVIP	Dirección IP flotante (virtual) para el clúster en la red de administración.	cadena	Ninguno	Sí
nodos	Direcciones CIP/SIP del conjunto inicial de nodos que componen el clúster. La IP de este nodo debe estar en la lista.	matriz de cadenas	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
número de orden	Número de pedido de venta alfanumérico. Requerido en plataformas basadas en software.	cadena	Ninguno	No (plataformas basadas en hardware) Sí (plataformas basadas en software)
contraseña	Contraseña inicial para la cuenta de administrador del clúster.	cadena	Ninguno	Sí
número de serie	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	Dirección IP flotante (virtual) para el clúster en la red de almacenamiento (iSCSI).	cadena	Ninguno	Sí
nombre de usuario	Nombre de usuario del administrador del clúster.	cadena	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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" : {}
}
```

Nueva versión

9,6

Encuentra más información

- ["Obtener configuración de Bootstrap"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Obtener configuración de Bootstrap

Puedes usar el `GetBootstrapConfig` Método para obtener información del clúster y del nodo a partir del archivo de configuración de arranque. Utilice este método de 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 del clúster cuando se crea un clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
nombre del clúster	Nombre del clúster.	cadena
MVIP	Dirección MVIP del clúster. Vacío si el nodo no forma parte de un clúster.	cadena
nombre del nodo	Nombre del nodo.	cadena
nodos	Lista de información sobre cada nodo que está esperando activamente para unirse al clúster. Valores posibles: • chassisType: (cadena) Plataforma de hardware del nodo. • cip: (cadena) Dirección IP del clúster del nodo. • compatible: (booleano) Indica si el nodo es compatible con el nodo contra el que se ejecutó la llamada a la API. • nombre de host: (cadena) Nombre de host del nodo. • mip: (cadena) La dirección IP de administración IPv4 del nodo. • mipV6: (cadena) La dirección IP de administración IPv6 del nodo. • nodeType: (cadena) Nombre del modelo del nodo. • versión: (cadena) Versión del software actualmente instalado en el nodo.	matriz de objetos JSON

Nombre	Descripción	Tipo
svip	Dirección SVIP del clúster. Nulo si el nodo no forma parte de un clúster.	cadena
versión	Versión del software Element actualmente instalada en el nodo al que se llamó mediante este método de la API.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}

```

Métodos de la API de Drive

Agregar unidades

Puedes usar el `AddDrives` Método para agregar una o más unidades disponibles al clúster, lo que permite que las unidades alojen una parte de los datos del clúster.

Cuando se agrega un nodo de almacenamiento al clúster o se instalan nuevas unidades en un nodo existente, las nuevas unidades se marcan como disponibles y deben agregarse mediante `AddDrives` antes de poder utilizarlas. Utilice el [ListDrives](#) Método para mostrar las unidades que están disponibles para agregar. Al agregar una unidad, el sistema determina automáticamente el tipo de unidad que debe ser.

El método es asíncrono y devuelve un valor tan pronto como se inician los procesos para reequilibrar las unidades en el clúster. Sin embargo, el reequilibrio de los datos en el clúster con las unidades recién agregadas podría tardar más tiempo; el reequilibrio continúa incluso después de que se complete la llamada al método `AddDrives`. Puedes usar el [ObtenerResultadoAsíncrono](#) método para consultar el `asyncHandle` devuelto por el método. Una vez que el método `AddDrives` devuelva un resultado, puede utilizar el [ListSyncJobs](#) Método para ver el progreso del reequilibrio de datos con las nuevas unidades.



Cuando se agregan varias unidades, es más eficiente agregarlas en una sola llamada al método `AddDrives` en lugar de usar varios métodos individuales, uno para cada unidad. Esto reduce la cantidad de equilibrio de datos que debe producirse para estabilizar la carga de almacenamiento en el clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
unidades	Información sobre cada unidad que se añadirá al clúster. Valores posibles: • driveID: El ID de la unidad que se va a agregar (número entero). • tipo: El tipo de unidad que se va a agregar (cadena de texto). Los valores válidos son "slice", "block" o "volume". Si se omite, el sistema asigna el tipo correcto.	matriz de objetos JSON	Ninguno	Sí (el tipo es opcional)

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
manejador asíncrono	Valor de identificador utilizado para obtener el resultado de la operación.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:


```
{
  "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
  }
}
```

Nueva versión

9,6

Encuentra más información

- [ObtenerResultadoAsíncrono](#)
- [ListDrives](#)
- [ListSyncJobs](#)

Información sobre el hardware de la unidad

Puedes usar el `GetDriveHardwareInfo` Método para obtener toda la información de

hardware de la unidad dada. Esto generalmente incluye fabricantes, vendedores, versiones y otra información de identificación de hardware asociada.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
driveID	Identificador de la unidad para la solicitud.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
resultado	Se devolvió la información de hardware para el driveID especificado.	Información de hardware

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  }
}
```

Nueva versión

9,6

Encuentra más información

[ListDrives](#)

GetDriveStats

Puedes usar el `GetDriveStats` Método para obtener mediciones de actividad de alto nivel para una sola unidad. Los valores son acumulativos desde la adición de la unidad al clúster. Algunos valores son específicos de las unidades de bloque. Al ejecutar este método, se devuelven datos estadísticos tanto para unidades de bloque como para unidades de metadatos.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
driveID	Identificador de la unidad para la solicitud.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Estadísticas de la unidad	Información de actividad de la unidad para el ID de unidad especificado.	Estadísticas de la unidad

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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 para una unidad de metadatos de 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
    }
  }
}
```

Nueva versión

9,6

Encuentra más información

[ListDrives](#)

ListDrives

Puedes usar el `ListDrives` Método para listar las unidades que existen en los nodos activos del clúster. Este método devuelve las unidades que se han agregado como metadatos de volumen o unidades de bloque, así como las unidades que no se han agregado y están disponibles.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
unidades	Lista de unidades en el clúster.	conducir información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}

```

Nueva versión

9,6

ListDriveStats

Puedes usar el `ListDriveStats` Método para listar las mediciones de actividad de alto nivel para múltiples unidades en el clúster. Por defecto, este método devuelve estadísticas para todas las unidades del clúster, y estas mediciones son acumulativas desde la adición de la unidad al clúster. Algunos valores que devuelve 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	Requerido
unidades	Lista de identificadores de unidad (driveID) para los que se devolverán las estadísticas de la unidad. Si omite este parámetro, se devolverán las mediciones de todas las unidades.	matriz de enteros	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Estadísticas de la unidad	Lista de información de actividad de cada unidad.	Estadísticas de la unidad formación
errores	Esta lista contiene el ID de la unidad y el mensaje de error asociado. Siempre está presente y vacío si no hay errores.	matriz de objetos JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
        }
      }
    ]
  }
}

```

Nueva versión

9,6

Encuentra más información

[GetDriveStats](#)

Eliminar unidades

Puedes usar el `RemoveDrives` Método para eliminar de forma proactiva las unidades

que forman parte del clúster. Podrías utilizar este método al reducir la capacidad del clúster o al prepararte 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 "Disponibles". Las unidades de la lista "Disponibles" se eliminan completamente del sistema y no tienen servicios en ejecución ni datos activos.

`RemoveDrives` es un método asíncrono. Dependiendo de la capacidad total de las unidades que se extraen, la migración de todos los datos podría tardar varios minutos.

Al extraer varias unidades, utilice una sola `RemoveDrives` llamada a un método en lugar de múltiples 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 en el clúster.

También puede eliminar unidades con estado "fallido" mediante `RemoveDrives`. Cuando se extrae una unidad con estado "fallido", la unidad no vuelve a tener un estado "disponible" o "activo". La unidad no está disponible para su uso en el clúster.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
unidades	Lista de identificadores de unidades a eliminar del clúster.	matriz de enteros	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
manejador asíncrono	Valor de identificador utilizado para obtener el resultado de la operación.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}
```

Nueva versión

9,6

Encuentra más información

- [ObtenerResultadoAsíncrono](#)
- [ListDrives](#)

Unidades de borrado seguro

Puedes usar el `SecureEraseDrives` Método para eliminar cualquier dato residual de las unidades que tienen el estado "disponible". Podrías utilizar este método al reemplazar una unidad que se acerca al final de su vida útil y que contenía datos confidenciales. Este método utiliza un comando de Unidad de Borrado de Seguridad para escribir un patrón predeterminado en la unidad y restablecer la clave de cifrado en la misma. Este método asíncrono puede tardar varios minutos en completarse.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
unidades	Lista de identificadores de unidades para borrar de forma segura.	matriz de enteros	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
manejador asíncrono	Valor de identificador utilizado para obtener el resultado de la operación.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}
```

Nueva versión

9,6

Encuentra más información

- [ObtenerResultadoAsíncrono](#)
- [ListDrives](#)

Métodos de la API de Fibre Channel

Obtener asignaciones de LUN de acceso al volumen

Puedes usar el `GetVolumeAccessGroupLunAssignments` Método para recuperar detalles sobre las asignaciones LUN de un grupo de acceso a volúmenes especificado.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de grupo de acceso al volumen	Un identificador único de grupo de acceso a volumen utilizado para devolver información.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Asignaciones de grupo de acceso de volumen	Una lista de todos los puertos físicos Fibre Channel, o un puerto para un solo nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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}
      ]
    }
  }
}
```

Nueva versión

9,6

Información del puerto del canal de fibra

Puedes usar el `ListFibreChannelPortInfo` Método para listar información sobre los puertos Fibre Channel.

Este método de API está diseñado para su uso en nodos individuales; se requiere un nombre de usuario y una contraseña para acceder a nodos Fibre Channel individuales. Sin embargo, este método se puede utilizar en el clúster si el parámetro de fuerza está configurado como verdadero. Cuando se utiliza en el clúster, se muestran todas las interfaces Fibre Channel.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
fuerza	Establecer en verdadero para ejecutar en todos los nodos del clúster.	booleano	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Puertos de canal de fibra	Una lista de todos los puertos físicos Fibre Channel, o un puerto para un solo nodo.	Puerto de canal de fibra formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  ]
}
}
}
}
}
}
}

```

Nueva versión

9,6

Lista de sesiones de FibreChannel

Puedes usar el `ListFibreChannelSessions` Método para listar información sobre las sesiones de Fibre Channel en un clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
sesiones	Una lista de objetos que describen las sesiones Fibre Channel activas en el clúster.	sesión formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```

{
  "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
      }
    ]
  }
}

```

Nueva versión

9,6

Información del puerto del canal de fibra del nodo de lista

Puedes usar el `ListNodeFibreChannelPortInfo` Método para listar información sobre los puertos Fibre Channel en un nodo.

Este método de API está diseñado para su uso en nodos individuales; se requiere un nombre de usuario y una contraseña para acceder a nodos Fibre Channel individuales. Cuando se utiliza en el clúster, se muestran todas las interfaces Fibre Channel.

Parámetro

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Puertos de canal de fibra	Una lista de todos los puertos físicos Fibre Channel, o un puerto para un solo nodo.	Puerto de canal de fibra formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
]
}
}

```

Nueva versión

9,6

Modificar asignaciones de Lun de grupo de acceso a volumen

Puedes usar el `ModifyVolumeAccessGroupLunAssignments` Método para definir asignaciones LUN personalizadas para volúmenes específicos.

Este método solo modifica los valores LUN establecidos en el parámetro lunAssignments del grupo de acceso al volumen. Todas las demás asignaciones de LUN permanecen sin cambios.

Los valores de asignación de LUN deben ser únicos para los volúmenes en un grupo de acceso a volúmenes. No se pueden definir valores LUN duplicados dentro de un grupo de acceso a volúmenes. Sin embargo, puede volver a utilizar los mismos valores de LUN en diferentes grupos de acceso a volúmenes.



Los valores LUN válidos son de 0 a 16383. El sistema genera una excepción si se introduce un valor LUN fuera de este rango. Ninguna de las asignaciones LUN especificadas se modifica si hay una excepción.

PRECAUCIÓN:

Si se modifica la asignación de LUN para un volumen con E/S activa, la E/S puede verse interrumpida. Debe modificar 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	Requerido
ID de grupo de acceso al volumen	ID de grupo de acceso a volumen único para el cual se modificarán las asignaciones de LUN.	entero	Ninguno	Sí
Tareas del mediodía	Los identificadores de volumen con nuevos valores LUN asignados.	matriz de enteros	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Asignaciones de grupo de acceso de volumen	Un objeto que contiene detalles de las asignaciones LUN del grupo de acceso a volúmenes modificado.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
  }
}
```

Nueva versión

9,6

Métodos de la API del iniciador

CrearIniciadores

Puedes usar `CreateInitiators` para crear múltiples nuevos IQN de iniciador o nombres de puerto mundial (WWPN) y, opcionalmente, asignarles alias y atributos. Cuando uses `CreateInitiators` Para crear nuevos iniciadores, también puede agregarlos a grupos de acceso por volumen.

Si la operación no logra crear uno de los iniciadores proporcionados en el parámetro, el método devuelve un error y no crea ningún iniciador (no es posible la finalización parcial).

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
iniciadores	Una lista de objetos que contienen las características de cada nuevo iniciador. Objetos: • alias: (Opcional) El nombre descriptivo que se asignará a este iniciador. (cadena) • attributes: (Opcional) Un conjunto de atributos JSON para asignar a este iniciador. (Objeto JSON) • chapUsername: (Opcional) El nombre de usuario CHAP único para este iniciador. Se utiliza el nombre del iniciador (IQN) por defecto si no se especifica durante la creación y <code>requireChap</code> es verdadero. (cadena) • initiatorSecret: (Opcional) El secreto CHAP utilizado para autenticar al iniciador. Se utilizará un secreto generado aleatoriamente por defecto si no se especifica durante la creación y <code>requireChap</code> es verdadero. (cadena)	matriz de objetos JSON	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

- name:

Nombre	Descripción	Tipo
iniciadores	Lista de objetos que describen los iniciadores recién creados.	iniciador formación

Error

- requireChap:

(Opcional)
Este método puede devolver el siguiente error:
Verdadero si se

Nombre	Descripción
xIniciadorExiste	Se devuelve si el nombre del iniciador que eligió ya existe.

Ejemplo de solicitud

- targetSecret:

(Opcional) El
secreto CHAP
utilizado para

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": []
      }
    ]
  }
}

```

Nueva versión

9,6

Encuentra más información

[Iniciadores de listas](#)

EliminarIniciadores

Puedes usar `DeleteInitiators` eliminar uno o más iniciadores del sistema (y de cualquier volumen o grupo de acceso a volúmenes asociado).

Si `DeleteInitiators` Si no se puede eliminar uno de los iniciadores proporcionados en el parámetro, el sistema devuelve un error y no elimina ningún iniciador (no es posible la finalización parcial).

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
iniciadores	Una matriz de identificadores de iniciadores a eliminar.	matriz de enteros	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Error

Este método puede devolver el siguiente error:

Nombre	Descripción
xIniciadorNoExiste	Se devuelve si el nombre del iniciador que ha elegido no existe.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "id": 5101,
  "method": "DeleteInitiators",
  "params": {
    "initiators": [
      145,
      147
    ]
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 5101,
  "result": {}
}
```

Nueva versión

9,6

Iniciadores de listas

Puedes usar el `ListInitiators` Método para obtener la lista de IQN de iniciadores o nombres de puertos mundiales (WWPN).

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
iniciadores	Una lista de identificadores de iniciador para recuperar. Puede proporcionar este parámetro o el parámetro <code>startInitiatorID</code> , pero no ambos.	matriz de enteros	Ninguno	No
ID de iniciador de inicio	El ID del iniciador desde el cual comenzar la lista. Puede proporcionar este parámetro o el parámetro de <code>iniciadores</code> , pero no ambos.	entero	0	No
límite	El número máximo de objetos iniciadores que se devolverán.	entero	(ilimitado)	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
iniciadores	Lista de información del iniciador.	iniciador formación

Excepciones

Este método puede tener la siguiente excepción:

Nombre	Descripción
xParámetro no válido	Se produce un error si se incluyen los parámetros startInitiatorID e initiators en la misma llamada al método.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
        ]
      }
    ]
  }
}
```

Nueva versión

9,6

ModificarIniciadores

Puedes usar el `ModifyInitiators` método para cambiar los atributos de uno o más iniciadores existentes.

No se puede cambiar el nombre de un iniciador existente. Si necesitas cambiar el nombre de un iniciador, primero bórralo con el [EliminarIniciadores](#) método y crear uno nuevo con el [CrearIniciadores](#) método.

Si ModifyInitiators no logra cambiar uno de los iniciadores proporcionados en el parámetro, el método devuelve un error y no modifica ningún iniciador (no es posible la finalización parcial).

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido

iniciadores	Una lista de objetos que contiene las características de cada iniciador a modificar. Objetos posibles: • alias: (Opcional) Un nuevo nombre descriptivo para asignar al iniciador. (cadena) • attributes: (Opcional) Un nuevo conjunto de atributos JSON para asignar 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 a modificar. (entero) • initiatorSecret: (Opcional) Un nuevo secreto CHAP utilizado para autenticar al iniciador. (cadena) • requireChap: (Opcional) Verdadero si CHAP es	matriz de objetos JSON	Ninguno	Sí

Valor de retorno necesario para este iniciador.
Este método tiene el siguiente valor de retorno:
(booleano)

Nombre	Descripción	Tipo
iniciadores	Lista de objetos que describen los iniciadores recientemente modificados.	iniciadorformación

Ejemplo de solicitud (cuando se utiliza la autenticación OAuth 2.0 mutua)
Las solicitudes para este método son similares al siguiente ejemplo:
(cadena)

```
{
  "id": 6683,
  "method": "ModifyInitiators",
  "params": {
    "initiators": [
      {
        "initiatorID": 2,
        "alias": "alias1",
        "volumeAccessGroupID": null
      },
      {
        "initiatorID": 3,
        "alias": "alias2",
        "volumeAccessGroupID": 1
      }
    ]
  }
}
```

Ejemplo de respuesta GroupID: (Opcional) El ID del grupo de acceso al
Este método devuelve una respuesta similar al siguiente ejemplo:

volumen al que se debe agregar el iniciador. Si el iniciador pertenecía previamente a un grupo de acceso a volúmenes diferente, se elimina del grupo de acceso a volúmenes anterior. 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
        ]
      }
    ]
  }
}
```

Nueva versión

9,6

Encuentra más información

- [CrearIniciadores](#)
- [EliminarIniciadores](#)

Métodos de la API LDAP

Agregar administrador de clúster Ldap

Puedes usar el `AddLdapClusterAdmin` para agregar un nuevo usuario administrador de clúster LDAP. Un administrador de clúster LDAP puede gestionar el clúster utilizando la API y las herramientas de gestión. Las cuentas de administrador del clúster LDAP son completamente independientes y no guardan relación con las cuentas de inquilino estándar.

Parámetros

También puede utilizar este método para agregar un grupo LDAP que se haya definido en Active Directory®. El nivel de acceso que se otorga al grupo se transmite a los usuarios individuales del grupo LDAP.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
acceso	Controla qué métodos puede usar este administrador de clúster.	matriz de cadenas	Ninguno	Sí
aceptar el EULA	Acepte el Acuerdo de Licencia de Usuario Final. Establézcalo en verdadero para agregar 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	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
nombre de usuario	Nombre de usuario distinguido para el nuevo administrador del clúster LDAP.	cadena	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": {}
}
```

Nueva versión

9,6

Encuentra más información

[Control de acceso](#)

Habilitar autenticación LDAP

Puedes usar el `EnableLdapAuthentication` Método para configurar una conexión de directorio LDAP para la autenticación LDAP en un clúster. Los usuarios que sean miembros del directorio LDAP podrán iniciar sesión en el sistema de almacenamiento utilizando sus credenciales LDAP.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
tipo de autenticación	Identifica qué método de autenticación de usuario se debe utilizar. Valores posibles: • DirectBind • SearchAndBind	cadena	Buscar y enlazar	No
groupSearchBaseDN	El DN base del árbol para iniciar la búsqueda del subárbol de grupo.	cadena	Ninguno	No
tipo de búsqueda de grupo	Controla el filtro de búsqueda de grupo predeterminado utilizado. Valores posibles: • NoGroups: No hay soporte para grupos. • Active Directory: Membresía anidada de todos los grupos de Active Directory de un usuario. • MemberDN: Grupos de estilo MemberDN (nivel único).	cadena	Directorio activo	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
URI del servidor	Una lista de URI de servidores LDAP o LDAPS separadas por comas. Puede agregar un puerto personalizado al final de un URI LDAP o LDAPS utilizando dos puntos seguidos del número de puerto. Por ejemplo, el URI "ldap://1.2.3.4" usa el puerto predeterminado y el URI "ldaps://1.2.3.4:123" usa el puerto personalizado 123.	matriz de cadenas	Ninguno	Sí
userSearchBaseDN	El DN base del árbol para iniciar la búsqueda de subárboles. Este parámetro es obligatorio cuando se utiliza un authType de SearchAndBind.	cadena	Ninguno	No
searchBindDN	Un DN completo para iniciar sesión y realizar una búsqueda LDAP del usuario. El DN requiere acceso de lectura al directorio LDAP. Este parámetro es obligatorio cuando se utiliza un authType de SearchAndBind.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
buscarContraseñaVinculada	La contraseña de la cuenta searchBindDN utilizada para la búsqueda. Este parámetro es obligatorio cuando se utiliza un authType de SearchAndBind.	cadena	Ninguno	Sí
filtro de búsqueda de usuarios	El filtro de búsqueda LDAP que se debe utilizar al consultar el servidor LDAP. La cadena debe contener el texto de marcador de posición "%USERNAME%", que se reemplaza con el nombre de usuario del usuario que se autentica. Por ejemplo, (&(objectClass=person)(sAMAccountName=%USERNAME%)) utilizará el campo sAMAccountName en Active Directory para que coincida con el nombre de usuario ingresado al iniciar sesión en el clúster. Este parámetro es obligatorio cuando se utiliza un authType de SearchAndBind.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
plantilla de DN de usuario	Una plantilla de cadena utilizada para definir un patrón para construir un nombre distinguido de usuario (DN) completo. La cadena debe contener el texto de marcador de posición "%USERNAME%", que se reemplaza con el nombre de usuario del usuario que se autentica. Este parámetro es obligatorio cuando se utiliza un authType de DirectBind.	cadena	Ninguno	Sí
groupSearchCustomFilter	Para usar con el tipo de búsqueda CustomFilter, un filtro LDAP que se utilizará para devolver los DN de los grupos de un usuario. La cadena puede contener el texto de marcador de posición %USERNAME% y %USERDN%, que se reemplazará con su nombre de usuario y nombre de usuario completo según sea necesario.	cadena	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": {
  }
}
```

Nueva versión

9,6

Deshabilitar la autenticación LDAP

Puedes usar el `DisableLdapAuthentication` Método para deshabilitar la autenticación LDAP y eliminar todas las configuraciones LDAP. Este método no elimina ninguna cuenta de administrador de clúster configurada para usuarios o grupos. Una vez deshabilitada la autenticación LDAP, los administradores del clúster que estén configurados para usarla ya no podrán acceder al clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DisableLdapAuthentication",
  "params": {},
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nueva versión

9,6

Obtener configuración LDAP

Puedes usar el `GetLdapConfiguration` Método para obtener la configuración LDAP actualmente activa en el clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno.

Nombre	Descripción	Tipo
Configuración LDAP	Lista de la configuración LDAP actual. Esta llamada a la API no devuelve el texto plano de la contraseña de la cuenta de búsqueda. Nota: Si la autenticación LDAP está actualmente deshabilitada, todas las configuraciones devueltas estarán vacías, con la excepción de "authType" y "groupSearchType", que se establecen en "SearchAndBind" y "ActiveDirectory" respectivamente.	Configuración LDAP

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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%))"
    }
  }
}

```

Nueva versión

9,6

Prueba de autenticación LDAP

Puedes usar el `TestLdapAuthentication` Método para validar la configuración de autenticación LDAP actualmente habilitada. Si la configuración es correcta, la llamada a la API devuelve la pertenencia a grupos del usuario analizado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nombre de usuario	El nombre de usuario que se va a probar.	cadena	Ninguno	Sí
contraseña	La contraseña del nombre de usuario que se va a probar.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
Configuración LDAP	Un objeto LdapConfiguration para probar. Si proporciona este parámetro, el sistema probará la configuración proporcionada incluso si la autenticación LDAP está actualmente deshabilitada.	Configuración LDAP	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
grupos	Lista de grupos LDAP que incluyen al usuario analizado como miembro.	formación
userDN	Nombre distinguido LDAP completo del usuario evaluado.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

Métodos de la API de autenticación multifactor

Agregar administrador de clúster de IDIP

Puedes usar el `AddIpClusterAdmin` Método para agregar un usuario administrador de clúster autenticado por un proveedor de identidad (IdP) de terceros. Las cuentas de administrador del clúster IdP se configuran en función de la información de valor de atributo SAML proporcionada en la aserción SAML del IdP asociada al usuario. Si un usuario se autentica correctamente con el IdP y tiene declaraciones de atributos SAML dentro de la aserción SAML que coinciden con varias cuentas de administrador del clúster IdP, el usuario tendrá el nivel de acceso combinado de esas cuentas de administrador del clúster IdP coincidentes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
acceso	Controla qué métodos puede usar este administrador de clúster IdP.	matriz de cadenas	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
aceptar el EULA	Acepte el Acuerdo de Licencia de Usuario Final. Establézcalo en verdadero para agregar 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	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
nombre de usuario	Una asignación de valor de atributo SAML a un administrador de clúster IdP (por ejemplo, correo electrónico= test@example.com). Esto se puede definir utilizando un sujeto SAML específico. NameID o como una entrada en la declaración de atributos SAML, como por ejemplo eduPersonAffiliation.	cadena	Ninguno	Sí

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
ID de administrador del clúster	Identificador único para el administrador del clúster recién creado.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}
```

Nueva versión

12,0

Crear configuración de Idp

Puedes usar el `CreateIdpConfiguration` método para crear una relación de confianza potencial para la autenticación utilizando un proveedor de identidad (IdP) de terceros para el clúster. Se requiere un certificado de proveedor de servicios SAML para la comunicación con el IdP. Este certificado se genera según sea necesario y es devuelto por esta llamada a la API.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
idpMetadata	Metadatos del IdP para almacenar.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
idpName	Nombre utilizado para identificar un proveedor de identidad (IdP) para el inicio de sesión único (SSO) SAML 2.0.	cadena	Ninguno	Sí

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
idpConfigInfo	Información sobre la configuración del proveedor de identidad (IdP) de terceros.	"idpConfigInfo"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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://priver.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MIID...SlBHi\n
-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}
```

Nueva versión

12,0

Eliminar sesión de autenticación

Puedes usar el `DeleteAuthSession` Método para eliminar una sesión de autenticación de usuario individual. Si el usuario que realiza la llamada no pertenece al grupo de acceso `ClusterAdmins / Administrator`, solo se podrá eliminar la sesión de autenticación perteneciente a dicho usuario.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de sesión	Identificador único de la sesión de autenticación que se va a eliminar.	UUID	Ninguno	Sí

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
sesión	Información de sesión para la sesión de autenticación de eliminación.	"información de sesión de autenticación"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  }
}
```

Nueva versión

12,0

Eliminar sesiones de autenticación por administrador de clúster

Puedes usar el `DeleteAuthSessionsByClusterAdmin` método para eliminar todas las sesiones de autenticación asociadas con el especificado `ClusterAdminID`. Si el `ClusterAdminID` especificado corresponde 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 para su posible eliminación, utilice el método `ListAuthSessionsByClusterAdmin` con el `ClusterAdminID` parámetro.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de administrador del clúster	Identificador único para el administrador del clúster.	entero	Ninguno	Sí

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
sesiones	Información de sesión para las sesiones de autenticación eliminadas.	"información de sesión de autenticación"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  ]
}
```

Nueva versión

12,0

EliminarSesionesDeAutenticaciónPorNombreDeUsuario

Puedes usar el `DeleteAuthSessionsByUsername` Método para eliminar todas las sesiones de autenticación de un usuario o usuarios determinados. Un usuario que no pertenezca al grupo de acceso `ClusterAdmins/Administrator` solo puede eliminar sus propias sesiones. Un usuario con privilegios de `ClusterAdmins/Administrator` puede eliminar las sesiones pertenecientes a cualquier usuario. Para ver la lista de sesiones que podrían eliminarse, utilice `ListAuthSessionsByUsername` con los mismos parámetros. Para ver una lista de sesiones para su posible eliminación, utilice la `ListAuthSessionsByUsername` método con el mismo parámetro.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
método de autenticación	Método de autenticación de las sesiones de usuario que se van a eliminar. Solo un usuario perteneciente al grupo de acceso ClusterAdmins/Administrator 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 o el NameID del IdP del usuario. Si el IdP no está configurado para devolver ninguna de las dos opciones, esto especifica un UUID aleatorio emitido cuando se creó la sesión.	método de autenticación	Ninguno	No
nombre de usuario	Identificador único del usuario.	cadena	Ninguno	No

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo

sesiones	Información de sesión para las sesiones de autenticación eliminadas.	"información de sesión de autenticación"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  ]
}
```

Nueva versión

12,0

Eliminar configuración de IDp

Puedes usar el `DeleteIdpConfiguration` Método para eliminar una configuración existente de un IdP de terceros para el clúster. Eliminar la última configuración del IdP elimina el certificado del proveedor de servicios SAML del clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
idpConfigurationID	UUID para la configuración del IdP de terceros.	UUID	Ninguno	No
idpName	Nombre utilizado para identificar y recuperar un proveedor de identidad (IdP) para el inicio de sesión único (SSO) SAML 2.0.	cadena	Ninguno	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": {}
}
```

Nueva versión

12,0

Deshabilitar la autenticación Idp

Puedes usar el `DisableIdpAuthentication` Método para deshabilitar la compatibilidad con la autenticación mediante proveedores de identidad de terceros para el clúster. Una vez deshabilitado, los usuarios autenticados por proveedores de identidad de terceros ya no pueden acceder al clúster y cualquier sesión autenticada activa queda invalidada/desconectada. Los administradores de LDAP y del clúster pueden acceder al clúster a través de las interfaces de usuario compatibles.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DisableIdpAuthentication",
  "params": {}
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "result": {}
}
```

Nueva versión

12,0

Habilitar autenticación Idp

Puedes usar el `EnableIdpAuthentication` método para habilitar el soporte para la autenticación utilizando IdP de terceros para el clúster. Una vez habilitada la autenticación IdP, los administradores de LDAP y del clúster ya no pueden acceder al clúster a través de las interfaces de usuario compatibles y cualquier sesión autenticada activa se invalida o desconecta. Solo los usuarios autenticados por proveedores de identidad de terceros pueden acceder al clúster a través de las interfaces de usuario compatibles.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
idpConfigurationID	UUID para la configuración del IdP de terceros. Si solo existe una configuración de IdP, entonces la configuración predeterminada es habilitar esa configuración. Si solo tiene una única IdpConfiguration, no es necesario proporcionar el parámetro idpConfigurationID.	UUID	Ninguno	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "EnableIdpAuthentication",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "result": {}
}
```

Nueva versión

12,0

Obtener estado de autenticación Idp

Puedes usar el `GetIdpAuthenticationState` Método para devolver información sobre el estado de la autenticación utilizando proveedores de identidad de terceros.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
activado	Indica si la autenticación de IdP de terceros está habilitada.	booleano

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetIdpAuthenticationState"
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "result": {"enabled": true}
}
```

Nueva versión

12,0

ListarSesionesDeAutenticaciónActivas

Puedes usar el `ListActiveAuthSessions` Método para listar todas las sesiones autenticadas activas. Solo los usuarios con derechos de acceso administrativo pueden llamar a este método.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
sesiones	Información de sesión para las sesiones de autenticación.	"información de sesión de autenticación"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  ]
}
```

Nueva versión

12,0

Configuraciones de ListIdp

Puedes usar el `ListIdpConfigurations` Método para listar las configuraciones de los IdP de terceros. Opcionalmente, puede proporcionar cualquiera de los siguientes elementos: `enabledOnly` bandera para recuperar la configuración IdP actualmente habilitada o un UUID de metadatos IdP o nombre IdP para consultar información sobre una configuración IdP específica.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
habilitado	Filtra el resultado para devolver la configuración de IdP actualmente habilitada.	booleano	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
idpConfigurationID	UUID para la configuración del IdP de terceros.	UUID	Ninguno	No
idpName	Recupera la información de configuración del IdP para un nombre de IdP específico.	cadena	Ninguno	No

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
idpConfigInfos	Información sobre la(s) configuración(es) del IdP de terceros.	"idpConfigInfo"formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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://priver.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MI...BHi\n
-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}
```

Nueva versión

12,0

Actualizar configuración de IDp

Puedes usar 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	Requerido
generarNuevoCertificado	Cuando se especifica como verdadero, se genera una nueva clave y certificado SAML que reemplaza al par existente. Nota: Reemplazar el 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 proporcionan o se establecen en falso, el certificado y la clave SAML permanecen sin cambios.	booleano	Ninguno	No
idpConfigurationID	UUID para la configuración del IdP de terceros.	UUID	Ninguno	No
idpMetadata	Metadatos del IdP para 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 identidad (IdP) para el inicio de sesión único (SSO) SAML 2.0.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nuevoldpName	Si se especifica, este nombre reemplaza al nombre anterior del IdP.	cadena	Ninguno	No

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
idpConfigInfo	Información relativa a la configuración del IdP de terceros.	"idpConfigInfo"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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://priver.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MI...BHi\n
-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}
```

Nueva versión

12,0

Métodos de la API de autenticación de sesión

ListAuthSessionsByClusterAdmin

Puedes usar el `ListAuthSessionsByClusterAdmin` método para listar todas las sesiones de autenticación asociadas con el especificado `ClusterAdminID`. Si se especifica `ClusterAdminID` Si se asigna a un grupo de usuarios, se mostrarán 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	Requerido
ID de administrador del clúster	Identificador único para el administrador del clúster.	entero	Ninguno	Sí

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
sesiones	Lista de información de sesión para las sesiones de autenticación.	"información de sesión de autenticación"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  ]
}
```

Nueva versión

12,0

Listar sesiones de autenticación por nombre de usuario

Puedes usar el `ListAuthSessionsByUsername` Método para listar todas las sesiones de autenticación del usuario especificado. Un usuario que no tenga privilegios de administrador o del grupo de acceso `ClusterAdmins` solo podrá listar sus propias sesiones. Un usuario con privilegios de Administrador de clúster puede listar las sesiones pertenecientes a cualquier usuario.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
método de autenticación	Método de autenticación de las sesiones de usuario que se mostrarán. Solo un usuario perteneciente al grupo de acceso ClusterAdmins/Administrator 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 o el NameID del IdP del usuario. Si el IdP no está configurado para devolver ninguna de las dos opciones, esto especifica un UUID aleatorio emitido cuando se creó la sesión.	método de autenticación	Ninguno	Sí
nombre de usuario	Identificador único del usuario.	cadena	Ninguno	Sí

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo

sesiones	Lista de información de sesión para las sesiones de autenticación.	"información de sesión de autenticación"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  ]
}
```

Nueva versión

12,0

Métodos de la API de Node

ComprobarPingEnVlan

Puedes usar el `CheckPingOnVlan` Método para probar la conectividad de red en una VLAN temporal al realizar la validación de red previa al despliegue. `CheckPingOnVlan` Crea una interfaz VLAN temporal, envía paquetes ICMP a todos los nodos del clúster de almacenamiento utilizando la interfaz VLAN y, a continuación, elimina la interfaz.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
intentos	Especifica el número de veces que el sistema debe repetir el ping de prueba.	entero	5	No
hosts	Especifica una lista de direcciones o nombres de host de dispositivos a los que hacer ping, separados por comas.	cadena	Los nodos del clúster	No
interfaz	La interfaz existente (base) desde la cual se deben enviar los pings. Valores posibles: • Bond10G: Enviar pings desde la interfaz Bond10G. • Bond1G: Enviar pings desde la interfaz Bond1G.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
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
Tiempo de espera de ping (milisegundos)	Especifica el número de milisegundos que se deben esperar para cada respuesta de ping individual.	entero	500 ms	No
prohibir la fragmentación	Habilita la bandera DF (No Fragmentar) para los paquetes ICMP.	booleano	FALSO	No
sourceAddressV4	La dirección IPv4 de origen que se utilizará en los paquetes ping ICMP.	cadena	Ninguno	Sí
sourceAddressV6	La dirección IPv6 de origen que se utilizará en los paquetes ping ICMP.	cadena	Ninguno	Sí
tiempo de espera total en segundos	Especifica el tiempo en segundos que el ping debe esperar una respuesta del sistema antes de realizar el siguiente intento de ping o finalizar el proceso.	entero	5	No
etiqueta de red virtual	El ID de VLAN que se utilizará al enviar los paquetes ping.	entero	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
resultado	Lista de cada IP con la que el nodo pudo comunicarse y estadísticas de respuesta de ping.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": {
    "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
    }
  }
}

```

Nueva versión

11,1

Verificar adiciones de nodos propuestas

Puedes usar el `CheckProposedNodeAdditions` Método para probar un conjunto de nodos de almacenamiento para comprobar si se pueden agregar a un clúster de almacenamiento sin errores ni violaciones de las mejores prácticas.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nodos	Una lista de direcciones IP de almacenamiento de nodos de almacenamiento que están listos para ser agregados a un clúster de almacenamiento.	matriz de cadenas	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Cluster propuesto válido	Indica si los nodos de almacenamiento propuestos conformarían o no un clúster de almacenamiento válido. Valores posibles: • verdadero • FALSO	booleano

Errores de clúster propuestos	Errores que se producirían si se creara un clúster de almacenamiento utilizando los nodos de almacenamiento propuestos. Posibles códigos de error: • <code>`nodesNoCapacity`</code> Los nodos no tenían capacidad utilizable. • <code>`nodesTooLarge`</code> Los nodos constituyen una porción demasiado grande de la capacidad del clúster para el esquema de protección activa. • <code>`nodesConnectFailed`</code> No se pudo conectar con los nodos para consultar la configuración del hardware. • <code>`nodesQueryFailed`</code> No se pudo consultar la configuración de hardware de los nodos. • <code>`nodesClusterMember`</code> Las direcciones IP para los nodos ya están en uso en el clúster. • <code>`nonFipsNodeCapable`</code> No se puede agregar un nodo no compatible con FIPS al clúster de almacenamiento mientras la función de cifrado de unidad FIPS 140-2 está habilitada. • <code>`nonFipsDrivesCapable`</code> 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 para este método son similares al siguiente ejemplo:

```
{
  "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": [ ]
  }
}
```

Nueva versión

11,0

Crear paquete de soporte de clúster

Puedes usar el `CreateClusterSupportBundle` en el nodo de administración para recopilar paquetes de soporte de todos los nodos de un clúster. Los paquetes de soporte de nodos individuales están comprimidos como archivos tar.gz. El paquete de soporte del clúster es un archivo tar que contiene los paquetes de soporte de los nodos. Este método solo se puede ejecutar en un nodo de administración; no funciona cuando se ejecuta en un nodo de almacenamiento.

Parámetros



Debes llamar a este método contra el nodo de administración. Por ejemplo:

```
https://<management node IP>:442/json-rpc/10.0
```

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
permitirIncompleto	Permite que el script continúe ejecutándose si no se pueden recopilar paquetes de uno o más de los nodos.	booleano	Ninguno	No
nombre del paquete	Nombre único para cada paquete de soporte creado. Si no se proporciona ningún nombre, se utilizará "supportbundle" y el nombre del nodo como nombre del archivo.	cadena	Ninguno	No
MVIP	El MVIP del clúster. Los paquetes se recopilan de todos los nodos del clúster. Este parámetro es obligatorio si no se especifica el parámetro de nodos.	cadena	Ninguno	Sí
nodos	Las direcciones IP de los nodos desde los que se recopilarán los paquetes. Utilice nodos o mvip, pero no ambos, para especificar los nodos desde los que recopilar paquetes. Este parámetro es obligatorio si no se especifica mvip.	matriz de cadenas	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
contraseña	La contraseña de administrador del clúster. Nota: Esta contraseña se mostrará como texto al ingresarla.	cadena	Ninguno	Sí
nombre de usuario	El nombre de usuario del administrador del clúster.	cadena	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

Crear paquete de soporte

Puedes usar `CreateSupportBundle` para crear un archivo de paquete de soporte en el directorio del nodo. Tras su creación, el paquete se almacena en el nodo como un 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	Requerido
nombre del paquete	Nombre único para el paquete de soporte. Si no se proporciona ningún nombre, se utilizará "supportbundle" y el nombre del nodo como nombre de archivo.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
extraArgs	Utilice '--compress gz' para crear el paquete de soporte como un archivo tar.gz.	cadena	Ninguno	No
tiempo de espera en segundos	Número de segundos que se ejecuta el script del paquete de soporte.	entero	1500	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
detalles	Los detalles del paquete de soporte. Valores posibles: • bundleName: El nombre especificado en el método CreateSupportBundleAPI. Si no se especifica ningún nombre, se utiliza "supportbundle". • extraArgs: Los argumentos que se pasan con este método. • archivos: Una lista de los archivos del paquete de soporte que creó el sistema. • Salida: La salida de la línea de comandos del script que creó el paquete de soporte. • timeoutSec: El número de segundos que el script del paquete de soporte se ejecuta antes de detenerse. • url: URL del paquete de soporte creado.	Objeto JSON
duración	El tiempo utilizado para crear el paquete de soporte en el formato: HH:MM:SS.ssssss.	cadena
resultado	El éxito o el fracaso de la operación del paquete de soporte.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

Eliminar todos los paquetes de soporte

Puedes usar el `DeleteAllSupportBundles` método para eliminar todos los paquetes de soporte generados con el `CreateSupportBundle` Método API.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DeleteAllSupportBundles",
  "params": {}
},
"id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nueva versión

9,6

Desactivar el modo de mantenimiento

Puedes usar el `DisableMaintenanceMode` Método para sacar un nodo de almacenamiento del modo de mantenimiento. Solo debes desactivar el modo de mantenimiento una vez que hayas completado el mantenimiento y el nodo esté en línea.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nodos	Lista de identificadores de nodos de almacenamiento que se deben sacar del modo de mantenimiento.	matriz de enteros	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
manejador asíncrono	Puede utilizar el método <code>GetAsyncResult</code> para recuperar este <code>asyncHandle</code> y determinar cuándo finaliza la transición al modo de mantenimiento.	entero
modo actual	Estado actual del modo de mantenimiento del nodo. Valores posibles: • Desactivado: No se ha solicitado ningún mantenimiento. • Error de recuperación: El nodo no pudo recuperarse del modo de mantenimiento. • Inesperado: Se detectó que el nodo estaba fuera de línea, pero en modo Deshabilitado. • Recuperación tras mantenimiento: El nodo se encuentra en proceso de recuperación tras haber estado en modo de mantenimiento. • Preparación para el mantenimiento: Se están tomando medidas para preparar un nodo para realizar el mantenimiento. • ListoParaMantenimiento: El nodo está listo para que se le realice el mantenimiento.	Modo de mantenimiento (cadena)

modo solicitado	Estado del modo de mantenimiento solicitado para el nodo. Valores posibles: • Desactivado: No se ha solicitado ningún mantenimiento. • Error de recuperación: El nodo no pudo recuperarse del modo de mantenimiento. • Inesperado: Se detectó que el nodo estaba fuera de línea, pero en modo Deshabilitado. • Recuperación tras mantenimiento: El nodo se encuentra en proceso de recuperación tras haber estado en modo de mantenimiento. • Preparación para el mantenimiento: Se están tomando medidas para preparar un nodo para realizar el mantenimiento. • ListoParaMantenimiento: El nodo está listo para que se le realice el mantenimiento.	Modo de mantenimiento (cadena)

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
}
```

Nueva versión

12,2

Encuentra más información

["Conceptos del modo de mantenimiento de almacenamiento NetApp HCI"](#)

Deshabilitar SSH

Puedes usar el `DisableSsh` Método para deshabilitar el servicio SSH para un único nodo de almacenamiento. Este método no afecta la duración del tiempo de espera del servicio SSH en todo el clúster.

Parámetro

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
activado	Estado del servicio SSH para este nodo.	booleano

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:


```
{
  "method": "DisableSsh",
  "params": {
    },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {"enabled": false}
}
```

Habilitar modo de mantenimiento

Puedes usar el `EnableMaintenanceMode` Método para preparar un nodo de almacenamiento para mantenimiento. Los escenarios de mantenimiento incluyen cualquier tarea que requiera apagar o reiniciar el nodo.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
<code>forceWithUnresolvedFaults</code>	Se debe habilitar el modo de mantenimiento forzado para este nodo incluso con fallos de clúster que bloqueen el sistema.	booleano	FALSO	No
<code>nodos</code>	La lista de identificadores de nodo que se pondrán en modo de mantenimiento. Solo se admite un nodo a la vez.	matriz de enteros	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
Límite de intercambio primario por minuto	Número de porciones primarias a intercambiar por minuto. Si no se especifica, todas las porciones primarias se intercambiarán a la vez.	entero	Ninguno	No
se acabó el tiempo	Especifica cuánto tiempo debe permanecer habilitado el modo de mantenimiento antes de que se desactive automáticamente. Formateado como una cadena de tiempo (por ejemplo, HH:mm:ss). Si no se especifica, el modo de mantenimiento permanecerá activado hasta que se desactive explícitamente.	cadena	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
manejador asíncrono	Puede utilizar el método GetAsyncResult para recuperar este asyncHandle y determinar cuándo finaliza la transición al modo de mantenimiento.	entero

modo actual	Estado actual del modo de mantenimiento del nodo. Valores posibles: • Desactivado: No se ha solicitado ningún mantenimiento. • Error de recuperación: El nodo no pudo recuperarse del modo de mantenimiento. • Recuperación tras mantenimiento: El nodo se encuentra en proceso de recuperación tras haber estado en modo de mantenimiento. • Preparación para el mantenimiento: Se están tomando medidas para preparar un nodo para realizar el mantenimiento. • ListoParaMantenimiento: El nodo está listo para que se le realice el mantenimiento.	Modo de mantenimiento (cadena)
modo solicitado	Estado del modo de mantenimiento solicitado para el nodo. Valores posibles: • Desactivado: No se ha solicitado ningún mantenimiento. • Error de recuperación: El nodo no pudo recuperarse del modo de mantenimiento. • Recuperación tras mantenimiento: El nodo se encuentra en proceso de recuperación tras haber estado en modo de mantenimiento. • Preparación para el mantenimiento: Se están tomando medidas para preparar un nodo para realizar el mantenimiento. • ListoParaMantenimiento: El nodo está listo para que se le realice el mantenimiento.	Modo de mantenimiento (cadena)

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

12,2

Encuentra más información

["Conceptos del modo de mantenimiento de almacenamiento NetApp HCI"](#)

Habilitar SSH

Puedes usar el `EnableSsh` Método para habilitar el servicio Secure Shell (SSH) para un solo nodo. Este método no afecta la duración del tiempo de espera de SSH en todo el clúster y no exime al nodo de que SSH se deshabilite debido al tiempo de espera de SSH global.

Parámetro

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
activado	Estado del servicio SSH para este nodo.	booleano

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "EnableSsh",
  "params": {
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {"enabled": true}
}
```

Obtener configuración de clúster

Puedes usar el `GetClusterConfig` Método API para devolver información sobre la configuración del 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 de retorno:

Nombre	Descripción	Tipo
clúster	Información de configuración del clúster que el nodo utiliza para comunicarse con el clúster.	clúster

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

Obtener estado del clúster

Puedes usar 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 de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
clúster	Nombre del clúster.	cadena
estado	• Disponible: El nodo no ha sido configurado con un nombre de clúster. • Pendiente: El nodo está pendiente para un clúster con nombre específico y se puede agregar. • Activo: El nodo es un miembro activo de un clúster y no puede agregarse a otro clúster.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetClusterState",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" :
    "cluster" : "Cluster101"
    "state" : "Active"
}
```

Nueva versión

9,6

Obtener configuración

Puedes usar el `GetConfig` Método API para obtener toda la información de configuración de un nodo. Este método de la API incluye la misma información disponible en ambos. `GetClusterConfig` y `GetNetworkConfig` Métodos de la API.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
configuración	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 con el 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 para este método son similares al siguiente ejemplo:


```
{
  "method": "GetConfig",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Debido a la extensión de este ejemplo de respuesta, se documenta en un tema complementario.

Nueva versión

9,6

Encuentra más información

- [Obtener configuración de clúster](#)
- [Obtener configuración de red](#)
- [Obtener configuración](#)

Obtener configuración de la unidad

Puedes usar el `GetDriveConfig` Método para obtener información de la unidad para los recuentos esperados de unidades de segmento y bloque, así como el número de unidades de segmento y bloque que están actualmente conectadas al nodo.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Configuración de la unidad	Información sobre las unidades conectadas al nodo.	conducir

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{  
  "method": "GetDriveConfig",  
  "params": {},  
  "id" : 1  
}
```

Ejemplo de respuesta

Las respuestas para este método son similares al siguiente ejemplo. Debido a su longitud, la respuesta contiene información solo para una unidad de un 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
    }
  }
}

```

Obtener configuración de hardware

Puedes usar el `GetHardwareConfig` Método para obtener la información de configuración de hardware de un nodo. Estos datos de configuración están destinados para uso interno. Para obtener un inventario más útil de los componentes del hardware del sistema en tiempo real, utilice `GetHardwareInfo` método en su lugar.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
configuración de hardware	Lista de información de hardware y configuración actual.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetHardwareConfig",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Las respuestas para este método son similares al siguiente ejemplo.

```
{
  "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
    }
}
}
}

```

Nueva versión

9,6

Obtener información de hardware

Puedes usar el `GetHardwareInfo` Método para obtener información y estado del hardware en tiempo real para un solo nodo. La información sobre el hardware generalmente incluye fabricantes, proveedores, versiones, unidades y otra información de identificación asociada.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
fuerza	Establezca este parámetro "force" en verdadero para ejecutarlo en todos los nodos del clúster.	booleano	FALSO	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Información de hardware	Información de hardware del nodo.	Información de hardware

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    },
    ...
]
}
}
}

```

Nueva versión

9,6

GetIpmiConfig

Puedes usar el `GetIpmiConfig` Método para recuperar información de sensores de hardware de los sensores que se encuentran en su nodo.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo
Tipo de chasis	Se utiliza para mostrar información sobre cada tipo de chasis de nodo. Valores posibles: • all: devuelve información de los sensores para cada tipo de chasis. • {tipo de chasis}: devuelve información de los sensores para un tipo de chasis especificado.	cadena

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
nombre del sensor	Nombre del sensor que se ha encontrado.	cadena
ID de sensor único	Identificador único del sensor.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    ],
  }
}
```

Nueva versión

9,6

GetIpmiInfo

Puedes usar el `GetIpmiInfo` Método para mostrar un informe detallado de los sensores (objetos) de los ventiladores de los nodos, las temperaturas de entrada y salida de aire y las fuentes de alimentación que son monitoreadas por el sistema.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
sensores	Información detallada de cada sensor dentro de un nodo.	matriz de objetos JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetIpmiInfo",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Debido a la longitud de la respuesta devuelta por este método de la API, se han eliminado intencionadamente partes de la misma de este documento. Se incluyen las partes de la información del hardware que el sistema monitoriza para garantizar que el nodo funcione 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"
    },
    .
    .
    .
    }
    ]
    }
    }
    }
    }

```

Nueva versión

9,6

Obtener configuración de red

Puedes usar 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 de retorno:

Nombre	Descripción	Tipo
red	Tipos de conexión de red y configuración actual para cada interfaz de red del nodo.	red (todas las interfaces)

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetNetworkConfig",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Debido a la extensión de este ejemplo de respuesta, se documenta en un tema complementario.

Nueva versión

9,6

Encuentra más información

[Obtener configuración de red](#)

ObtenerInterfazDeRed

Puedes usar 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	Requerido
interfaz	El nombre de la interfaz para obtener información sobre cada nodo. Valores posibles: • Bond1G • Bond10G	cadena	Ninguno	No
fuerza	Establezca este parámetro en verdadero para ejecutarlo en todos los nodos del clúster.	booleano	FALSO	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
nodos	Una matriz de objetos que describe la interfaz de cada nodo de almacenamiento en el 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: (Interfaz de red) Información de configuración de la interfaz para este nodo de almacenamiento.	matriz de objetos JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
        }
    }
}
]
}

```

```
}
```

Nueva versión

9,6

ObtenerCifrasTlsActivasDeNodo

Puedes usar el `GetNodeActiveTlsCiphers` Método en un solo nodo para obtener una lista de los cifrados TLS que actualmente se aceptan en este nodo. Puedes utilizar este método en nodos de gestión y almacenamiento.

Parámetro

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Cifrados obligatorios	Lista de conjuntos de cifrado TLS obligatorios para el nodo. Se trata de cifrados que están siempre activos en el nodo.	cadena
Cifrados suplementarios	Lista de conjuntos de cifrado TLS suplementarios para el nodo.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    ]
  }
}

```

Informe de unidades GetNodeFips

Puedes usar el `GetNodeFipsDrivesReport` Método para comprobar el estado de la capacidad de cifrado de la unidad FIPS 140-2 de un único nodo en el clúster de almacenamiento. Debe ejecutar este método en un nodo de almacenamiento individual.

Parámetro

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Unidades fips	Un objeto JSON que contiene el estado de la compatibilidad con la característica FIPS 140-2 para este nodo. Valores posibles: • Ninguno: El nodo no es compatible con FIPS. • Parcial: El nodo es compatible con FIPS, pero no todas las unidades del nodo son unidades FIPS. • Listo: El nodo es compatible con FIPS y todas las unidades del nodo son unidades FIPS (o no hay unidades presentes).	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetNodeFipsDrivesReport",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "fipsDrives": "None"
  }
}
```

Nueva versión

11,5

Obtener certificado SSL del nodo

Puedes usar el `GetNodeSSLCertificate` Método para recuperar el certificado SSL

que está actualmente activo en el nodo de administración.

Parámetros



Debes llamar a este método contra el nodo de administración. Por ejemplo:

```
https://<management node IP>:442/json-rpc/10.0
```

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
certificado	El texto completo del certificado codificado en formato PEM.	cadena
detalles	Información decodificada del certificado.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
    "method" : "GetNodeSSLCertificate",
    "params" : {},
    "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
    "id": 1,
    "result": {
        "certificate": "-----BEGIN CERTIFICATE-----
\nMIIEEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGS Ib3DQEBBQUAMIGDMQswCQYD\nVUuzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\nA1UEChMYV2hh dCBIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkB Fh53\n\ naGF0aGFwcGVuc0B2ZWdhc3N0YXlzaW4udmVnYXMwHhcNMTCwMzA4MjI lMDI2WhcN\n\n MjcwMzA4MjI lMDI2WjCBGzELMAkGA1UEBhMCVVmx CzaJBgNVBAgTAK5WMRUwEwYD\n\n VQQHFAXWZWhcywgQmFieSExITAfBgNVBAoTGFdoYXQgSGFWcGVucyBpb iBWZWhd\n\n \ ncy4uL jEtMCSqGS Ib3DQEJAR Yed2hhdGhhcHB1bnNAdm
```



```
VnYXNzdGF5c2luLnZl\nZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f
nLKQNWEMR\n6akeDKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH
P4\nt6P/Si0aYr4ovx15wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nmrgp
GZQF3iOSIcBhtLKE5186JVT6j5dg6yjUGQO352ylc9HXHcn6lb/jyl0DmVNU\nnZ0caQwAmIS3J
moyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K6lS\nn7dg9cyXu4afXcgKy14Ji
NBvqbBjhgJtE76yAy6rThu0xM3jjdkcb9Y8miNzx+AC\nnq+itawIDAQABo4HrMIHoMB0GA1Ud
DgQWBBrvvBRPno5S34zGRhrnDJyTsdnEbTCB\nnuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nnA1UEBhMCVVMxCzAJBgNVBAGTAK5WMRUwEwYDVQOHFAxW
ZWdhcywgQmFieSEExITAf\nnBgNVBAoTGFdoYXQSGFwGVucyBpbjBWZWdhcy4uLjEtMCsGCSqG
S1b3DQEJARYe\nd2hhdGhhcHB1bnNAdmVnYXNzdGF5c2luLnZlZ2FzgkAzBsiFZjjf/MwDAYD
VR0T\nnBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s71mQPECwVLfiE/ndtIbnpe\nnMq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7Jyfs3714rRolFpX6N\nniebEgAaE5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dH0lQ+WYnoO/eIMy0coT26JB15H\nnDEwvdl+DwKxnS1cx1v
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nnHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\nn7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAJJDg
l0QoQDWNDoTerBs80nwiouA==\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"
    }
  }
}
```

ObtenerCifradosTLSCompatiblesConNodo

Puedes usar el `GetNodeSupportedTlsCiphers` Método en un solo nodo para obtener una lista de los cifrados TLS que actualmente son compatibles con este nodo. Puedes utilizar este método en nodos de gestión y almacenamiento.

Parámetro

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Cifrados obligatorios	Lista de conjuntos de cifrado TLS obligatorios para el nodo. Se trata de cifrados que están siempre activos en el nodo.	cadena
Cifrados suplementarios por defecto	Lista de conjuntos de cifrado TLS suplementarios predeterminados para el nodo. Los cifrados suplementarios se restauran a esta lista cuando se ejecuta el método API <code>ResetNodeSupplementalTlsCiphers</code> .	cadena
Cifrados suplementarios compatibles	Lista de conjuntos de cifrado TLS suplementarios disponibles que puede configurar con el método API <code>SetNodeSupplementalTlsCiphers</code> .	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    ]
  }
}

```

Obtener información del parche

Puedes usar el `GetPatchInfo` Método para obtener información sobre los parches de software Element instalados en un nodo de almacenamiento.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
force	Fuerza la ejecución del método en todos los nodos del clúster de almacenamiento. Esto solo es necesario cuando se envía la API a una dirección IP de clúster en lugar de a un solo nodo. Valores posibles: • true • false	booleano	false	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
parches	Objeto que contiene información sobre los parches instalados en este nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
        ]
      }
    }
  }
}

```

Nueva versión

12,3

ObtenerOperaciónPendiente

Puedes usar el `GetPendingOperation` Método para detectar una operación en un nodo que se encuentra actualmente en curso. Este método también puede utilizarse para informar cuando una operación ha finalizado.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
pendiente	Valores posibles: • Es cierto: la operación aún está en curso. • FALSO: La operación ya no está en curso.	booleano
operación	Nombre de la operación que está en curso o que ha finalizado.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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",
    }
  }
}
```

Nueva versión

9,6

Obtener información Ssh

Puedes usar 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 de retorno:

Nombre	Descripción	Tipo
resultado	Estado del servicio SSH para este nodo.	booleano

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method" : "GetSshInfo",
  "params" : {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "enabled": false
  }
}
```

Hardware de la unidad de lista

Puedes usar el `ListDriveHardware` Método para listar todas las unidades conectadas a un nodo. Cuando se utiliza en nodos individuales, este método devuelve información sobre el hardware de la unidad. Cuando se utiliza en el nodo maestro del clúster MVIP, este método devuelve información de todas las unidades en todos los nodos.

Parámetros



La línea "securitySupported": true de la respuesta del método no implica que las unidades sean capaces de cifrar; solo que se puede consultar el estado de seguridad. Si tiene un tipo de nodo con un número de modelo que termina en "-NE", los comandos para habilitar las funciones de seguridad en estas unidades fallarán.

Este método tiene el siguiente parámetro:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
fuerza	Establezca el valor en verdadero para ejecutar este método en todos los nodos.	booleano	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Hardware de la unidad	Se devolvió la información del hardware de la unidad para el nodo.	matriz de objetos JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}

```

Nueva versión

9,6

Encuentra más información

[Habilitar cifrado en reposo](#)

Lista de interfaces de red

Puedes usar el `ListNetworkInterfaces` Método para listar información sobre cada interfaz de red en un nodo. Este método de API está diseñado para su uso en nodos individuales; se requiere autenticación mediante ID de usuario y contraseña para acceder a nodos individuales. Sin embargo, puede utilizar este método en el clúster si al parámetro `force` se le asigna el valor verdadero en la llamada al método. Cuando se utiliza el parámetro en el clúster, se enumeran todas las interfaces.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
fuerza	Valores posibles: • Verdadero: Se devuelve información sobre todas las interfaces de red del clúster. • Falso: No se devuelve ninguna información.	booleano	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

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 <code>force = true</code>).	Interfaz de red formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
            }
          ]
        }
      }
    ]
  }
}
```


Parámetro

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Estadísticas de interfaz de red	Una lista de información estadística de red, como el número de paquetes descartados y varios tipos de errores de red, para cada interfaz de red de un nodo de almacenamiento.	Estadísticas de interfaz de red formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
  ]
}

```

Nueva versión

12,3

Pruebas de lista

Puedes usar el `ListTests` Método para listar 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 de retorno:

Nombre	Descripción	Tipo
pruebas	Lista de pruebas que se pueden realizar en el nodo.	matriz de cadenas

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    ]
  }
}
```

Nueva versión

9,6

Utilidades de lista

Puedes usar el `ListUtilities` Método para listar 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 de retorno:

Nombre	Descripción	Tipo
servicios públicos	Lista de utilidades actualmente disponibles para ejecutarse en el nodo.	matriz de cadenas

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    ]
  }
}
```

Nueva versión

9,6

Eliminar certificado SSL del nodo

Puedes usar el `RemoveNodeSSLCertificate` Método para eliminar el certificado SSL

de usuario y la clave privada del nodo de administración. Una vez eliminados el certificado y la clave privada, el nodo de administración se configura para usar el certificado y la clave privada predeterminados.

Parámetros



Debes llamar a este método contra el nodo de administración. Por ejemplo:

```
https://<management node IP>:442/json-rpc/10.0
```

Este método no tiene parámetros de entrada.

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method" : "RemoveNodeSSLCertificate",
  "params" : {},
  "id" : 3
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 3,
  "result" : {}
}
```

Restablecer unidades

Puedes usar el `ResetDrives` Método para inicializar de forma proactiva las unidades y eliminar todos los datos que residen actualmente en una unidad. Posteriormente, la unidad se puede reutilizar en un nodo existente o utilizarse en un nodo actualizado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
unidades	Lista de nombres de dispositivos (no identificadores de unidad) para restablecer.	cadena	Ninguno	Sí
fuerza	Establezca el valor en verdadero para reiniciar la unidad.	booleano	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
detalles	Detalles de las unidades que se están reiniciando.	matriz de objetos JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

Restablecer nodo

Puedes usar el `ResetNode` Método para restablecer un nodo a la configuración de fábrica. Al llamar a este método, se eliminan del nodo todos los datos, paquetes (actualizaciones de software, etc.), configuraciones y archivos de registro. 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` solo se puede utilizar en nodos que se encuentren en estado "Disponible". No se puede utilizar en nodos que estén "activos" en un clúster, ni en estado "pendiente".

PRECAUCIÓN:

Este método borra cualquier dato de cliente que se encuentre en el nodo.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
construir	Se utiliza para especificar la URL de una imagen de software Element remota a la que se restablecerá el nodo.	URL	Ninguno	No
fuerza	Establecer en verdadero para reiniciar el nodo.	booleano	Ninguno	Sí
opciones	Se utiliza para introducir las especificaciones para ejecutar las operaciones de reinicio. Si fuera necesario, el soporte de NetApp proporcionará los detalles.	Objeto JSON	Ninguno	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}

```

```
}  
}
```

Nueva versión

9,6

Restablecer nodoCifradosTlsSuplementarios

Puedes usar el `ResetNodeSupplementalTlsCiphers` Método para restaurar la lista de cifrados TLS suplementarios a la predeterminada. Puedes usar este comando en los nodos de administración.

Parámetro



Debes llamar a este método contra el nodo de administración. Por ejemplo:

```
https://<management node IP>:442/json-rpc/10.0
```

Este método no tiene parámetros de entrada.

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{  
  "method": "ResetNodeSupplementalTlsCiphers",  
  "params": {},  
  "id" : 1  
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{  
  "id" : 1,  
  "result" : {}  
}
```

Reiniciar la red

Puedes usar 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 provoca una pérdida temporal de la conectividad de red.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
fuerza	Establézcalo en verdadero para reiniciar los servicios de red en un nodo.	booleano	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "RestartNetworking",
  "params": {
    "force" : true
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{ "id" : 1,
  "result" : {}
}
```

Nueva versión

9,6

Reiniciar servicios

Puedes usar el `RestartServices` Método para reiniciar los servicios en un nodo.

Parámetros

PRECAUCIÓN:

Este método provoca una interrupción temporal de los servicios del nodo.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
fuerza	Establecer en verdadero para reiniciar los servicios en un nodo.	booleano	Ninguno	Sí
servicio	Nombre del servicio que se reiniciará.	cadena	Ninguno	No
acción	Acción a realizar en el servicio (iniciar, detener, reiniciar).	cadena	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
detalles	El resultado del procedimiento de reinicio del servicio, incluyendo los errores (si los hubiera).	Objeto JSON
duración	El tiempo, en segundos, que tardó en reiniciarse los servicios en el nodo.	cadena
resultado	Resultados del reinicio.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:


```
{
  "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"
  }
}
```

Nueva versión

9,6

ConfigurarClúster

Puedes usar 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 actual de la interfaz del clúster para un nodo, ejecute el siguiente comando: `GetClusterConfig` Método API.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
clúster	Atributos de configuración que deben modificarse durante esta llamada al método. Solo los campos que desee modificar deben añadirse a este método como miembros en este parámetro.	clúster	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
clúster	Información de configuración que el nodo utiliza para comunicarse con el clúster.	clúster

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  }
}
```

Nueva versión

9,6

Configurar

Puedes usar el `SetConfig` Método para configurar la información de red y clúster para el nodo. Este método incluye la misma configuración en un único método de API que está disponible utilizando ambos. `SetClusterConfig` y `SetNetworkConfig` métodos. Con este método solo deben incluirse los campos que desee modificar.

Parámetro

PRECAUCIÓN:

Cambiar el modo de enlace en un nodo puede provocar una pérdida temporal de la conectividad de la red.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
clúster	Información del clúster que identifica cómo se comunica el nodo de almacenamiento con el clúster de almacenamiento con el que está asociado.	clúster	Ninguno	No
red	Tipos de conexión de red y configuración actual para cada interfaz de red del nodo.	red (todas las interfaces)	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
configuración	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 con el 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 para este método son similares al siguiente ejemplo:

```
{
  "method": "SetConfig",
  "params": {
    "cluster": {
      "name": "MyHostname"
    },
    "network": {
      "Bond10G": {
        "bond-mode": "ALB"
      }
    }
  }
}
```

Ejemplo de respuesta

La respuesta de este método es la misma que la que devuelve el método GetConfig. Cuando se utiliza SetConfig, se pueden ver todos los campos para la visualización del objeto y los valores actualizados.

Nueva versión

9,6

Encuentra más información

- [ConfigurarClúster](#)
- [Configurar configuración de red](#)
- [Obtener configuración](#)

Configurar configuración de red

Puedes usar el SetNetworkConfig Método para configurar la red de un nodo. Para mostrar la configuración de red actual de un nodo, ejecute el siguiente comando: GetNetworkConfig Método API.

Parámetro

PRECAUCIÓN:

Cambiar el modo de enlace en un nodo puede provocar una pérdida temporal de la conectividad de la red.

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
red	Un objeto que contiene la configuración de red del nodo para modificar. Solo necesitas añadir los campos que quieras modificar a este método como atributos en este parámetro.	red (todas las interfaces)	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
red	La configuración de red nueva y actual para el nodo.	red (todas las interfaces)

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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 respuesta del método `GetNetworkConfig`. El método muestra todos los miembros de cada objeto e incluye los nuevos valores para cualquier miembro que haya cambiado.

Nueva versión

9,6

Encuentra más información

- [Obtener configuración de red](#)
- [Obtener configuración de red](#)

SetNodeSSLCertificate

Puedes usar el `SetNodeSSLCertificate` Método para configurar un certificado SSL de usuario y una clave privada para el nodo de administración.



Después de utilizar la API, debe reiniciar el nodo de administración.

Parámetros



Debes llamar a este método contra el nodo de administración. Por ejemplo:

```
https://<management node IP>:442/json-rpc/10.0
```

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
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 sistemas operativos y navegadores comunes. Si la extensión no está presente, la API rechazará el certificado por ser inválido.	cadena	Ninguno	Sí
clave privada	La versión de texto codificada en PEM de la clave privada.	cadena	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method" : "SetNodeSSLCertificate",
  "params" : {
    "privateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEA8U+28fnLKQNWEMMR6akeDKuehSpS79odLGigI18qlCV/AUY5\nZLjqsT
jBvTJVRv44yoCTgNrx36U7FHP4t6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7Je\nlOB6AD7fmiTweP
20HRYpZvY+Uz7LYEFCmrpgGZQF3iOSIcBHtLKE5186JVT6j5dg\n6yJUGQO352ylc9HXHcn6lb
/jy10DmVNUZ0caQwAmIS3Jmoyx+zj/Ya4WKq+2SqTA\nX7bX0F3wHHfXnZlHnM8fET5N/9A+K6
lS7dg9cyXu4afXcgKy14JiNBvqbBjhGJtE\n76yAy6rTHu0xM3jjdkcb9Y8miNzxF+ACq+itaw
IDAQABAOIBAH1jlIzr6/sltqVW\n00qVC/49dyNu+KWVSq92ti9rFe7hBPueh9gklh78hP9Qli
tLkir3YK4GFsTFUMux\n7z1NRCxA/4LrmLSkAjW2kRXDfVl2bwZq0ua9NefGw92O8D2OZvbuOx
k7Put2p6se\nnfgNzSjf2SI5DIX3UME5dDN5FByu52CJ9mI4U16ngbWln2wc4nsxJg0aAEkzB7w
```



```
"certificate": "-----BEGIN CERTIFICATE-----\n\nmIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSib3DQEBBQUAMIGDMQswCQYD\nJUVUzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\nBIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKWyJKoZIhvcNAQkBfH53\nN0YXlzaW4udmVnYXMwHhcNMTCwMzA4MjI1MDI2WhcN\nUEBhMCVVMxCzAJBgNVBAGTAk5WMRUwEwYD\n\nvYXNzdGF5c2luLnZl\n\nnLKQNWEWMR\n\nGZQF3iOsICBHtLKE5186JVT6j5dg6yJUGQO352ylc9HXHCn6lb/jyl0DmVNU\nmoys+zj/Ya4WKq+2SqTAX7bXOF3wHHfXnZlHnM8fET5N/9A+K6lS\nNBvqbBjhGJtE76yAy6rTHu0xM3jjdkcb9Y8miNzx+F+AC\nDgQWBBrvvBRPno5S34zGRhrnDJyTsdnEbTCB\n\nZWDhcywgQmFieSExITAf\n\nVR0T\n\no5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7JyfS3714rRolFpX6N\nWvB6zgiAcMRIKqu3DmJ7y3CFGk9dHolQ+WYnoO/eIMy0coT26JB15H\nERv5lg1gua6AE3tBrlov8qlG4zMJboo3YEwMFwxLkxAFXR\nr4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n10QoQDWNDOTeRBsz80nwioUA==\n\n-----END CERTIFICATE-----\n"}\n\n    "id" : 2\n}
```

```
{
  "id" : 2,
  "result" : {}
}
```

SetNodeSupplementalTlsCiphers

Puedes usar el `SetNodeSupplementalTlsCiphers` Método para especificar la lista de cifrados TLS suplementarios. Puedes usar este comando en los nodos de administración.

Parámetro



Debes llamar a este método contra el nodo de administración. Por ejemplo:

```
https://<management node IP>:442/json-rpc/10.0
```

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
Cifrados suplementarios	Los nombres de los conjuntos de cifrado suplementarios utilizan el esquema de nomenclatura de OpenSSL. El uso de nombres de conjuntos de cifrado no distingue entre mayúsculas y minúsculas.	cadena	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Cifrados obligatorios	Lista de conjuntos de cifrado TLS obligatorios para el nodo. Se trata de cifrados que están siempre activos en el nodo.	cadena

Nombre	Descripción	Tipo
Cifrados suplementarios	Lista de conjuntos de cifrado TLS suplementarios para el nodo.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    ]
  }
}
```

Cerrar

Puedes usar el `Shutdown` Método para reiniciar o apagar los nodos de un clúster. Con este método puede apagar un solo nodo, varios nodos o todos los nodos del clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nodos	Lista de NodeIDs para los nodos que se reiniciarán o apagarán.	matriz de enteros	Ninguno	Sí
opción	Medidas a tomar para el grupo. Valores posibles: • reiniciar: Reinicia el clúster. • detener: Realiza un apagado completo.	cadena	Reanudar	No

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    ]
  }
}
```

Nueva versión

9,6

TestConnectEnsemble

Puedes usar el `TestConnectEnsemble` Método para verificar la conectividad con un conjunto de bases de datos específico. Por defecto, utiliza el conjunto del clúster con el que está asociado el nodo. Alternativamente, puede proporcionar un conjunto diferente para probar la conectividad.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
conjunto	Una lista separada por comas de direcciones IP de clústeres de nodos de conjunto para pruebas de conectividad.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

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 requerido para ejecutar la prueba. • result: (cadena) Los resultados de la prueba completa.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

TestConnectMvip

Puedes usar el `TestConnectMvip` Método para probar la conexión de administración con el clúster de almacenamiento. La prueba envía un ping al MVIP y ejecuta un método API simple para verificar la conectividad.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
MVIP	Puede pasar este valor para probar la conexión de administración de un MVIP diferente. No es necesario utilizar este valor al probar la conexión con el clúster de destino.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
detalles	Información sobre la operación de prueba (objeto JSON): • <code>connected</code>: Indica si la prueba pudo conectarse al MVIP (booleano) • <code>mvip</code>: El MVIP probado contra (cadena) • <code>`pingBytes`</code> Detalles de las pruebas de ping con 56 bytes y 1500 bytes (objeto) ◦ <code>`56`</code> Resultados de la prueba de ping de 56 bytes (objeto JSON): ▪ <code>individualResponseTimes</code>: Lista de tiempos de respuesta de cada nodo del conjunto (matriz de cadenas) ▪ <code>individualStatus</code>: Lista del estado de ping de cada nodo del conjunto (matriz booleana) ▪ <code>responseTime</code>: Tiempo promedio de respuesta al ping (cadena) ▪ <code>successful</code>: Indica si la prueba de ping fue exitosa (booleano) ◦ <code>`1500`</code> Resultados de la prueba de ping de 1500 bytes (objeto JSON): ▪ <code>individualResponseTimes</code>: Lista de tiempos de respuesta de cada nodo del conjunto (matriz de cadenas) ▪ <code>individualStatus</code>: Lista del estado de ping de cada nodo del conjunto (matriz booleana) ▪ <code>responseTime</code>: Tiempo promedio de respuesta al ping (cadena)	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:
"successful": Indica si la prueba de ping fue

```
{
  "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",
```

```

        "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"
}
}

```

Nueva versión

9,6

TestConnectSvip

Puedes usar el `TestConnectSvip` Método para probar la conexión de almacenamiento al clúster de almacenamiento. La prueba envía un ping al SVIP mediante paquetes ICMP y, cuando tiene éxito, se conecta como iniciador iSCSI.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
svip	Puede pasar este valor para probar la conexión de administración de una SVIP diferente. No es necesario utilizar este valor al probar la conexión con el clúster de destino.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
detalles	Información sobre la operación de prueba (objeto JSON): • <code>connected</code>: Indica si la prueba pudo conectarse a la SVIP (booleano) • <code>svip</code>: El SVIP fue probado contra (cadena) • <code>`pingBytes`</code> Detalles de las pruebas de ping con 56 bytes y 9000 bytes (objeto) ◦ <code>`56`</code> Resultados de la prueba de ping de 56 bytes (objeto JSON): ▪ <code>individualResponseTimes</code>: Lista de tiempos de respuesta de cada nodo del conjunto (matriz de cadenas) ▪ <code>individualStatus</code>: Lista del estado de ping de cada nodo del conjunto (matriz booleana) ▪ <code>responseTime</code>: Tiempo promedio de respuesta al ping (cadena) ▪ <code>successful</code>: Indica si la prueba de ping fue exitosa (booleano) ◦ <code>`9000`</code> Resultados de la prueba de ping de 9000 bytes (objeto JSON): ▪ <code>individualResponseTimes</code>: Lista de tiempos de respuesta de cada nodo del conjunto (matriz de cadenas) ▪ <code>individualStatus</code>: Lista del estado de ping de cada nodo del conjunto (matriz booleana) ▪ <code>responseTime</code>: Tiempo promedio de respuesta al ping (cadena)	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:
"successful": Indica si la prueba de ping fue

```
{
  "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"
}
}

```

Nueva versión

9,6

Pruebas de manejo

Puedes usar 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 cualquier fallo en los resultados de las pruebas de validación.

Parámetros

Solo puedes usar 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	Requerido
fuerza	Establecer en verdadero para probar las unidades en el nodo.	booleano	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
minutos	Especifica el número de minutos que durará la prueba.	entero	10	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
detalles	Información sobre el éxito o el fracaso de la operación de prueba.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "TestDrives",
  "params": {
    "force": true,
    "minutes" : 10
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una tabla que contiene los resultados de las pruebas para cada unidad del nodo.

Nueva versión

9,6

Configuración de hardware de prueba

Puedes usar el `TestHardwareConfig` Método para realizar pruebas de hardware en un nodo. Las opciones de prueba incluyen la verificación de las configuraciones de hardware, las versiones de firmware y que todas las unidades estén presentes.

Parámetros



Estas pruebas no están diseñadas para detectar fallos de hardware.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
limpio	Inicia la prueba de configuración de hardware con una caché limpia. Valores posibles: • verdadero: Elimina el archivo de resultados de pruebas almacenado en caché y vuelve a ejecutar las pruebas. • falso: Recupera los resultados de una prueba almacenada en caché.	booleano	FALSO	No
fuerza	El parámetro de fuerza debe incluirse en este método para reiniciar correctamente el nodo.	booleano	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
detalles	Detalles de la configuración del hardware.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "TestHardwareConfig",
  "params": {
    "force": true
  },
  "id" : 1
}
```

Ejemplo de respuesta

Debido a la extensión de este ejemplo de respuesta, se documenta en un tema complementario.

Nueva versión

9,6

Encuentra más información

[Configuración de hardware de prueba](#)

PruebaLocateCluster

Puedes usar el `TestLocateCluster` Método para validar que el nodo puede localizar el clúster especificado en la configuración del clúster. El resultado valida que el clúster se ha creado y enumera los nodos del conjunto del clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
detalles	Información sobre el éxito o el fracaso de la operación de prueba.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

Prueba de conectividad local

Puedes usar el `TestLocalConnectivity` método para hacer ping a la IP del 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 de retorno:

Nombre	Descripción	Tipo
detalles	Tiempos de respuesta individuales al ping para cada nodo en el clúster local activo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "TestLocalConnectivity",
  "params": {},
  "id": 1
}
```

Ejemplo de respuesta

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
        ]
      }
    }
  }
}
```

```

        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"
}

```

Nueva versión

9,6

Configuración de red de prueba

Puedes usar el `TestNetworkConfig` Método para comprobar que la configuración de red configurada coincide con la configuración de red que se está utilizando en el sistema.

Parámetros

Cuando configura un nodo con el método `SetNetworkConfig`, en la interfaz de usuario o en la interfaz de usuario de texto, la configuración se valida y se almacena. La prueba de la API `TestNetworkConfig` utiliza la configuración almacenada para la lógica posterior a la validación. Por ejemplo, en caso de un corte de energía o una falla de red, puede usar este método de API para asegurarse de que un nodo esté funcionando con la configuración de red almacenada más reciente. Esto valida que no hay errores en la configuración y que se está utilizando la configuración actual.

Esta prueba está diseñada para mostrar únicamente los fallos en la respuesta. Si no hay errores, esta prueba no devuelve ningún resultado. Vea los siguientes ejemplos de respuesta.

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
detalles	Contiene cualquier error encontrado al validar la configuración de red almacenada actualmente con la configuración de red en ejecución.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "TestNetworkConfig",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta 1

Si no se detectan errores, no se devuelve ninguna respuesta.

```
{
  "id" : 1,
  "result": {
    "details": {
      "network": {...}
    },
    "duration": "00:00:00.144514",
    "result": "Passed"
  }
}
```

Ejemplo de respuesta 2

Ejemplo de una 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 faltante.

```
{
  "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"
  }
}
```

Nueva versión

9,6

Encuentra más información

[Configurar configuración de red](#)

Prueba de ping

Puedes usar el `TestPing` Método para probar la conectividad de red a todos los nodos del clúster en interfaces de 1G y 10G utilizando paquetes ICMP. La prueba utiliza los tamaños MTU apropiados para cada paquete según la configuración MTU en la configuración de red. `TestPing` No crea una interfaz VLAN temporal.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
intentos	Especifica el número de veces que el sistema debe repetir el ping de prueba.	entero	5	No
hosts	Especifica una lista de direcciones o nombres de host de dispositivos a los que hacer ping, separados por comas. Si no se especifican hosts, el método realiza un ping a los hosts del clúster de almacenamiento.	cadena	Ninguno	No
interfaz	La interfaz existente (base) desde la cual se deben enviar los pings. Valores posibles: • <code>`Bond10G`</code> Enviar pings desde la interfaz Bond10G. • <code>`Bond1G`</code> Enviar pings desde la interfaz Bond1G.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
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
Tiempo de espera de ping (milisegundos)	Especifica el número de milisegundos que se deben esperar para cada respuesta de ping individual.	entero	500 milisegundos	No
prohibir la fragmentación	Habilita la bandera DF (No Fragmentar) para los paquetes ICMP.	booleano	FALSO	No
sourceAddressV4	La dirección IPv4 de origen que se utilizará en los paquetes ping ICMP.	cadena	Ninguno	No
sourceAddressV6	La dirección IPv6 de origen que se utilizará en los paquetes ping ICMP.	cadena	Ninguno	No
tiempo de espera total en segundos	Especifica el tiempo en segundos que el ping debe esperar una respuesta del sistema antes de realizar el siguiente intento de ping o finalizar el proceso.	entero	5	No
etiqueta de red virtual	El ID de VLAN que se utilizará al enviar los paquetes ping.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
detalles	Lista de cada IP con la que el nodo pudo comunicarse y estadísticas de respuesta de ping.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}

```

Nueva versión

5,0

Prueba de conectividad remota

Puedes usar `TestRemoteConnectivity` Método para hacer ping a cada nodo del clúster remoto y comprobar la conexión con la base de datos del conjunto remoto. Los

clústeres deben estar emparejados para obtener resultados útiles con este método. Si falla la conexión remota a la base de datos, la respuesta del sistema enumera las excepciones.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
detalles	Tiempos de respuesta individuales al ping para cada nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
}

```

Nueva versión

9,6

Métodos de la API de replicación

orden de operaciones de emparejamiento de clústeres

Debe establecer una conexión entre un par de clústeres de almacenamiento que ejecutan el software Element antes de poder utilizar la replicación remota.

Utilice el siguiente conjunto de métodos de la API para establecer una conexión de clúster:

- [Iniciar emparejamiento de clústeres](#):

Este método de la API crea y devuelve una clave de emparejamiento que se utiliza para establecer un par de clústeres. La clave está codificada y contiene información que se utiliza para establecer comunicaciones entre clústeres. Un único clúster puede emparejarse con hasta cuatro clústeres más. Sin embargo, se debe generar una nueva clave para cada par de clústeres. El [Iniciar emparejamiento de clústeres](#) Este método genera una nueva clave cada vez que se llama. Utilice cada clave única con el [Emparejamiento de clústeres completo](#) método para emparejar cada clúster adicional.



Por motivos de seguridad, la clave de emparejamiento no debe enviarse a otros usuarios por correo electrónico. La clave contiene un nombre de usuario y una contraseña.

- [Emparejamiento de clústeres completo:](#)

Este método utiliza la clave de emparejamiento creada con el [Iniciar emparejamiento de clústeres](#) Método API para crear un par de clústeres. Emitir el [Emparejamiento de clústeres completo](#) Método API con el parámetro clusterPairingKey al destino. El clúster de origen es el clúster que creó la clave.

Encuentra más información

- [Iniciar emparejamiento de clústeres](#)
- [Emparejamiento de clústeres completo](#)

Orden de operaciones de emparejamiento de volúmenes

Debe crear un par de clústeres entre dos clústeres correspondientes antes de que se puedan emparejar los volúmenes.

Utilice el siguiente conjunto de métodos de la API para establecer una conexión de clúster:

- [Emparejamiento de volumen inicial:](#)

Este método de la API crea y devuelve una clave de emparejamiento de volúmenes que se utiliza para crear un par de volúmenes. La clave contiene información que se utiliza para establecer comunicaciones entre volúmenes.

- [Emparejamiento de volumen completo:](#)

Este método utiliza la clave de emparejamiento creada con el [Emparejamiento de volumen inicial](#) Método API para crear un par de volúmenes. Emitir el [Emparejamiento de volumen completo](#) Método API con los parámetros volumeID y volumePairingKey al volumen de destino.

Solo uno de los volúmenes emparejados puede identificarse como volumen objetivo de replicación. Utilice el [Modificar par de volúmenes](#) Método API para establecer la dirección de la replicación de datos del volumen identificando qué volumen es el destino. Los datos se replican desde el volumen de origen al volumen de destino.

Encuentra más información

- [Emparejamiento de volumen inicial](#)
- [Emparejamiento de volumen completo](#)
- [Modificar par de volúmenes](#)

Modos de replicación compatibles para clústeres emparejados

En los clústeres emparejados se admiten los siguientes modos de replicación:

- Replicación asíncrona de datos: Los datos enviados al volumen de destino de la replicación se envían de forma asíncrona. El sistema no espera a que se envíe una confirmación antes de escribir los datos.

- Replicación síncrona de datos: Los datos enviados al volumen de destino de la replicación se envían de forma síncrona. Cuando el sistema confirma las operaciones de E/S enviadas desde el host, se envía una confirmación del sistema de vuelta al host y los datos se envían al volumen de destino de replicación.
- Replicación de datos solo con instantáneas: Solo las instantáneas de volumen se replican en el clúster de destino.

Emparejamiento de clústeres completo

El `CompleteClusterPairing` Este método es el segundo paso en el 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	Requerido
clave de emparejamiento de clúster	Una cadena de caracteres que se devuelve desde el Iniciar emparejamiento de clústeres Método API.	cadena	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
clusterPairID	Identificador único para el par de clústeres.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "CompleteClusterPairing",
  "params": {
    "clusterPairingKey" :
    "7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223
a2231636561313336322d346338662d343631612d626537322d37343536366139353364326
6222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d6330755
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a3931333134323634392c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {
    "clusterPairID" : 1
  }
}
```

Nueva versión

9,6

Encuentra más información

[Iniciar emparejamiento de clústeres](#)

Emparejamiento de volumen completo

Puedes usar `CompleteVolumePairing` para completar el emparejamiento de los dos volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de volumen	El identificador del volumen que completará el par de volúmenes.	entero	Ninguno	Sí
clave de emparejamiento de volumen	La clave devuelta por Emparejamiento de volumen inicial Método API.	cadena	Ninguno	Sí

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "CompleteVolumePairing",
  "params": {
    "volumeID" : 12,
    "volumePairingKey" :
"7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223
a2231636561313336322d346338662d343631612d626537322d37343536366139353364326
6222c22636c75737465725556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d6330755
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a3931333134323634392c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
    },
    "id" : 1
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nueva versión

9,6

Encuentra más información

[Emparejamiento de volumen inicial](#)

ListClusterPairs

Puedes usar el `ListClusterPairs` Método para listar todos los clústeres que están emparejados con el clúster actual. Este método devuelve información sobre los emparejamientos de clústeres activos y pendientes, como estadísticas sobre el emparejamiento actual, así como la conectividad y la latencia (en milisegundos) del emparejamiento de clústeres.

Parámetro

Este método no tiene parámetros de entrada:

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
clusterPairs	Información sobre cada grupo emparejado.	clusterPair información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": "9866fbef-c2f8-4df3-beb9-58a5c4e49c9b",
        "clusterUUID": 5487,
        "latency": 1,
        "mvip": "172.1.1.5",
        "status": "Connected"
        "version": "8.0.0.1361"
      },
      {
        "clusterName": "cluster3",
        "clusterPairID": 2,
        "clusterPairUUID": "8132a699-ce82-41e0-b406-fb914f976042",
        "clusterUUID": 1383,
        "latency": 1,
        "mvip": "172.1.1.6",
        "status": "Connected"
        "version": "8.0.0.1361"
      }
    ]
  }
}

```

Nueva versión

9,6

Lista de volúmenes emparejados activos

Puedes usar el `ListActivePairedVolumes` Método para listar todos los volúmenes activos asociados a un volumen. Este método devuelve información sobre los volúmenes con emparejamientos activos y pendientes.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
volúmenes	Información de volumen para los volúmenes emparejados.	volumen Parformación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ListActivePairedVolumes",
  "params": {
    },
  "id" : 1
}
```

Ejemplo de respuesta

Las respuestas para este método son similares al siguiente ejemplo:

```
{
  "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": "306f746f000000018f47acc0100000000",
"scsiNAADeviceID": "6f47acc100000000306f746f000000018",
"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"
    }
]
}
}
}
}

```

Nueva versión

9,6

Modificar par de volúmenes

Puedes usar el `ModifyVolumePair` Método para pausar o reiniciar la replicación entre un par de volúmenes. Este método se configura 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	Requerido
ID de volumen	Número de identificación del volumen que se va a modificar.	entero	Ninguno	Sí
pausa manual	La replicación remota se puede pausar o reiniciar en el volumen de origen (lectura/escritura). Valores posibles: • verdadero: Pausar la replicación de volumen. • Falso: Reiniciar la replicación de volumen. Si no se especifica ningún valor, no se realiza ningún cambio en la replicación.	booleano	Ninguno	No

modo	Modo de replicación de volumen. Valores posibles: • Asíncrono: Las escrituras se confirman cuando se completan localmente. El clúster no espera a que las escrituras se repliquen en el clúster de destino. • Sincronización: La fuente confirma la escritura cuando los datos se almacenan localmente y en el clúster remoto. • Solo instantáneas: Solo se replican las instantáneas creadas en el clúster de origen. Las escrituras activas desde el volumen de origen no se replican.	cadena	Ninguno	No

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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" : {}
}
```

Nueva versión

9,6

Eliminar par de clústeres

Puedes usar el `RemoveClusterPair` Método para cerrar las conexiones abiertas entre dos grupos emparejados.

Parámetro



Antes de eliminar un par de clústeres, primero debe eliminar todos los emparejamientos de volúmenes con los clústeres mediante el método API `RemoveVolumePair`.

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
clusterPairID	Identificador único utilizado para emparejar dos clústeres.	entero	Ninguno	Sí

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "RemoveClusterPair",
  "params": {
    "clusterPairID": 1
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nueva versión

9,6

Eliminar par de volúmenes

Puedes usar el `RemoveVolumePair` Método para eliminar el emparejamiento remoto entre dos volúmenes. Utilice este método tanto en el volumen de origen como en el de destino que estén emparejados. Cuando se elimina la información de emparejamiento de volúmenes, los datos ya no se replican hacia ni desde el volumen.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de volumen	Identificador del volumen en el que se debe detener el proceso de replicación.	entero	Ninguno	Sí

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "RemoveVolumePair",
  "params": {
    "volumeID": 5
  }
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
  }
}
```

Nueva versión

9,6

Iniciar emparejamiento de clústeres

Puedes usar el `StartClusterPairing` Método para crear una clave codificada a partir de un clúster que se utiliza para emparejarse con otro clúster. La clave creada a partir de este método de la API se utiliza en el `CompleteClusterPairing` Método para establecer un emparejamiento de clústeres. Puedes emparejar un clúster con un máximo de otros cuatro clústeres.

Parámetro

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
clave de emparejamiento de clúster	Una cadena de caracteres que utiliza el Emparejamiento de clústeres completo Método API.	cadena
clusterPairID	Identificador único para el par de clústeres.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "StartClusterPairing",
  "params": {
    },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "clusterPairID": 1,
    "clusterPairingKey":
"7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223a2231636561313336322d346338662d343631612d626537322d373435363661393533643266222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a223139322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d6330755222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c22727063436f6e6e656374696f6e4944223a3931333134323634392c22757365726e616d65223a225f5f53465f706169725f50597a796647704c7246564432444a42227d"
    }
  }
}
```

Nueva versión

9,6

Encuentra más información

[Emparejamiento de clústeres completo](#)

Emparejamiento de volumen inicial

Puedes usar el `StartVolumePairing` Método para crear una clave codificada a partir de un volumen que se utiliza para emparejarlo con otro volumen. La clave que crea este método se utiliza en el `CompleteVolumePairing` método para establecer un emparejamiento de volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
modo	El modo del volumen en el que se inicia el proceso de emparejamiento. Este modo solo se puede configurar si el volumen es el volumen de origen. Valores posibles: • `Async` Los trabajos se confirman cuando se completan localmente. El clúster no espera a que las escrituras se repliquen en el clúster de destino. (Valor predeterminado si no se especifica ningún parámetro de modo). • `Sync` La fuente confirma la escritura cuando los datos se almacenan localmente y en el clúster remoto. • `SnapshotsOnly` Solo se replican las instantáneas creadas en el clúster de origen. Las escrituras activas desde el volumen de origen no se replican.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de volumen	El identificador del volumen en el que se iniciará el proceso de emparejamiento.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
clave de emparejamiento de volumen	Una cadena de caracteres que utiliza el Emparejamiento de volumen completo Método API.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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" :
    "7b226d766970223a223139322e3136382e3133392e31323222c22766f6c756d654944223
    a312c22766f6c756d654e616d65223a2254657374222c22766f6c756d65506169725555494
    4223a2236393632346663622d323032652d343332352d613536392d6563396336353563376
    23561227d"
  }
}
```

Nueva versión

9,6

Encuentra más información

[Emparejamiento de volumen completo](#)

Métodos de la API de seguridad

Agregar servidor de claves al proveedor Kmip

Puedes usar el `AddKeyServerToProviderKmip` método para asignar un servidor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) al proveedor de claves especificado. Durante la asignación, se contacta con el servidor para verificar su 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. Puedes eliminar la asignación usando el `RemoveKeyServerFromProviderKmip` método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del proveedor de clave	El ID del proveedor de claves al que se asignará el servidor de claves.	entero	Ninguno	Sí
ID del servidor de claves	El ID del servidor de claves a asignar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor. La tarea se considera exitosa siempre y cuando no se devuelva ningún error.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "AddKeyServerToProviderKnip",
  "params": {
    "keyProviderID": 1,
    "keyServerID": 15
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result":
    {}
}
```

Nueva versión

11,7

CrearKeyProviderKnip

Puedes usar el `CreateKeyProviderKnip` Método para crear un proveedor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) con el nombre especificado. Un proveedor de claves define un mecanismo y una ubicación para recuperar las claves de autenticación. Cuando se crea un nuevo proveedor de claves KMIP, este no tiene asignado ningún servidor de claves KMIP. Para crear un servidor de claves KMIP, utilice el `CreateKeyServerKnip` método. Para asignarlo a un proveedor, consulte `AddKeyServerToProviderKnip`.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nombre del proveedor de clave	El nombre que se asociará con el proveedor de claves KMIP creado. Este nombre se utiliza únicamente con fines ilustrativos y no necesita ser único.	cadena	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
kmipKeyProvider	Un objeto que contiene detalles sobre el proveedor de claves recién creado.	"KeyProviderKmip"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
  }
}

```

Nueva versión

11,7

CrearKeyServerKmip

Puedes usar el `CreateKeyServerKmip` Método para crear un servidor de claves del 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 las direcciones IP de todos los nodos del servidor en el parámetro `kmipKeyServerHostnames`. Puedes usar el `TestKeyServerKmip` Método para probar un servidor de claves.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
Certificado kmipCa	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 clústeres de servidores clave donde los servidores individuales utilizan diferentes CA, proporcione una cadena concatenada que contenga los certificados raíz de todas las CA.	cadena	Ninguno	Sí
Certificado de cliente kmip	Un certificado PKCS#10 X.509 codificado en Base64 con formato PEM utilizado por el cliente Solidfire KMIP.	cadena	Ninguno	Sí
Nombres de host del servidor de claves kmip	Conjunto de nombres de host o direcciones IP asociadas a este servidor de claves KMIP. Solo se deben proporcionar varios nombres de host o direcciones IP si los servidores clave están en una configuración de clúster.	matriz de cadenas	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
kmipKeyServerName	El nombre del servidor de claves KMIP. Este nombre se utiliza únicamente con fines ilustrativos y no necesita ser único.	cadena	Ninguno	Sí
kmipKeyServerPort	El número de puerto asociado con este servidor de claves KMIP (normalmente 5696).	entero	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Servidor de claves kmip	Un objeto que contiene detalles sobre el servidor de claves recién creado.	"KeyServerKmip"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
  }
}

```

Nueva versión

11,7

Crear par de claves públicas y privadas

Puedes usar el `CreatePublicPrivateKeyPair` Método para crear claves SSL públicas y privadas. Puede utilizar estas claves para generar solicitudes de firma de certificados. Solo puede haber un par de claves en uso por cada clúster de almacenamiento. Antes de utilizar este método para reemplazar las claves existentes, asegúrese de que ningún proveedor siga utilizando dichas claves.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nombre común	El campo Nombre común (CN) del nombre distinguido X.509.	cadena	Ninguno	No
país	El campo de nombre distinguido País © de X.509.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
dirección de correo electrónico	El nombre distinguido X.509 Campo de dirección de correo electrónico (MAIL).	cadena	Ninguno	No
localidad	El campo de nombre distinguido X.509 Nombre de localidad (L).	cadena	Ninguno	No
organización	El campo de nombre distinguido X.509 Nombre de la organización (O).	cadena	Ninguno	No
unidad organizativa	El campo Nombre de la unidad organizativa del nombre distintivo X.509 (OU).	cadena	Ninguno	No
estado	El campo de nombre distinguido X.509 Estado o Nombre de provincia (ST o SP o S).	cadena	Ninguno	No

Valores de retorno

Este método no devuelve ningún valor. Si no hay ningún error, la creación de la clave se considera exitosa.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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":
    {}
}
```

Nueva versión

11,7

EliminarKeyProviderKnip

Puedes usar el `DeleteKeyProviderKnip` Método para eliminar el proveedor de claves inactivo especificado del Protocolo de Interoperabilidad de Gestión de Claves (KMIP).

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del proveedor de clave	El ID del proveedor de claves que se va a eliminar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor. La operación de eliminación se considera exitosa siempre y cuando no haya ningún error.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DeleteKeyProviderKmip",
  "params": {
    "keyProviderID": "1"
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result":
    {}
}
```

Nueva versión

11,7

EliminarKeyServerKmip

Puedes usar el `DeleteKeyServerKmip` Método para eliminar un servidor de claves KMIP (Key Management Interoperability Protocol) existente. Puedes eliminar un servidor de claves a menos que sea el último asignado a su proveedor y que dicho proveedor esté proporcionando claves que se encuentren actualmente en uso.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del servidor de claves	El ID del servidor de claves KMIP que se va a eliminar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor. La operación de eliminación se considera exitosa si no hay errores.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DeleteKeyServerKmip",
  "params": {
    "keyServerID": 15
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result":
    {}
}
```

Nueva versión

11,7

Deshabilitar el cifrado en reposo

Puedes usar el `DisableEncryptionAtRest` método para eliminar el cifrado que se aplicó previamente al clúster utilizando el `EnableEncryptionAtRest` método. Este método de desactivación es asíncrono y devuelve una respuesta antes de que se desactive el cifrado. Puedes usar el `GetClusterInfo` Método para consultar al sistema y comprobar cuándo ha finalizado el proceso.



- No puede utilizar este método para deshabilitar el cifrado de software en reposo. Para deshabilitar el cifrado de software en reposo, necesita ["crear un nuevo clúster"](#) con el cifrado de software en reposo desactivado.
- Para ver el estado actual del cifrado en reposo, el cifrado de software en reposo o ambos en el clúster, utilice la siguiente información: ["método para obtener información del clúster"](#). Puedes usar el `GetSoftwareEncryptionAtRestInfo` ["Método para obtener información sobre el clúster que utiliza para cifrar los datos en reposo."](#)

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DisableEncryptionAtRest",
  "params": {},
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nueva versión

9,6

Encuentra más información

- ["Obtener información del clúster"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Habilitar cifrado en reposo

Puedes usar el `EnableEncryptionAtRest` Método para habilitar el cifrado en reposo del Estándar de Cifrado Avanzado (AES) de 256 bits en el clúster, de modo que el clúster pueda administrar la clave de cifrado utilizada para las unidades en cada nodo. Esta función no está habilitada de forma predeterminada.



- Para ver el estado actual del cifrado en reposo y/o del cifrado de software en reposo en el clúster, utilice la siguiente información: ["método para obtener información del clúster"](#) . Puedes usar el `GetSoftwareEncryptionAtRestInfo` ["Método para obtener información sobre el clúster que utiliza para cifrar los datos en reposo."](#).
- Este método no permite el cifrado de software en reposo. Esto solo se puede hacer utilizando el ["método de creación de clúster"](#) con `enableSoftwareEncryptionAtRest` empezar a `true` .

Cuando se habilita el cifrado en reposo, el clúster administra automáticamente las claves de cifrado internamente para las unidades en cada nodo del clúster.

Si se especifica un `keyProviderID`, la contraseña se genera y se recupera según el tipo de proveedor de claves. Normalmente, esto se realiza utilizando un servidor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) en el caso de un proveedor de claves KMIP. Tras esta operación, el proveedor especificado se considera activo y no se puede eliminar hasta que se deshabilite el cifrado en reposo mediante el `DisableEncryptionAtRest` método.



Si tiene un tipo de nodo con un número de modelo que termina en "-NE", el `EnableEncryptionAtRest` La llamada al método fallará con la respuesta "Cifrado no permitido". El clúster detectó un nodo no cifrable.



Solo debe habilitar o deshabilitar el cifrado cuando el clúster esté en funcionamiento y 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 que se habilite el cifrado. Puedes usar el `GetClusterInfo` Método para consultar al sistema y comprobar cuándo ha finalizado el proceso.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del proveedor de clave	El ID de un proveedor de claves KMIP a utilizar.	entero	Ninguno	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "EnableEncryptionAtRest",
  "params": {},
  "id": 1
}
```

Ejemplos de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo del método `EnableEncryptionAtRest`. No hay resultados que reportar.

```
{
  "id": 1,
  "result": {}
}
```

Mientras se habilita el cifrado en reposo en un clúster, `GetClusterInfo` devuelve un resultado que describe el estado del cifrado en reposo (`encryptionAtRestState`) como `"habilitado"`. Una vez que el cifrado en reposo esté completamente habilitado, el estado devuelto cambiará 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"
    }
  }
}
```

Nueva versión

9,6

Encuentra más información

- ["Unidades de borrado seguro"](#)
- ["Obtener información del clúster"](#)
- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Solicitud de firma de certificado de cliente

Puedes usar el `GetClientCertificateSignRequest` Método para generar una solicitud de firma de certificado que pueda ser firmada por una autoridad de certificación para generar un certificado de cliente para el clúster. Se necesitan certificados firmados para establecer una relación de confianza para interactuar con servicios externos.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Solicitud de firma de certificado de cliente	Solicitud de firma de certificado de cliente X.509 con codificación Base64 en formato PEM y formato PKCS#10.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetClientCertificateSignRequest",
  "params": {
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```
{
  "id": 1,
  "result":
    {
      "clientCertificateSignRequest":
        "MIIBYjCCATMCAQAwgYkxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
    }
}
```

Nueva versión

11,7

ObtenerProveedorDeClavesKmip

Puedes usar el `GetKeyProviderKmip` método para recuperar información sobre el proveedor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) especificado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del proveedor de clave	El ID del objeto proveedor de claves KMIP que se devolverá.	entero	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
kmipKeyProvider	Un objeto que contiene detalles sobre el proveedor de claves solicitado.	"KeyProviderKmip"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    }
  }
}
```

Nueva versión

11,7

ObtenerKeyServerKmip

Puedes usar el `GetKeyServerKmip` método para devolver información sobre el servidor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) especificado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del servidor de claves	El ID del servidor de claves KMIP del que se devolverá información.	entero	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Servidor de claves kmip	Un objeto que contiene detalles sobre el servidor de claves solicitado.	"KeyServerKmip"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
  }
}

```

Nueva versión

11,7

Obtener información de cifrado de software en reposo

Puedes usar el `GetSoftwareEncryptionAtRestInfo` Método para obtener información sobre el cifrado de software en reposo que utiliza el clúster para cifrar los datos en reposo.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Parámetro	Descripción	Tipo	Opcional
Información de clave maestra	Información sobre la clave maestra actual de cifrado en reposo del software.	Información de clave de cifrado	Verdadero

Parámetro	Descripción	Tipo	Opcional
rekeyMasterKeyAsyncResultID	El ID del resultado asíncrono de la operación de re-clave actual o más reciente (si la hay), si aún no se ha eliminado. GetAsyncResult La salida incluirá un newKey campo que contiene información sobre la nueva clave maestra y un keyToDecommission campo que contiene información sobre la clave anterior.	entero	Verdadero
estado	Estado actual del cifrado de software en reposo. Los valores posibles son disabled o enabled .	cadena	FALSO
versión	Un número de versión que se incrementa cada vez que se habilita el cifrado de software en reposo.	entero	FALSO

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}
```

Nueva versión

12,3

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Proveedores de claves de lista Kmip

Puedes usar el `ListKeyProvidersKmip` Método para recuperar una lista de todos los proveedores de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) existentes. Puedes filtrar la lista especificando parámetros adicionales.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
keyProviderIsActive	Los filtros devolvieron objetos de servidor de claves KMIP en función de si están activos o no. Valores posibles: • verdadero: Devuelve solo los proveedores de claves KMIP que están activos (proporcionando claves que se están utilizando actualmente). • false: Devuelve solo los proveedores de claves KMIP que están inactivos (no proporcionan ninguna clave y pueden ser eliminados). Si se omite, los proveedores de claves KMIP devueltos no se filtran en función de si están activos o no.	booleano	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
kmipKeyProviderHasServerAssigned	Los filtros devolvieron proveedores de claves KMIP en función de si tenían asignado un servidor de claves KMIP. Valores posibles: • verdadero: Devuelve solo 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 devueltos no se filtran en función de si tienen asignado un servidor de claves KMIP.	booleano	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Proveedores de claves kmip	Lista de proveedores de claves KMIP que se han creado.	"KeyProviderKmp"formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:


```
{
  "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"
      }
    ]
  }
}
```

Nueva versión

11,7

Lista de servidores clave Kmip

Puedes usar el `ListKeyServersKmip` Método para listar todos los servidores de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) que se han creado. Puede filtrar los resultados especificando parámetros adicionales.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del proveedor de clave	Cuando se especifica, el método solo devuelve los servidores de claves KMIP que están asignados al proveedor de claves KMIP especificado. Si se omite, los servidores de claves KMIP devueltos no se filtrarán en función de si están asignados al proveedor de claves KMIP especificado.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
kmipAssignedProvidersActive	Los filtros devolvieron objetos de servidor de claves KMIP en función de si están activos o no. Valores posibles: • verdadero: Devuelve solo los servidores de claves KMIP que están activos (proporcionando claves que se están utilizando actualmente). • false: Devuelve solo los servidores de claves KMIP que están inactivos (no proporcionan ninguna clave y pueden ser eliminados). Si se omite, los servidores de claves KMIP devueltos no se filtran en función de si están activos o no.	booleano	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
kmipTieneProveedorAsignado	Los filtros devolvieron servidores de claves KMIP en función de si tenían asignado un proveedor de claves KMIP. Valores posibles: • verdadero: Devuelve solo 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 devueltos no se filtran en función de si tienen asignado un proveedor de claves KMIP.	booleano	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Servidores de claves kmip	La lista completa de servidores clave KMIP que se han creado.	"KeyServerKmp"formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
  ]
}
```

Nueva versión

11,7

ModificarKeyServerKmip

Puedes usar el `ModifyKeyServerKmip` Método para modificar un servidor de claves KMIP (Key Management Interoperability Protocol) existente a los atributos especificados. Aunque el único parámetro obligatorio es el `keyServerID`, una solicitud que contenga únicamente el `keyServerID` no realizará ninguna acción ni devolverá ningún error. Cualquier otro parámetro que especifique reemplazará los valores existentes para el servidor de claves con el `keyServerID` especificado. Durante la operación se contacta con el servidor clave para asegurar que funciona correctamente. Puede proporcionar varios nombres de host o direcciones IP con el parámetro `kmipKeyServerHostnames`, pero solo si los servidores clave están en una configuración de clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del servidor de claves	El ID del servidor de claves KMIP que se va a modificar.	entero	Ninguno	Sí
Certificado kmipCa	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 clústeres de servidores clave donde los servidores individuales utilizan diferentes CA, proporcione una cadena concatenada que contenga los certificados raíz de todas las CA.	cadena	Ninguno	No
Certificado de cliente kmip	Un certificado PKCS#10 X.509 codificado en Base64 con formato PEM utilizado por el cliente Solidfire KMIP.	cadena	Ninguno	No

Nombres de host del servidor de claves kmip	Conjunto de nombres de host o direcciones IP asociadas a este servidor de claves KMIP. Solo se deben proporcionar varios nombres de host o direcciones IP si los servidores clave están en una configuración de clúster.	matriz de cadenas	Ninguno	No
kmipKeyServerName	El nombre del servidor de claves KMIP. Este nombre se utiliza únicamente con fines ilustrativos y no necesita ser único.	cadena	Ninguno	No
kmipKeyServerPort	El número de puerto asociado con este servidor de claves KMIP (normalmente 5696).	entero	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Servidor de claves kmip	Un objeto que contiene detalles sobre el servidor de claves recientemente modificado.	"KeyServerKmp"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      }
    }
}
```

Nueva versión

11,7

Clave maestra de cifrado de software en reposo

Puedes usar el `RekeySoftwareEncryptionAtRestMasterKey` Método para volver a generar la clave maestra de cifrado en reposo del software utilizada para cifrar las DEK

(claves de cifrado de datos). Durante la creación del clúster, el cifrado de software en reposo se configura para utilizar la gestión de claves internas (IKM). Este método de re-clave se puede utilizar después de la creación del clúster para usar IKM o Administración de claves externas (EKM).

Parámetros

Este método tiene los siguientes parámetros de entrada. Si el `keyManagementType` Si no se especifica ningún parámetro, la operación de cambio de clave se realiza utilizando la configuración de gestión de claves existente. Si el `keyManagementType` está especificado y el proveedor de claves es externo, el `keyProviderID` También debe utilizarse el parámetro.

Parámetro	Descripción	Tipo	Opcional
tipo de gestión de claves	El tipo de gestión de claves utilizado para administrar la clave maestra. Los valores posibles son: <code>Internal</code> : Recodificar utilizando la gestión interna de claves. <code>External</code> : Recodificar utilizando la gestión de claves externa. Si no se especifica este parámetro, la operación de cambio de clave se realiza utilizando la configuración de gestión de claves existente.	cadena	Verdadero
ID del proveedor de clave	El identificador del proveedor de claves a utilizar. Este es un valor único que se devuelve como parte de uno de los <code>CreateKeyProvider</code> métodos. El ID solo es necesario cuando <code>keyManagementType</code> es <code>External</code> y, por lo demás, no es válido.	entero	Verdadero

Valores de retorno

Este método tiene los siguientes valores de retorno:

Parámetro	Descripción	Tipo	Opcional
manejador asíncrono	Determine el estado de la operación de recodificación utilizando esto <code>asyncHandle</code> valor con <code>GetAsyncResult</code> . <code>GetAsyncResult</code> La salida incluirá un <code>newKey</code> campo que contiene información sobre la nueva clave maestra y un <code>keyToDecommission</code> campo que contiene información sobre la clave anterior.	entero	FALSO

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "rekeysoftwareencryptionatrestmasterkey",
  "params": {
    "keyManagementType": "external",
    "keyProviderID": "<ID number>"
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "asyncHandle": 1
}
```

Nueva versión

12,3

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Eliminar servidor de claves del proveedor Kmix

Puedes usar el `RemoveKeyServerFromProviderKmix` método para desasignar el servidor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) especificado del proveedor al que estaba asignado. Puedes desasignar un servidor de claves de su proveedor a menos que sea el último y su proveedor esté activo (proporcionando claves que se están utilizando 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	Requerido
ID del servidor de claves	El ID del servidor de claves KMIP que se va a desasignar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor. La eliminación se considera exitosa siempre que no se devuelva ningún error.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "RemoveKeyServerFromProviderKmix",
  "params": {
    "keyServerID": 1
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result":
    {}
}
```

Nueva versión

11,7

Firmar claves Ssh

Después de habilitar SSH en el clúster mediante "[Método HabilitarSSH](#)", puedes usar el `SignSshKeys` Método para obtener acceso a una shell en un nodo.

A partir del elemento 12.5, `sfreadonly` Es una nueva cuenta del sistema que permite la resolución de problemas básicos en un nodo. Esta API permite el acceso SSH mediante `sfreadonly` Cuenta del sistema en todos los nodos del clúster.



Salvo indicación expresa del Soporte de NetApp , cualquier modificación del sistema no está soportada, anulará su contrato de soporte y puede provocar inestabilidad o inaccesibilidad de los datos.

Después de utilizar este método, debe copiar el llavero de la respuesta, guardarlo en el sistema que iniciará la conexión SSH y, a continuación, ejecutar el siguiente comando:

```
ssh -i <identity_file> sfreadonly@<node_ip>
```

`identity\_file` es un archivo del cual se lee la identidad (clave privada) para la autenticación de clave pública y `node\_ip` es la dirección IP del nodo. Para obtener más información sobre `identity\_file` , consulte la página del manual de SSH.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
duración	Número entero del 1 al 24 que refleja el número de horas que la clave firmada será válida. Si no se especifica la duración, se utiliza el valor predeterminado.	entero	1	No
clave pública	Si se proporciona, este parámetro solo devolverá la clave pública firmada en lugar de crear un llavero completo para el usuario.  Las claves públicas se envían utilizando la barra de direcciones de un navegador con + se interpretan como signos espaciados y de ruptura.	cadena	Nulo	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
sfadmin	Permite el acceso a la cuenta de shell sfadmin cuando se realiza la llamada a la API con acceso al clúster supportAdmin, o cuando el nodo no está en un clúster.	booleano	FALSO	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
estado del generador de claves	Contiene la identidad en la clave firmada, las entidades autorizadas y las fechas de inicio y fin válidas para la clave.	cadena
clave_privada	El valor de una clave SSH privada solo se devuelve si la API genera un llavero completo para el usuario final.  El valor está codificado en Base64; debe decodificarlo cuando se escriba en un archivo para garantizar que se lea como una clave privada válida.	cadena

Nombre	Descripción	Tipo
clave_pública	El valor de una clave SSH pública solo se devuelve si la API genera un llavero completo para el usuario final.  Cuando se pasa un parámetro <code>public_key</code> al método de la API, solo se tiene en cuenta el parámetro <code>public_key</code>. <code>signed_public_key</code> El valor se devuelve en la respuesta.	cadena
clave pública firmada	La clave pública SSH que resulta de firmar la clave pública, ya sea que esta haya sido proporcionada por el usuario o generada por la API.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "SignSshKeys",
  "params": {
    "duration": 2,
    "publicKey": <string>
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```

{
  "id": null,
  "result": {
    "signedKeys": {
      "keygen_status": <keygen_status>,
      "signed_public_key": <signed_public_key>
    }
  }
}

```

En este ejemplo, se firma y se devuelve una clave pública que es válida durante un período de tiempo de entre 1 y 24 horas.

Nueva versión

12,5

TestKeyProviderK mip

Puedes usar el `TestKeyProviderK mip` método para comprobar si el proveedor 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	Requerido
ID del proveedor de clave	El ID del proveedor de claves a probar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor. La prueba se considera exitosa siempre y cuando no se devuelva ningún error.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:


```
{
  "method": "TestKeyProviderKmip",
  "params": {
    "keyProviderID": 15
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result":
    {}
}
```

Nueva versión

11,7

Servidor de claves de prueba Kmip

Puedes usar el `TestKeyServerKmip` método para comprobar 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	Requerido
ID del servidor de claves	El ID del servidor de claves KMIP que se va a probar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor. La prueba se considera exitosa si no se devuelven errores.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "TestKeyServerKnip",
  "params": {
    "keyServerID": 15
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result":
    {}
}
```

Nueva versión

11,7

Métodos de la API de SnapMirror

Abortar SnapMirrorRelationship

La interfaz web del software Element utiliza `AbortSnapMirrorRelationship` Método para detener las transferencias de SnapMirror que se han iniciado pero aún no se han completado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	El ID del punto final del sistema de almacenamiento ONTAP remoto que se comunica con el clúster de almacenamiento Element.	entero	Ninguno	Sí
volumen de destino	El volumen de destino en la relación SnapMirror .	snapMirrorVolumeInfo	Ninguno	Sí
Punto de control claro	Determina si se debe borrar o no el punto de control de reinicio. Valores posibles: • verdadero • FALSO	booleano	FALSO	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
snapMirrorRelationship	Un objeto que contiene información sobre la relación SnapMirror abortada.	snapMirrorRelationship

Nueva versión

10,1

Relación BreakSnapMirror

La interfaz web de Element utiliza `BreakSnapMirrorRelationship` Método para romper una relación SnapMirror . Cuando se rompe una relación SnapMirror , el volumen de destino se convierte en un volumen de lectura y escritura independiente, y entonces puede divergir del origen. Puedes restablecer la relación con el `ResyncSnapMirrorRelationship` Método API. Este método requiere que el clúster ONTAP esté disponible.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	El ID del punto final del sistema de almacenamiento ONTAP remoto que se comunica con el clúster de almacenamiento Element.	entero	Ninguno	Sí
volumen de destino	El volumen de destino en la relación SnapMirror .	snapMirrorVolumeInfo	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
snapMirrorRelationship	Un objeto que contiene información sobre la relación SnapMirror rota.	snapMirrorRelationship

Nueva versión

10,1

Encuentra más información

[BreakSnapMirrorVolume](#)

BreakSnapMirrorVolume

La interfaz web de Element utiliza `BreakSnapMirrorVolume` Método para romper la relación SnapMirror entre un contenedor de origen ONTAP y un volumen de destino Element. La interrupción de un volumen Element SnapMirror resulta útil si un sistema ONTAP deja de estar disponible mientras se replican datos en un volumen Element. Esta función permite a un administrador de almacenamiento tomar el control de un volumen Element SnapMirror , romper su relación con el sistema ONTAP remoto y revertir el volumen a una instantánea anterior.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de volumen	El volumen sobre el que se realizará la operación de ruptura. El modo de acceso al volumen debe ser snapMirrorTarget.	entero	Ninguno	Sí
ID de instantánea	Revierte el volumen al estado de instantánea identificado por este ID. El comportamiento predeterminado es volver a la instantánea más reciente.	entero	Ninguno	No
preservar	Conservar cualquier instantánea más reciente que la instantánea identificada por snapshotID. Valores posibles: • verdadero: Conservar las instantáneas más recientes que snapshotID. • false: No conservar instantáneas más recientes que snapshotID. Si es falso, se eliminarán todas las instantáneas más recientes que snapshotID.	booleano	FALSO	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
acceso	Modo de acceso al volumen resultante. Valores posibles: • leer/escribir • Solo lectura • bloqueado	cadena	leer/escribir	No

Valores de retorno

Este método no devuelve ningún valor.

Nueva versión

10,0

Encuentra más información

[Relación BreakSnapMirror](#)

Crear punto final de SnapMirror

La interfaz web de Element utiliza `CreateSnapMirrorEndpoint` Método para crear una relación con un punto de conexión SnapMirror remoto.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
gestión de la propiedad intelectual	La dirección IP de administración del extremo SnapMirror remoto.	cadena	Ninguno	Sí
nombre de usuario	El nombre de usuario de administración para el sistema ONTAP .	cadena	Ninguno	Sí
contraseña	La contraseña de administración del sistema ONTAP .	cadena	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
snapMirrorEndpoint	El nuevo punto de conexión SnapMirror .	snapMirrorEndpoint

Nueva versión

10,0

CrearPuntoFinalDeSnapMirrorNoAdministrado

El sistema de almacenamiento de software Element utiliza el `CreateSnapMirrorEndpointUnmanaged` Método para permitir que los puntos de conexión SnapMirror remotos y no administrados se comuniquen con un clúster de almacenamiento Element. Los puntos de conexión no administrados no se pueden gestionar mediante las API de Element SnapMirror . Deben gestionarse con el software de gestión ONTAP o con API.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nombre del clúster	El nombre del punto final.	cadena	Ninguno	Sí
direcciones ip	La lista de direcciones IP para un clúster de sistemas de almacenamiento ONTAP que deben comunicarse con este clúster de almacenamiento Element.	matriz de cadenas	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo

snapMirrorEndpoint	El nuevo punto de conexión SnapMirror .	snapMirrorEndpoint

Nueva versión

10,3

CrearRelaciónSnapMirror

La interfaz web de Element utiliza CreateSnapMirrorRelationship Método para crear una relación de protección de datos extendida SnapMirror entre un punto de origen y un punto de destino.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	El ID del punto final del sistema de almacenamiento ONTAP remoto que se comunica con el clúster de almacenamiento Element.	entero	Ninguno	Sí
Volumen de origen	El volumen de la fuente en la relación.	snapMirrorVolumeInfo	Ninguno	Sí
volumen de destino	El volumen de destino en la relación.	snapMirrorVolumeInfo	Ninguno	Sí
tipo de relación	El 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	Requerido
nombre de la política	Especifica el nombre de la política ONTAP SnapMirror para la relación. Si no se especifica, el nombre de política predeterminado es MirrorLatest.	cadena	Ninguno	No
nombre del horario	El nombre de la tarea cron preexistente en el sistema ONTAP que se utiliza para actualizar la relación SnapMirror . Si no se ha designado una programación, las actualizaciones de snapMirror no se programan y deben actualizarse manualmente.	cadena	Ninguno	No
tasa de transferencia máxima	Especifica la velocidad máxima de transferencia de datos entre los volúmenes en kilobytes por segundo. El valor predeterminado, 0, es ilimitado y permite que la relación SnapMirror utilice completamente el ancho de banda de red disponible.	entero	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
snapMirrorRelationship	Información sobre la relación SnapMirror recién creada.	snapMirrorRelationship

Nueva versión

10,1

CrearVolumenSnapMirror

La interfaz web de Element utiliza `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	Requerido
ID de punto final de SnapMirror	El ID del punto final del sistema de almacenamiento ONTAP remoto que se comunica con el clúster de almacenamiento Element.	entero	Ninguno	Sí
vserver	El nombre del servidor virtual.	cadena	Ninguno	Sí
nombre	Nombre del volumen ONTAP de destino.	cadena	Ninguno	Sí
tipo	El tipo de volumen. Valores posibles: • rw: Volumen de lectura y escritura • ls: Volumen de reparto de carga • dp: Volumen de protección de datos Si no se proporciona ningún tipo, el tipo predeterminado es dp.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
agregar	El agregado ONTAP contenedor en el que se creará el volumen. Puede utilizar ListSnapMirrorAggregates para obtener información sobre los agregados ONTAP disponibles.	cadena	Ninguno	Sí
tamaño	El tamaño del volumen en bytes.	entero	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
snapMirrorVolume	Información sobre un volumen de SnapMirror .	snapMirrorVolume

Nueva versión

10,1

Eliminar puntos finales de SnapMirror

La interfaz web de Element utiliza `DeleteSnapMirrorEndpoints` eliminar uno o más puntos de conexión de SnapMirror del sistema.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
IDs de punto final de SnapMirror	Una matriz de identificadores de puntos de conexión de SnapMirror para eliminar.	matriz de enteros	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Nueva versión

10,0

EliminarRelacionesDeSnapMirror

La interfaz web de Element utiliza `DeleteSnapMirrorRelationships` Método para eliminar una o más relaciones SnapMirror entre un punto de origen y un punto de destino.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	El ID del punto final del sistema de almacenamiento ONTAP remoto que se comunica con el clúster de almacenamiento Element.	entero	Ninguno	Sí
volúmenes de destino	El volumen o volúmenes de destino en la relación SnapMirror .	snapMirrorVolumeInformation	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
resultado	Si la acción de eliminación se realizó correctamente, este objeto contiene un mensaje de éxito. Si la acción falla, contiene un mensaje de error.	Objeto JSON

Nueva versión

10,1

Información de la versión de GetOntap

La interfaz web de Element utiliza `GetOntapVersionInfo` para obtener información sobre la compatibilidad de versiones de API del clúster ONTAP en una relación SnapMirror .

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	Si se proporciona, el sistema muestra la información de versión del punto final con el <code>snapMirrorEndpointID</code> especificado. Si no se proporciona, el sistema muestra la información de versión de todos los endpoints SnapMirror conocidos.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
<code>ontapVersionInfo</code>	Información sobre la versión del software del punto final ONTAP .	ontapVersionInfo información

Nueva versión

10,1

ObtenerIdentidadDeClústerDeSnapMirror

La interfaz web del software Element utiliza `GetSnapMirrorClusterIdentity` para obtener información de identidad sobre el clúster ONTAP .

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	Si se proporciona, el sistema enumera la identidad del clúster del punto final con el snapMirrorEndpointID especificado. Si no se proporciona, el sistema enumera la identidad del clúster de todos los puntos de conexión SnapMirror conocidos.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorClusterIdentity	Una lista de identidades de clúster de los puntos de conexión de SnapMirror .	snapMirrorClusterIdentity formación

Nueva versión

10,1

InicializarRelaciónSnapMirror

La interfaz web del software Element utiliza `InitializeSnapMirrorRelationship` Método para inicializar el volumen de destino en una relación SnapMirror mediante la realización de una transferencia de línea base inicial entre clústeres.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	El identificador del sistema ONTAP remoto.	entero	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
volumen de destino	El volumen de destino en la relación SnapMirror .	snapMirrorVolumeInfo	Ninguno	Sí
tasa de transferencia máxima	Especifica la velocidad máxima de transferencia de datos entre los volúmenes en kilobytes por segundo. El valor predeterminado, 0, es ilimitado y permite que la relación SnapMirror utilice completamente el ancho de banda de red disponible.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorRelationship	Información sobre la relación SnapMirror inicializada.	snapMirrorRelationship

Nueva versión

10,1

Agregados de ListSnapMirror

La interfaz web del software Element utiliza `ListSnapMirrorAggregates` Método para listar todos los agregados SnapMirror que están disponibles en el sistema ONTAP remoto. Un agregado describe un conjunto de recursos de almacenamiento físico.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	Devuelve únicamente los agregados asociados con el ID de punto final especificado. Si no se proporciona un ID de punto de conexión, el sistema enumera los agregados de todos los puntos de conexión SnapMirror conocidos.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Agregados de SnapMirror	Una lista de los agregados disponibles en el sistema de almacenamiento ONTAP .	snapMirrorAggregate formación

Nueva versión

10,1

ListSnapMirrorEndpoints

La interfaz web del software Element utiliza `ListSnapMirrorEndpoints` Método para listar todos los puntos de conexión 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	Requerido
IDs de punto final de SnapMirror	Devuelve únicamente los objetos asociados a estos identificadores. Si no se proporcionan identificadores o la matriz está vacía, el método devuelve todos los identificadores de punto final de SnapMirror .	matriz de enteros	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorEndpoints	Una lista de los endpoints de SnapMirror existentes.	snapMirrorEndpoint información

Nueva versión

10,0

ListSnapMirrorLuns

La interfaz web del software Element utiliza `ListSnapMirrorLuns` Método para listar la información LUN para la relación SnapMirror desde el clúster ONTAP remoto.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	Enumere únicamente la información de LUN asociada con el ID de punto final especificado.	entero	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
volumen de destino	El volumen de destino en la relación SnapMirror .	snapMirrorVolumInfo	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
snapMirrorLunInfos	Una lista de objetos que contiene información sobre las LUN de SnapMirror .	snapMirrorLunInfo información

Nueva versión

10,1

ListSnapMirrorNetworkInterfaces

La interfaz web del software Element utiliza `ListSnapMirrorNetworkInterfaces` Método para listar todas las interfaces SnapMirror disponibles en un sistema ONTAP remoto.

Parámetro

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	Devuelve únicamente las interfaces de red asociadas al ID de punto final especificado. Si no se proporciona un ID de punto final, el sistema enumera las interfaces de todos los puntos finales SnapMirror conocidos.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
rol de interfaz	Enumere únicamente la interfaz de red que cumple la función especificada.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
interfaces de red snapMirror	Una lista de las interfaces de red SnapMirror disponibles en el sistema de almacenamiento ONTAP remoto.	snapMirrorNetworkInterface formación

Nueva versión

10,1

Nodos de espejo de ListSnap

La interfaz web del software Element utiliza `ListSnapMirrorNodes` Método para obtener una lista de nodos en un clúster ONTAP remoto.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	Si se proporciona, el sistema enumera los nodos del punto final con el <code>snapMirrorEndpointID</code> especificado. Si no se proporciona, el sistema enumera los nodos de todos los puntos de conexión SnapMirror conocidos.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorNodes	Una lista de los nodos en el clúster ONTAP .	snapMirrorNode formación

Nueva versión

10,1

Políticas de espejo de ListSnap

La interfaz web del software Element utiliza `ListSnapMirrorPolicies` Método para listar todas las políticas de SnapMirror en un sistema ONTAP remoto.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	Enumere únicamente las políticas asociadas con el ID de punto final especificado. Si no se proporciona un ID de punto de conexión, el sistema enumera las políticas de todos los puntos de conexión SnapMirror conocidos.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Políticas de SnapMirror	Una lista de las políticas de SnapMirror en el sistema de almacenamiento ONTAP .	snapMirrorPolicy formación

Nueva versión

10,1

Lista de horarios de reflejo de ajuste

La interfaz web del software Element utiliza `ListSnapMirrorSchedules` Método para obtener una lista de las programaciones disponibles en un clúster ONTAP remoto.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	Si se proporciona, el sistema muestra las programaciones del punto de conexión con el ID de punto de conexión SnapMirror especificado. Si no se proporciona, el sistema muestra las programaciones de todos los puntos de conexión SnapMirror conocidos.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorSchedules	Una lista de las programaciones de SnapMirror en el clúster ONTAP remoto.	snapMirrorJobScheduleCronInfo for mación

Nueva versión

10,1

Relaciones de espejo de ajuste de lista

La interfaz web del software Element utiliza `ListSnapMirrorRelationships` método para listar 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	Requerido
ID de punto final de SnapMirror	Enumere únicamente las relaciones asociadas con el ID de punto final especificado. Si no se proporciona un ID de punto de conexión, el sistema enumera las relaciones de todos los puntos de conexión SnapMirror conocidos.	entero	Ninguno	No
volumen de destino	Enumere las relaciones asociadas con el volumen de destino especificado.	snapMirrorVolumeInfo	Ninguno	No
Volumen de origen	Enumera las relaciones asociadas al volumen de origen especificado.	snapMirrorVolumeInfo	Ninguno	No
vserver	Enumera las relaciones en el Vserver especificado.	cadena	Ninguno	No
ID de relación	Enumera las relaciones asociadas con el ID de relación especificado.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo

snapMirrorRelationships	Una lista de objetos que contienen información sobre las relaciones de SnapMirror .	snapMirrorRelationship información

Nueva versión

10,1

ListSnapMirrorVolumes

La interfaz web del software Element utiliza `ListSnapMirrorVolumes` Método para listar 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	Requerido
ID de punto final de SnapMirror	Enumere únicamente los volúmenes asociados con el ID de punto final especificado. Si no se proporciona un ID de punto de conexión, el sistema enumera los volúmenes de todos los puntos de conexión SnapMirror conocidos.	entero	Ninguno	No
vserver	Enumera los volúmenes alojados en el Vserver especificado. El Vserver debe ser de tipo "datos".	cadena	Ninguno	No
nombre	Enumere únicamente los volúmenes ONTAP con el nombre especificado.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
tipo	Enumere únicamente los volúmenes ONTAP del tipo especificado. Valores posibles: • rw: Volúmenes de lectura y escritura • ls: Volúmenes de balanceo de carga • dp: Volúmenes de protección de datos	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorVolumes	Una lista de los volúmenes SnapMirror disponibles en el sistema de almacenamiento ONTAP .	snapMirrorVolume formación

Nueva versión

10,1

Lista de servidores virtuales de SnapMirror

La interfaz web del software Element utiliza `ListSnapMirrorVservers` Método para listar todos los servidores virtuales SnapMirror disponibles en un sistema ONTAP remoto.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	Enumere únicamente los Vservers asociados con el ID de punto de conexión especificado. Si no se proporciona un ID de punto de conexión, el sistema enumera los Vservers de todos los puntos de conexión SnapMirror conocidos.	entero	Ninguno	No
vserverType	Lista solo los Vservers del tipo especificado. Valores posibles: • administración • data • nodo • sistema	cadena	Ninguno	No
vserverName	Lista solo los Vservers con el nombre especificado.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
SnapMirrorVservers	Lista de los servidores virtuales SnapMirror disponibles en el sistema de almacenamiento ONTAP .	snapMirrorVserver formación

Nueva versión

10,1

Modificar el punto final de SnapMirror

La interfaz web del software Element utiliza `ModifySnapMirrorEndpoint` Método para cambiar el nombre y los atributos de administración de un punto de conexión SnapMirror .

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	El punto de conexión SnapMirror que se va a modificar.	entero	Ninguno	Sí
gestión de la propiedad intelectual	La nueva dirección IP de gestión para el sistema ONTAP .	cadena	Ninguno	No
nombre de usuario	El nuevo nombre de usuario de administración para el sistema ONTAP .	cadena	Ninguno	No
contraseña	La nueva contraseña de administración para el sistema ONTAP .	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorEndpoint	Información sobre el punto de conexión SnapMirror modificado.	snapMirrorEndpoint

Nueva versión

10,0

ModificarSnapMirrorEndpoint (no administrado)

El software Element utiliza esta versión de `ModifySnapMirrorEndpoint` Método para modificar el nombre del clúster de almacenamiento o los atributos de dirección IP para un punto de conexión SnapMirror no administrado. Los puntos de conexión no

administrados no se pueden gestionar mediante las API de Element SnapMirror . Deben gestionarse con el software de gestión ONTAP o con API.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	El punto de conexión SnapMirror que se va a modificar.	entero	Ninguno	Sí
nombre del clúster	El nuevo nombre del punto de conexión.	cadena	Ninguno	No
direcciones ip	La nueva lista de direcciones IP para un clúster de sistemas de almacenamiento ONTAP que deben comunicarse con este clúster de almacenamiento Element.	matriz de cadenas	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorEndpoint	Información sobre el punto de conexión SnapMirror modificado.	snapMirrorEndpoint

Nueva versión

10,3

Modificar relación de SnapMirror

Puedes usar `ModifySnapMirrorRelationship` para cambiar los intervalos en los que se produce una instantánea programada. También puedes eliminar o pausar una programación utilizando este método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
volumen de destino	El volumen de destino en la relación SnapMirror .	snapMirrorVolumeinfo	Ninguno	Sí
tasa de transferencia máxima	Especifica la velocidad máxima de transferencia de datos entre los volúmenes en kilobytes por segundo. El valor predeterminado, 0, es ilimitado y permite que la relación SnapMirror utilice completamente el ancho de banda de red disponible.	entero	Ninguno	No
nombre de la política	Especifica el nombre de la política ONTAP SnapMirror para la relación.	cadena	Ninguno	No
nombre del horario	El nombre de la tarea cron preexistente en el sistema ONTAP que se utiliza para actualizar la relación SnapMirror .	cadena	Ninguno	No
ID de punto final de SnapMirror	El ID del punto final del sistema de almacenamiento ONTAP remoto que se comunica con el clúster de almacenamiento Element.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorRelationship	Un objeto que contiene los atributos de relación SnapMirror modificados.	snapMirrorRelationship

Nueva versión

10,1

ActualizarRelaciónSnapMirror

La interfaz web del software Element utiliza `UpdateSnapMirrorRelationship` Método para convertir el volumen de destino en una relación SnapMirror en una réplica actualizada del volumen de origen.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	El ID del punto final del sistema de almacenamiento ONTAP remoto que se comunica con el clúster de almacenamiento Element.	entero	Ninguno	Sí
volumen de destino	El volumen de destino en la relación SnapMirror .	snapMirrorVolumeinfo	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
tasa de transferencia máxima	Especifica la velocidad máxima de transferencia de datos entre los volúmenes en kilobytes por segundo. El valor predeterminado, 0, es ilimitado y permite que la relación SnapMirror utilice completamente el ancho de banda de red disponible.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorRelationship	Un objeto que contiene información sobre la relación SnapMirror actualizada.	snapMirrorRelationship

Nueva versión

10,1

Relación de espejo de QuiesceSnap

La interfaz web del software Element utiliza `QuiesceSnapMirrorRelationship` Método para deshabilitar futuras transferencias de datos para una relación SnapMirror . Si hay una transferencia en curso, el estado de la relación pasa a ser "en pausa" hasta que se complete la transferencia. Si se interrumpe la transferencia actual, no se reiniciará. Puede volver a habilitar las transferencias de datos para la relación utilizando `ResumeSnapMirrorRelationship` Método API.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	El ID del punto final del sistema de almacenamiento ONTAP remoto que se comunica con el clúster de almacenamiento Element.	entero	Ninguno	Sí
volumen de destino	El volumen de destino en la relación SnapMirror .	snapMirrorVolumeinfo	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorRelationship	Un objeto que contiene información sobre la relación SnapMirror quiescente.	snapMirrorRelationship

Nueva versión

10,1

Relación de ResumeSnapMirror

La interfaz web del software Element utiliza `ResumeSnapMirrorRelationship` Método para habilitar futuras transferencias para una relación SnapMirror inactiva.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	El ID del punto final del sistema de almacenamiento ONTAP remoto que se comunica con el clúster de almacenamiento Element.	entero	Ninguno	Sí
volumen de destino	El volumen de destino en la relación SnapMirror .	snapMirrorVolumeinfo	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorRelationship	Un objeto que contiene información sobre la relación SnapMirror reanudada.	snapMirrorRelationship

Nueva versión

10,1

ResincronizarSnapMirrorRelationship

La interfaz web del software Element utiliza `ResyncSnapMirrorRelationship` método para establecer o restablecer una relación de espejo entre un punto final de origen y un punto final de destino. Al resincronizar una relación, el sistema elimina las instantáneas del volumen de destino que sean más recientes que la copia de instantánea común y, a continuación, monta el volumen de destino como un volumen de protección de datos con la copia de instantánea común como copia de instantánea exportada.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de punto final de SnapMirror	El ID del punto final del sistema de almacenamiento ONTAP remoto que se comunica con el clúster de almacenamiento Element.	entero	Ninguno	Sí
volumen de destino	El volumen de destino en la relación SnapMirror .	snapMirrorVolumeinfo	Ninguno	Sí
tasa de transferencia máxima	Especifica la velocidad máxima de transferencia de datos entre los volúmenes en kilobytes por segundo. El valor predeterminado, 0, es ilimitado y permite que la relación SnapMirror utilice completamente el ancho de banda de red disponible.	entero	Ninguno	No
Volumen de origen	El volumen de origen en la relación SnapMirror .	snapMirrorVolumeinfo	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
snapMirrorRelationship	Un objeto que contiene información sobre la relación SnapMirror resincronizada.	snapMirrorRelationship

Nueva versión

10,1

Métodos de la API de configuración del sistema

DeshabilitarBmcColdReset

Puedes usar el `DisableBmcColdReset` Método para deshabilitar la tarea en segundo plano que reinicia periódicamente el controlador de administración de la placa base (BMC) para todos los nodos del clúster.

Parámetro

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
cBmcResetDurationMinutes	Devuelve el tiempo transcurrido entre los intervalos de reinicio. El intervalo siempre debe ser 0 después de que se complete el comando.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DisableBmcColdReset",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "cBmcResetDurationMinutes": 0
  }
}
```

Nueva versión

12,0

Deshabilitar ClusterSsh

Puedes usar el `DisableClusterSsh` Método para deshabilitar el servicio SSH para todo el clúster de almacenamiento. Cuando agregue nodos al clúster de almacenamiento, los nuevos nodos heredarán esta configuración de todo el clúster.

Parámetro

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
resultado	Un objeto JSON que contiene el estado del servicio SSH para el clúster de almacenamiento, el tiempo restante hasta que se deshabilite SSH y el estado del servicio SSH para cada nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      } ]
    }
  }
}
```

Nueva versión

10,3

Deshabilitar SNMP

Puedes usar el `DisableSnm` Método para deshabilitar SNMP en los nodos del clúster.

Parámetro

Este método no tiene parámetros de entrada.

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DisableSnmp",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "result" : {},
  "id" : 1
}
```

Nueva versión

9,6

Habilitar reinicio en frío de BMC

Puedes usar el `EnableBmcColdReset` Método para habilitar una tarea en segundo plano que restablezca periódicamente el controlador de administración de la placa base (BMC) para todos los nodos del clúster.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
se acabó el tiempo	Tiempo transcurrido entre operaciones de reinicio del BMC , en minutos.	entero	20160 minutos	No

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
cBmcResetDurationMinutes	Devuelve el tiempo transcurrido entre los intervalos de reinicio. El intervalo siempre debe ser 0 después de que se complete el comando.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "EnableBmcColdReset",
  "params": {
    "timeout": 36000
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "cBmcResetDurationMinutes": 36000
  }
}
```

Nueva versión

12,0

Habilitar ClusterSsh

Puedes usar 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	Requerido
duración	El tiempo que permanecerá habilitado el servicio SSH.	cadena	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
resultado	Un objeto JSON que contiene el estado del servicio SSH para el clúster de almacenamiento, el tiempo restante hasta que se deshabilite SSH y el estado del servicio SSH para cada nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      } ]
    }
  }
}

```

Nueva versión

10,3

Habilitar SNMP

Puedes usar el `EnableSnmip` Método para habilitar SNMP en los nodos del clúster. Cuando se habilita SNMP, la acción se aplica a todos los nodos del clúster y los valores que se pasan reemplazan todos los valores establecidos en cualquier llamada anterior a `EnableSnmip`.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
snmpV3Enabled	Si se establece en verdadero, entonces SNMP v3 se habilita en cada nodo del clúster. Si se establece en falso, entonces SNMP v2 está habilitado.	booleano	FALSO	No

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "EnableSnmp",
  "params": {
    "snmpV3Enabled" : "true"
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nueva versión

9,6

ObtenerPropiedadesDeAsignaciónDeContenedor

Puedes usar el `GetBinAssignmentProperties` Método para recuperar las propiedades de asignación de contenedores en la base de datos.

Parámetro

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
propiedades	Detalla las propiedades de todas las asignaciones de contenedores actuales en la base de datos.	matriz binAssignmentProperties

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": []
    }
}
}

```

Nueva versión

12,0

Obtener información SSH del clúster

Puedes usar el `GetClusterSshInfo` Método para consultar el estado del servicio SSH para todo el clúster de almacenamiento.

Parámetro

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
resultado	Un objeto JSON que contiene el estado del servicio SSH para el clúster de almacenamiento, el tiempo restante hasta que se deshabilite SSH y el estado del servicio SSH para cada nodo.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```

{
  "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
      } ]
    }
  }
```

Nueva versión

10,3

ObtenerEstructuraDeClúster

Puedes usar el `GetClusterStructure` Método para realizar una copia de seguridad de la información de configuración actual del clúster de almacenamiento. Si se modifica la configuración del clúster de almacenamiento mientras se ejecuta este método, el contenido de la copia de seguridad de la configuración será impredecible. Puede guardar estos datos en un archivo de texto y restaurarlos en otros clústeres, o en el mismo clúster en caso de desastre.

Parámetro

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
resultado	Un objeto JSON que contiene la información de configuración actual del clúster de almacenamiento.	Estructura del clúster

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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>
}
```

Nueva versión

10,3

Informe GetFips

Puedes usar el `GetFipsReport` Método para comprobar el estado de compatibilidad con la función de cifrado FIPS 140-2 de todos los nodos del clúster de almacenamiento.

Parámetro

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

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 de error para cada nodo que no respondió a la consulta.	Informe fips

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
        }
      }
    ]
  }
}

```

Nueva versión

10,3

Obtener configuración de Lldp

Puedes usar el `GetLldpConfig` Método para obtener la configuración del Protocolo de Descubrimiento de Capa de Enlace (LLDP) para cada nodo de un clúster de almacenamiento.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
lldpConfig	Información sobre la configuración LLDP del clúster de almacenamiento.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
  }
}
```

Obtener información de Lldp

Puedes usar el `GetLldpInfo` Método para obtener la configuración del Protocolo de Descubrimiento de Capa de Enlace (LLDP) para cada nodo de un clúster de almacenamiento o para un nodo de almacenamiento individual.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
lldpInfo	Información sobre el chasis, la interfaz y la configuración LLDP de los vecinos para cada nodo de un clúster de almacenamiento.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetLldpInfo",
  "id" : 1
}
```

Ejemplo de respuesta

Debido a la extensión de este ejemplo de respuesta, se documenta en un tema complementario.

Nueva versión

11,0

Encuentra más información

[Obtener información de Lldp](#)

Informe de unidades GetNodeFips

Puedes usar el `GetNodeFipsDrivesReport` Método para comprobar el estado de la capacidad de cifrado de la unidad FIPS 140-2 de un único nodo en el clúster de almacenamiento. Debe ejecutar este método en un nodo de almacenamiento individual.

Parámetro

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Unidades fips	Un objeto JSON que contiene el estado de la compatibilidad con la característica FIPS 140-2 para este nodo. Valores posibles: • Ninguno: El nodo no es compatible con FIPS. • Parcial: El nodo es compatible con FIPS, pero no todas las unidades del nodo son unidades FIPS. • Listo: El nodo es compatible con FIPS y todas las unidades del nodo son unidades FIPS (o no hay unidades presentes).	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetNodeFipsDrivesReport",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "fipsDrives": "None"
  }
}
```

Nueva versión

11,5

Obtener información NTP

Puedes usar el `GetNtpInfo` Método para obtener la información de configuración actual

del protocolo de tiempo de red (NTP).

Parámetro

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
servidores	Lista de servidores NTP.	matriz de cadenas
cliente de difusión	Indica si los nodos del clúster están o no a la escucha de mensajes NTP de difusión. Valores posibles: • verdadero • FALSO	booleano

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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" ]
  }
}
```

Nueva versión

9,6

Obtener información de NVRAM

Puedes usar el `GetNvramInfo` Método para obtener información de cada nodo sobre la tarjeta NVRAM .

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
fuerza	El parámetro de fuerza debe incluirse en este método para que se ejecute correctamente en todos los nodos del clúster.	booleano	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
nvramInfo	Matrices de eventos y errores detectados en la tarjeta NVRAM .	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetNvramInfo",
  "params": {
    "force": true
  },
  "id" : 1
}
```

Ejemplo de respuesta

Debido a la extensión de este ejemplo de respuesta, se documenta en un tema complementario.

Nueva versión

9,6

Encuentra más información

[Obtener información de NVRAM](#)

ObtenerDiseñoDeDominioDeProtección

Puedes usar el `GetProtectionDomainLayout` Método para devolver toda la información del dominio de protección para un clúster, incluyendo en qué chasis y en qué dominio de protección personalizado se encuentra cada nodo.

Parámetro

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
diseño de dominio de protección	Lista de nodos, cada uno con sus dominios de protección asociados.	Lista JSON de "Dominios de protección de nodos" objetos.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": "QTF2914008D",
            "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"
    }
  ]
}

```

```
]
}
}
```

Nueva versión

12,0

Obtener hosts de registro remoto

Puedes usar 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 de retorno:

Nombre	Descripción	Tipo
hosts remotos	Lista de direcciones IP e información de puertos de los hosts configurados para recibir información de registro reenviada.	servidor de registro información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}
```

Nueva versión

9,6

Encuentra más información

[Configurar hosts de registro remoto](#)

Obtener ACL SNMP

Puedes usar 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 de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
redes	Lista de redes y el tipo de acceso que tienen a los servidores SNMP que se ejecutan en los nodos del clúster. Este valor está presente si SNMP v3 está deshabilitado.	red formación

Nombre	Descripción	Tipo
usuarios de usm	Lista de usuarios y el tipo de acceso que tienen a los servidores SNMP que se ejecutan en los nodos del clúster. Este valor está presente si SNMP v3 está habilitado.	usmUser formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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",
      }
    ]
  }
}
```

Nueva versión

9,6

Obtener información SNMP

Puedes usar el `GetSnmpInfo` Método para obtener la información de configuración actual del protocolo simple de administración de red (SNMP).

Parámetros



GetSnmplInfo está obsoleto para versiones posteriores a la versión 8.0 de Element. El [Obtener estado SNMP](#) y [SetSnmplACL](#) Estos métodos reemplazan al método GetSnmplInfo.

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
redes	Lista de redes y tipos de acceso habilitados para SNMP. Nota: La opción "Redes" solo se muestra si SNMP v3 está deshabilitado.	red
activado	Indica si los nodos del clúster están configurados para SNMP. Valores posibles: • verdadero • FALSO	booleano
snmpV3Enabled	Si el nodo del clúster está configurado para SNMP v3. Valores posibles: • verdadero • FALSO	booleano
usuarios de usm	Si SNMP v3 está habilitado, el clúster devuelve una lista de parámetros de acceso de usuario para SNMP. Esto se devuelve en lugar del parámetro de redes.	usmUser

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetSnmplInfo",
  "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"
      }
    ]
  }
}
```

Nueva versión

9,6

Encuentra más información

- [Obtener estado SNMP](#)
- [SetSnmpACL](#)

Obtener estado SNMP

Puedes usar el `GetSnmpState` Método para obtener el estado actual de la función SNMP.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
activado	Valores posibles: • verdadero • FALSO El valor predeterminado es falso. Devuelve verdadero si los nodos del clúster están configurados para SNMP.	booleano
snmpV3Enabled	Valores posibles: • verdadero • FALSO El valor predeterminado es falso. Devuelve verdadero si los nodos del clúster están configurados para SNMP v3.	booleano

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetSnmpState",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {
    "enabled": true,
    "snmpV3Enabled": false
  }
}
```

Nueva versión

9,6

Encuentra más información

[SetSnmpACL](#)

Obtener información de trampa SNMP

Puedes usar el `GetSnmpTrapInfo` Método para obtener la información de configuración actual de las trampas SNMP.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Receptores de trampas	Lista de hosts que recibirán las trampas generadas por el clúster.	Destinatario de trampa SNMP formación
clusterFaultTrapsEnabled	El valor verdadero indica que se ha configurado una notificación <code>solidFireClusterFaultNotification</code> para que se envíe a la lista de destinatarios de la trampa cuando se registre un fallo del clúster.	booleano
Trampas de resolución de fallos de clúster habilitadas	El valor verdadero indica que se ha configurado una notificación <code>solidFireClusterFaultResolvedNotification</code> para que se envíe a la lista de destinatarios de la trampa cuando se resuelva un fallo del clúster.	booleano
clusterEventTrapsEnabled	El valor verdadero indica que se ha configurado una notificación <code>solidFireClusterEventNotification</code> para que se envíe a la lista de destinatarios de trampas cuando se registre un evento de clúster.	booleano

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}
```

Nueva versión

9,6

Obtener certificado SSL

Puedes usar el `GetSSLCertificate` Método para recuperar el certificado SSL que está actualmente activo en los nodos de almacenamiento del clúster.


```

DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAGTAk5WMRUwEwYDVQHFAXW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbjBWZWdhcy4uLjEtMCsGCSqG
SIb3DQEJARYe\nd2hhdGhhcHBlnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjjf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s7lmQPECwVLfiE/ndtIbnpe\nmQq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7Jyfs3714rRolFpX6N\nniebEgAae5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dH0lQ+WYnoO/eIMy0coT26JB15H\nnDEwvdl+DwKxnS1cx1v
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nnHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\nn7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAjJDg
10QoQDWNDoTerBs80nwiouA==\n-----END CERTIFICATE-----\n",
    "details": {
        "issuer":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org",
        "modulus":
"F14FB6F1F9CB290356116311E9A91E0CAB9E852A52EFDA1D2C68A0235F2A94257F0146396
4B8EAB138C1BD325546FE38CA809380DAF1DFA53B1473F8B7A3FF4A2D1A62BE28BF1979C03
A44337432CB924F07B25E94E07A003EDF9A24F078FDB41D162966F63E533ECB6041429AB82
9199405DE239221C047B4B284E75F3A2554FA8F9760EB28D41903B7E76CA573D1D71DC9FA9
5BFE3CA5D0399535467471A430026212DC99A8CB1FB38FF61AE162AAFB64AA4C05FB6D7D05
DF01C77D79D99479CCF1F113E4DFFD03E2BA952EDD83D7325EEE1A7D77202B2D78262341BE
A6C18E1809B44EFAC80CBAAD31EED313378E376471BF58F2688DCF117E002ABE8AD6B",
        "notAfter": "2027-03-06T22:50:26Z",
        "notBefore": "2017-03-08T22:50:26Z",
        "serial": "CC1B221598E37FF3",
        "sha1Fingerprint":
"1D:70:7A:6F:18:8A:CD:29:50:C7:95:B1:DD:5E:63:21:F4:FA:6E:21",
        "subject":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org"
    }
}
}

```

Nueva versión

10,0

Niveles de dominio de protección de listas

Puedes usar 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 continuar leyendo y escribiendo datos en caso de una falla, y los niveles de resiliencia indican la capacidad del clúster de almacenamiento para recuperarse automáticamente de una o más fallas.

Parámetro

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
niveles de dominio de protección	Una lista de los diferentes niveles del dominio de protección, donde cada uno proporciona información sobre la tolerancia y la resiliencia del clúster de almacenamiento.	Nivel de dominio de protección

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
}
]
}
}

```

Nueva versión

11,0

Eliminar certificado SSL

Puedes usar el `RemoveSSLCertificate` Método para eliminar el certificado SSL de usuario y la clave privada para los nodos de almacenamiento en el clúster. Una vez eliminados el certificado y la clave privada, los nodos de almacenamiento se configuran para usar el certificado y la clave privada predeterminados.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method" : "RemoveSSLCertificate",
  "params" : {},
  "id" : 3
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 3,
  "result" : {}
}
```

Nueva versión

10,0

Restablecer configuración de red

Puedes usar 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 ajustes predeterminados de fábrica.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ResetNetworkConfig",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método no devuelve ninguna respuesta.

Nueva versión

11,0

Restablecer cifrados TLS suplementarios

Puedes usar el `ResetSupplementalTlsCiphers` Método para restaurar la lista de cifrados TLS suplementarios a la predeterminada. Puedes utilizar este método en todo el clúster.

Parámetro

Este método no tiene parámetros de entrada.

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ResetSupplementalTlsCiphers",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nueva versión

11,3

Establecer estructura de clúster

Puedes usar el `SetClusterStructure` Método para restaurar la información de configuración del clúster de almacenamiento a partir de una copia de seguridad. Cuando llamas al método, pasas el objeto `clusterStructure` que contiene la información de configuración que deseas 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 actual del clúster de almacenamiento.	Estructura del clúster

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
resultado	Manejador de resultados asíncronos.	manejador asíncrono

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}
```

Nueva versión

10,3

ConfigurarLldp

Puedes usar el `SetLldpConfig` Método para configurar los ajustes del Protocolo de descubrimiento de capa de enlace (LLDP) para un clúster de almacenamiento.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
habilitarOtrosProtocolos	Habilitar el uso automático de otros protocolos de detección: CDP, FDP, EDP y SONMP.	booleano	verdadero	No
enableMed	Habilitar la detección de puntos finales multimedia (LLDP-MED).	booleano	FALSO	No
habilitarLldp	Habilitar o deshabilitar LLDP.	booleano	verdadero	No

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
lldpConfig	Información sobre la configuración LLDP actual del clúster de almacenamiento, incluyendo los ajustes recientemente modificados.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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

Puedes usar el `SetNtpInfo` Método para configurar NTP en los nodos del clúster. Los valores que configure con esta interfaz se aplicarán a todos los nodos del clúster. Si un servidor de difusión NTP transmite periódicamente información horaria en su red, puede configurar opcionalmente los nodos como clientes de difusión.

Parámetros



Asegúrese de utilizar servidores NTP que sean internos a su red, en lugar de los predeterminados de instalación.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
servidores	Lista de servidores NTP para agregar a la configuración NTP de cada nodo.	matriz de cadenas	Ninguno	Sí
cliente de difusión	Habilita cada nodo del clúster como cliente de difusión.	booleano	FALSO	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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" : {}
}
```

Nueva versión

9,6

Establecer diseño de dominio de protección

Puedes usar el `SetProtectionDomainLayout` Método para asignar nodos a dominios de protección personalizados.

Se debe proporcionar información para todos los nodos activos del clúster y no se puede proporcionar información para los nodos inactivos. Todos los nodos de un chasis determinado deben estar asignados al mismo dominio de protección personalizado. Debe proporcionarse el mismo `protectionDomainType` para todos los nodos. No deben incluirse `protectionDomainTypes` que no sean personalizados, como `node` y `chassis`. Si se proporciona alguno de estos, los dominios de protección personalizados se ignoran y se devuelve un error apropiado.



Los dominios de protección personalizados no son compatibles con las siguientes configuraciones:

- clústeres de almacenamiento que contienen chasis compartidos
- clústeres de almacenamiento de dos nodos

El método devuelve un error cuando se utiliza en clústeres de almacenamiento con estas configuraciones.

Parámetro

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
diseño de dominio de protección	Información del dominio de protección para cada nodo.	Lista JSON de "Dominios de protección de nodos" objetos.	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
diseño de dominio de protección	Lista de nodos, cada uno con sus dominios de protección asociados.	Lista JSON de "Dominios de protección de nodos" objetos.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```

{
  "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"
        }
      ]
    }
  ]
}

```

Nueva versión

12,0

Configurar hosts de registro remoto

Puedes usar el `SetRemoteLoggingHosts` Método para configurar el registro remoto desde los nodos del clúster de almacenamiento a un servidor o servidores de registro centralizados. El registro remoto se realiza a través de TCP utilizando el puerto predeterminado 514. Esta API no añade nada a los hosts de registro existentes. En cambio, reemplaza lo que existe actualmente con nuevos valores especificados por este método de la API. Puedes usar `GetRemoteLoggingHosts` para determinar cuáles son los hosts de registro actuales y luego usar `SetRemoteLoggingHosts` para establecer la lista deseada de hosts de registro actuales y nuevos.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
hosts remotos	Lista de hosts que son destinatarios de mensajes de registro.	servidor de registro formación	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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" : {}
}
```

Nueva versión

9,6

Encuentra más información

[Obtener hosts de registro remoto](#)

SetSnmppACL

Puedes usar el `SetSnmppACL` Método para configurar los permisos de acceso SNMP en los nodos del clúster. Los valores que establezca con esta interfaz se aplicarán a todos los nodos del clúster, y los valores que se pasen reemplazarán todos los valores

establecidos en cualquier llamada anterior a `SetSnmPACL` . Tenga en cuenta también que los valores establecidos con esta interfaz reemplazan todos los valores de red o `usmUsers` establecidos con la `SetSnmPInfo` método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
redes	Lista de redes y el tipo de acceso que tienen a los servidores SNMP que se ejecutan en los nodos del clúster. Consulte el objeto de red SNMP para conocer los valores de red posibles. Este parámetro es obligatorio si SNMP v3 está deshabilitado.	red	Ninguno	No
usuarios de usm	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 obligatorio si SNMP v3 está habilitado.	usmUser	Ninguno	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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" : {}
}
```

Nueva versión

9,6

Encuentra más información

[SetSnmPInfo](#)

SetSnmPInfo

Puedes usar el `SetSnmPInfo` Método para configurar SNMP versión 2 y versión 3 en nodos de clúster. Los valores que establezca con esta interfaz se aplicarán a todos los nodos del clúster, y los valores que se pasen reemplazarán todos los valores establecidos en cualquier llamada anterior a `SetSnmPInfo` .

Parámetros



`SetSnmPInfo` está obsoleto para las versiones 6.0 y posteriores de Element. Utilice el [Habilitar SNMP](#) y [SetSnmPACL](#) métodos en su lugar.

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
redes	Lista de redes y el tipo de acceso que tienen a los servidores SNMP que se ejecutan en los nodos del clúster. Consulte el SNMP. red objeto para valores posibles. Este parámetro solo es necesario para SNMP v2.	red formación	Ninguno	No
activado	Si se establece en verdadero, SNMP se habilita en cada nodo del clúster.	booleano	FALSO	No
snmpV3Enabled	Si se establece en verdadero, SNMP v3 se habilita en cada nodo del clúster.	booleano	FALSO	No
usuarios de usm	Si SNMP v3 está habilitado, este valor debe pasarse en lugar del parámetro de redes. Este parámetro solo es necesario para SNMP v3.	usmUser	Ninguno	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud con SNMP v3 habilitado

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "SetSnmInfo",
  "params": {
    "enabled": true,
    "snmpV3Enabled": true,
    "usmUsers": [
      {
        "name": "user1",
        "access": "rouser",
        "secLevel": "auth",
        "password": "name1",
        "passphrase": "yourpassphrase"
      }
    ]
  },
  "id": 1
}
```

Ejemplo de solicitud con SNMP v2 habilitado

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "SetSnmInfo",
  "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" :{
  }
}
```

Nueva versión

9,6

SetSnmptTrapInfo

Puedes usar el `SetSnmptTrapInfo` Método para habilitar y deshabilitar la generación de notificaciones SNMP de clúster (traps) y para especificar el conjunto de hosts que reciben las notificaciones. Los valores que pasas con cada `SetSnmptTrapInfo` La llamada al método reemplaza todos los valores establecidos en cualquier llamada anterior.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo
Receptores de trampas	Lista de hosts que recibirán las alertas generadas por el clúster de almacenamiento. Se requiere al menos un objeto si se habilita cualquiera de los tipos de trampa. Este parámetro solo es necesario si algún parámetro booleano está configurado como verdadero. (Sin valor predeterminado. (No es obligatorio.)	Destinatario de trampa SNMPformación
clusterFaultTrapsEnabled	Si se establece en verdadero, se envía una notificación de fallo de clúster correspondiente a la lista configurada de destinatarios de traps cuando se registra un fallo de clúster. (Valor predeterminado: falso. (No es obligatorio.)	booleano

Nombre	Descripción	Tipo
Trampas de resolución de fallos de clúster habilitadas	Si se establece en verdadero, se envía una notificación de resolución de fallo de clúster correspondiente a la lista configurada de destinatarios de traps cuando se resuelve un fallo de clúster. (Valor predeterminado: falso. (No es obligatorio.)	booleano
clusterEventTrapsEnabled	Si se establece en verdadero, se envía una notificación de evento de clúster correspondiente a la lista configurada de destinatarios de trampas cuando se registra un evento de clúster. (Valor predeterminado: falso. (No es obligatorio.)	booleano

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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" : {}
}
```

Nueva versión

9,6

Establecer certificado SSL

Puedes usar el `SetSSLCertificate` Método para configurar un certificado SSL de usuario y una clave privada para los nodos de almacenamiento en el clúster.



Después de utilizar la API, debe reiniciar el nodo de administración.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
certificado	La versión de texto del certificado codificada en PEM. Nota: Al configurar un certificado de nodo o clúster, el certificado debe incluir la extensión <code>extendedKeyUsage</code> para <code>serverAuth</code> . Esta extensión permite utilizar el certificado sin errores en sistemas operativos y navegadores comunes. Si la extensión no está presente, la API rechazará el certificado por ser inválido.	cadena	Ninguno	Sí
clave privada	La versión de texto codificada en PEM de la clave privada.	cadena	Ninguno	Sí

940

```

NBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzxF+AC\nq+itawIDAQABo4HrMIHoMB0GA1Ud
DgQWBBrvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYDVQQHFAxW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbjBWZWdhcy4uLjEtMCSGCSqG
SIB3DQEJARYe\nd2hhdGhhcHBlnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjJf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s7lmQPECwVLfiE/ndtIbnpe\nmQ
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7Jyfs3714rRolFpX6N\niebEgAae5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dH0lQ+WYnoO/eIMy0coT26JB15H\nnDEwvdl+DwknS1cx1v
ERv51glgua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nnHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAJJDg
l0QoQDWNDoTerBs80nwiouA==\n-----END CERTIFICATE-----\n"
    },
    "id" : 2
  }

```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```

{
  "id" : 2,
  "result" : {}
}

```

Nueva versión

10,0

SnmpSendTestTraps

`SnmpSendTestTraps` te permite probar la funcionalidad SNMP para un clúster. Este método indica al clúster que envíe traps 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 de retorno:

Nombre	Descripción	Tipo
estado	Estado de la prueba.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "SnmpSendTestTraps",
  "params": {},
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "status": "complete"
  }
}
```

Nueva versión

9,6

Disponibilidad de direcciones de prueba

Puedes usar el `TestAddressAvailability` Método para comprobar si una determinada dirección IP está en uso en una interfaz dentro del clúster de almacenamiento.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
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

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
etiqueta de red virtual	El ID de VLAN de destino.	entero	Ninguno	No
se acabó el tiempo	Tiempo de espera en segundos para probar la dirección de destino.	entero	5	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
DIRECCIÓN	La dirección IP probada.	cadena
disponible	Verdadero si la dirección IP solicitada está en uso, y falso si no lo está.	booleano

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}
```

Nueva versión

11,0

Métodos de API de redes multiinquilino

Convenciones de nomenclatura de redes virtuales

Los sistemas de almacenamiento NetApp Element utilizan números que aumentan de forma monótona como identificadores únicos para todos los objetos del sistema.

Cuando se crea un nuevo volumen, el nuevo ID de volumen es un incremento de exactamente 1. Esta convención también se aplica a las redes virtuales en clústeres de almacenamiento que ejecutan el software Element. La primera red virtual que cree en un clúster de Element tiene un VirtualNetworkID de 1. Este ID no es lo mismo que un número de etiqueta VLAN.

Puedes usar VirtualNetworkID y VirtualNetworkTag (etiqueta VLAN) indistintamente donde se indique en los métodos de la API.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

Agregar red virtual

Puedes usar el `AddVirtualNetwork` Método para agregar una nueva red virtual a una configuración de clúster.

Al agregar una red virtual, se crea una interfaz para cada nodo y cada interfaz requiere una dirección IP de red virtual. El número de direcciones IP que especifique como parámetro para este método de API debe ser igual o mayor que el número de nodos del clúster. El sistema aprovisiona direcciones de red virtuales de forma masiva y las asigna automáticamente a nodos individuales. No es necesario asignar manualmente direcciones de red virtuales a los nodos.



El método `AddVirtualNetwork` se utiliza únicamente para crear una nueva red virtual. Si desea realizar cambios en una red virtual existente, utilice el [Modificar red virtual](#) método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
bloques de direcciones	Rango único de direcciones IP para incluir en la red virtual. Miembros requeridos para el objeto: • inicio: El inicio del rango de direcciones IP. (cadena) • tamaño: El número de direcciones IP que se incluirán en el bloque. (entero)	matriz de objetos JSON	Ninguno	Sí
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
puerta	La dirección IP de una puerta de enlace de la red virtual. Este parámetro solo es válido si el parámetro de espacio de nombres está establecido en verdadero.	cadena	Ninguno	No
nombre	Un nombre definido por el usuario para la nueva red virtual.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
espacio de nombres	Cuando se establece en verdadero, habilita la funcionalidad de VLAN de almacenamiento enrutable mediante la creación y configuración de un espacio de nombres y la red virtual contenida en él.	booleano	Ninguno	No
máscara de red	Máscara de red única para la red virtual que se está creando.	cadena	Ninguno	Sí
svip	Dirección IP de almacenamiento única para la red virtual que se está creando.	cadena	Ninguno	Sí
etiqueta de red virtual	Una etiqueta de red virtual (VLAN) única. Los valores admitidos son del 1 al 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 falso.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
ID de red virtual	El ID de red virtual de la nueva red virtual.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
}
```

Nueva versión

9,6

Modificar red virtual

Puedes usar el `ModifyVirtualNetwork` Método para cambiar los atributos de una red virtual existente.

Este método le permite agregar o eliminar bloques de direcciones, cambiar la máscara de red o modificar el nombre o la descripción de la red virtual. También puede utilizarlo para habilitar o deshabilitar espacios de nombres, así como para agregar o eliminar una puerta de enlace si los espacios de nombres están habilitados en la red virtual.



Este método requiere el virtualNetworkID o el virtualNetworkTag como parámetro, pero no ambos.

PRECAUCIÓN:

Habilitar o deshabilitar la funcionalidad de VLAN de almacenamiento enrutable para una red virtual existente mediante el cambio del parámetro de espacio de nombres interrumpe cualquier tráfico manejado por la red virtual. Lo mejor es cambiar el parámetro de espacio de nombres durante una ventana de mantenimiento programada.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de red virtual	Identificador único de la red virtual que se va a modificar. Este es el ID de red virtual asignado por el clúster.	entero	Ninguno	No
etiqueta de red virtual	La etiqueta de red que identifica la red virtual que se va a modificar.	entero	Ninguno	No

bloques de direcciones	El nuevo bloque de direcciones que se debe configurar para esta red virtual. Esto podría incluir nuevos bloques de direcciones para agregar al objeto existente u omitir bloques de direcciones no utilizados que deban eliminarse. Como alternativa, puede ampliar o reducir el tamaño de los bloques de direcciones existentes. Solo se puede aumentar el tamaño de los bloques de direcciones iniciales para un objeto de red virtual; nunca se puede disminuir. Miembros requeridos para este objeto: • inicio: El inicio del rango de direcciones IP. (cadena) • tamaño: El número de direcciones IP que se incluirán en el bloque. (entero)	Objeto JSON	Ninguno	No
puerta	La dirección IP de una puerta de enlace de la red virtual. Este parámetro solo es válido si el parámetro de espacio de nombres está establecido en verdadero.	cadena	Ninguno	No

atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
nombre	El nuevo nombre de la red virtual.	cadena	Ninguno	No
espacio de nombres	Cuando se establece en verdadero, habilita la funcionalidad de VLAN de almacenamiento enrutable recreando la red virtual y configurando un espacio de nombres para contenerla. Cuando se establece en falso, deshabilita la funcionalidad VRF para la red virtual. Cambiar este valor interrumpe el tráfico que circula por 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 de una red virtual no se puede cambiar. Debe crear una nueva red virtual para utilizar una dirección SVIP diferente.	cadena	Ninguno	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": {
  }
}
```

Nueva versión

9,6

Lista de redes virtuales

Puedes usar el `ListVirtualNetworks` Método para listar todas las redes virtuales configuradas para el clúster.

Puede utilizar este método para verificar la configuración de la red virtual en el clúster. Este método no requiere parámetros. Sin embargo, para filtrar los resultados, puede pasar uno o más valores de virtualNetworkID o virtualNetworkTag.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de red virtual	ID de red para filtrar la lista por una única red virtual.	entero	Ninguno	No
etiqueta de red virtual	Etiqueta de red para filtrar la lista por una única red virtual.	entero	Ninguno	No
IDs de red virtuales	Identificadores de red para incluir en la lista.	matriz de enteros	Ninguno	No
Etiquetas de red virtuales	Etiqueta de red para incluir en la lista.	matriz de enteros	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
redes virtuales	Objeto que contiene direcciones IP de red virtual.	red virtual

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}
```

```

    }
  ],
  "attributes": null,
  "gateway": "10.26.240.254",
  "name": "2240",
  "namespace": false,
  "netmask": "255.255.255.0",
  "svip": "10.26.240.200",
  "virtualNetworkID": 2240
},
{
}
]
}

```

Nueva versión

9,6

Eliminar red virtual

Puedes usar el `RemoveVirtualNetwork` Método para eliminar una red virtual añadida previamente.



Este método requiere el `virtualNetworkID` o el `virtualNetworkTag` como parámetro, pero no ambos.



No se puede eliminar una red virtual si hay iniciadores asociados a ella. Primero desvincule los iniciadores y luego elimine la red virtual.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de red virtual	ID de red que identifica la red virtual que se va a eliminar.	entero	Ninguno	Sí
etiqueta de red virtual	Etiqueta de red que identifica la red virtual que se va a eliminar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "RemoveVirtualNetwork",
  "params": {
    "virtualNetworkID": 5
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nueva versión

9,6

Métodos de la API de volumen

CancelarClon

Puedes usar el `CancelClone` Método para detener un proceso de clonación o copia de volumen en curso. Cuando se cancela una operación de clonación de grupo, el sistema la completa y elimina el `asyncHandle` asociado a la operación.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de clon	El ID del clon para el proceso de clonación en curso.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "CancelClone",
  "params": {
    "cloneID" : 5,
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nueva versión

9,6

CancelarClonDeGrupo

Puedes usar el `CancelGroupClone` Método para detener un proceso de clonación en curso que se está produciendo en un grupo de volúmenes. Cuando se cancela una operación de clonación de grupo, el sistema la completa y elimina el `asyncHandle` asociado a la operación.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de clon de grupo	El ID del clon para el proceso de clonación en curso.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "CancelGroupClone",
  "params": {
    "cloneID" : 5,
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result" : {}
}
```

Nueva versión

9,6

Clonar múltiples volúmenes

Puedes usar el `CloneMultipleVolumes` Método para crear un clon de un grupo de volúmenes especificados. Se puede asignar un conjunto coherente de características a un grupo de varios volúmenes cuando se clonan juntos.

Antes de utilizar el parámetro `groupSnapshotID` para clonar los volúmenes en una instantánea de grupo, primero debe crear la instantánea de grupo utilizando el [CrearInstantáneaDeGrupo](#) Método API o interfaz web. El uso de `groupSnapshotID` es opcional al clonar varios volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
acceso	Nuevo método de acceso predeterminado para los nuevos volúmenes si no se modifica mediante la información pasada en la matriz del volumen.	cadena	Ninguno	No
habilitarSnapMirrorReplication	Determina si el volumen se puede utilizar para la replicación con puntos de conexión SnapMirror . Valores posibles: • verdadero • FALSO	booleano	FALSO	No
ID de instantánea del grupo	ID de la instantánea del grupo que se utilizará como base para la clonación.	entero	Ninguno	No
nuevo ID de cuenta	Nuevo ID de cuenta para los volúmenes si no se sobrescribe con la información pasada en la matriz de volúmenes.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
volúmenes	Conjunto de miembros que usted especifique para los nuevos volúmenes. Miembros: • ID del volumen: (Obligatorio) • acceso: (Opcional) Puede ser uno de readOnly, readWrite, locked 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 para los nuevos volúmenes. • nuevoTamaño: (Opcional) Tamaño total del volumen, en bytes. El tamaño se redondea al megabyte más cercano. Si no se especifican los miembros opcionales, los valores se heredan de los volúmenes de origen.	matriz de objetos JSON	Ninguno	Sí (volumeID)

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
manejador asíncrono	Valor devuelto por una llamada a un método asíncrono.	entero
ID de clon de grupo	Identificador único del nuevo clon de grupo.	entero
miembros	Lista de IDs de volumen para los pares de volúmenes de origen y destino.	matriz de objetos JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}
```

Nueva versión

9,6

Clonar volumen

Puedes usar el `CloneVolume` Método para crear una copia de un volumen. Este método es asíncrono y puede tardar un tiempo variable en completarse.

El proceso de clonación comienza inmediatamente cuando realizas la `CloneVolume` La solicitud es representativa del estado del volumen cuando se emite el método de la API. Puedes usar el [ObtenerResultadoAsíncrono](#) método para determinar cuándo finaliza el proceso de clonación y el nuevo volumen está disponible para conexiones. Puedes usar [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 está clonando. Puedes cambiar estos ajustes con [Modificar volumen](#) .



Los volúmenes clonados no heredan la pertenencia al grupo de acceso al volumen del volumen de origen.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
acceso	Se ha permitido el acceso al nuevo volumen. Si no se especifica un valor, el valor de acceso no cambia. Valores posibles: • <code>readOnly</code>: (Opcional) Solo se permiten operaciones de lectura. • <code>readWrite</code>(Opcional) Se permiten lecturas y escrituras. • <code>locked</code>(Opcional) No se permiten lecturas ni escrituras. Si no se especifica, se utiliza el valor de acceso del volumen que se está clonando. • <code>replicationTarget</code>: (Opcional) Identifique un volumen como el volumen objetivo para un conjunto de volúmenes emparejados. Si el volumen no está emparejado, el estado de acceso queda bloqueado.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
enable512e	Especifica si el nuevo volumen debe utilizar la emulación de sectores de 512 bytes. Si no se especifica, se utiliza la configuración del volumen que se está clonando.	booleano	Ajuste del volumen original	No
habilitarSnapMirrorReplication	Determina si el volumen se puede utilizar para la replicación con puntos de conexión SnapMirror . Valores posibles: • verdadero • FALSO	booleano	FALSO	No
nombre	Nombre del nuevo volumen clonado; debe tener entre 1 y 64 caracteres de longitud.	cadena	Ninguno	Sí
nuevo ID de cuenta	ID de cuenta del propietario del nuevo volumen. Si no se especifica, se utiliza el ID de cuenta del propietario del volumen que se está clonando.	entero	ID de cuenta del propietario del volumen original	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nuevoTamaño	Nuevo tamaño del volumen, en bytes. Podría ser mayor o menor que el tamaño del volumen que se está clonando. Si no se especifica, el tamaño del volumen no se modifica. El tamaño se redondea al MB más cercano.	entero	Ninguno	No
ID de instantánea	Identificador de la instantánea que se utiliza como fuente del clon. Si no se proporciona un ID, se utiliza el volumen activo actual.	entero	Ninguno	No
ID de volumen	ID del volumen que se va a clonar.	entero	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
manejador asíncrono	El valor del identificador utilizado para obtener el resultado de la operación.	entero
ID de clon	El ID del clon para el volumen recién clonado.	entero
curva	Los valores de la curva QoS aplicados al clon.	Objeto JSON
volume	Un objeto que contiene información sobre el volumen recién clonado.	volume
ID de volumen	ID del volumen recién clonado.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": "6a7961790000002a8f47acc0100000000",
"scsiNAADeviceID": "6f47acc1000000006a7961790000002a8",
"sliceCount": 0,
"status": "init",
"totalSize": 1000341504,
"virtualVolumeID": null,
"volumeAccessGroups": [],
"volumeID": 680,
"volumePairs": []
},
"volumeID": 680
}
}

```

Nueva versión

9,6

Encuentra más información

- [ObtenerResultadoAsíncrono](#)
- [ListSyncJobs](#)
- [Modificar volumen](#)

Volumen de copia

Puedes usar el `CopyVolume` Método para sobrescribir el contenido de datos de un volumen existente con el contenido de datos de otro volumen (o instantánea). Los atributos del volumen de destino, como IQN, configuración QoS, tamaño, cuenta y pertenencia al grupo de acceso al volumen, no se modifican. El volumen de destino debe existir previamente y debe tener el mismo tamaño que el volumen de origen.

Lo mejor es que los clientes desmonten el volumen de destino antes de que comience la operación. Si el volumen de destino se modifica durante la operación, los cambios se perderán. Esta operación puede tardar un tiempo variable en completarse. Puedes usar el [ObtenerResultadoAsíncrono](#) 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	Requerido
ID de volumen de destino	ID del volumen que se va a sobrescribir.	entero	Ninguno	Sí
ID de volumen	ID del volumen que se va a leer.	entero	Ninguno	Sí
ID de instantánea	Identificador de la instantánea que se utiliza como fuente del clon. Si no se proporciona un ID, se utiliza el volumen activo actual.	entero	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
manejador asíncrono	Valor de identificador utilizado para obtener el resultado de la operación.	entero
ID de clon	CloneID para el volumen recién clonado.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}
```

Nueva versión

9,6

Encuentra más información

- [ObtenerResultadoAsíncrono](#)
- [ListSyncJobs](#)

Crear política de QoS

Puedes usar el `CreateQoSPolicy` Método para crear un objeto `QoSPolicy` que posteriormente se puede aplicar a un volumen al crearlo o modificarlo. Una política de QoS tiene un ID único, un nombre y una configuración de QoS.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nombre	El nombre de la política de QoS; por ejemplo, oro, platino o plata.	cadena	Ninguno	Sí
QoS	La configuración de QoS que representa esta política.	Calidad de servicio	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Política de calidad de servicio	El objeto <code>QoSPolicy</code> recién creado.	Política de QoS

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": []
    }
  }
}

```

Nueva versión

10,0

Crear volumen

Puedes usar el `CreateVolume` Método para crear un nuevo volumen vacío en el clúster. Tan pronto como se crea el volumen, este está disponible para la conexión a través de iSCSI.

Los volúmenes creados sin valores QoS especificados utilizan los valores predeterminados. Puede ver los valores predeterminados de un volumen utilizando la `GetDefaultQoS` método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
access	Modo de acceso al volumen. Si se incluye este parámetro, el único valor admitido es snapMirrorTarget.	cadena	Ninguno	No
accountID	El ID de la cuenta propietaria de este volumen.	entero	Ninguno	Sí
associateWithQoSPolicy	Asocie el volumen con la política QoS especificada. Valores posibles: • <code>true</code> Asocie el volumen con la política QoS especificada en el parámetro QoSPolicyID. • <code>false</code> No asocie el volumen con la política QoS especificada en el parámetro QoSPolicyID. Cuando es falso, se elimina cualquier asociación de política existente, independientemente de si se especifica una política QoS en el parámetro QoSPolicy.	booleano	verdadero	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
attributes	Lista de pares nombre-valor en formato de objeto JSON. El tamaño total de los atributos debe ser inferior a 1000 B, o 1 KB, incluidos los caracteres de formato JSON.	Objeto JSON	Ninguno	No
dontMoveforIopsRebalance	Evitar que un volumen se mueva al equilibrar la carga con IOPS reales. Esta configuración está disponible a partir de Element 12.8 y solo es efectiva cuando "Balanceo de carga de volumen en IOPS reales" está habilitado. Valores posibles: • <code>true`</code> El volumen no realiza el balanceo de carga en función de las IOPS reales.</li> <li>• <code>false`</code> El volumen realiza el balanceo de carga en función de las IOPS reales. Nota: El equilibrio para alta disponibilidad (fallo de nodo) tiene prioridad sobre VolumeLoadBalanceOnActualIOPS y dontMoveforIopsRebalance .	booleano	FALSO	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
enable512e	Habilitar la emulación de sectores de 512 bytes. Valores posibles: • `true` El volumen proporciona emulación de sectores de 512 bytes. • `false` La emulación 512e no está habilitada.	booleano	Ninguno	Sí
enableSnapMirrorReplication	Determina si el volumen se puede utilizar para la replicación con puntos de conexión SnapMirror . Valores posibles: • true • false	booleano	FALSO	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
fifoSize	Especifica el número máximo de instantáneas First-In-First-Out (FIFO) admitidas por el volumen. Tenga en cuenta que tanto las instantáneas FIFO como las no FIFO utilizan el mismo conjunto de ranuras de instantáneas disponibles en un volumen. Utilice esta opción para limitar el consumo de instantáneas FIFO de las ranuras de instantáneas disponibles. Si se omite, el valor predeterminado es 24.	entero	24	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
minFifoSize	Especifica el número mínimo de ranuras de instantáneas First-In-First-Out (FIFO) reservadas por el volumen. Esto garantiza que, si se utilizan instantáneas FIFO e instantáneas no FIFO en un volumen, las instantáneas no FIFO no consuman involuntariamente demasiadas ranuras FIFO. También garantiza que siempre haya disponible al menos esta cantidad de instantáneas FIFO. Dado que las instantáneas FIFO y no FIFO comparten el mismo grupo, 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 al volumen (puede ser especificado por el usuario). No es necesario que sea único, pero es recomendable. Debe tener entre 1 y 64 caracteres de longitud.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
qos	La configuración inicial de calidad de servicio para este volumen. Si no se especifica ninguno, se utilizarán los valores predeterminados. Valores posibles: • minIOPS • maxIOPS • burstIOPS	Objeto QoS	Ninguno	No
qosPolicyID	El ID de la política cuya configuración QoS se debe aplicar a los volúmenes especificados. Este parámetro es mutuamente excluyente con el qos parámetro.	entero	Ninguno	No
totalSize	Tamaño total del volumen, en bytes. El tamaño se redondea al megabyte más cercano.	entero	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
volume	Objeto que contiene información sobre el volumen recién creado.	volume
ID de volumen	El ID del volumen recién creado.	entero

Nombre	Descripción	Tipo
curva	La curva es un conjunto de pares clave-valor. Las claves son los tamaños de E/S en bytes. Los valores representan el coste de realizar una OIP con un tamaño de I/S específico. La curva se calcula en relación con una operación de 4096 bytes configurada a 100 IOPS.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "CreateVolume",
  "params": {
    "name": "testit",
    "accountID": 22,
    "dontMoveForIopsRebalance": true,
    "totalSize": 1000000000000,
    "enable512e": false,
    "attributes": {},
    "qos": {
      "minIOPS": 500,
      "maxIOPS": 27000,
      "burstIOPS": 27000,
      "burstTime": 60
    }
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "curve": {
      "1048576": 15000,
      "131072": 1950,
      "16384": 270,
```

```

        "262144": 3900,
        "32768": 500,
        "4096": 100,
        "524288": 7600,
        "65536": 1000,
        "8192": 160
    },
    "volume": {
        "access": "readWrite",
        "accountID": 22,
        "attributes": {},
        "blockSize": 4096,
        "createTime": "2024-04-02T13:03:02Z",
        "currentProtectionScheme": "doubleHelix",
        "deleteTime": "",
        "dontMoveForIopsRebalance": true,
        "enable512e": false,
        "enableSnapMirrorReplication": false,
        "fifoSize": 24,
        "iqn": "iqn.2010-01.com.solidfire:mysqldata.677",
        "lastAccessTime": null,
        "lastAccessTimeIO": null,
        "minFifoSize": 0,
        "name": "testit",
        "previousProtectionScheme": null,
        "purgeTime": "",
        "qos": {
            "burstIOPS": 27000,
            "burstTime": 60,
            "curve": {
                "1048576": 15000,
                "131072": 1950,
                "16384": 270,
                "262144": 3900,
                "32768": 500,
                "4096": 100,
                "524288": 7600,
                "65536": 1000,
                "8192": 160
            },
            "maxIOPS": 27000,
            "minIOPS": 500
        },
        "qosPolicyID": null,
        "scsiEUIDeviceID": "3365657500000140f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000003365657500000140",
    },

```

```

        "sliceCount": 0,
        "status": "active",
        "totalSize": 1000000716800,
        "virtualVolumeID": null,
        "volumeAccessGroups": [],
        "volumeConsistencyGroupUUID": "8ed68e57-13ee-47df-8381-
29b125142718",
        "volumeID": 320,
        "volumePairs": [],
        "volumeUUID": "e0e2c938-4ecd-4de9-albe-f6b17c93ce5d"
    },
    "volumeID": 320
}
}

```

Nueva versión

9,6

Encuentra más información

[Obtener QoS predeterminado](#)

Crear destino de copia de seguridad

Puedes usar `CreateBackupTarget` para crear y almacenar información sobre el destino de las copias de seguridad, de modo que no tenga que volver a introducirla cada vez que se cree una copia de seguridad.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nombre	Nombre del destino de la copia de seguridad.	cadena	Ninguno	Sí
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	Sí (pero puede estar vacío)

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
ID de destino de respaldo	Se ha asignado un identificador único al nuevo destino de la copia de seguridad.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "CreateBackupTarget",
  "params": {
    "name": "mytargetbackup"
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "backupTargetID": 1
  }
}
```

Nueva versión

9,6

Eliminar política de QoS

Puedes usar el `DeleteQoSPolicy` Método para eliminar una política QoS del sistema. La configuración QoS para todos los volúmenes creados o modificados con esta política no se verá afectada.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de política de qos	El ID de la política QoS que se va a eliminar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "id": 663,
  "method": "DeleteQoSPolicy",
  "params": {
    "qosPolicyID": 4
  }
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 663,
  "result": {}
}
```

Nueva versión

9,6

Eliminar volumen

Puedes usar el `DeleteVolume` Método para marcar un volumen activo para su eliminación. Cuando se marca, el volumen se purga (se elimina permanentemente) después de que transcurre el intervalo de limpieza.

Tras realizar una solicitud para eliminar un volumen, se terminan inmediatamente todas las conexiones iSCSI activas al volumen y no se permiten más conexiones mientras el volumen se encuentra en este estado. No se devuelve un volumen marcado en las solicitudes de detección de destino.

Las instantáneas de un volumen que haya sido marcado para su eliminación no se verán afectadas. Las

instantáneas se conservan hasta que el volumen se elimina del sistema. Si un volumen está marcado para su eliminación y tiene una operación de lectura o escritura masiva de volumen en curso, dicha operación se detiene.

Si el volumen que elimina está emparejado con otro volumen, la replicación entre los volúmenes emparejados se suspende y no se transfieren datos hacia ni desde él mientras esté en estado eliminado. El volumen remoto con el que estaba emparejado el volumen eliminado entra en un estado `PausedMisconfigured` y ya no se envían datos hacia él ni desde el volumen eliminado. Hasta que se elimine el volumen borrado, se puede restaurar y reanudar la transferencia de datos. Si el volumen eliminado se borra del sistema, el volumen con el que estaba emparejado entra en un estado `StoppedMisconfigured` y se elimina el estado de emparejamiento de volúmenes. El volumen purgado queda permanentemente inaccesible.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de volumen	El identificador del volumen que se va a eliminar.	entero	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
volume	Objeto que contiene información sobre el volumen eliminado.	volume
ID de volumen	El ID del volumen eliminado.	entero
curva	La curva es un conjunto de pares clave-valor. Las claves son los tamaños de E/S en bytes. Los valores representan el coste de realizar una OIP con un tamaño de I/S específico. La curva se calcula en relación con una operación de 4096 bytes configurada a 100 IOPS.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:


```
{
  "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": []
}
}
}

```

Nueva versión

9,6

Eliminar volúmenes

Puedes usar el `DeleteVolumes` método para marcar múltiples (hasta 500) volúmenes activos para su eliminación. Cuando se marca, el volumen se purga (se elimina permanentemente) después de que transcurre el intervalo de limpieza.

Después de realizar una solicitud para eliminar volúmenes, cualquier conexión iSCSI activa a los volúmenes se termina inmediatamente y no se permiten más conexiones mientras los volúmenes se encuentran en este estado. No se devuelve un volumen marcado en las solicitudes de detección de destino.

Las instantáneas de un volumen que haya sido marcado para su eliminación no se verán afectadas. Las instantáneas se conservan hasta que el volumen se elimina del sistema. Si un volumen está marcado para su eliminación y tiene una operación de lectura o escritura masiva de volumen en curso, dicha operación se detiene.

Si los volúmenes que elimina están emparejados con un volumen, la replicación entre los volúmenes emparejados se suspende y no se transfieren datos hacia ni desde ellos mientras estén en estado eliminado. Los volúmenes remotos con los que estaban emparejados los volúmenes eliminados entran en un estado `PausedMisconfigured` y ya no se envían datos a ellos ni desde los volúmenes eliminados. Hasta que se eliminen los volúmenes borrados, se pueden restaurar y se reanudarán las transferencias de datos. Si los volúmenes eliminados se purgan del sistema, los volúmenes con los que estaban emparejados entran en un estado `StoppedMisconfigured` y se elimina el estado de emparejamiento de volúmenes. Los volúmenes eliminados quedan permanentemente inaccesibles.

Parámetros

Este método tiene los siguientes parámetros de entrada.



Se requiere al menos uno de los siguientes parámetros, y debe utilizar solo uno de ellos (son todos mutuamente excluyentes).

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
IDs de volumen	La lista de identificadores de los volúmenes que se eliminarán del sistema.	matriz de enteros	Ninguno	Ver nota.
ID de grupo de acceso de volumen	Una lista de identificadores de grupos de acceso a volúmenes. Todos los volúmenes de todos los grupos de acceso a volúmenes que especifique en esta lista se eliminarán del sistema.	matriz de enteros	Ninguno	Ver nota.
ID de cuenta	Una lista de identificadores de cuenta. Todos los volúmenes de estas cuentas se eliminan del sistema.	matriz de enteros	Ninguno	Ver nota.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
volúmenes	Información sobre el volumen recién eliminado.	volume
curva	La curva es un conjunto de pares clave-valor. Las claves son los tamaños de E/S en bytes. Los valores representan el coste de realizar una OIP con un tamaño de I/S específico. La curva se calcula en relación con una operación de 4096 bytes configurada a 100 IOPS.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": "707a7372000000001f47acc0100000000",
      "scsiNAADeviceID": "6f47acc1000000000707a737200000001",
      "status": "active",
      "totalSize": 10000003072,
      "virtualVolumeID": 5,
      "volumeAccessGroups": [],
      "volumePairs": [],
      "volumeID": 1
    } ]
  }
}

```

Nueva versión

9,6

ObtenerObjetivoDeCopiaDeSeguridad

Puedes usar el `GetBackupTarget` Método para obtener información sobre un destino de copia de seguridad específico que haya creado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
ID de destino de respaldo	Identificador único asignado al destino de la copia de seguridad.	entero	Ninguno	Sí
nombre	Nombre del destino de la copia de seguridad.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
destino de respaldo	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  }
}

```

Nueva versión

9,6

Obtener estadísticas de volumen

Puedes usar el `GetVolumeStats` Método para obtener mediciones de actividad de alto nivel para un solo volumen. Los valores son acumulativos desde la creación del volumen.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de volumen	Especifica el volumen para el cual se recopilan las estadísticas.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
estadísticas de volumen	Información sobre el volumen de actividad.	estadísticas de volumen

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": 4,
        "asyncDelay": null,
        "averageIOPSize": 5970,
        "burstIOPSCredit": 0,
        "clientQueueDepth": 0,
        "desiredMetadataHosts": null,
        "latencyUSec": 474,
        "metadataHosts": {
          "deadSecondaries": [],
          "liveSecondaries": [
            13
          ],
          "primary": 25
        },
        "nonZeroBlocks": 34931222,
        "normalizedIOPS": 4,
        "readBytes": 1282491003392,
        "readBytesLastSample": 0,
        "readLatencyUSec": 0,
        "readLatencyUSecTotal": 4581669750,
        "readOps": 15592933,
        "readOpsLastSample": 0,
        "samplePeriodMSec": 500,
        "sliceIopsStats": {
          "largeStatistics": {
            "averageReadIops": 17,
            "averageTotalIops": 43,
```



```

        "averageWriteIops": 26,
        "nSamples": 24,
        "peakReadIops": 19,
        "peakTotalIops": 47,
        "peakWriteIops": 30,
        "sliceID": 1
    },
    "smallStatistics": {
        "averageReadIops": 17,
        "averageTotalIops": 42,
        "averageWriteIops": 25,
        "nSamples": 120,
        "peakReadIops": 173,
        "peakTotalIops": 249,
        "peakWriteIops": 77,
        "sliceID": 1
    }
},
"throttle": 0,
"timestamp": "2025-02-03T21:18:38.880100Z",
"unalignedReads": 167319,
"unalignedWrites": 90836,
"volumeAccessGroups": [
    1
],
"volumeID": 1,
"volumeSize": 2147483648000,
"volumeUtilization": 0.00026666666666666667,
"writeBytes": 1385173585408,
"writeBytesLastSample": 12288,
"writeLatencyUsec": 474,
"writeLatencyUsecTotal": 11233350905,
"writeOps": 157060458,
"writeOpsLastSample": 2,
"zeroBlocks": 489356778
}
}
}

```

Nueva versión

9,6

Obtener QoS predeterminado

Puedes usar el `GetDefaultQoS` método para obtener los valores de calidad de servicio

(QoS) predeterminados para un volumen recién creado.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Calidad de servicio	Los valores QoS predeterminados.	Calidad de servicio

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}

```

Nueva versión

9,6

Obtener política de QoS

Puedes usar el `GetQoSPolicy` Método para obtener detalles sobre una política QoS específica del sistema.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de política de qos	El ID de la póliza que se va a recuperar.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Política de calidad de servicio	Detalles de la política de QoS solicitada.	Política de QoS

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      ]
    }
  }
}

```

Nueva versión

10,0

Obtener recuento de volumen

Puedes usar el `GetVolumeCount` Método para obtener el número de volúmenes que se encuentran actualmente en el sistema.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
contar	Número de volúmenes actualmente en el sistema.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetVolumeCount",
  "params": {
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "count": 7
  }
}
```

Nueva versión

9,6

ObtenerEficiencia de Volumen

Puedes usar el `GetVolumeEfficiency` Método para obtener información sobre un volumen. Para calcular la capacidad, solo se utiliza el volumen que se proporciona como parámetro en este método de la API.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de volumen	Especifica el volumen para el cual se calcula la capacidad.	entero	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
compresión	La cantidad de espacio que se ahorra al comprimir datos en un solo volumen. Se expresa como una proporción, donde 1 significa que los datos se han almacenado sin comprimir.	flotar
deduplicación	La cantidad de espacio que se ahorra en un solo volumen al no duplicar datos. Expresado como una proporción.	flotar
volúmenes faltantes	Los volúmenes de los que no se pudieron obtener datos de eficiencia. La falta de volúmenes puede deberse a que la recolección de basura (GC) tenga menos de una hora de antigüedad, a una pérdida temporal de la red o a servicios reiniciados desde el ciclo de GC.	matriz de enteros
aprovisionamiento ligero	La proporción de espacio utilizado con respecto a la cantidad de espacio asignado para almacenar datos. Expresado como una proporción.	flotar
marca de tiempo	La última vez que se recopilaron datos de eficiencia después de GC.	cadena de datos ISO 8601

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

Listar volúmenes activos

Puedes usar el `ListActiveVolumes` Método para obtener la lista de volúmenes activos actualmente en el sistema. La lista de volúmenes está ordenada por ID de volumen y puede devolverse en varias partes (páginas).

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
incluir volúmenes virtuales	Los volúmenes virtuales se incluyen en la respuesta de forma predeterminada. Para excluir volúmenes virtuales, establezca el valor en falso.	booleano	verdadero	No
ID de volumen de inicio	Volumen inicial a devolver. Si no existe ningún volumen con este VolumeID, se utiliza el siguiente volumen en orden de VolumeID como inicio de la lista. Para navegar por la lista, pase el VolumeID del último volumen de la respuesta anterior + 1.	entero	0	No
límite	Número máximo de objetos de información de volumen a devolver. 0 (cero) devuelve todos los volúmenes (ilimitados).	entero	(ilimitado)	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
volúmenes	Lista de volúmenes activos.	volume información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ListActiveVolumes",
  "params": {
    "startVolumeID" : 0,
    "limit" : 1000
  },
  "id" : 1
}
```

Ejemplo de respuesta

Debido a la extensión de este ejemplo de respuesta, se documenta en un tema complementario.

Nueva versión

9,6

ListBackupTargets

Puedes usar el `ListBackupTargets` Método para obtener información sobre 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 de retorno:

Nombre	Descripción	Tipo
destinos de respaldo	Objetos devueltos para cada destino de copia de seguridad. Objetos incluidos: • atributos: Lista de pares nombre-valor en formato de objeto JSON. (Objeto JSON) • backupTargetID: Identificador único asignado al destino de la copia de seguridad. (entero) • nombre: Nombre del destino de la copia de seguridad. (cadena)	Objeto JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}
```

Nueva versión

9,6

Lista de trabajos de volumen masivo

Puedes usar el `ListBulkVolumeJobs` Método para obtener información sobre cada operación de lectura o escritura de volumen masivo que se produce en el sistema.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Trabajos de gran volumen	Un conjunto de información para cada trabajo de gran volumen.	Trabajo de gran volumen información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": "eafffb0526d4fb47107061f09bfc9a806",
        "percentComplete": 8,
        "remainingTime": 506,
        "script": "bv_internal.py",
        "snapshotID": 509,
        "srcVolumeID": 3,
        "status": "running",
        "type": "read"
      }
    ]
  }
}

```

Nueva versión

9,6

Lista de volúmenes eliminados

Puedes usar el `ListDeletedVolumes` Método para recuperar la lista de volúmenes que han sido marcados para su eliminación y purgados del sistema.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
incluir volúmenes virtuales	Los volúmenes virtuales se incluyen en la respuesta de forma predeterminada. Para excluir volúmenes virtuales, establezca el valor en falso.	booleano	verdadero	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
volúmenes	Lista de volúmenes eliminados.	volume formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ListDeletedVolumes",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Las respuestas para este método son similares al siguiente ejemplo:

```

{
  "id": 1,
  "result": {
    "volumes": [
      {
        "access": "readWrite",
        "accountID": 2,
        "attributes": {},
        "blockSize": 4096,
        "createTime": "2018-06-24T03:13:13Z",
        "deleteTime": "2018-07-22T16:12:39Z",
        "enable512e": true,
        "iqn": "iqn.2010-01.com.solidfire:0oto.deletethis.23",
        "name": "deleteThis",
        "purgeTime": "2016-07-23T00:12:39Z",
        "qos": {
          "burstIOPS": 15000,
          "burstTime": 60,
          "curve": {
            "4096": 100,
            "8192": 160,
            "16384": 270,
            "32768": 500,
            "65536": 1000,
            "131072": 1950,
            "262144": 3900,
            "524288": 7600,
            "1048576": 15000
          },
          "maxIOPS": 15000,
          "minIOPS": 50
        },
        "scsiEUIDeviceID": "306f746f000000017f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000000306f746f000000017",
        "sliceCount": 1,
        "status": "deleted",
        "totalSize": 1396703232,
        "virtualVolumeID": null,
        "volumeAccessGroups": [],
        "volumeID": 23,
        "volumePairs": []
      }
    ]
  }
}

```

Nueva versión

9,6

Lista de políticas de QoS

Puedes usar el `ListQoSPolicies` Método para listar la configuración de todas las políticas de QoS en el sistema.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Políticas de QoS	Una lista con detalles sobre cada política de QoS.	Política de QoS formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    ]
}
]
}
}

```

Nueva versión

10,0

ListSyncJobs

Puedes usar el `ListSyncJobs` Método para obtener información sobre los trabajos de sincronización que se están ejecutando en un clúster de almacenamiento Element. Este método devuelve información sobre trabajos de segmentación, clonación, bloqueo y sincronización remota.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
sincronizar trabajos	Lista de objetos que describen los procesos de sincronización que se están ejecutando actualmente en el sistema.	trabajo de sincronización información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
]
}

```

Nueva versión

9,6

ListVolumeQoSHistogramas

Puedes usar el `ListVolumeQoSHistogramas` Método para generar un histograma del uso de QoS de volumen para un volumen o varios volúmenes. Esto le permite comprender mejor cómo los volúmenes utilizan QoS.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
IDs de volumen	Una lista opcional de identificadores de volumen que especifican para qué volúmenes se deben generar histogramas de QoS.	matriz de enteros	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Histogramas de calidad de servicio	Una lista de objetos que describe el uso del volumen para uno o más volúmenes.	matriz de objetos JSON

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
}
]
}
}

```

Lista de volúmenes

Puedes usar el `ListVolumes` Método para obtener una lista de los volúmenes que se encuentran en un clúster. Puede especificar los volúmenes que desea que aparezcan en la lista utilizando los parámetros disponibles.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
cuentas	Solo se devolverán los volúmenes que pertenezcan a las cuentas que especifique aquí. Mutuamente excluyente con el parámetro <code>volumeIDs</code> .	matriz de enteros	Ninguno	No
incluir volúmenes virtuales	Los volúmenes virtuales se incluyen en la respuesta de forma predeterminada. Para excluir volúmenes virtuales, establezca el valor en falso.	booleano	verdadero	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
esEmparejado	Devuelve los volúmenes que están emparejados o no emparejados. Valores posibles: • verdadero: Devuelve todos los volúmenes emparejados. • falso: Devuelve todos los volúmenes no emparejados.	booleano	Ninguno	No
límite	Le permite establecer el número máximo de resultados de volumen que se devuelven. Mutuamente excluyente con el parámetro volumeIDs.	entero	10000	No
ID de volumen de inicio	Solo se devuelven los volúmenes con un ID mayor o igual a este valor. Mutuamente excluyente con el parámetro volumeIDs.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
IDs de volumen	Una lista de identificadores de volumen. Si se especifica este parámetro, los demás parámetros solo operarán sobre este conjunto de volúmenes. Mutuamente excluyente con los parámetros accounts, startVolumeID y limit.	matriz de enteros	No	No
nombre del volumen	Solo se devuelve la información del objeto de volumen que coincida con el nombre del volumen.	cadena	No	No
estado del volumen	Solo se devuelven los volúmenes con un estado igual al valor de estado. Valores posibles: • creación • instantáneas • activo • eliminado	cadena	No	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
volúmenes	Lista de volúmenes.	volume formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:


```
{
  "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": "6a796179000000001f47acc0100000000",
        "scsiNAADeviceID": "6f47acc10000000006a79617900000001",
        "sliceCount": 1,
        "status": "active",
        "totalSize": 5000658944,
        "virtualVolumeID": null,
        "volumeAccessGroups": [],
        "volumeID": 1,
        "volumePairs": []
      }
    ]
  }
}

```

Nueva versión

9,6

Estadísticas de volumen de lista

Puedes usar 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 son acumulativos desde la creación del volumen.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
incluir volúmenes virtuales	Los volúmenes virtuales se incluyen en la respuesta de forma predeterminada. Para excluir volúmenes virtuales, establezca el valor en falso.	booleano	verdadero	No
IDs de volumen	Una lista de volúmenes desde los que recuperar información sobre la actividad.	matriz de enteros	No	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
estadísticas de volumen	Lista de información sobre el volumen de actividad.	estadísticas de volumen información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
]
}
}

```

Nueva versión

9,6

Listar volúmenes para la cuenta

Puedes usar el `ListVolumesForAccount` Método para listar los volúmenes activos y (pendientes de eliminación) de una cuenta.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
incluir volúmenes virtuales	Los volúmenes virtuales se incluyen en la respuesta de forma predeterminada. Para excluir volúmenes virtuales, establezca el valor en falso.	booleano	verdadero	No
ID de cuenta	Se devuelven todos los volúmenes pertenecientes a esta cuenta.	entero	No	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
volúmenes	Lista de información de volumen.	volume formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ListVolumesForAccount",
  "params": {
    "accountID" : 1
  },
  "id" : 1
}
```

Ejemplo de respuesta

Las respuestas para este método son similares al siguiente ejemplo:

```

{
  "id": 1,
  "result": {
    "volumes": [
      {
        "access": "readWrite",
        "accountID": 1,
        "attributes": {},
        "blockSize": 4096,
        "createTime": "2018-07-22T16:15:25Z",
        "deleteTime": "",
        "enable512e": false,
        "iqn": "iqn.2010-01.com.solidfire:0oto.test1.25",
        "name": "test1",
        "purgeTime": "",
        "qos": {
          "burstIOPS": 15000,
          "burstTime": 60,
          "curve": {
            "4096": 100,
            "8192": 160,
            "16384": 270,
            "32768": 500,
            "65536": 1000,
            "131072": 1950,
            "262144": 3900,
            "524288": 7600,
            "1048576": 15000
          },
          "maxIOPS": 15000,
          "minIOPS": 50
        },
        "scsiEUIDeviceID": "306f746f000000019f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000000306f746f000000019",
        "sliceCount": 1,
        "status": "active",
        "totalSize": 1000341504,
        "virtualVolumeID": null,
        "volumeAccessGroups": [],
        "volumeID": 25,
        "volumePairs": []
      }
    ]
  }
}

```

Nueva versión

9,6

ListVolumeStatsByAccount

Puedes usar el `ListVolumeStatsByAccount` Método para listar las mediciones de actividad de alto nivel para cada cuenta. Los valores se suman a partir de todos los volúmenes que posee la cuenta.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
incluir volúmenes virtuales	Los volúmenes virtuales se incluyen en la respuesta de forma predeterminada. Para excluir volúmenes virtuales, establezca el valor en falso.	booleano	verdadero	No
cuentas	Una lista de identificadores de cuenta para los que se devolverán las estadísticas de volumen. Si se omite, se devuelven las estadísticas de todas las cuentas.	matriz de enteros	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
estadísticas de volumen	Lista de información de actividad de volumen para cada cuenta. Nota: El miembro <code>volumeID</code> es 0 para cada entrada, ya que los valores representan la suma de todos los volúmenes que posee la cuenta.	estadísticas de volumen información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}
```

Nueva versión

9,6

Lista de estadísticas de volumen por volumen virtual

Puedes usar el `ListVolumeStatsByVirtualVolume` Método para listar las estadísticas de volumen para cualquier volumen del sistema que esté asociado con un volumen virtual. Las estadísticas son acumulativas desde la creación del volumen.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
IDs de volumen virtual	Una lista de uno o más identificadores de volumen virtual de los que recuperar información. Si se especifica este parámetro, el método devuelve información únicamente sobre estos volúmenes virtuales.	matriz de cadenas UUID	No	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
estadísticas de volumen	Una lista de objetos que contiene información de actividad para cada volumen virtual del sistema.	estadísticas de volumen información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}

```

```
}
```

Nueva versión

9,6

Listar estadísticas de volumen por volumen

Puedes usar el `ListVolumeStatsByVolume` método para listar las mediciones de actividad de alto nivel para cada volumen, por volumen. Los valores son acumulativos desde la creación del volumen.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
incluir volúmenes virtuales	Los volúmenes virtuales se incluyen en la respuesta de forma predeterminada. Para excluir volúmenes virtuales, establezca el valor en falso.	booleano	verdadero	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
estadísticas de volumen	Lista de información sobre el volumen de actividad.	estadísticas de volumen formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ListVolumeStatsByVolume",
  "params": {},
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "volumeStats": [
      {
        "accountID": 1,
        "actualIOPS": 4,
        "asyncDelay": null,
        "averageIOPSize": 5970,
        "burstIOPSCredit": 0,
        "clientQueueDepth": 0,
        "desiredMetadataHosts": null,
        "latencyUSec": 474,
        "metadataHosts": {
          "deadSecondaries": [],
          "liveSecondaries": [
            13
          ],
          "primary": 25
        },
        "nonZeroBlocks": 34931222,
        "normalizedIOPS": 4,
        "readBytes": 1282491003392,
        "readBytesLastSample": 0,
        "readLatencyUSec": 0,
        "readLatencyUSecTotal": 4581669750,
        "readOps": 15592933,
        "readOpsLastSample": 0,
        "samplePeriodMSec": 500,
        "sliceIopsStats": {
          "largeStatistics": {
            "averageReadIops": 17,
            "averageTotalIops": 43,
            "averageWriteIops": 26,
            "nSamples": 24,
            "peakReadIops": 19,
            "peakTotalIops": 47,
            "peakWriteIops": 30,
            "sliceID": 1
          },
          "smallStatistics": {
            "averageReadIops": 17,
```

```

        "averageTotalIops": 42,
        "averageWriteIops": 25,
        "nSamples": 120,
        "peakReadIops": 173,
        "peakTotalIops": 249,
        "peakWriteIops": 77,
        "sliceID": 1
    },
    "throttle": 0,
    "timestamp": "2025-02-03T21:18:38.880100Z",
    "unalignedReads": 167319,
    "unalignedWrites": 90836,
    "volumeAccessGroups": [
        1
    ],
    "volumeID": 1,
    "volumeSize": 2147483648000,
    "volumeUtilization": 0.00026666666666666667,
    "writeBytes": 1385173585408,
    "writeBytesLastSample": 12288,
    "writeLatencyUsec": 474,
    "writeLatencyUsecTotal": 11233350905,
    "writeOps": 157060458,
    "writeOpsLastSample": 2,
    "zeroBlocks": 489356778
}
]
}
}

```

Nueva versión

9,6

Lista de estadísticas de volumen por grupo de acceso de volumen

Puedes usar el `ListVolumeStatsByVolumeAccessGroup` Método para listar las mediciones de actividad total para todos los volúmenes que son miembros de los grupos de acceso a volúmenes especificados.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
incluir volúmenes virtuales	Los volúmenes virtuales se incluyen en la respuesta de forma predeterminada. Para excluir volúmenes virtuales, establezca el valor en falso.	booleano	verdadero	No
grupos de acceso de volumen	Una matriz de IDs de grupos de acceso a volumen para los que se devuelve la actividad de volumen. Si se omite, se devuelven las estadísticas de todos los grupos de acceso a volumen.	matriz de enteros	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
estadísticas de volumen	Lista de información de actividad de volumen para todos los volúmenes en el grupo de acceso de volumen especificado. Nota: El miembro volumeID es 0 para cada entrada, porque los valores representan la suma de todos los volúmenes que posee la cuenta.	estadísticas de volumen

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}
```

Nueva versión

9,6

Modificar destino de copia de seguridad

Puedes usar el `ModifyBackupTarget` Método para cambiar los atributos de un destino de copia de seguridad.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de destino de respaldo	Identificador único del objetivo a modificar.	entero	Ninguno	Sí
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
nombre	Nuevo nombre para el destino de la copia de seguridad.	cadena	Ninguno	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": {}
}
```

Nueva versión

9,6

Modificar la política de QoS

Puedes usar el `ModifyQoSPolicy` Método para modificar una política QoS existente en el sistema.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de política de qos	El ID de la política que se va a modificar.	entero	Ninguno	Sí
nombre	Si se proporciona, el nombre de la política de QoS (por ejemplo, oro, platino, plata) se cambia a este valor.	cadena	Ninguno	No
QoS	Si se proporcionan, los ajustes de QoS para esta política se cambiarán a estos ajustes. Puede proporcionar valores QoS parciales y cambiar solo algunas de las configuraciones QoS.	Objeto QoS	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Política de calidad de servicio	Detalles de la política de QoS recientemente modificada.	Política de QoS

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      ]
    }
  }
}

```

Nueva versión

10,0

Modificar volumen

Puedes usar el `ModifyVolume` Método para modificar la configuración de un volumen existente. Puede realizar modificaciones en un volumen a la vez y los cambios se aplicarán de inmediato.

Si no especificas valores de QoS al modificar un volumen, estos permanecerán iguales que antes de la modificación. Puede recuperar los valores QoS predeterminados para un volumen recién creado ejecutando el siguiente comando. `GetDefaultQoS` método.

Cuando necesite aumentar el tamaño de un volumen que se está replicando, hágalo en el siguiente orden para evitar errores de replicación:

1. Aumentar el tamaño del volumen con acceso de destino de replicación.
2. Aumente el tamaño de la fuente o del volumen con acceso de lectura/escritura.

Asegúrese de que tanto el volumen de destino como el de origen tengan el mismo tamaño.



Si cambia el estado de acceso a bloqueado o replicationTarget, se terminarán todas las conexiones iSCSI existentes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de volumen	El ID del volumen que se va a modificar.	entero	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
acceso	Se permitió el acceso al volumen. Valores posibles: • <code>`readOnly`</code> Solo se permiten operaciones de lectura. • <code>`readWrite`</code> Se permiten lecturas y escrituras. • <code>`locked`</code> No se permiten lecturas ni escrituras. Si no se especifica, el valor de acceso no cambia. • <code>`replicationTarget`</code> Identificar un volumen como el volumen objetivo para un conjunto de volúmenes emparejados. Si el volumen no está emparejado, el estado de acceso queda bloqueado. Si no se especifica un valor, el valor de acceso no cambia. • <code>`snapMirrorTarget`</code> Identificar un volumen como volumen de destino para la replicación de SnapMirror .	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de cuenta	El ID de cuenta al que se reasigna el volumen. Si no se especifica ninguno, se utiliza el nombre de cuenta anterior.	entero	Ninguno	No
asociarseConQoSPolicy	Asocie el volumen con la política QoS especificada. Valores posibles: • `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 falso, se elimina cualquier asociación de política existente, independientemente de si se especifica una política QoS en el parámetro QoSPolicy.	booleano	Ninguno	No
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
crearTiempo	Una cadena de fecha ISO 8601 para establecer como la nueva fecha de creación del volumen. Requerido si setCreateTime está establecido en verdadero.	Cadena ISO 8601	Ninguno	No
dontMoveforIopsRebalance	Evitar que un volumen se mueva al equilibrar la carga con IOPS reales. Esta configuración está disponible a partir de Element 12.8 y solo es efectiva cuando "Balanceo de carga de volumen en IOPS reales" está habilitado. Valores posibles: • `true` El volumen no realiza el balanceo de carga en función de las IOPS reales. • `false` El volumen realiza el balanceo de carga en función de las IOPS reales. Nota: El equilibrio para alta disponibilidad (fallo de nodo) tiene prioridad sobre VolumeLoadBalanceOnActualIOPS y dontMoveforIopsRebalance .	booleano	FALSO	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
habilitarSnapMirrorReplication	Determina si el volumen se puede utilizar para la replicación con puntos de conexión SnapMirror . Valores posibles: • true • false	booleano	FALSO	No
fifoSize	Especifica el número máximo de instantáneas First-In-First-Out (FIFO) admitidas por el volumen. Tenga en cuenta que tanto las instantáneas FIFO como las no FIFO utilizan el mismo conjunto de ranuras de instantáneas disponibles en un volumen. Utilice esta opción para limitar el consumo de instantáneas FIFO de las ranuras de instantáneas disponibles. Tenga en cuenta que no puede modificar este valor para que sea menor que el recuento actual de instantáneas FIFO.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
tamaño mínimo de Fifo	Especifica el número de ranuras de instantáneas que están reservadas únicamente para instantáneas First-In-First-Out (FIFO). Dado que las instantáneas FIFO y no FIFO comparten el mismo grupo, el parámetro minFifoSize reduce el número total de instantáneas no FIFO posibles en la misma cantidad. Tenga en cuenta que no puede modificar este valor de manera que entre en conflicto con el recuento actual de instantáneas no FIFO.	entero	Ninguno	No
modo	Modo de replicación de volumen. Valores posibles: • <code>asynch</code>: Espera a que el sistema confirme que los datos están almacenados en la fuente antes de escribirlos en el destino. • <code>`sync`</code>: No espera la confirmación de transmisión de datos desde la fuente para comenzar a escribir datos en el destino.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
QoS	Los nuevos ajustes de calidad de servicio para este volumen. Si no se especifica, la configuración de QoS no se modifica. Valores posibles: • minIOPS • maxIOPS • burstIOPS	Calidad de servicio	Ninguno	No
ID de política de qos	El ID de la política cuya configuración QoS se debe aplicar a los volúmenes especificados. Este parámetro es mutuamente excluyente con el parámetro qos.	entero	Ninguno	No
establecerHoraDeCreación	Establézcalo en verdadero para cambiar la fecha registrada de creación del volumen.	booleano	Ninguno	No
tamaño total	El nuevo tamaño del volumen en bytes. 1000000000 es igual a 1 GB. El tamaño se redondea al megabyte más cercano. Este parámetro solo puede utilizarse para aumentar el tamaño de un volumen.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
volume	Objeto que contiene información sobre el volumen recientemente modificado.	volume

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ModifyVolume",
  "params": {
    "volumeID": 319,
    "access": "readWrite",
    "dontMoveForIopsRebalance": false
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "volume": {
      "access": "readWrite",
      "accountID": 22,
      "attributes": {},
      "blockSize": 4096,
      "createTime": "2024-04-01T19:39:40Z",
      "currentProtectionScheme": "doubleHelix",
      "deleteTime": "",
      "dontMoveForIopsRebalance": false,
      "enable512e": false,
      "enableSnapMirrorReplication": false,
      "fifoSize": 24,
      "iqn": "iqn.2010-01.com.solidfire:3eeu.suite40.319",
      "lastAccessTime": "2024-04-02T12:41:34Z",
      "lastAccessTimeIO": "2024-04-01T20:41:19Z",
      "minFifoSize": 0,
      "name": "suite40",
      "previousProtectionScheme": null,

```

```

    "purgeTime": "",
    "qos": {
      "burstIOPS": 27000,
      "burstTime": 60,
      "curve": {
        "1048576": 15000,
        "131072": 1950,
        "16384": 270,
        "262144": 3900,
        "32768": 500, "4096": 100,
        "524288": 7600,
        "65536": 1000,
        "8192": 160
      },
      "maxIOPS": 27000,
      "minIOPS": 500
    },
    "qosPolicyID": null,
    "scsiEUIDeviceID": "336565750000013ff47acc0100000000",
    "scsiNAADeviceID": "6f47acc100000000336565750000013f",
    "sliceCount": 1,
    "status": "active",
    "totalSize": 1000000716800,
    "virtualVolumeID": null,
    "volumeAccessGroups": [
      22
    ],
    "volumeConsistencyGroupUUID": "3003109e-6e75-444c-8cee-470d641a09c3",
    "volumeID": 319,
    "volumePairs": [],
    "volumeUUID": "78203136-b0eb-454b-9f67-2c867ec7d7bb"
  }
}

```

Nueva versión

9,6

Encuentra más información

[Obtener QoS predeterminado](#)

Modificar volúmenes

Puedes usar el `ModifyVolumes` Método para configurar hasta 500 volúmenes

existentes a la vez. Los cambios se producen de inmediato. Si `ModifyVolumes` Si no se modifica ninguno de los volúmenes especificados, ninguno de los volúmenes especificados se modifica.

Si no especifica valores de QoS al modificar los volúmenes, los valores de QoS para cada volumen permanecerán sin cambios. Puede recuperar los valores QoS predeterminados para un volumen recién creado ejecutando el siguiente comando. `GetDefaultQoS` método.

Cuando necesite aumentar el tamaño de los volúmenes que se están replicando, hágalo en el siguiente orden para evitar errores de replicación:

1. Aumentar el tamaño del volumen con acceso de destino de replicación.
2. Aumente el tamaño de la fuente o del volumen con acceso de lectura/escritura.

Asegúrese de que tanto el volumen de destino como el de origen tengan el mismo tamaño.



Si cambia el estado de acceso a bloqueado o `replicationTarget`, se terminarán todas las conexiones iSCSI existentes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
acceso	Se permitió el acceso a los volúmenes. Valores posibles: • `readOnly` Solo 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` Identificar un volumen como el volumen objetivo para un conjunto de volúmenes emparejados. Si el volumen no está emparejado, el estado de acceso queda bloqueado. Si no se especifica un valor, el valor de acceso no cambia.	cadena	Ninguno	No
ID de cuenta	El ID de cuenta al que se reasignan los volúmenes. Si no se especifica ninguno, se utiliza el nombre de cuenta anterior.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
asociarseConQoSPolicy	Asocie el volumen con la política QoS especificada. Valores posibles: • <code>true</code> Asocie el volumen con la política QoS especificada en el parámetro QoSPolicyID. • <code>false</code> No asocie el volumen con la política QoS especificada en el parámetro QoSPolicyID. Cuando es falso, se elimina cualquier asociación de política existente, independientemente de si se especifica una política QoS en el parámetro QoSPolicy.	booleano	Ninguno	No
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
crearTiempo	Una cadena de fecha ISO 8601 para establecer como la nueva fecha de creación del volumen. Requerido si setCreateTime está establecido en verdadero.	Cadena ISO 8601	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
dontMoveforIopsRebalance	Evitar que un volumen se mueva al equilibrar la carga con IOPS reales. Esta configuración está disponible a partir de Element 12.8 y solo es efectiva cuando "Balanceo de carga de volumen en IOPS reales" está habilitado. Valores posibles: • <code>true</code> El volumen no realiza el balanceo de carga en función de las IOPS reales. • <code>false</code> El volumen realiza el balanceo de carga en función de las IOPS reales. Nota: El equilibrio para alta disponibilidad (fallo de nodo) tiene prioridad sobre VolumeLoadBalanceOnActualIOPS y dontMoveforIopsRebalance.	booleano	FALSO	No
habilitarSnapMirrorReplication	Determina si el volumen se puede utilizar para la replicación con puntos de conexión SnapMirror. Valores posibles: • <code>true</code> • <code>false</code>	booleano	FALSO	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
fifoSize	Especifica el número máximo de instantáneas First-In-First-Out (FIFO) admitidas por el volumen. Tenga en cuenta que tanto las instantáneas FIFO como las no FIFO utilizan el mismo conjunto de ranuras de instantáneas disponibles en un volumen. Utilice esta opción para limitar el consumo de instantáneas FIFO de las ranuras de instantáneas disponibles. Tenga en cuenta que no puede modificar este valor para que sea menor que el recuento actual de instantáneas FIFO.	entero	Ninguno	No
tamaño mínimo de Fifo	Especifica el número de ranuras de instantáneas que están reservadas únicamente para instantáneas First-In-First-Out (FIFO). Dado que las instantáneas FIFO y no FIFO comparten el mismo grupo, el parámetro minFifoSize reduce el número total de instantáneas no FIFO posibles en la misma cantidad. Tenga en cuenta que no puede modificar este valor de manera que entre en conflicto con el recuento actual de instantáneas no FIFO.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
modo	Modo de replicación de volumen. Valores posibles: • <code>asynch</code>: Espera a que el sistema confirme que los datos están almacenados en la fuente antes de escribirlos en el destino. • <code>`sync`</code>: No espera la confirmación de transmisión de datos desde la fuente para comenzar a escribir datos en el destino.	cadena	Ninguno	No
QoS	Los nuevos ajustes de calidad de servicio para los volúmenes. Si no se especifica, la configuración de QoS no se modifica. Valores posibles: • <code>minIOPS</code> • <code>maxIOPS</code> • <code>burstIOPS</code>	Calidad de servicio	Ninguno	No
ID de política de qos	El ID de la política cuya configuración QoS se debe aplicar a los volúmenes especificados. Este parámetro es mutuamente excluyente con el parámetro qos.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
establecerHoraDeCreación	Establézcalo en verdadero para cambiar la fecha registrada de creación del volumen.	booleano	Ninguno	No
tamaño total	El nuevo tamaño de los volúmenes en bytes. 1000000000 es igual a 1 GB. El tamaño se redondea al megabyte más cercano. Este parámetro solo puede utilizarse para aumentar el tamaño de un volumen.	entero	Ninguno	No
IDs de volumen	Una lista de identificadores de volumen para los volúmenes que se van a modificar.	matriz de enteros	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
volume	Una matriz de objetos que contiene información sobre cada volumen recién modificado.	volume formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "ModifyVolumes",
  "params": {
    "volumeIDs": [319,22],
    "access": "readWrite",
    "dontMoveForIopsRebalance": false
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "volumes":
    {
      "access": "readWrite",
      "accountID": 22,
      "attributes": {},
      "blockSize": 4096,
      "createTime": "2024-04-01T19:39:40Z",
      "currentProtectionScheme": "doubleHelix",
      "deleteTime": "",
      "dontMoveForIopsRebalance": false,
      "enable512e": false,
      "enableSnapMirrorReplication": false,
      "fifoSize": 24,
      "iqn": "iqn.2010-01.com.solidfire:3eeu.suite40.319",
      "lastAccessTime": "2024-04-02T12:41:34Z",
      "lastAccessTimeIO": "2024-04-01T20:41:19Z",
      "minFifoSize": 0,
      "name": "suite40",
      "previousProtectionScheme": null,
      "purgeTime": "",
      "qos": {
        "burstIOPS": 27000,
        "burstTime": 60,
        "curve": {
          "1048576": 15000,
          "131072": 1950,
          "16384": 270,
          "262144": 3900,

```

```

        "32768": 500,
        "4096": 100,
        "524288": 7600,
        "65536": 1000,
        "8192": 160
    },
    "maxIOPS": 27000,
    "minIOPS": 500
},
"qosPolicyID": null,
"scsiEUIDeviceID": "336565750000013ff47acc0100000000",
"scsiNAADeviceID": "6f47acc100000000336565750000013f",
"sliceCount": 1,
"status": "active",
"totalSize": 1000000716800,
"virtualVolumeID": null,
"volumeAccessGroups": [
22
],
"volumeConsistencyGroupUUID": "3003109e-6e75-444c-8cee-
470d641a09c3",
"volumeID": 319,
"volumePairs": [],
"
}
}
}

```

Nueva versión

9,6

Encuentra más información

[Obtener QoS predeterminado](#)

Purga de volumen eliminado

Puedes usar el `PurgeDeletedVolume` Método para eliminar de forma inmediata y permanente un volumen que ha sido borrado. Debes eliminar un volumen usando `DeleteVolume` antes de que pueda ser purgado.

Los volúmenes se purgan automáticamente después de un período de tiempo, por lo que el uso de este método no suele ser necesario.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de volumen	El ID del volumen que se va a purgar.	entero	No	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "PurgeDeletedVolume",
  "params": {
    "volumeID" : 5
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result": {}
}
```

Nueva versión

9,6

Encuentra más información

[Eliminar volumen](#)

Eliminar volúmenes eliminados

Puedes usar el `PurgeDeletedVolumes` Método para eliminar de forma inmediata y permanente los volúmenes que se han borrado; puede utilizar este método para eliminar hasta 500 volúmenes a la vez.

Debe eliminar los volúmenes usando `DeleteVolumes` antes de que puedan ser eliminados. Los volúmenes se purgan automáticamente después de un período de tiempo, por lo que el uso de este método no suele ser necesario.



Si se elimina una gran cantidad de volúmenes a la vez, o si cada uno de los volúmenes que se eliminan tiene muchas instantáneas asociadas, el método podría fallar y devolver el error "xDBCConnectionLoss". Si esto ocurre, vuelva a intentar la llamada al método con menos volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
IDs de volumen	Una lista de los ID de volumen de los volúmenes que se eliminarán del sistema.	matriz de enteros	No	No
ID de cuenta	Una lista de identificadores de cuenta. Todos los volúmenes de todas las cuentas especificadas se eliminan del sistema.	matriz de enteros	No	No
ID de grupo de acceso de volumen	Una lista de IDs de grupos de acceso a volumen. Todos los volúmenes de todos los grupos de acceso a volúmenes especificados se eliminan del sistema.	matriz de enteros	No	No

Nota: Solo se puede especificar uno de los parámetros anteriores por llamada al método. Especificar más de uno, o ninguno, da como resultado un error.

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:


```
{
  "method": "PurgeDeletedVolumes",
  "params": {
    "accountIDs" : [1, 2, 3]
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result": {}
}
```

Nueva versión

9,6

Encuentra más información

[Eliminar volúmenes](#)

Eliminar destino de copia de seguridad

Puedes usar el `RemoveBackupTarget` Método para eliminar destinos de copia de seguridad.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de destino de respaldo	Identificador único del objetivo a eliminar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "RemoveBackupTarget",
  "params": {
    "backupTargetID" : 1
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nueva versión

9,6

Restaurar volumen eliminado

Puedes usar el `RestoreDeletedVolume` Método para volver a marcar un volumen eliminado como activo. 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	Requerido
ID de volumen	El ID del volumen eliminado que se va a restaurar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "RestoreDeletedVolume",
  "params": {
    "volumeID" : 5
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result": {}
}
```

Nueva versión

9,6

Establecer QoS predeterminado

Puedes usar el `SetDefaultQoS` método para configurar los valores predeterminados de Calidad de Servicio (QoS) (medidos en entradas y salidas por segundo, o IOPS) para un volumen.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
minIOPS	El número mínimo de IOPS sostenidas que el clúster proporciona a un volumen.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
IOPS máximas	El número máximo de IOPS sostenidas que el clúster proporciona a un volumen.	entero	Ninguno	No
ráfaga IOPS	La cantidad máxima de IOPS permitida en un escenario de ráfaga corta.	entero	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
minIOPS	El número mínimo de IOPS sostenidas que el clúster proporciona a un volumen.	entero
IOPS máximas	El número máximo de IOPS sostenidas que el clúster proporciona a un volumen.	entero
ráfaga IOPS	La cantidad máxima de IOPS permitida en un escenario de ráfaga corta.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}
```

Nueva versión

9,6

Iniciar lectura de volumen masivo

Puedes usar el `StartBulkVolumeRead` Método para iniciar una sesión de lectura masiva de volumen en un volumen especificado.

Solo dos procesos de volumen masivo pueden ejecutarse simultáneamente en un volumen. Al inicializar la sesión, los datos se leen desde un volumen de almacenamiento SolidFire para almacenarse en una fuente de copia de seguridad externa. Se accede a los datos externos mediante un servidor web que se ejecuta en un nodo de almacenamiento Element. La información de interacción con el servidor para el acceso a datos externos se transmite mediante un script que se ejecuta en el sistema de almacenamiento.

Al inicio de una operación de lectura masiva de volumen, se crea una instantánea del volumen y esta se elimina una vez finalizada la lectura. También puede leer una instantánea del volumen introduciendo el ID de la instantánea como parámetro. Cuando se lee una instantánea anterior, el sistema no crea una nueva instantánea del volumen, ni elimina la instantánea anterior una vez finalizada la lectura.



Este proceso crea una nueva instantánea si no se proporciona el ID de una instantánea existente. Se pueden crear instantáneas si la capacidad del clúster se encuentra en la etapa 2 o 3. No se crean instantáneas cuando la capacidad del clúster se encuentra en la etapa 4 o 5.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
formato	El formato de los datos de volumen. Puede ser cualquiera de los siguientes: • `uncompressed` Se devuelve cada byte del volumen sin compresión alguna. • `native` Se devuelven datos opacos que son más pequeños y se almacenan y escriben de manera más eficiente en una escritura de volumen masivo posterior.	cadena	Ninguno	Sí
ID de volumen	El identificador del volumen que se va a leer.	entero	Ninguno	Sí
ID de instantánea	El ID de una instantánea creada previamente que se utilizó para lecturas de volumen masivas. Si no se introduce ningún ID, se realiza una instantánea de la imagen del volumen activo actual.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
guion	El nombre de un script ejecutable. Si no se proporciona un nombre de script, la clave y la URL son necesarias para acceder a los nodos de almacenamiento de Element. El script 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
Parámetros del script	Parámetros JSON para pasar al script.	Objeto JSON	Ninguno	No
atributos	Lista de pares nombre-valor en formato de objeto JSON. " Más información ".	Objeto JSON	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
manejador asíncrono	El ID del proceso asíncrono que se comprobará para verificar su finalización.	entero
llave	Clave opaca que identifica de forma única la sesión.	cadena
URL	URL para acceder al servidor web del nodo.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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/"
  }
}
```

Nueva versión

9,6

Iniciar escritura masiva de volumen

Puedes usar el `StartBulkVolumeWrite` Método para iniciar una sesión de escritura masiva de volumen en un volumen especificado.

Solo dos procesos de volumen masivo pueden ejecutarse simultáneamente en un volumen. Al inicializar la sesión, los datos se escriben en un volumen de almacenamiento de Element desde una fuente de copia de seguridad externa. Se accede a los datos externos mediante un servidor web que se ejecuta en un nodo de almacenamiento Element. La información de interacción con el servidor para el acceso a datos externos se transmite mediante un script que se ejecuta en el sistema de almacenamiento.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
formato	El formato de los datos de volumen. Puede ser cualquiera de los siguientes: • <code>`uncompressed`</code> Se devuelve cada byte del volumen sin compresión alguna. • <code>`native`</code> Se devuelven datos opacos que son más pequeños y se almacenan y escriben de manera más eficiente en una escritura de volumen masivo posterior.	cadena	Ninguno	Sí
ID de volumen	El identificador del volumen en el que se va a escribir.	entero	Ninguno	Sí
guion	El nombre de un script ejecutable. Si no se proporciona un nombre de script, la clave y la URL son necesarias para acceder a los nodos de almacenamiento de Element. El script 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
Parámetros del script	Parámetros JSON para pasar al script.	Objeto JSON	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
atributos	Lista de pares nombre-valor en formato de objeto JSON. "Más información" .	Objeto JSON	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
manejador asíncrono	El ID del proceso asíncrono que se comprobará para verificar su finalización.	entero
llave	Clave opaca que identifica de forma única la sesión.	cadena
URL	URL para acceder al servidor web del nodo.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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/"
  }
}
```

Nueva versión

9,6

Actualizar estado del volumen masivo

Puedes usar el `UpdateBulkVolumeStatus` método para actualizar el estado de un trabajo de volumen masivo que inició con el `StartBulkVolumeRead` o `StartBulkVolumeWrite` métodos.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
llave	La clave asignada durante la inicialización de un Iniciar lectura de volumen masivo o Iniciar escritura masiva de volumen sesión .	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
estado	El sistema establece el estado del trabajo de volumen masivo dado. Valores posibles: • En ejecución: Trabajos que aún están activos. • Completados: Trabajos que se han realizado. • Fracasaron: Trabajos que fracasaron.	cadena	Ninguno	Sí
porcentaje completado	Porcentaje de avance del trabajo de gran volumen.	cadena	Ninguno	No
mensaje	Devuelve el estado del trabajo de volumen masivo cuando este se ha completado.	cadena	Ninguno	No
atributos	Atributos JSON; actualiza lo que hay en el trabajo de volumen masivo.	Objeto JSON	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
estado	Estado de la sesión solicitada. Estado devuelto: • preparante • activo • hecho • fallido	cadena

atributos	Devuelve los atributos que se especificaron 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 aún está activa.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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/"
  }
}
```

Nueva versión

9,6

Encuentra más información

- [Iniciar lectura de volumen masivo](#)
- [Iniciar escritura masiva de volumen](#)

Métodos de la API de grupos de acceso por volumen

AgregarIniciadoresAlGrupoDeAccesoPorVolumen

Puedes usar el `AddInitiatorsToVolumeAccessGroup` Método para agregar iniciadores a un grupo de acceso a volumen específico.

El formato aceptado de un IQN iniciador es `iqn.yyyy-mm`, donde `y` y `m` son dígitos, seguidos de texto que solo debe contener dígitos, caracteres alfabéticos en minúscula, un punto (`.`), dos puntos (`:`) o un guion (`-`). Vea el siguiente ejemplo:

```
iqn.2010-01.com.solidfire:17oi.solidfire-0.1
```

El formato aceptado de un WWPN de iniciador de Fibre Channel es `Aa:bB:CC:dd:11:22:33:44`, o `AabBCCdd11223344`. Vea 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	Requerido
iniciadores	Lista de identificadores o nombres de iniciador (IQN y WWPN) que se incluirán en el grupo de acceso por volumen. Si se proporciona una lista de nombres de iniciadores, estos se crearán si aún no existen. Si se pasa una lista de identificadores de iniciadores, el método devuelve un error si alguno de los iniciadores no existe. El uso de nombres de iniciadores está obsoleto; debe utilizar identificadores de iniciador siempre que sea posible.	matriz de enteros o matriz de cadenas (obsoleto)		Sí
ID de grupo de acceso al volumen	El ID del grupo de acceso al volumen al que se añadirá el iniciador.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
volumeAccessGroup	Un objeto que contiene información sobre el grupo de acceso a volúmenes recientemente modificado.	volumeAccessGroup

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      ]
    }
  }
}
```

Nueva versión

9,6

Agregar volúmenes al grupo de acceso a volúmenes

Puedes usar el AddVolumesToVolumeAccessGroup Método para agregar volúmenes

a un grupo de acceso a volúmenes específico.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
volúmenes	Lista de ID de volumen para agregar al grupo de acceso a volúmenes.	matriz de enteros	Ninguno	Sí
ID de grupo de acceso al volumen	ID del grupo de acceso a volúmenes al que se agregan los volúmenes.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
volumeAccessGroup	Un objeto que contiene información sobre el grupo de acceso a volúmenes recientemente modificado.	volumeAccessGroup

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      ]
    }
  }
}
```

Nueva versión

9,6

Crear grupo de acceso a volumen

Puedes usar `CreateVolumeAccessGroup` para crear un nuevo grupo de acceso a volúmenes. Al crear el grupo de acceso a volúmenes, debe darle un nombre y, opcionalmente, puede introducir iniciadores y volúmenes.

Cualquier IQN iniciador que agregue al grupo de acceso a volúmenes podrá acceder a cualquier volumen del grupo sin autenticación CHAP.



Los volúmenes clonados no heredan la pertenencia al grupo de acceso al volumen del volumen de origen.

Tenga en cuenta lo siguiente al crear grupos de acceso a volúmenes:

- Un grupo de acceso por volumen puede contener hasta 64 IQN de iniciador.
- Un iniciador solo puede pertenecer a un grupo de acceso a volúmenes.

- Un grupo de acceso a volúmenes puede contener hasta 2000 volúmenes.
- Cada grupo de acceso a volúmenes puede pertenecer a un máximo de cuatro grupos de acceso a volúmenes.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
iniciadores	Lista de identificadores o nombres de iniciador (IQN y WWPN) que se incluirán en el grupo de acceso por volumen. Si se proporciona una lista de nombres de iniciadores, estos se crearán si aún no existen. Si se pasa una lista de identificadores de iniciadores, el método devuelve un error si alguno de los iniciadores no existe. El uso de nombres de iniciadores está obsoleto; debe utilizar identificadores de iniciador siempre que sea posible.	matriz de enteros o matriz de cadenas (obsoleto)		No
nombre	Nombre del grupo de acceso al volumen. No es necesario que sea único, pero es recomendable. Debe tener entre 1 y 64 caracteres de longitud.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
volúmenes	Lista de ID de volumen que se incluirán en el grupo de acceso a volúmenes.	matriz de enteros		No
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	{}	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
volumeAccessGroup	Un objeto que contiene información sobre el grupo de acceso a volúmenes recién creado.	volumeAccessGroup
ID de grupo de acceso al volumen	El ID del grupo de acceso a volúmenes recién creado.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}

```

Nueva versión

9,6

Encuentra más información

- [ObtenerResultadoAsíncrono](#)
- [ListSyncJobs](#)
- [Modificar volumen](#)

Eliminar grupo de acceso al volumen

Puedes usar `DeleteVolumeAccessGroup` Eliminar un grupo de acceso a volumen.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de grupo de acceso al volumen	El ID del grupo de acceso al volumen que se va a eliminar.	entero	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
eliminarIniciadoresHuérfanos	Especifica si se deben eliminar los objetos iniciadores o no. Valores posibles: • verdadero: Eliminar los objetos iniciadores después de que se eliminen de un grupo de acceso a volúmenes. • falso: No elimine los objetos iniciadores después de que se eliminen de un grupo de acceso a volúmenes. Este es el valor predeterminado.	booleano	FALSO	No
fuerza	Agregar esta bandera forzará la eliminación del grupo de acceso al volumen, incluso si tiene un ID o etiqueta de red virtual. Valores posibles: • Verdadero: Se eliminará el grupo de acceso al volumen. • falso: Valor predeterminado. No elimine el grupo de acceso al volumen si tiene un ID de red virtual o una etiqueta.	booleano	FALSO	No

Valores de retorno

Este método no tiene valores de retorno.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DeleteVolumeAccessGroup",
  "params": {
    "force": true,
    "volumeAccessGroupID" : 3
  },
  "id" : 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id" : 1,
  "result": {}
}
```

Nueva versión

9,6

Listar grupos de acceso de volumen

Puedes usar el `ListVolumeAccessGroups` Método para obtener información sobre los grupos de acceso a volúmenes que se encuentran actualmente en el sistema.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
límite	Número máximo de objetos <code>volumeAccessGroup</code> que se devolverán. Mutuamente excluyente con el parámetro <code>volumeAccessGroups</code> .	entero	Ilimitada	No
<code>startVolumeAccessGroupID</code>	El ID del grupo de acceso por volumen en el que se debe comenzar el listado. Mutuamente excluyente con el parámetro <code>volumeAccessGroups</code> .	entero	0	No
grupos de acceso de volumen	Lista de valores <code>volumeAccessGroupID</code> a recuperar. Mutuamente excluyentes con los parámetros <code>startVolumeAccessGroupID</code> y <code>limit</code> .	matriz de enteros		No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
grupos de acceso de volumen	Una lista de objetos que describe cada grupo de acceso a volúmenes.	volumeAccessGroup formación
Grupos de acceso a volumen no encontrados	El sistema no ha encontrado una lista de grupos de acceso a volúmenes. Se presenta si utilizó el parámetro <code>volumeAccessGroups</code> y el sistema no pudo encontrar uno o más grupos de acceso a volumen que especificó.	matriz de enteros

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": []
      }
    ]
  }
}
```

Nueva versión

9,6

Eliminar volúmenes del grupo de acceso a volúmenes

Puedes usar el `RemoveVolumesFromVolumeAccessGroup` Método para eliminar volúmenes de un grupo de acceso a volúmenes específico.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de grupo de acceso al volumen	ID del grupo de acceso al volumen del que se eliminarán los volúmenes.	entero	Ninguno	Sí
volúmenes	IDs de volumen de los volúmenes que se eliminarán del grupo de acceso a volúmenes.	matriz de enteros	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
volumeAccessGroup	Un objeto que contiene información sobre el grupo de acceso a volúmenes recientemente modificado.	volumeAccessGroup

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": []
    }
  }
}
```

Nueva versión

9,6

EliminarIniciadoresDelGrupoDeAccesoPorVolumen

Puedes usar el `RemoveInitiatorsFromVolumeAccessGroup` Método para eliminar iniciadores de un grupo de acceso a volumen específico.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de grupo de acceso al volumen	El ID del grupo de acceso al volumen del que se eliminan los iniciadores.	entero	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
iniciadores	Lista de identificadores o nombres de iniciador (IQN y WWPN) que se incluirán en el grupo de acceso por volumen. Si se proporciona una lista de nombres de iniciadores, estos se crearán si aún no existen. Si se pasa una lista de identificadores de iniciadores, el método devuelve un error si alguno de los iniciadores no existe. El uso de nombres de iniciadores está obsoleto; debe utilizar identificadores de iniciador siempre que sea posible.	matriz de enteros (recomendado) o matriz de cadenas (obsoleto)	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
eliminarIniciadoresHuérfanos	Especifica si se deben eliminar los objetos iniciadores después de que se eliminen de un grupo de acceso a volúmenes o no. Valores posibles: • verdadero: Eliminar los objetos iniciadores después de que se eliminen de un grupo de acceso a volúmenes. • falso: No elimine los objetos iniciadores después de que se eliminen de un grupo de acceso a volúmenes. Este es el valor predeterminado.	booleano	FALSO	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
volumeAccessGroup	Un objeto que contiene información sobre el grupo de acceso a volúmenes recientemente modificado.	volumeAccessGroup

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      ]
    }
  }
}
```

Nueva versión

9,6

Modificar grupo de acceso al volumen

Puedes usar el `ModifyVolumeAccessGroup` Método para actualizar los iniciadores y agregar o eliminar volúmenes de un grupo de acceso a volúmenes.

Si un iniciador o volumen especificado es un duplicado de lo que existe actualmente, el grupo de acceso al volumen se deja tal cual. Si no especifica un valor para volúmenes o iniciadores, la lista actual de iniciadores y volúmenes no se modifica.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de grupo de acceso al volumen	El ID del grupo de acceso al volumen que se va a modificar.	entero	Ninguno	Sí
nombre	El nuevo nombre para este grupo de acceso por volumen.	cadena	Ninguno	No
atributos	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
iniciadores	Lista de identificadores o nombres de iniciador (IQN y WWPN) que se incluirán en el grupo de acceso por volumen. Si se proporciona una lista de nombres de iniciadores, estos se crearán si aún no existen. Si se pasa una lista de identificadores de iniciadores, el método devuelve un error si alguno de los iniciadores no existe. El uso de nombres de iniciadores está obsoleto; debe utilizar identificadores de iniciador siempre que sea posible.	matriz de enteros (recomendado) o matriz de cadenas (obsoleto)	Ninguno	No

eliminarIniciadoresHuérfanos	Especifica si se deben eliminar los objetos iniciadores después de que se eliminen de un grupo de acceso a volúmenes o no. Valores posibles: • verdadero: Eliminar los objetos iniciadores después de que se eliminen de un grupo de acceso a volúmenes. • falso: No elimine los objetos iniciadores después de que se eliminen de un grupo de acceso a volúmenes. Este es el valor predeterminado.	booleano	FALSO	No
volúmenes	Lista de identificadores de volumen de los volúmenes que se van a modificar.	matriz de enteros	Ninguno	volumeAccessGroup

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
volumeAccessGroup	Un objeto que contiene información sobre el grupo de acceso a volúmenes recientemente modificado.	volumeAccessGroup

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:


```

{
  "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
      ]
    }
  }
}

```

Nueva versión

9,6

Encuentra más información

- [AgregarIniciadoresAlGrupoDeAccesoPorVolumen](#)
- [Agregar volúmenes al grupo de acceso a volúmenes](#)
- [EliminarIniciadoresDelGrupoDeAccesoPorVolumen](#)
- [Eliminar volúmenes del grupo de acceso a volúmenes](#)

ObtenerEficienciaDeGrupoDeAccesoDeVolumen

Puedes usar el `GetVolumeAccessGroupEfficiency` Método para obtener información sobre la eficiencia de un grupo de acceso por volumen. Para calcular la capacidad, solo se utiliza el grupo de acceso al volumen que proporcione como parámetro en este método de la API.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de grupo de acceso al volumen	Especifica el grupo de acceso al volumen para el cual se calcula la capacidad.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
compresión	Cantidad de espacio ahorrado mediante la compresión de datos para todos los volúmenes del grupo de acceso a volúmenes. Se expresa como una relación donde un valor de 1 significa que los datos se han almacenado sin compresión.	flotar

deduplicación	La cantidad de espacio ahorrado al no duplicar datos para todos los volúmenes en el grupo de acceso a volúmenes. Expresado como una proporción.	flotar
aprovisionamiento ligero	La proporción de espacio utilizado con respecto a la cantidad de espacio asignado para almacenar datos. Expresado como una proporción.	flotar
marca de tiempo	La última vez que se recopilaron datos de eficiencia fue después de la recogida de basura.	cadena de datos ISO 8601
volúmenes faltantes	Los volúmenes de los que no se pudieron obtener datos de eficiencia. La falta de volúmenes puede deberse a una recolección de basura reciente, a una pérdida de red temporal o a servicios reiniciados desde el último ciclo de recolección de basura.	matriz de enteros

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

Métodos de la API de instantáneas de volumen

Resumen de instantáneas

Una instantánea de volumen es una copia de un volumen en un momento dado. Puedes usar instantáneas para restaurar un volumen al estado en el que se encontraba en el momento en que se creó la instantánea.

Puede agrupar las instantáneas de volumen para que los volúmenes relacionados se puedan respaldar o revertir de manera coherente. Una instantánea de grupo captura una imagen puntual de todos los archivos de corte de volumen. Luego, puede usar la imagen para revertir un grupo de volúmenes a un estado puntual y garantizar que todos los datos sean coherentes en todos los volúmenes del grupo.

Puede programar instantáneas de volumen para que se realicen de forma autónoma a intervalos definidos. Puedes definir intervalos por tiempo, días de la semana o días del mes. También puede utilizar instantáneas programadas para garantizar que se realicen copias de seguridad de las instantáneas en un almacenamiento remoto con fines de archivado.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Documentación para versiones anteriores de los productos NetApp SolidFire y Element"](#)

CrearInstantáneaDeGrupo

Puedes usar `CreateGroupSnapshot` para crear una copia puntual de un grupo de volúmenes.

Puede utilizar esta instantánea más adelante como copia de seguridad o para revertir cambios y así garantizar que los datos del grupo de volúmenes sean coherentes en el momento en que creó la instantánea.

LLENADO_DEL_CLÚSTER



Puede crear instantáneas si la plenitud del clúster se encuentra en la etapa 1, 2 o 3. No se pueden crear instantáneas cuando la capacidad del clúster alcanza la etapa 4 o 5.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
attributes	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
enableRemoteReplication	Especifica si la instantánea se replicará en el almacenamiento remoto o no. Valores posibles: • `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	Requerido
ensureSerialCreation	Especifica que no se debe crear la instantánea si hay una replicación de instantánea anterior en curso. Los valores posibles son: • <code>true</code>: Esto garantiza que solo se replique una instantánea a la vez. La creación de una nueva instantánea fallará si la replicación de una instantánea anterior aún está en curso. • <code>false</code>: Por defecto. Se permite la creación de esta instantánea si otra replicación de instantánea aún está en curso.	booleano	false	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
expirationTime	Especifique el tiempo después del cual se puede eliminar la instantánea. No se puede utilizar con <code>retention</code>. Si ninguno de los dos <code>expirationTime</code>, o <code>retention</code> Si se especifican, la instantánea no caducará. El formato de hora es una cadena de fecha ISO 8601 para la expiración basada en el tiempo; de lo contrario, no expirará. Un valor de <code>null</code> hace que la instantánea se conserve de forma permanente. Un valor de <code>fifo</code> hace que la instantánea se conserve en base al orden de llegada (FIFO), en relación con otras instantáneas FIFO en el volumen. La API fallará si no hay espacio FIFO disponible.	cadena de fecha ISO 8601	Ninguno	No
name	El nombre de la instantánea del grupo. Si no se introduce ningún nombre, se utiliza la fecha y hora en que se tomó la instantánea del grupo. La longitud máxima permitida para el nombre es de 255 caracteres.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
retention	Este parámetro es igual que el expirationTime parámetro, excepto que el formato de hora es HH:mm:ss. Si ninguno de los dos expirationTime ni retention Si se especifican, la instantánea no caducará.	cadena	Ninguno	No
snapMirrorLabel	La etiqueta utilizada por el software SnapMirror para especificar la política de retención de instantáneas en un punto final de SnapMirror .	cadena	Ninguno	No
volumes	Identificador único de la imagen de volumen desde la cual copiar.	matriz volumeID	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo

miembros	Lista de sumas de comprobación, IDs de volumen e IDs de instantáneas para cada miembro del grupo. Valores válidos: • Suma de comprobación: Una pequeña representación en cadena de los datos en la instantánea almacenada. Esta suma de comprobación se puede utilizar posteriormente para comparar otras instantáneas y detectar errores en los datos. (cadena) • snapshotID: Identificador único de la instantánea a partir de la cual se crea la nueva instantánea. El ID de la instantánea debe corresponder a una instantánea del volumen dado. (entero) • volumeID: El ID del volumen de origen de la instantánea. (entero)	matriz de objetos JSON
ID de instantánea del grupo	Identificador único de la nueva instantánea de grupo.	ID de instantánea de grupo
Instantánea de grupo	Objeto que contiene información sobre la instantánea de grupo recién creada.	Instantánea de grupo

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}

```

Nueva versión

9,6

Crear horario

Puedes usar `CreateSchedule` programar una instantánea automática de un volumen a intervalos definidos.

Posteriormente, puede utilizar la instantánea creada como copia de seguridad o para revertir cambios, a fin de garantizar que los datos de un volumen o grupo de volúmenes sean coherentes en el momento en que se creó la instantánea. Si programas una instantánea para que se ejecute en un período de tiempo que no sea divisible por 5 minutos, la instantánea se ejecutará en el siguiente período de tiempo que sea divisible por 5 minutos. Por ejemplo, si programa una instantánea para que se ejecute a las 12:42:00 UTC, se ejecutará a las 12:45:00 UTC. No se puede programar una instantánea para que se ejecute a intervalos inferiores a 5 minutos.



Puede crear instantáneas si la plenitud del clúster se encuentra en la etapa 1, 2 o 3. No se pueden crear instantáneas cuando la capacidad del clúster alcanza la etapa 4 o 5.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
attributes	Utilice la cadena “frecuencia” para indicar la frecuencia de la instantánea. Valores posibles: • Days of Week • Days of Month • Time Interval	Objeto JSON	Ninguno	No
hasError	Se necesita ayuda con la descripción	booleano	false	No
hours	Número de horas entre instantáneas recurrentes u hora en tiempo GMT en la que se realizará la instantánea en el modo Días de la semana o Días del mes. Los valores válidos son de 0 a 23.	entero	Ninguno	No
lastRunStatus	El resultado o estado de la última creación de instantánea programada.	cadena	Ninguno	No
name	El nombre de la instantánea. Si no se introduce ningún nombre, se utiliza la fecha y hora en que se tomó la instantánea del grupo. La longitud máxima permitida para el nombre es de 244 caracteres.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
minutes	Número de minutos entre instantáneas recurrentes o el minuto en hora GMT en que se producirá la instantánea en el modo Días de la semana o Días del mes. Los valores válidos son del 5 al 59.	entero	Ninguno	No
paused	Indica si se debe pausar la programación o no. Valores válidos: • true • false	booleano	Ninguno	No
recurring	Indica si la programación será recurrente o no. Los valores válidos son: • true • false	booleano	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
runNextInterval	Especifica si se debe ejecutar o no la instantánea la próxima vez que el planificador esté activo. Cuando se establece en verdadero, la instantánea programada se ejecuta la próxima vez que el programador esté activo y se restablece a falso. Los valores válidos son: • true • false	booleano	false	No
scheduleName	Nombre único para el horario. La longitud máxima permitida para el nombre del programa es de 244 caracteres.	cadena	Ninguno	Sí
scheduleType	Indica el tipo de horario que se va a crear. El valor válido es una instantánea.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
scheduleInfo	El nombre único asignado a la programación, el período de retención de la instantánea creada y el ID del volumen desde el cual se creó la instantánea. Valores válidos: • <code>volumeID</code>: El identificador del volumen que se incluirá en la instantánea. (entero) • <code>volumes</code>: Una lista de identificadores de volumen que se incluirán en la instantánea del grupo. (matriz de enteros) • <code>`name`</code> Nombre de la instantánea que se utilizará. (cadena) • <code>`enableRemote Replication`</code> Indica si la instantánea debe incluirse en la replicación remota. (booleano) • <code>retention</code>: Cantidad de tiempo que se conservará la instantánea en HH:mm:ss. Si está vacía, la instantánea se conserva indefinidamente. (cadena) • <code>`fifo`</code> La instantánea se conserva según	Objeto JSON	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
snapMirrorLabel	La etiqueta utilizada por el software SnapMirror para especificar la política de retención de instantáneas en un punto final de SnapMirror .	cadena	Ninguno	No
startingDate	Hora después de la cual se ejecutará el programa. Si no se ha configurado, el horario comienza inmediatamente. Formateado en hora UTC.	cadena de fecha ISO 8601	Ninguno	No
toBeDeleted	Especifica que esta programación de instantáneas debe eliminarse una vez completada la creación de la instantánea.	booleano	false	No
monthdays	Los días del mes en que se tomará la fotografía. Los valores válidos son del 1 al 31.	matriz de enteros	Ninguno	Sí (si se programa para días del mes)

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
weekdays	Día de la semana en que se creará la instantánea. Valores obligatorios (si se utilizan): • Day: 0 a 6 (de domingo a sábado) • Offset: para cada semana posible en un mes, del 1 al 6 (Si es mayor que 1, solo se coincidirá en el día N-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 instantánea se crea para este día de la semana, independientemente de en qué parte del mes caiga.	matriz de objetos JSON	Ninguno	Sí (si se programa por días de la semana)

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo

ID de programación	ID del horario creado.	entero
cronograma	Un objeto que contiene información sobre el horario recién creado.	cronograma

Ejemplo de solicitud 1

El siguiente ejemplo de programación tiene los siguientes parámetros:

- No se especifican horas ni minutos de inicio, por lo que el horario comienza lo más cerca posible de la medianoche (00:00:00Z).
- No es recurrente (solo se ejecutará una vez).
- Se ejecuta una vez, ya sea el primer domingo o miércoles después del 1 de junio de 2015, UTC 19:17:15Z (el día que ocurra primero).
- Incluye un solo 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

El siguiente ejemplo de programación tiene los siguientes parámetros:

- Es recurrente (se ejecutará en cada intervalo programado del mes a la hora especificada).

- Se ejecuta los días 1, 10, 15 y 30 de cada mes siguiente a la fecha de inicio.
- Se ejecuta a las 12:15 PM cada día en que está programado que ocurra.
- Incluye un solo 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

El siguiente ejemplo de programación tiene los siguientes parámetros:

- 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 los días segundo, tercero y cuarto de cada mes siguiente a la fecha de inicio.
- Se ejecuta a las 14:45 horas todos los días en que está programado que ocurra.
- 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
  }
}

```

Nueva versión

9,6

Crear instantánea

Puedes usar `CreateSnapshot` para crear una copia puntual de un volumen. Puede crear una instantánea desde cualquier volumen o desde una instantánea existente.

Si no proporciona un SnapshotID con este método de API, se creará una instantánea a partir de la rama activa del volumen. Si el volumen desde el que se crea la instantánea se está replicando en un clúster remoto, la instantánea también se puede replicar en el mismo destino. Utilice el parámetro enableRemoteReplication para habilitar la replicación de instantáneas.



Puede crear instantáneas si la plenitud del clúster se encuentra en la etapa 1, 2 o 3. No se pueden crear instantáneas cuando la capacidad del clúster alcanza la etapa 4 o 5.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
attributes	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
enableRemoteReplication	Especifica si la instantánea se replicará en el almacenamiento remoto o no. Valores posibles: • `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	Requerido
ensureSerialCreation	Especifica que no se debe crear la instantánea si hay una replicación de instantánea anterior en curso. Los valores posibles son: • <code>true</code>: Esto garantiza que solo se replique una instantánea a la vez. La creación de una nueva instantánea fallará si la replicación de una instantánea anterior aún está en curso. • <code>false</code>: Por defecto. Se permite la creación de esta instantánea si otra replicación de instantánea aún está en curso.	booleano	false	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
tiempo de expiración	Especifique el tiempo después del cual se puede eliminar la instantánea. No se puede utilizar con <code>retention</code> . Si no se especifica ni <code>expirationTime</code> ni <code>retention</code> , la instantánea no caducará. El formato de hora es una cadena de fecha ISO 8601 para la expiración basada en el tiempo; de lo contrario, no expirará. Un valor de <code>null</code> hace que la instantánea se conserve de forma permanente. Un valor de <code>fifo</code> hace que la instantánea se conserve según el principio de primero en entrar, primero en salir (FIFO), en relación con otras instantáneas FIFO en el volumen. La API fallará si no hay espacio FIFO disponible.	cadena	Ninguno	No
name	El nombre de la instantánea. Si no se introduce ningún nombre, se utiliza la fecha y hora en que se tomó la fotografía. La longitud máxima permitida para el nombre es de 255 caracteres.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
retention	Este parámetro es igual que el expirationTime parámetro, excepto que el formato de hora es HH:mm:ss. Si ninguno de los dos expirationTime ni retention Si se especifican, la instantánea no caducará.	cadena	Ninguno	No
snapMirrorLabel	La etiqueta utilizada por el software SnapMirror para especificar la política de retención de instantáneas en un punto final de SnapMirror .	cadena	Ninguno	No
snapshotID	Identificador único de la instantánea a partir de la cual se crea la nueva instantánea. El snapshotID proporcionado debe ser una instantánea del volumen dado.	entero	Ninguno	No
volumeID	Identificador único de la imagen de volumen desde la cual copiar.	entero	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo

suma de comprobación	Una cadena que representa los dígitos correctos en la instantánea almacenada. Esta suma de comprobación se puede utilizar posteriormente para comparar otras instantáneas y detectar errores en los datos.	cadena
ID de instantánea	Identificador único de la nueva instantánea.	ID de instantánea
instantánea	Un objeto que contiene información sobre la instantánea recién creada.	instantánea

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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

Se muestra una excepción `xNotPrimary` cuando `CreateSnapshot` Se llama a la API y no se puede crear la instantánea. Este es el comportamiento esperado. Inténtalo de nuevo `CreateSnapshot` Llamada a la API.

Nueva versión

9,6

Eliminar instantánea de grupo

Puedes usar `DeleteGroupSnapshot` Eliminar una instantánea de grupo.

Puede utilizar el parámetro `saveMembers` para conservar todas las instantáneas que se crearon para los volúmenes del grupo, pero se eliminará la asociación con el grupo.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de instantánea del grupo	Identificador único de la instantánea del grupo.	entero	Ninguno	Sí
salvarMiembros	Especifica qué se debe eliminar al eliminar una instantánea de grupo. Valores válidos: • Verdadero: Se conservan las instantáneas, pero se elimina la asociación con el grupo. • Falso: El grupo y las instantáneas se han eliminado.	booleano	FALSO	No

Valor de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DeleteGroupSnapshot",
  "params": {
    "groupSnapshotID": 10,
    "saveMembers" : true
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nueva versión

9,6

Eliminar instantánea

Puedes usar el `DeleteSnapshot` Método para eliminar una instantánea.

Una instantánea que actualmente está activa no se puede eliminar. Debes revertir la instantánea y activar otra antes de poder eliminar la instantánea actual.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de instantánea	El ID de la instantánea que se va a eliminar.	entero	Ninguno	Sí
<code>anularSnapMirrorHold</code>	Anular el bloqueo aplicado a las instantáneas durante la replicación. Puede utilizar este parámetro para eliminar instantáneas obsoletas de SnapMirror después de que se haya eliminado la relación SnapMirror asociada.	booleano	FALSO	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "DeleteSnapshot",
  "params": {
    "snapshotID": 8,
    "overrideSnapMirrorHold": true
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nueva versión

9,6

Encuentra más información

[Revertir a instantánea](#)

Obtener horario

Puedes usar `GetSchedule` para obtener información sobre una instantánea programada.

Puedes ver información sobre una programación específica si hay muchas programaciones de instantáneas en el sistema. Con este método también puede recuperar información sobre más de una programación especificando identificadores adicionales en el parámetro `scheduleID`.

Parámetro

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de programación	Identificador único del horario o de los horarios que se mostrarán.	entero	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
cronograma	Una matriz de atributos de programación.	cronograma formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": []
    }
  }
}

```

Nueva versión

9,6

Lista de instantáneas de grupo

Puedes usar `ListGroupSnapshots` Método para devolver información sobre todas las instantáneas de grupo que se han creado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de instantánea del grupo	Recuperar información para un ID de instantánea de grupo individual.	entero	Ninguno	No
volúmenes	Una matriz de identificadores de volumen únicos para consultar. Si no especifica este parámetro, se incluirán todas las instantáneas de grupo del clúster.	matriz volumeID	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Instantáneas de grupo	Una lista de objetos que contiene información sobre cada instantánea de grupo.	Instantánea de grupo formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
]

```

```
]
}
```

Nueva versión

9,6

Listas de horarios

Puedes usar `ListSchedules` Para obtener información sobre 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 de retorno:

Nombre	Descripción	Tipo
horarios	Una lista de los horarios que se encuentran actualmente en el clúster.	cronograma formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": []
  }
]
}
}

```

Nueva versión

9,6

Instantáneas de la lista

Puedes usar `ListSnapshots` para devolver los atributos de cada instantánea tomada en el volumen.

La información sobre las instantáneas que residen en el clúster de destino se mostrará en el clúster de origen cuando se llame a este método desde el clúster de origen.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de volumen	Recupera instantáneas de un volumen. Si no se proporciona <code>volumeID</code> , se devuelven todas las instantáneas de todos los volúmenes.	entero	Ninguno	No
ID de instantánea	Recupera información para un ID de instantánea individual.	entero	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
instantáneas	Información sobre cada instantánea para cada volumen. Si no se proporciona volumeID, se devuelven todas las instantáneas de todos los volúmenes. Las instantáneas que se encuentran en un grupo se devuelven con un ID de grupo.	instantánea información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}

```

Nueva versión

9,6

Modificar instantánea de grupo

Puedes usar `ModifyGroupSnapshot` para cambiar los atributos de un grupo de instantáneas. También puede utilizar este método para permitir que las instantáneas creadas en el volumen de lectura/escritura (origen) se repliquen de forma remota en un sistema de almacenamiento de destino.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
habilitar la replicación remota	Utilice esta opción para permitir que la instantánea creada se replique en un clúster remoto. Valores posibles: • `true` La instantánea se replicará en el almacenamiento remoto. • `false` La instantánea no se replicará en el almacenamiento remoto.	booleano	FALSO	No

tiempo de expiración	Especifique el tiempo después del cual se puede eliminar la instantánea. No se puede utilizar con retención. Si no se especifica ni el tiempo de expiración ni la retención de la instantánea original, la instantánea no caducará. El formato de hora es una cadena de fecha ISO 8601 para la caducidad basada en el tiempo; de lo contrario, no caducará. Un valor de <code>null</code> hace que la instantánea se conserve de forma permanente. Un valor de <code>fifo</code> hace que la instantánea se conserve en base al orden de llegada (FIFO), en relación con otras instantáneas FIFO en el volumen. La API fallará si no hay espacio FIFO disponible.	cadena de fecha ISO 8601	Ninguno	No
nombre	El nombre de la instantánea del grupo. Si no se introduce ningún nombre, se utiliza la fecha y hora en que se tomó la instantánea del grupo. La longitud máxima permitida para el nombre es de 255 caracteres.	cadena	Ninguno	No
ID de instantánea del grupo	El identificador del grupo de instantáneas.	cadena	Ninguno	Sí

snapMirrorLabel	La etiqueta utilizada por el software SnapMirror para especificar la política de retención de instantáneas en un punto final de SnapMirror .	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
Instantánea de grupo	Objeto que contiene información sobre la instantánea de grupo recién modificada.	Instantánea de grupo

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  }
}

```

Nueva versión

9,6

Modificar horario

Puedes usar `ModifySchedule` para cambiar los intervalos en los que se produce una instantánea programada. También puedes eliminar o pausar una programación utilizando este método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
atributos	Se utiliza para cambiar la frecuencia de aparición de la instantánea. Valores posibles: • Days of Week • Days of Month • Time Interval	Objeto JSON	Ninguno	No
horas	Número de horas entre instantáneas o hora en la que se realizará la instantánea en el modo Días de la semana o Días del mes. Los valores válidos son de 0 a 24.	cadena	Ninguno	No
nombre	El nombre de la instantánea. Si no se introduce ningún nombre, se utiliza la fecha y hora en que se tomó la instantánea del grupo. La longitud máxima permitida para el nombre es de 244 caracteres.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
minutos	Número de minutos entre instantáneas o minuto en el que se tomará la instantánea en el modo Días de la semana o Días del mes. Los valores válidos son de 0 a 59.	entero	Ninguno	No
último estado de ejecución	El resultado o estado de la última creación de instantánea programada.	cadena	Ninguno	No
pausa	Indica si se debe pausar la programación o no. Valores válidos: • true • false	booleano	Ninguno	No
periódico	Indica si la programación será recurrente o no. Los valores válidos son: • true • false	booleano	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ejecutarSiguienteIntervalo	Se utiliza para elegir si se debe ejecutar o no la instantánea la próxima vez que el programador esté activo. Valores válidos: • true • false Cuando se establece en verdadero, la instantánea programada se ejecuta la próxima vez que el programador esté activo y luego se restablece a falso.	booleano	FALSO	No
ID de programación	Identificador único del horario.	entero	Ninguno	Sí
nombre del horario	Nombre único para el horario. La longitud máxima permitida para el nombre del programa es de 244 caracteres.	cadena	Ninguno	No
Tipo de horario	Indica el tipo de horario que se va a crear. El único valor admitido es snapshot .	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
scheduleInfo	El nombre único asignado a la programación, el período de retención de la instantánea creada y el ID del volumen desde el cual se creó la instantánea. Valores válidos: • <code>`enableRemoteReplication`</code> Indica si la instantánea debe incluirse en la replicación remota. (booleano) • <code>ensureSerialCreation:</code> Especifica si se debe permitir la creación de una nueva instantánea si hay una replicación de instantánea anterior en curso. (booleano) • <code>`name`</code> Nombre de la instantánea que se utilizará. (cadena) • <code>retention:</code> El tiempo durante el cual se conserva la instantánea. Dependiendo de la hora, se muestra en uno de los siguientes formatos: ◦ <code>`fifo`</code> La instantánea se conserva según el principio de	"cronograma"	Ninguno	No
1136				

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
snapMirrorLabel	La etiqueta utilizada por el software SnapMirror para especificar la política de retención de instantáneas en un punto final de SnapMirror .	cadena	Ninguno	No
para ser eliminado	Indica si la programación está marcada para su eliminación. Valores válidos: • true • false	booleano	Ninguno	No
fecha de inicio	Indica la fecha en que comenzó o comenzará el horario por primera vez.	cadena de fecha ISO 8601	Ninguno	No
días del mes	Los días del mes en que se tomará la fotografía. Los valores válidos son del 1 al 31.	matriz de enteros	Ninguno	Sí
días laborables	Día de la semana en que se creará la instantánea. El día de la semana comienza el domingo con el valor 0 y un desplazamiento de 1.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo

cronograma	Un objeto que contiene los atributos de programación modificados.	cronograma

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
        }
      ]
    }
  }
}

```

Nueva versión

9,6

Modificar instantánea

Puedes usar `ModifySnapshot` para cambiar los atributos actualmente asignados a una instantánea. También puede utilizar este método para permitir que las instantáneas creadas en el volumen de lectura/escritura (origen) se repliquen de forma remota en un clúster de almacenamiento de destino que ejecute el software Element.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
habilitar la replicación remota	Utilice esta opción para permitir que la instantánea creada se replique en un clúster de almacenamiento remoto. Valores posibles: • <code>`true`</code> La instantánea se replicará en el almacenamiento remoto. • <code>`false`</code> La instantánea no se replicará en el almacenamiento remoto.	booleano	FALSO	No

tiempo de expiración	Especifique el tiempo después del cual se puede eliminar la instantánea. No se puede utilizar con retención. Si no se especifica ni el tiempo de expiración ni la retención de la instantánea original, la instantánea no caducará. El formato de hora es una cadena de fecha ISO 8601 para la expiración basada en el tiempo; de lo contrario, no expirará. Un valor nulo provoca que la instantánea se conserve de forma permanente. Un valor de fifo hace que la instantánea se conserve en base al orden de llegada (FIFO), en relación con otras instantáneas FIFO en el volumen. La API fallará si no hay espacio FIFO disponible.	cadena de fecha ISO 8601	Ninguno	No
nombre	El nombre de la instantánea. Si no se introduce ningún nombre, se utiliza la fecha y hora en que se tomó la fotografía. La longitud máxima permitida para el nombre es de 255 caracteres.	cadena	Ninguno	No

snapMirrorLabel	La etiqueta utilizada por el software SnapMirror para especificar la política de retención de instantáneas en un punto final de SnapMirror .	cadena	Ninguno	No
ID de instantánea	Identificador de la instantánea.	cadena	Ninguno	Sí

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
instantánea	Un objeto que contiene información sobre la instantánea recién modificada.	instantánea

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
  }
}
```

Nueva versión

9,6

Revertir a instantánea de grupo

Puedes usar `RollbackToGroupSnapshot` revertir todos los volúmenes individuales de un grupo de instantáneas a la instantánea individual de cada volumen.

Al revertir a una instantánea de grupo, se crea una instantánea temporal de cada volumen dentro de la instantánea de grupo.



- Se permite crear una instantánea si la plenitud del clúster está en la etapa 1, 2 o 3. No se crean instantáneas cuando la capacidad del clúster se encuentra en la etapa 4 o 5.
- Es posible que la reversión de volúmenes a una instantánea de grupo falle cuando la sincronización de segmentos esté en curso. Rever `RollbackToGroupSnapshot` una vez finalizada la sincronización.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
groupSnapshotID	Identificador único de la instantánea del grupo.	entero	Ninguno	Sí
attributes	Lista de pares nombre-valor en formato de objeto JSON.	Objeto JSON	Ninguno	No
name	Nombre de la instantánea de grupo del estado actual del volumen que se crea si saveCurrentState está establecido en verdadero. Si no se especifica un nombre, el nombre de las instantáneas (volumen de grupo e individual) se establecerá en una marca de tiempo del momento en que se produjo la reversión.	cadena	Ninguno	No
saveCurrentState	Especifica si se debe guardar o no la imagen del volumen activo anterior. Valores válidos: • `true` Se conserva la imagen del volumen activo anterior. • `false` Se ha eliminado la imagen de volumen activa anterior.	booleano	FALSO	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
miembros	Una matriz que contiene los ID de volumen y los ID de instantánea de los miembros de la instantánea del grupo. Valores: • Suma de comprobación: Una pequeña representación en cadena de los datos en la instantánea almacenada. Esta suma de comprobación se puede utilizar posteriormente para comparar otras instantáneas y detectar errores en los datos. (cadena) • snapshotID: Identificador único de la instantánea a partir de la cual se crea la nueva instantánea. El snapshotID debe ser una instantánea del volumen dado. (entero) • volumeID: El ID del volumen de origen de la instantánea. (entero)	matriz de objetos JSON
ID de instantánea del grupo	Si <code>saveCurrentState</code> se estableció en falso, este valor es nulo. Si <code>saveCurrentState</code> se estableció en verdadero, el ID único de la instantánea de grupo recién creada.	entero
Instantánea de grupo	Si <code>saveCurrentState</code> se estableció en falso, este valor es nulo. Si <code>saveCurrentState</code> se estableció en verdadero, un objeto que contiene información sobre la instantánea del grupo que <code>RollbackToGroupSnapshot</code> Acabo de retroceder a.	Instantánea de grupo

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}

```

Nueva versión

9,6

Revertir a instantánea

Puedes usar el `RollbackToSnapshot` Método para crear una instantánea existente de la imagen del volumen activo. Este método crea una nueva instantánea a partir de una instantánea existente.

La nueva instantánea se activa y la instantánea existente se conserva hasta que se elimine manualmente. La instantánea previamente activa se elimina a menos que configure el parámetro `saveCurrentState` en verdadero.

LLENADO_DEL_CLÚSTER



- Puede crear instantáneas si la plenitud del clúster se encuentra en la etapa 1, 2 o 3. No se pueden crear instantáneas cuando la capacidad del clúster alcanza la etapa 4 o 5.
- Es posible que se produzca un error al revertir un volumen a una instantánea cuando la sincronización de segmentos está en curso. Rever `RollbackToSnapshot` una vez finalizada la sincronización.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID de volumen	ID del volumen.	entero	Ninguno	Sí
atributos	Lista de pares nombre-valor en formato de objeto JSON.	atributos JSON	Ninguno	No
nombre	Nombre de la instantánea. Si no se proporciona ningún nombre, se utiliza el nombre de la instantánea a la que se está revirtiendo con "-copia" añadido al final del nombre.	cadena	Ninguno	No
ID de instantánea	ID de una instantánea creada previamente en el volumen dado.	entero	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
guardarEstadoActual	Especifica si se debe guardar o no la imagen del volumen activo anterior. Valores válidos: • Verdadero: Se conserva la imagen del volumen activo anterior. • Falso: La imagen de volumen activa anterior se ha eliminado.	booleano	FALSO	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
suma de comprobación	Una pequeña representación en cadena de los datos en la instantánea almacenada.	cadena
ID de instantánea	Si saveCurrentState se estableció en falso, este valor es nulo. Si saveCurrentState se estableció en verdadero, el ID único de la instantánea recién creada.	entero
instantánea	Si saveCurrentState se estableció en falso, este valor es nulo. Si saveCurrentState se estableció en verdadero, se creará un objeto que contiene información sobre la instantánea recién creada.	instantánea

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
  }
}
```

Nueva versión

9,6

Métodos de la API de volumen virtual

CrearContenedorDeAlmacenamiento

Puedes usar el `CreateStorageContainer` Método para crear un contenedor de almacenamiento de volumen virtual (VVol). Puede utilizar contenedores de almacenamiento para la generación de informes y la asignación de recursos. Necesitas crear al menos un contenedor de almacenamiento para utilizar la función de volúmenes virtuales.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nombre	Nombre del contenedor de almacenamiento. Respetar las restricciones de nomenclatura de cuentas de software de Element.	cadena	Ninguno	Sí
ID de cuenta	Cuenta de contenedor no de almacenamiento que se convertirá en un contenedor de almacenamiento.	entero	Ninguno	No
iniciadorSecreto	La clave secreta para la autenticación CHAP del iniciador.	cadena	Ninguno	No
secreto del objetivo	La clave secreta para la autenticación CHAP del objetivo.	cadena	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

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 para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  }
}
```

Nueva versión

9,6

Eliminar contenedores de almacenamiento

Puedes usar el `DeleteStorageContainers` Método para eliminar hasta 2000 contenedores de almacenamiento de volumen virtual (VVol) del sistema a la vez. Los contenedores de almacenamiento que retire no deben contener ningún VVols.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
IDs de contenedores de almacenamiento	Una lista de los identificadores de los contenedores de almacenamiento que se eliminarán. Puedes especificar hasta 2000 identificadores en la lista.	matriz UUID	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": {}
}
```

Nueva versión

9,6

Obtener la eficiencia del contenedor de almacenamiento

Puedes usar el `GetStorageContainerEfficiency` Método para recuperar información sobre la eficiencia de un contenedor de almacenamiento de volumen virtual.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del contenedor de almacenamiento	El identificador del contenedor de almacenamiento del que se recuperará la información de eficiencia.	entero	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
compresión	Cantidad de espacio ahorrado mediante la compresión de datos para todos los volúmenes virtuales en el contenedor de almacenamiento. Se expresa como una relación donde un valor de 1 significa que los datos se han almacenado sin compresión.	flotar
deduplicación	La cantidad de espacio ahorrado al no duplicar los datos de todos los volúmenes virtuales en el contenedor de almacenamiento. Expresado como una proporción.	flotar
volúmenes faltantes	Los volúmenes virtuales que no se pudieron consultar para obtener datos de eficiencia. La falta de volúmenes puede deberse a que el ciclo de recolección de basura (GC) tenga menos de una hora de antigüedad, a una pérdida temporal de conectividad de red o a servicios reiniciados desde el ciclo de GC.	matriz de enteros

aprovisionamiento ligero	La proporción de espacio utilizado con respecto a la cantidad de espacio asignado para almacenar datos. Expresado como una proporción.	flotar
marca de tiempo	La última vez que se recopilaron datos de eficiencia después de GC.	cadena de datos ISO 8601

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nueva versión

9,6

Obtener recuento de volúmenes virtuales

Puedes usar el `GetVirtualVolumeCount` Método para recuperar el número de volúmenes virtuales que se encuentran actualmente en el sistema.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
contar	Número de volúmenes virtuales actualmente en el sistema.	entero

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "method": "GetVirtualVolumeCount",
  "params": {
  },
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {
    "count": 5
  }
}
```

Nueva versión

9,6

ListProtocolEndpoints

Puedes usar el `ListProtocolEndpoints` Método para recuperar información sobre todos los puntos finales del protocolo en el clúster. Los puntos finales del protocolo controlan 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	Requerido
ID de punto final del protocolo	Una lista de identificadores de puntos finales del protocolo para los que se desea recuperar información. Si se omite este parámetro, el método devuelve información sobre todos los puntos finales del protocolo.	matriz UUID del punto de conexión del protocolo	Ninguno	No

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
puntos finales del protocolo	Lista de objetos que contienen información sobre cada punto final del protocolo en el sistema.	punto final del protocolo información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}

```

Nueva versión

9,6

Listar contenedores de almacenamiento

Puedes usar el `ListStorageContainers` Método para recuperar información sobre todos los contenedores de almacenamiento de volúmenes virtuales conocidos por el sistema.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
IDs de contenedores de almacenamiento	Una lista de identificadores de contenedores de almacenamiento de los que se recuperará información. Si se omite este parámetro, el método devuelve información sobre todos los contenedores de almacenamiento del sistema.	matriz UUID	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
contenedores de almacenamiento	Lista de objetos que contienen información sobre todos los contenedores de almacenamiento del sistema.	contenedor de almacenamiento información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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": []
      }
    ]
  }
}
```

Nueva versión

9,6

ListVirtualVolumeBindings

Puedes usar el `ListVirtualVolumeBindings` Método para obtener una lista de todos los volúmenes virtuales del clúster que están vinculados a puntos de conexión de protocolo.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
IDs de enlace de volumen virtual	Una lista de identificadores de enlace de volumen virtual para los que se recuperará información. Si se omite este parámetro, el método devuelve información sobre todos los enlaces de volumen virtual.	matriz de enteros	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
uniones	Una lista de objetos que describe todos los volúmenes virtuales del clúster que están vinculados a puntos finales de protocolo.	vinculante

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
      }
    ]
  }
}

```

Nueva versión

9,6

Listar hosts de volumen virtual

Puedes usar el `ListVirtualVolumeHosts` Método para obtener una lista de todos los hosts de volúmenes virtuales conocidos por el clúster. Un host de volumen virtual es un host VMware ESX que ha iniciado una sesión con el proveedor de la API VASA.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
IDs de host de volumen virtual	Una lista de identificadores de host de volúmenes virtuales para los que se recuperará información. Si se omite este parámetro, el método devuelve información sobre todos los hosts de volumen virtual.	matriz UUID de <code>virtualVolumeHostID</code>	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
hosts	Una lista de objetos que describen los hosts de volúmenes virtuales en el clúster.	anfitrión información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
        ]
      }
    ]
  }
}
```

Nueva versión

9,6

Listar volúmenes virtuales

Puedes usar el `ListVirtualVolumes` Método para listar los volúmenes virtuales que se encuentran actualmente en el sistema. Puede utilizar este método para listar todos los volúmenes virtuales, o solo un subconjunto.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
detalles	El nivel de detalle en la respuesta. Valores posibles: • Verdadero: Incluya más detalles sobre cada VVol en la respuesta. • Falso: Incluya el nivel de detalle estándar sobre cada VVol en la respuesta.	booleano	FALSO	No
límite	Número máximo de volúmenes virtuales a listar.	entero	10000	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
recursivo	Especifica si se debe incluir o no información sobre los hijos de cada VVol en la respuesta. Valores posibles: • Verdadero: 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 debe comenzar la lista en la respuesta.	Tipo UUID	Ninguno	No
IDs de volumen virtual	Una lista de identificadores de volúmenes virtuales de los que se desea recuperar información. Si omite este parámetro, el método devuelve información únicamente sobre estos volúmenes virtuales.	matriz UUID de virtualVolumeID	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
nextVirtualVolumeID	El identificador del siguiente volumen virtual en la lista.	UUID

volúmenes virtuales	Una lista de objetos que describe los volúmenes virtuales que se encuentran actualmente en el sistema.	volumen virtual formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
      }
    ]
  }
}

```

Nueva versión

9,6

Listar tareas de volumen virtual

Puedes usar el `ListVirtualVolumeTasks` Método para obtener una lista de tareas de volumen virtual en el sistema.

Parámetros

Este método tiene el siguiente parámetro de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
IDs de tareas de volumen virtual	Una lista de identificadores de tareas de volumen virtual para los que se debe recuperar información. Si se omite este parámetro, el método devuelve información sobre todas las tareas de volumen virtual.	matriz UUID	Ninguno	No

Valor de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
tareas	Una lista de objetos que describen las tareas de volumen virtual en el clúster.	tarea información

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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-667f6867fcd",
          "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"
      }
    ]
  }
}

```

Nueva versión

9,6

ModificarContenedorDeAlmacenamiento

Puedes usar 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	Requerido
ID del contenedor de almacenamiento	El identificador único del contenedor de almacenamiento de volumen virtual que se va a modificar.	UUID	Ninguno	Sí
iniciadorSecreto	El nuevo secreto para la autenticación CHAP para el iniciador.	cadena	Ninguno	No
secreto del objetivo	El nuevo secreto para la autenticación CHAP para el objetivo.	cadena	Ninguno	No

Valores de retorno

Este método tiene el siguiente valor de retorno:

Nombre	Descripción	Tipo
contenedor de almacenamiento	Información sobre el contenedor de almacenamiento recién creado.	contenedor de almacenamiento

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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"
    }
  }
}
```

Nueva versión

9,6

Control de acceso

Los métodos de la API de Element disponibles varían según el tipo de acceso que configure.



Existen tipos de acceso disponibles a través de la API que no están disponibles en la interfaz de usuario de Element.

cuentas

Los siguientes métodos están disponibles para el tipo de acceso a cuentas:

Agregar cuenta
ObtenerCuentaPorID
Modificar cuenta
ObtenerCuentaPorNombre
Lista de cuentas
Obtén la eficiencia de la cuenta
Eliminar cuenta

administrador

Todos los métodos están disponibles para el tipo de acceso de administrador.

administrador del clúster

Los siguientes métodos están disponibles para el tipo de acceso de administrador de clúster:

Agregar administrador de clúster
ListBackupTargets
AgregarIniciadoresAlGrupoDeAccesoPorVolumen
Lista de trabajos de volumen masivo
Agregar administrador de clúster Ldap
Lista de administradores de clúster
Agregar red virtual
ListClusterPairs
Agregar red virtual
Información del puerto del canal de fibra del nodo de lista
Agregar volumen al grupo de acceso por volumen
ListBackupTargets
Clonar múltiples volúmenes
Hardware de la unidad de lista
Emparejamiento de clústeres completo
Lista de sesiones de FibreChannel
Emparejamiento de volumen completo
Información del puerto del canal de fibra
Crear destino de copia de seguridad

Lista de instantáneas de grupo
Crear horario
Lista de volúmenes emparejados activos
Crear instantánea
Modificar destino de copia de seguridad
Crear paquete de soporte
Modificar administrador de clúster
Crear paquete de soporte de clúster
Modificar instantánea de grupo
CrearInstantáneaDeGrupo
Modificar UmbralCompletoDeClúster
Crear grupo de acceso a volumen
Modificar grupo de acceso al volumen
Eliminar todos los paquetes de soporte
Modificar asignaciones de Lun de grupo de acceso a volumen
Eliminar instantánea
Modificar par de volúmenes
Eliminar instantánea de grupo
Modificar red virtual
Eliminar grupo de acceso al volumen
Eliminar administrador del clúster
Deshabilitar el cifrado en reposo

Eliminar par de volúmenes
Deshabilitar la autenticación LDAP
Eliminar red virtual
Deshabilitar SNMP
Eliminar volúmenes del grupo de acceso a volúmenes
Habilitar cifrado en reposo
EliminarIniciadoresDelGrupoDeAccesoPorVolumen
Habilitar autenticación LDAP
Revertir a instantánea
Habilitar SNMP
Revertir a instantánea de grupo
ObtenerObjetivoDeCopiaDeSeguridad
SetLoginSessionInfo
Umbral completo del clúster
SetNtpInfo
Obtener ID de nodo maestro del clúster
SetSnmpACL
Obtener configuración de hardware
SetSnmpInfo
Obtener configuración LDAP
SetSnmpTrapInfo
Obtener información de sesión de inicio de sesión

Configurar hosts de registro remoto
Obtener información NTP
Cerrar
Obtener información de NVRAM
Iniciar lectura de volumen masivo
GetRawStats
Iniciar escritura masiva de volumen
Obtener ACL SNMP
Iniciar emparejamiento de clústeres
ObtenerEficienciaDeGrupoDeAccesoDeVolumen
Emparejamiento de volumen inicial
ObtenerAsignaciones de acceso al volumen
Prueba de autenticación LDAP
Obtener red virtual

unidades

Los siguientes métodos están disponibles para el tipo de acceso a las unidades:

ListDrives
Eliminar unidades
Agregar unidades
Unidades de borrado seguro

nodos

Los siguientes métodos están disponibles para el tipo de acceso a nodos:

Agregar nodos
Lista de nodos pendientes
Lista de nodos activos
Eliminar nodos

leer

Los siguientes métodos están disponibles para el tipo de acceso de lectura:

ObtenerCuentaPorID
Listar trabajos clonados
ObtenerCuentaPorNombre
Lista de volúmenes eliminados
ObtenerResultadoAsíncrono
Hardware de la unidad de lista
Obtener capacidad del clúster
ListDrives
Obtener QoS predeterminado
Lista de eventos
GetDriveStats
Lista de sesiones ISCSI
Obtener actualización de software
Lista de nodos pendientes
Obtener estadísticas de volumen
ListSyncJobs

Lista de cuentas
Listar grupos de acceso de volumen
Lista de nodos activos
ListVolumeStatsByAccount
Lista de nodos activos
Listar estadísticas de volumen por volumen
Listar volúmenes activos
Lista de estadísticas de volumen por grupo de acceso de volumen
Lista todos los nodos
Listar volúmenes para la cuenta
ListBackupTargets

informes

Los siguientes métodos están disponibles para el tipo de acceso de informes:

Borrar fallos de clúster
ObtenerEficiencia de Volumen
Obtén la eficiencia de la cuenta
Obtener estadísticas de volumen
Obtener capacidad del clúster
Listar trabajos clonados
Obtener información de hardware del clúster
ListClusterFaults
Obtener información del clúster

ListClusterPairs
Obtener ID de nodo maestro del clúster
Hardware de la unidad de lista
Obtener estadísticas del clúster
Lista de eventos
Información sobre el hardware de la unidad
Lista de sesiones ISCSI
GetDriveStats
Listas de horarios
Obtener configuración de red
Servicios de listas
Información del hardware del nodo
ListSyncJobs
Obtener estadísticas del nodo
Lista de redes virtuales
Obtener información SNMP
ListVolumeStatsByAccount
Obtener información de trampa SNMP
Listar estadísticas de volumen por volumen
ObtenerEficienciaDeGrupoDeAccesoDeVolumen
Lista de estadísticas de volumen por grupo de acceso de volumen

repositorios

El método ListAllNodes está disponible para el tipo de acceso a repositorios.

volúmenes

Los siguientes métodos están disponibles para el tipo de acceso a volúmenes:

Crear volumen
Eliminar volumen
Modificar destino de copia de seguridad
Clonar volumen
Eliminar emparejamiento de volumen
Modificar volúmenes
Clonar múltiples volúmenes
ObtenerObjetivoDeCopiaDeSeguridad
Modificar par de volúmenes
Crear destino de copia de seguridad
Obtener QoS predeterminado
Purga de volumen eliminado
Crear instantánea
Listar volúmenes activos
Eliminar destino de copia de seguridad
CrearInstantáneaDeGrupo
ListBackupTarget
Eliminar par de volúmenes
Emparejamiento de volumen completo

Lista de instantáneas de grupo
Restaurar volumen eliminado
Clonar múltiples volúmenes
Listar volúmenes para la cuenta
Revertir a instantánea de grupo
Eliminar instantánea de grupo
Lista de volúmenes eliminados
Revertir a instantánea
Eliminar instantánea
Lista de instantáneas de grupo
Iniciar lectura de volumen masivo
Iniciar escritura masiva de volumen
Emparejamiento de volumen inicial
Actualizar estado del volumen masivo

escribir

Los siguientes métodos están disponibles para el tipo de acceso de escritura:

Agregar unidades
Eliminar nodos
Agregar nodos
Eliminar cuenta
Agregar cuenta
Eliminar volúmenes del grupo de acceso a volúmenes

Agregar volumen a grupo de acceso a volumen
EliminarIniciadoresDelGrupoDeAccesoPorVolumen
AgregarIniciadoresAlGrupoDeAccesoPorVolumen
Eliminar grupo de acceso al volumen
Crear grupo de acceso a volumen
Eliminar volumen
Modificar grupo de acceso al volumen
Restaurar volumen eliminado
Modificar cuenta
Purga de volumen eliminado
Crear volumen
Modificar volumen
Clonar volumen
ObtenerResultadoAsíncrono
Eliminar unidades

Información relacionada

["Obtén información sobre los tipos de acceso disponibles en la interfaz de usuario de Element."](#)

Ejemplos de respuesta

Obtener configuración

El `GetConfig` El método devuelve una respuesta similar al siguiente ejemplo. Debido a su 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
}
}
}
}

```

Obtener información de hardware del clúster

El `GetClusterHardwareInfo` El método devuelve una respuesta similar al siguiente ejemplo.

```
{
  "id": null,
  "result": {
    "clusterHardwareInfo": {
      "drives": {
        "1": {
          "description": "ATA      Drive",
          "dev": "8:0",
          "devpath": "/dev/disk/by-id/scsi-SATA_VRFSD3400GNCVMT205121562-
part4",
          "driveSecurityAtMaximum": false,
          "driveSecurityFrozen": true,
          "driveSecurityLocked": false,
          "logicalname": "/dev/sda",
          "product": "VRFSD3400GNCVMTJS1",
          "securityFeatureEnabled": false,
          "securityFeatureSupported": true,
          "serial": "205121562",
          "size": 299988156416,
          "uuid": "febe39ae-4984-edc0-e3a7-3c47608cfac",
          "version": "515ABBF0"
        },
        "2": {...
      },
      "3": {...
    },
    "4": {...
  },
  "5": {...
}
```

```

    },
    "6": {...
  },
  .
  .
  .
  "44": {...
  }
  },
  "nodes":{
    "1":{
      Storage Node
      "core_DMI:0200": {
      "description": "Motherboard",
      "physid": "0",
      "vendor": "SolidFire"
    },
    "fiber:0_PCI:0000:04:00.0": {
      "businfo": "pci@0000:04:00.0",
      "clock": "33000000",
      "description": "Fibre Channel",
      "physid": "0",
      "product": "ISP8324-based 16Gb Fibre Channel to PCI Express
Adapter",
      "vendor": "QLogic Corp.",
      "version": "02",
      "width": "64"
    },
    "Repeat fiber information": {...}
    "Repeat fiber": {...},
    "Repeat fiber": {...},
  }
},
  "fans": {
    "Fan1A RPM": {
      "baseUnit": "RPM",
      "threshold": 840,
      "value": 4800
    },
    "Fan1B RPM": {...},
    .
    .
    .
    "Fan7B RPM": {...
  },
  "fibreChannelPorts": [
    {

```

```

    "firmware": "7.04.00 (d0d5)",
    "hbaPort": 1,
    "model": "QLE2672",
    "nPortID": "0x110c36",
    "pciSlot": 3,
    "serial": "BFE1341E09329",
    "speed": "8 Gbit",
    "state": "Online",
    "switchWwn": "20:01:00:2a:6a:a0:25:01",
    "wwnn": "5f:47:ac:c8:82:23:e0:00",
    "wwpn": "5f:47:ac:c0:82:23:e0:02"
  },
  {
    "firmware": "7.04.00 (d0d5)", {...}
    "firmware": "7.04.00 (d0d5)", {...}
    "firmware": "7.04.00 (d0d5)", {...}
  }
],
"hardwareConfig": {
  "BIOS_REVISION": {
    "Passed": true,
    "actual": "1.1",
    "comparator": ">=",
    "expected": "1.0"
  },
  "BIOS_VENDOR": {
    "Passed": true,
    "actual": "SolidFire",
    "comparator": "==",
    "expected": "SolidFire"
  },
  "BIOS_VERSION": {
    "Passed": true,
    "actual": "1.1.2",
    "comparator": ">=",
    "expected": "1.1.2"
  },
  "BMC_FIRMWARE_REVISION": {
    "Passed": true,
    "actual": "1.6",
    "comparator": ">=",
    "expected": "1.6"
  },
  "BMC_IPMI_VERSION": {
    "Passed": true,
    "actual": "2.0",

```

```

    "comparator": ">=",
    "expected": "2.0"
  },
  "CHASSIS_TYPE": {
    "Passed": true,
    "actual": "R620",
    "comparator": "==",
    "expected": "R620"
  },
  "CPU_CORES_00": {
    "Passed": true,
    "actual": "6",
    "comparator": "==",
    "expected": "6"
  },
  "CPU_CORES_01": {
    "Passed": true,
    "actual": "6",
    "comparator": "==",
    "expected": "6"
  },
  "CPU_CORES_ENABLED_00": {
    "Passed": true,
    "actual": "6",
    "comparator": "==",
    "expected": "6"
  },
  "CPU_CORES_ENABLED_01": {
    "Passed": true,
    "actual": "6",
    "comparator": "==",
    "expected": "6"
  },
  "CPU_MODEL_00": {
    "Passed": true,
    "actual": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
    "comparator": "==",
    "expected": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz"
  },
  "CPU_MODEL_01": {
    "Passed": true,
    "actual": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
    "comparator": "==",
    "expected": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz"
  },
  "CPU_THREADS_00": {

```

```

    "Passed": true,
    "actual": "12",
    "comparator": "==",
    "expected": "12"
  },
  "CPU_THREADS_01": {
    "Passed": true,
    "actual": "12",
    "comparator": "==",
    "expected": "12"
  },
  "DRIVE_SIZE_BYTES_SDIMM0": {
    "Passed": true,
    "actual": "100030242816",
    "comparator": ">=",
    "expected": "100030242816"
  },
  "FIBRE_CHANNEL_FIRMWARE_REVISION": {
    "Passed": true,
    "actual": "FW:v7.04.00",
    "comparator": "==",
    "expected": "FW:v7.04.00"
  },
  "FIBRE_CHANNEL_MODEL": {
    "Passed": true,
    "actual": "QLE2672",
    "comparator": "==",
    "expected": "QLE2672"
  },
  "IDRAC_VERSION": {
    "Passed": true,
    "actual": "1.06.06",
    "comparator": ">=",
    "expected": "1.06.06"
  },
  "LIFECYCLE_VERSION": {
    "Passed": true,
    "actual": "1.0.0.5747",
    "comparator": ">=",
    "expected": "1.0.0.5747"
  },
  "MEMORY_GB": {
    "Passed": true,
    "actual": "32",
    "comparator": ">=",
    "expected": "32"
  }

```

```

},
"MEMORY_MHZ_00": {
  "Passed": true,
  "actual": "1333",
  "comparator": ">=",
  "expected": "1333"
},
"MEMORY_MHZ_01": {
  "Passed": true,
  "actual": "1333",
  "comparator": ">=",
  "expected": "1333"
},
"MEMORY_MHZ_02": {
  "Passed": true,
  "actual": "1333",
  "comparator": ">=",
  "expected": "1333"
},
"MEMORY_MHZ_03": {
  "Passed": true,
  "actual": "1333",
  "comparator": ">=",
  "expected": "1333"
},
"NETWORK_DRIVER_ETH0": {
  "Passed": true,
  "actual": "bnx2x",
  "comparator": "=~",
  "expected": "^bnx2x$"
},
{
  "NETWORK_DRIVER_ETH1":, {...
},
  "NETWORK_DRIVER_ETH2":, {...
},
  "NETWORK_DRIVER_ETH3":, {...
},
  "NETWORK_DRIVER_ETH4":, {...
},
  "NETWORK_DRIVER_ETH5":, {...
},
"NODE_TYPE": {
  "Passed": true,
  "actual": "FC0025",
  "comparator": "==",

```

```

    "expected": "FC0025"
  },
  "NUM_CPU": {
    "Passed": true,
    "actual": "2",
    "comparator": "==",
    "expected": "2"
  },
  "NUM_DRIVES": {
    "Passed": true,
    "actual": "0",
    "comparator": "==",
    "expected": "0"
  },
  "NUM_DRIVES_INTERNAL": {
    "Passed": true,
    "actual": "1",
    "comparator": "==",
    "expected": "1"
  },
  "NUM_FIBRE_CHANNEL_PORTS": {
    "Passed": true,
    "actual": "4",
    "comparator": "==",
    "expected": "4"
  },
  "NVRAM_VENDOR": {
    "Passed": true,
    "actual": "",
    "comparator": "==",
    "expected": ""
  },
  "ROOT_DRIVE_REMOVABLE": {
    "Passed": true,
    "actual": "false",
    "comparator": "==",
    "expected": "false"
  }
},
"memory": {
  "firmware_": {
    "capacity": "8323072",
    "date": "03/08/2012",
    "description": "BIOS",
    "physid": "0",
    "size": "65536",

```



```

    "vendor": "SolidFire",
    "version": "1.1.2"
  },
  "memory_DMI:1000": {
    "description": "System Memory",
    "physid": "1000",
    "size": "34359738368",
    "slot": "System board or motherboard"
  }
},
"network": {
  "network:0_PCI:0000:01:00.0": {
    "businfo": "pci@0000:01:00.0",
    "capacity": "1000000000",
    "clock": "33000000",
    "description": "Ethernet interface",
    "logicalname": "eth0",
    "physid": "0",
    "product": "NetXtreme II BCM57800 1/10 Gigabit Ethernet",
    "serial": "c8:1f:66:e0:97:2a",
    "vendor": "Broadcom Corporation",
    "version": "10",
    "width": "64"
  },
  "network:0_PCI:0000:41:00.0": {...
},
  "network:1_PCI:0000:01:00.1": {...
},
  "network:1_PCI:0000:41:00.1": {...
},
  "network:2_PCI:0000:01:00.2": {...
},
  "network:3_PCI:0000:01:00.3": {...
}
},
"networkInterfaces": {
  "Bond10G": {
    "isConfigured": true,
    "isUp": true
  },
  "Bond1G": {
    "isConfigured": true,
    "isUp": true
  },
  "eth0": {
    "isConfigured": true,

```

```

    "isUp": true
  },
  "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"
    },
    {... 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",
    "modelName": "RMS-200",
    "serialNumber": "0000862"
  },
  "smart": {
    "availableSpace": "0%",
    "availableSpaceThreshold": "0%",
    "controllerBusyTimeMinutes": "6793",
    "criticalErrorVector": "0x0",
    "mediaErrors": "0",
    "numberOf512ByteBlocksRead": "10530088847",
    "numberOf512ByteBlocksWritten": "1752499439063",
    "numberOfErrorInfoLogs": "1",
    "numberOfHostReadCommands": "235317769",
    "numberOfHostWriteCommands": "126030374065",
    "numberOfPowerCycles": "709",
    "powerOnHours": "11223",
    "temperature": "324 Kelvin",
    "unsafeShutdowns": "357"
  },
  "origin": null,
  "platform": {
    "chassisType": "R620",
    "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
    "nodeMemoryGB": 32,
    "nodeType": "FC0025"
  },
  "powerSupplies": {
    "PS1 status": {
      "powerSupplyFailureDetected": false,
      "powerSupplyHasAC": true,
      "powerSupplyPredictiveFailureDetected": false,
      "powerSupplyPresent": true,
      "powerSupplyPresentLastCheck": true
    },
    "PS2 status": {
      "powerSupplyFailureDetected": false,

```

```

    "powerSupplyHasAC": true,
    "powerSupplyPredictiveFailureDetected": false,
    "powerSupplyPresent": true,
    "powerSupplyPresentLastCheck": true
  }
},
"storage": {
  "storage_PCI:0000:00:1f.2": {
    "businfo": "pci@0000:00:1f.2",
    "clock": "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
}

```

```

    }
  }
}

```

Obtener información de Lldp

El `GetLldpInfo` El método devuelve una respuesta similar al siguiente ejemplo.

```

{
  "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"  
}  
  
]  
  
}  
  
}
```

Obtener configuración de red

El `GetNetworkConfig` El método devuelve una respuesta similar al siguiente ejemplo.

```
{
  "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)

El GetNodeHardwareInfo El método para iSCSI devuelve una respuesta similar al siguiente ejemplo.

```

{
    "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)

El GetNodeHardwareInfo El método para nodos Fibre Channel devuelve una respuesta similar al siguiente ejemplo.

```

{
  "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": "330000000",
"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": "330000000",
"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": "330000000",
"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": "660000000",
    "description": "SATA controller",
    "physid": "1f.2",
    "product": "C600/X79 series chipset 6-Port SATA AHCI Controller",
    "vendor": "Intel Corporation",
    "version": "05",
    "width": "32"
  }
},
"system": {
  "fcv-2_DMI:0100": {
    "description": "Rack Mount Chassis",
    "product": "(SKU=NotProvided;ModelName=)",
    "serial": "HTX1DZ1",
    "width": "64"
  }
},
"temperatures": {
  "Exhaust Temp": {
    "baseUnit": "C",
    "threshold": 70,
    "value": 38
  },
  "Inlet Temp": {
    "baseUnit": "C",
    "threshold": 42,
    "value": 13
  },
  "uuid": "4C4C4544-004D-5310-8052-C4C04F335431"
}
}

```

Obtener información de NVRAM

El `GetNvramInfo` El método devuelve una respuesta similar al siguiente ejemplo.

```
{
  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"
}
}

```

Lista de nodos activos

El `ListActiveNodes` El método devuelve una respuesta similar al siguiente ejemplo.

```

{
  "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": {

```

```

2.50GHz",
        "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
        }
    ]
}
]
}
}

```

Listar volúmenes activos

El `ListActiveVolumes` El método devuelve una respuesta similar al siguiente ejemplo.

```
{
  "id": 1,
  "result": {
    "volumes": [
      {
        "access": "readWrite",
        "accountID": 1,
        "attributes": {},
        "blockSize": 4096,
        "createTime": "2016-06-23T14:19:12Z",
        "deleteTime": "",
        "enable512e": false,
        "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo1.1",
        "name": "HulkDemo1",
        "purgeTime": "",
        "qos": {
          "burstIOPS": 1500,
          "burstTime": 60,
          "curve": {
            "4096": 100,
            "8192": 160,
            "16384": 270,
            "32768": 500,
            "65536": 1000,
            "131072": 1950,
            "262144": 3900,
            "524288": 7600,
            "1048576": 15000
          },
          "maxIOPS": 1000,
          "minIOPS": 100
        },
        "scsiEUIDeviceID": "306f746f000000001f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000000306f746f00000001",
        "sliceCount": 1,
        "status": "active",
        "totalSize": 53687091200,
        "virtualVolumeID": null,
        "volumeAccessGroups": [
          1
        ],
        "volumeID": 1,
      }
    ]
  }
}
```

```

        "volumePairs": []
    },
    {
        "access": "readWrite",
        "accountID": 1,
        "attributes": {},
        "blockSize": 4096,
        "createTime": "2016-06-23T14:19:14Z",
        "deleteTime": "",
        "enable512e": false,
        "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo6.6",
        "name": "HulkDemo6",
        "purgeTime": "",
        "qos": {
            "burstIOPS": 1500,
            "burstTime": 60,
            "curve": {
                "4096": 100,
                "8192": 160,
                "16384": 270,
                "32768": 500,
                "65536": 1000,
                "131072": 1950,
                "262144": 3900,
                "524288": 7600,
                "1048576": 15000
            },
            "maxIOPS": 1000,
            "minIOPS": 100
        },
        "scsiEUIDeviceID": "306f746f000000006f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000000306f746f00000006",
        "sliceCount": 1,
        "status": "active",
        "totalSize": 53687091200,
        "virtualVolumeID": null,
        "volumeAccessGroups": [
            1
        ],
        "volumeID": 6,
        "volumePairs": []
    },
    {
        "access": "readWrite",
        "accountID": 1,
        "attributes": {},

```



```

    "blockSize": 4096,
    "createTime": "2016-06-23T14:19:14Z",
    "deleteTime": "",
    "enable512e": false,
    "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo7.7",
    "name": "HulkDemo7",
    "purgeTime": "",
    "qos": {
      "burstIOPS": 1500,
      "burstTime": 60,
      "curve": {
        "4096": 100,
        "8192": 160,
        "16384": 270,
        "32768": 500,
        "65536": 1000,
        "131072": 1950,
        "262144": 3900,
        "524288": 7600,
        "1048576": 15000
      },
      "maxIOPS": 1000,
      "minIOPS": 100
    },
    "scsiEUIDeviceID": "306f746f000000007f47acc01000000000",
    "scsiNAADeviceID": "6f47acc1000000000306f746f000000007",
    "sliceCount": 1,
    "status": "active",
    "totalSize": 53687091200,
    "virtualVolumeID": null,
    "volumeAccessGroups": [
      1
    ],
    "volumeID": 7,
    "volumePairs": []
  },
  {
    "access": "readWrite",
    "accountID": 1,
    "attributes": {},
    "blockSize": 4096,
    "createTime": "2016-06-23T14:19:15Z",
    "deleteTime": "",
    "enable512e": false,
    "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo8.8",
    "name": "HulkDemo8",

```

```

    "purgeTime": "",
    "qos": {
      "burstIOPS": 1500,
      "burstTime": 60,
      "curve": {
        "4096": 100,
        "8192": 160,
        "16384": 270,
        "32768": 500,
        "65536": 1000,
        "131072": 1950,
        "262144": 3900,
        "524288": 7600,
        "1048576": 15000
      },
      "maxIOPS": 1000,
      "minIOPS": 100
    },
    "scsiEUIDeviceID": "306f746f000000008f47acc01000000000",
    "scsiNAADeviceID": "6f47acc1000000000306f746f000000008",
    "sliceCount": 1,
    "status": "active",
    "totalSize": 53687091200,
    "virtualVolumeID": null,
    "volumeAccessGroups": [
      1
    ],
    "volumeID": 8,
    "volumePairs": []
  },
  {
    "access": "readWrite",
    "accountID": 1,
    "attributes": {},
    "blockSize": 4096,
    "createTime": "2016-06-23T14:19:15Z",
    "deleteTime": "",
    "enable512e": false,
    "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo9.9",
    "name": "HulkDemo9",
    "purgeTime": "",
    "qos": {
      "burstIOPS": 1500,
      "burstTime": 60,
      "curve": {
        "4096": 100,

```

```

        "8192": 160,
        "16384": 270,
        "32768": 500,
        "65536": 1000,
        "131072": 1950,
        "262144": 3900,
        "524288": 7600,
        "1048576": 15000
    },
    "maxIOPS": 1000,
    "minIOPS": 100
},
"scsiEUIDeviceID": "306f746f00000009f47acc0100000000",
"scsiNAADeviceID": "6f47acc100000000306f746f00000009",
"sliceCount": 1,
"status": "active",
"totalSize": 53687091200,
"virtualVolumeID": null,
"volumeAccessGroups": [
    1
],
"volumeID": 9,
"volumePairs": []
},
{
    "access": "readWrite",
    "accountID": 1,
    "attributes": {},
    "blockSize": 4096,
    "createTime": "2016-06-23T14:19:16Z",
    "deleteTime": "",
    "enable512e": false,
    "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo12.12",
    "name": "HulkDemo12",
    "purgeTime": "",
    "qos": {
        "burstIOPS": 1500,
        "burstTime": 60,
        "curve": {
            "4096": 100,
            "8192": 160,
            "16384": 270,
            "32768": 500,
            "65536": 1000,
            "131072": 1950,
            "262144": 3900,

```

```

        "524288": 7600,
        "1048576": 15000
    },
    "maxIOPS": 1000,
    "minIOPS": 100
},
"scsiEUIDeviceID": "306f746f00000000cf47acc0100000000",
"scsiNAADeviceID": "6f47acc1000000000306f746f0000000c",
"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": "306f746f000000012f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000000306f746f000000012",
        "sliceCount": 1,
        "status": "active",
        "totalSize": 53687091200,
        "virtualVolumeID": null,
        "volumeAccessGroups": [
            1
        ],
        "volumeID": 18,
        "volumePairs": []
    },

```

```

{
  "access": "readWrite",
  "accountID": 1,
  "attributes": {},
  "blockSize": 4096,
  "createTime": "2016-06-24T15:21:59Z",
  "deleteTime": "",
  "enable512e": true,
  "iqn": "iqn.2010-01.com.solidfire:0oto.bk.24",
  "name": "BK",
  "purgeTime": "",
  "qos": {
    "burstIOPS": 15000,
    "burstTime": 60,
    "curve": {
      "4096": 100,
      "8192": 160,
      "16384": 270,
      "32768": 500,
      "65536": 1000,
      "131072": 1950,
      "262144": 3900,
      "524288": 7600,
      "1048576": 15000
    },
    "maxIOPS": 15000,
    "minIOPS": 50
  },
  "scsiEUIDeviceID": "306f746f000000018f47acc0100000000",
  "scsiNAADeviceID": "6f47acc1000000000306f746f000000018",
  "sliceCount": 1,
  "status": "active",
  "totalSize": 10737418240,
  "virtualVolumeID": null,
  "volumeAccessGroups": [],
  "volumeID": 24,
  "volumePairs": [
    {
      "clusterPairID": 2,
      "remoteReplication": {
        "mode": "Async",
        "pauseLimit": 3145728000,
        "remoteServiceID": 14,
        "resumeDetails": "",
        "snapshotReplication": {
          "state": "Idle",

```

```

        "stateDetails": ""
    },
    "state": "Active",
    "stateDetails": ""
},
"remoteSliceID": 8,
"remoteVolumeID": 8,
"remoteVolumeName": "PairingDoc",
"volumePairUUID": "229fcbf3-2d35-4625-865a-
d04bb9455cef"
    }
}
]
}
}
}

```

Configuración de hardware de prueba

El TestHardwareConfig El método devuelve una respuesta similar al siguiente ejemplo.

```

{
  "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 complemento NetApp Element para vCenter Server proporciona un complemento a la interfaz de VMware vSphere para que pueda administrar y supervisar clústeres de almacenamiento que ejecutan el software NetApp Element .

Para obtener información sobre el complemento Element para vCenter Server, consulte la ["Documentación del complemento NetApp Element para vCenter Server"](#) .

Para más información

- ["Documentación del software SolidFire y Element"](#)

Monitorea el almacenamiento con SolidFire Active IQ

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

En SolidFire Active IQ encontrará la siguiente información sobre su sistema:

- Número de nodos y estado de los nodos: sano, fuera de línea o con fallos.
- Representación gráfica del uso de CPU y memoria, y de la limitación de nodos.
- 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 de las máquinas virtuales

Para obtener más información sobre SolidFire Active IQ, consulte la ["Documentación de SolidFire Active IQ"](#).

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- [Sitio de soporte de NetApp > Herramientas para Active IQ](#)

Trabajar con el nodo de gestión

Descripción general del nodo de gestión

Puede utilizar el nodo de administración (mNode) para usar los servicios del sistema, administrar 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 resolución de problemas.



Como práctica recomendada, asocie solo un nodo de administración con una instancia de VMware vCenter y evite definir los mismos recursos de almacenamiento y computación o instancias de vCenter en varios nodos de administración.

Para los clústeres que ejecutan la versión 11.3 o posterior del software Element, puede trabajar con el nodo de administración utilizando una de las dos interfaces siguientes:

- Con la interfaz de usuario del nodo de administración([https://\[mNode IP\]:442](https://[mNode IP]:442)), puede realizar cambios en la configuración de red y clúster, ejecutar pruebas del sistema o utilizar utilidades del sistema.
- Con la interfaz de usuario de la API REST integrada([https://\[mNode IP\]/mnode](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 del nivel de servicio o la administración de activos.

Instalar o recuperar un nodo de administración:

- ["Instalar un nodo de administración"](#)
- ["Configurar un controlador de interfaz de red \(NIC\) de almacenamiento"](#)
- ["Recuperar un nodo de administración"](#)

Acceda al nodo de administración:

- ["Acceda al nodo de administración \(interfaz de usuario o API REST\)."](#)

Cambiar el certificado SSL predeterminado:

- ["Cambiar el certificado SSL predeterminado del nodo de administración"](#)

Realizar tareas con la interfaz de usuario del nodo de administración:

- ["Descripción general de la interfaz de usuario del nodo de administración"](#)

Realizar tareas con las API REST del nodo de gestión:

- ["Descripción general de la interfaz de usuario de la API REST del nodo de administración"](#)

Deshabilite o habilite la funcionalidad SSH remota o inicie una sesión de túnel de soporte remoto con el Soporte de NetApp para ayudarle a solucionar problemas:

- ["Acceso a nodos de almacenamiento mediante SSH para la resolución de problemas básicos"](#)
 - ["Habilitar conexiones remotas de soporte de NetApp"](#)
 - ["Gestionar la funcionalidad SSH en el nodo de administración"](#)

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Instalar o recuperar un nodo de administración

Instalar un nodo de administración

Puede instalar manualmente el nodo de administración para su clúster que ejecuta el software NetApp Element utilizando la imagen adecuada para su configuración.

Este proceso manual está destinado a los administradores de almacenamiento all-flash SolidFire que no utilizan el motor de implementación de NetApp para la instalación del nodo de administración.

Antes de empezar

- Su versión de clúster ejecuta el software NetApp Element 11.3 o posterior.
- Su instalación utiliza IPv4. El nodo de gestión 11.3 no admite IPv6.



Si necesita compatibilidad con IPv6, puede usar el nodo de administración 11.1.

- Tiene usted permiso para descargar software del sitio de soporte de NetApp .
- Has identificado el tipo de imagen de nodo de administración correcto para tu plataforma:

Plataforma	tipo de imagen de instalación
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

- (Nodo de administración 12.0 y posteriores con servidor proxy) Ha actualizado NetApp Hybrid Cloud Control a la versión 2.16 de los servicios de administración 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 implementaciones existentes.

Antes de seguir este procedimiento, debe comprender ["Volúmenes persistentes"](#) y si desea utilizarlos o no. Los volúmenes persistentes son opcionales, pero se recomiendan para la recuperación de datos de configuración del nodo de administración en caso de pérdida de una máquina virtual (VM).

Paso 1: Descargue la ISO o el archivo OVA e implemente la máquina virtual.

Descargue la ISO o OVA apropiada del sitio de soporte de NetApp e instale la máquina virtual.

Pasos

1. Descarga el archivo OVA o ISO para tu instalación desde el "[Software Element](#)" página en el sitio de soporte de NetApp .
 - a. Seleccione **Descargar la última versión** y acepte el CLUF.
 - b. Seleccione la imagen del nodo de administración que desea descargar.
2. Si descargaste el archivo OVA, sigue estos pasos:
 - a. Despliegue el OVA.
 - b. Si su clúster de almacenamiento está en una subred separada de su nodo de administración (eth0) y desea utilizar volúmenes persistentes, agregue un segundo controlador de interfaz de red (NIC) a la máquina virtual en la subred de almacenamiento (por ejemplo, eth1) o asegúrese de que la red de administración pueda enrutar a la red de almacenamiento.
3. Si descargaste la imagen ISO, sigue estos pasos:
 - a. Crea una nueva máquina virtual de 64 bits desde tu hipervisor con la siguiente configuración:
 - Seis CPU virtuales
 - 24 GB de RAM
 - Tipo de adaptador de almacenamiento configurado como LSI Logic Parallel



El valor predeterminado para su nodo de administración podría ser LSI Logic SAS. En la ventana **Nueva máquina virtual**, verifique 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, aprovisionamiento ligero
- Una interfaz de red virtual con acceso a Internet y acceso al almacenamiento MVIP.
- (Opcional) Una interfaz de red virtual con acceso de red de administración al clúster de almacenamiento. Si su clúster de almacenamiento está en una subred separada de su nodo de administración (eth0) y desea utilizar volúmenes persistentes, agregue un segundo controlador de interfaz de red (NIC) a la máquina virtual en la subred de almacenamiento (eth1) o asegúrese de que la red de administración pueda enrutar a la red de almacenamiento.



No encienda la máquina virtual antes del paso que indica que debe hacerlo más adelante en este procedimiento.

- b. Adjunte la imagen ISO a la máquina virtual e inicie desde la imagen de instalación .iso.



La instalación de un nodo de administración utilizando la imagen podría provocar una demora de 30 segundos antes de que aparezca la pantalla de inicio.

4. Encienda la máquina virtual del nodo de administración una vez finalizada la instalación.

Paso 2: Cree el nodo de administración admin y configure la red.

Una vez finalizada la instalación de la máquina virtual, cree el usuario administrador del nodo de administración y configure la red del nodo de administración.

Pasos

1. Utilizando la interfaz de usuario de terminal (TUI), cree un usuario administrador de nodo de gestión.



Para desplazarse por las opciones del menú, pulse las teclas de flecha arriba o abajo. Para desplazarse por los botones, pulse Tab. Para pasar de los botones a los campos, pulse Tab. Para navegar entre los campos, pulse las teclas de flecha arriba o abajo.

2. Si existe en la red un servidor DHCP (Protocolo de configuración dinámica de host) 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 administración en una red vSphere sin DHCP, como iSCSI.
 - b. Reinicie la máquina virtual o reinicie la red de la máquina virtual.
 - c. Utilizando la TUI, configure la IP correcta en la red de administración con una MTU mayor o igual a 1500 bytes.
 - d. Reasigna la red de máquina virtual correcta a la máquina virtual.



Un servidor DHCP que asigna direcciones IP con una MTU inferior a 1500 bytes puede impedirle configurar la red del nodo de administración o utilizar la interfaz de usuario del nodo de administración.

3. Configure la red del nodo de administración (eth0).



Si necesita una NIC adicional para aislar el tráfico de almacenamiento, consulte las instrucciones para configurar otra NIC: "[Configurar un controlador de interfaz de red \(NIC\) de almacenamiento](#)".

Paso 3: Configurar la sincronización horaria

Antes de configurar el nodo de administración, sincronice la hora entre el nodo de administración y el clúster de almacenamiento.

Pasos

1. Verifique que la hora esté sincronizada entre el nodo de administración 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 administración 12.3.1, proceda a [subpaso \(f\)](#) para completar la configuración de sincronización horaria.

1. Inicie sesión en el nodo de administración mediante SSH o la consola proporcionada por su hipervisor.
2. Detengan a NTPD:

```
sudo service ntpd stop
```

3. Edita el archivo de configuración NTP `/etc/ntp.conf` :
 - a. Comenta las líneas de los servidores predeterminados (`server 0.gentoo.pool.ntp.org`) añadiendo un `#` Delante de cada uno.
 - b. Agregue una nueva línea por cada servidor de hora predeterminado que desee agregar. Los servidores de hora predeterminados deben ser los mismos servidores NTP que se utilizan en el clúster

de almacenamiento que 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 haya terminado.

4. Fuerza una sincronización NTP con el servidor recién agregado.

```
sudo ntpd -gq
```

5. Reinicie NTPD.

```
sudo service ntpd start
```

6. Deshabilitar la sincronización horaria con el host a través del hipervisor (el siguiente es un ejemplo de VMware):



Si implementa el mNode en un entorno de hipervisor distinto de VMware, por ejemplo, desde la imagen .iso en un entorno Openstack, consulte la documentación del hipervisor para obtener los comandos equivalentes.

a. Desactivar la sincronización horaria periódica:

```
vmware-toolbox-cmd timesync disable
```

b. Mostrar y confirmar el estado actual del servicio:

```
vmware-toolbox-cmd timesync status
```

c. En vSphere, verifique que el Synchronize guest time with host La casilla está desmarcada en las opciones de la máquina virtual.



No habilite esta opción si va a realizar cambios en la máquina virtual en el futuro.



No edite el NTP después de completar la configuración de sincronización horaria, ya que esto afecta al NTP cuando se ejecuta. [comando de configuración](#) en el nodo de gestión.

Paso 4: Configurar el nodo de administración

Configure el nodo de administración utilizando el `setup-mnode` dominio.

Pasos

1. Configure y ejecute el comando de configuración del nodo de administración:



Se le solicitará que introduzca las contraseñas en una ventana segura. Si su clúster está detrás de un servidor proxy, debe configurar los ajustes del proxy para poder acceder a una red pública.

```
sudo /sf/packages/mnode/setup-mnode --mnode_admin_user [username]
--storage_mvip [mvip] --storage_username [username] --telemetry_active
[true]
```

- a. Reemplace el valor entre corchetes [] (incluidos los corchetes) para cada uno de los siguientes parámetros obligatorios:



La forma abreviada del nombre del comando está entre paréntesis () y puede sustituir al nombre completo.

- **--mnode_admin_user (-mu) [nombre de usuario]**: El nombre de usuario para la cuenta de administrador del nodo de administración. Es probable que este sea el nombre de usuario de la cuenta de usuario que utilizó para iniciar sesión en el nodo de administración.
 - **--storage_mvip (-sm) [dirección MVIP]**: La dirección IP virtual de administración (MVIP) del clúster de almacenamiento que ejecuta el software Element. Configure el nodo de administración con el mismo clúster de almacenamiento que utilizó durante [Configuración de servidores NTP](#).
 - **--storage_username (-su) [nombre de usuario]**: El nombre de usuario del administrador del clúster de almacenamiento para el clúster especificado por el `--storage_mvip` parámetro.
 - **--telemetry_active (-t) [true]**: Conserva el valor verdadero que habilita la recopilación de datos para análisis por parte de Active IQ.
- b. (Opcional): Agregue los parámetros del punto final de Active IQ al comando:
 - **--remote_host (-rh) [AIQ_endpoint]**: El punto final donde se envían los datos de telemetría de Active IQ para su procesamiento. Si no se incluye el parámetro, se utiliza el punto de conexión predeterminado.
 - c. (Recomendado): Agregue los siguientes parámetros de volumen persistente. No modifique ni elimine la cuenta ni los volúmenes creados para la funcionalidad de volúmenes persistentes, ya que se producirá una pérdida de la capacidad de administración.
 - **--use_persistent_volumes (-pv) [true/false, valor predeterminado: false]**: Habilita o deshabilita los volúmenes persistentes. Introduzca el valor "true" para habilitar la funcionalidad de volúmenes persistentes.
 - **--persistent_volumes_account (-pva) [nombre_de_cuenta]**: Si `--use_persistent_volumes` está configurado como verdadero, utilice este parámetro e introduzca el nombre de la cuenta de almacenamiento que se utilizará para los volúmenes persistentes.



Utilice un nombre de cuenta único para los volúmenes persistentes que sea diferente de cualquier nombre de cuenta existente en el clúster. Es de vital importancia mantener la cuenta de volúmenes persistentes separada del resto de su 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 utilizará con volúmenes persistentes. Esto solo es necesario si el nodo de administración gestiona varios clústeres de almacenamiento. Si no se administran varios clústeres, se utilizará el MVIP de clúster predeterminado.

d. Configurar un servidor proxy:

- **--use_proxy (-up) [true/false, default: false]**: Habilita o deshabilita el uso del proxy. Este parámetro es necesario para configurar un servidor proxy.
- **--proxy_hostname_or_ip (-pi) [host]**: El nombre de host o IP del proxy. Esto es necesario si quieres usar un proxy. Si especifica esto, se le pedirá que ingrese la información. `--proxy_port`.
- **--proxy_username (-pu) [nombre de usuario]**: El nombre de usuario del proxy. Este parámetro es opcional.
- **--proxy_password (-pp) [contraseña]**: La contraseña del proxy. Este parámetro es opcional.
- **--proxy_port (-pq) [puerto, valor predeterminado: 0]**: El puerto proxy. Si especifica esto, se le pedirá que introduzca el nombre de host o la IP del proxy. (`--proxy_hostname_or_ip`).
- **--proxy_ssh_port (-ps) [puerto, predeterminado: 443]**: El puerto proxy SSH. Por defecto, se utiliza el puerto 443.

e. (Opcional) Utilice la ayuda de parámetros si necesita información adicional sobre cada parámetro:

- **--help (-h)**: Devuelve información sobre cada parámetro. Los parámetros se definen como obligatorios u opcionales en función del despliegue inicial. Los requisitos de los parámetros de actualización y reimplementación pueden variar.

f. Ejecutar el `setup-mnode` dominio.

Paso 5: Configurar los recursos del controlador

Localice el ID de instalación y agregue un recurso de controlador de vCenter.

Pasos

1. Localice el ID de instalación:

- a. Desde un navegador, inicie sesión en la interfaz de usuario de la API REST del nodo de administración:
- b. Vaya al MVIP de almacenamiento e inicie sesión. Esta acción hará que el certificado sea aceptado para el siguiente paso.
- c. Abra la interfaz de usuario de la API REST del servicio de inventario en el nodo de administración:

```
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 del cliente como `mnode-client`.
- iii. Seleccione **Autorizar** para iniciar una sesión.
- e. Desde la interfaz de usuario de la API REST, seleccione **GET /installations**.
- f. Seleccione **Probarlo**.
- g. Seleccione **Ejecutar**.
- h. Del cuerpo de la respuesta con código 200, copie y guarde el `id` para la instalación para su uso en un paso posterior.

Su instalación tiene una configuración de activos base que se creó durante la instalación o actualización.

2. Agregue un recurso de controlador de vCenter para NetApp Hybrid Cloud Control a los recursos conocidos del nodo de administración:

- a. Acceda a la interfaz de usuario de la API del servicio mnode en el nodo de administración introduciendo la dirección IP del nodo de administración seguida de `/mnode`:

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

- b. Seleccione **Autorizar** o cualquier icono de candado y complete lo siguiente:

- i. Introduzca el nombre de usuario y la contraseña del clúster.
- ii. Introduzca el ID del cliente como `mnode-client`.
- iii. Seleccione **Autorizar** para iniciar una sesión.
- iv. Cerrar la ventana.

- c. Seleccione **POST /assets/{asset_id}/controllers** para agregar un sub-recurso de controlador.



Deberá crear un nuevo rol de NetApp HCC en vCenter para agregar un subactivo de controlador. Esta nueva función de NetApp HCC limitará la vista de servicios del nodo de administración a activos exclusivos de NetApp. Ver ["Cree un rol de NetApp HCC en vCenter."](#)

- d. Seleccione **Probarlo**.
- e. Introduzca el ID del recurso base principal que copió al portapapeles en el campo **asset_id**.
- f. Introduzca los valores de carga útil requeridos con el tipo `vCenter` y las credenciales de vCenter.
- g. Seleccione **Ejecutar**.

Encuentra más información

- ["Volúmenes persistentes"](#)
- ["Agregar un activo de controlador al nodo de administración"](#)
- ["Configure una NIC de almacenamiento."](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Cree un rol de NetApp HCC en vCenter.

Deberá crear un rol de NetApp HCC en vCenter para agregar manualmente activos de vCenter (controladores) al nodo de administración después de la instalación o para modificar los controladores existentes.

Esta función de NetApp HCC limita la vista de servicios del nodo de administración a activos exclusivos de NetApp.

Acerca de esta tarea

- Este procedimiento describe los pasos disponibles en la versión 6.7 de vSphere. La interfaz de usuario de vSphere puede diferir ligeramente de la descrita, dependiendo de la versión de vSphere instalada. Para obtener ayuda adicional, consulte la documentación de VMware vCenter.
- A ["crear un nuevo rol de NetApp HCC"](#) Primero, debes configurar una nueva cuenta de usuario en vCenter, crear un rol de NetApp HCC y, a continuación, asignar los permisos de usuario.
- Para las configuraciones de host NetApp ESXi, debe actualizar la cuenta de usuario creada por NDE al nuevo rol de NetApp HCC:
 - Usar ["esta opción"](#) Si su host NetApp ESXi no existe dentro de un clúster de hosts de vCenter
 - Usar ["esta opción"](#) Si su host NetApp ESXi se encuentra dentro de un clúster de hosts de vCenter
- Puede ["configurar un recurso de controlador"](#) que ya existe en el nodo de gestión.
- Utilice el nuevo rol de NetApp HCC para ["agregar un activo"](#) al nodo de gestión.

Crear un nuevo rol de NetApp HCC

Configure una nueva cuenta de usuario en vCenter, cree un rol de NetApp HCC y, a continuación, asigne los permisos de usuario.

Configurar una nueva cuenta de usuario en vCenter

Siga los siguientes pasos para configurar una nueva cuenta de usuario en vCenter.

Pasos

1. Inicie sesión en el cliente web de vSphere como `administrator@vsphere.local` o equivalente.
2. Desde el menú, seleccione **Administración**.
3. En la sección **Inicio de sesión único**, seleccione **Usuarios y Grupos**.
4. En la lista **Dominio**, seleccione `vsphere.local` o su dominio LDAP.
5. Seleccione **Agregar usuario**.
6. Complete el formulario **Agregar usuario**.

Cree un nuevo rol de NetApp HCC en vCenter.

Realice los siguientes pasos para crear un nuevo rol de NetApp HCC en vCenter.

Pasos

1. Seleccione **Editar rol** y asigne los permisos necesarios.
2. En el panel de navegación izquierdo, seleccione **Global**.
3. Seleccione **Diagnóstico y Licencias**.

4. En el panel de navegación izquierdo, seleccione **Hosts**.
5. Seleccione **Mantenimiento, Energía, Configuración de partición de almacenamiento y Firmware**.
6. Guardar como NetApp Role .

Asignar permisos de usuario a vCenter

Realice los siguientes pasos para asignar los permisos de usuario al nuevo rol de NetApp HCC en vCenter.

Pasos

1. Desde el menú, seleccione **Hosts y Clusters**.
2. En el panel de navegación izquierdo, seleccione una de las siguientes opciones:
 - El vCenter de nivel superior.
 - El vCenter que desee si está en modo vinculado.



- A partir del complemento NetApp Element para vCenter Server 5.0, para usar ["Modo vinculado de vCenter"](#) , registre el complemento Element desde un nodo de administración independiente para cada servidor vCenter que administre clústeres de almacenamiento NetApp SolidFire (recomendado).
- Utilizando el complemento NetApp Element para vCenter Server 4.10 y versiones anteriores para administrar los recursos del clúster desde otros servidores vCenter ["Modo vinculado de vCenter"](#) se limita únicamente a clústeres de almacenamiento local.

3. En el panel de navegación derecho, seleccione **Permisos**.
4. Seleccione el icono **+** para agregar el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccionar `vsphere.local` o su dominio LDAP
- b. Utilice la función de búsqueda para encontrar el nuevo usuario que creó en [Configurar una nueva cuenta de usuario en vCenter](#) .
- c. Seleccionar NetApp Role .



NO seleccione **Propagar a los hijos**.

Add Permission

satyabra-vcenter01.mgmt.ict.openengla... X

User: vsphere.local

Q netapp

Role: NetApp Role

☐ Propagate to children

CANCEL

OK

Asignar permisos de usuario al centro de datos

Realice los siguientes pasos para asignar los permisos de usuario al centro de datos en vCenter.

Pasos

1. En el panel izquierdo, seleccione **Centro de datos**.
2. En el panel de navegación derecho, seleccione **Permisos**.
3. Seleccione el icono + para agregar el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccionar `vsphere.local` o su dominio LDAP.
- b. Utilice la función de búsqueda para encontrar el nuevo usuario de HCC que creó en [Configurar una nueva cuenta de usuario en vCenter](#).
- c. Seleccionar `ReadOnly role`.



NO seleccione **Propagar a los hijos**.

Asignar permisos de usuario a los almacenes de datos de NetApp HCI

Realice los siguientes pasos para asignar los permisos de usuario a los almacenes de datos de NetApp HCI en vCenter.

Pasos

1. En el panel izquierdo, seleccione **Centro de datos**.

2. Crea una nueva carpeta de almacenamiento. Haz clic con el botón derecho en **Centro de datos** y selecciona **Crear carpeta de almacenamiento**.
3. Transfiere todos los almacenes de datos de NetApp HCI desde el clúster de almacenamiento y el nodo de cómputo local a la nueva carpeta de almacenamiento.
4. Seleccione la nueva carpeta de almacenamiento.
5. En el panel de navegación derecho, seleccione **Permisos**.
6. Seleccione el icono **+** para agregar el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccionar `vsphere.local` o su dominio LDAP.
- b. Utilice la función de búsqueda para encontrar el nuevo usuario de HCC que creó en [Configurar una nueva cuenta de usuario en vCenter](#).
- c. Seleccionar `Administrator role`
- d. Seleccione **Propagar a los hijos**.

Asignar permisos de usuario a un clúster de hosts NetApp

Realice los siguientes pasos para asignar los permisos de usuario a un clúster de hosts NetApp en vCenter.

Pasos

1. En el panel de navegación izquierdo, seleccione el clúster de host de NetApp.
2. En el panel de navegación derecho, seleccione **Permisos**.
3. Seleccione el icono **+** para agregar el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccionar `vsphere.local` o su dominio LDAP.
- b. Utilice la función de búsqueda para encontrar el nuevo usuario de HCC que creó en [Configurar una nueva cuenta de usuario en vCenter](#).
- c. Seleccionar `NetApp Role` o `Administrator`.
- d. Seleccione **Propagar a los hijos**.

Configuraciones de host NetApp ESXi

Para las configuraciones de host NetApp ESXi, debe actualizar la cuenta de usuario creada por NDE al nuevo rol de NetApp HCC.

El host NetApp ESXi no existe en un clúster de hosts de vCenter.

Si el host NetApp ESXi no existe dentro de un clúster de hosts de vCenter, puede utilizar el siguiente procedimiento para asignar el rol de NetApp HCC y los permisos de usuario en vCenter.

Pasos

1. Desde el menú, seleccione **Hosts y Clusters**.
2. En el panel de navegación izquierdo, seleccione el host NetApp ESXi.
3. En el panel de navegación derecho, seleccione **Permisos**.

4. Seleccione el icono **+** para agregar el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccionar `vsphere.local` o su dominio LDAP.
- b. Utilice la función de búsqueda para encontrar el nuevo usuario que creó en [Configurar una nueva cuenta de usuario en vCenter](#).
- c. Seleccionar `NetApp Role` o `Administrator`.

5. Seleccione **Propagar a los hijos**.

El host NetApp ESXi existe en un clúster de hosts de vCenter.

Si existe un host NetApp ESXi dentro de un clúster de hosts vCenter con otros hosts ESXi de proveedores, puede utilizar el siguiente procedimiento para asignar el rol HCC de NetApp y los permisos de usuario en vCenter.

1. Desde el menú, seleccione **Hosts y Clusters**.
2. En el panel de navegación izquierdo, expanda el clúster host deseado.
3. En el panel de navegación derecho, seleccione **Permisos**.
4. Seleccione el icono **+** para agregar el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccionar `vsphere.local` o su dominio LDAP.
- b. Utilice la función de búsqueda para encontrar el nuevo usuario que creó en [Configurar una nueva cuenta de usuario en vCenter](#).
- c. Seleccionar `NetApp Role`.



NO seleccione **Propagar a los hijos**.

5. En el panel de navegación izquierdo, seleccione un host NetApp ESXi.
6. En el panel de navegación derecho, seleccione **Permisos**.
7. Seleccione el icono **+** para agregar el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccionar `vsphere.local` o su dominio LDAP.
- b. Utilice la función de búsqueda para encontrar el nuevo usuario que creó en [Configurar una nueva cuenta de usuario en vCenter](#).
- c. Seleccionar `NetApp Role` o `Administrator`.
- d. Seleccione **Propagar a los hijos**.

8. Repita el procedimiento para los hosts NetApp ESXi restantes en el clúster de hosts.

El activo del controlador ya existe en el nodo de administración.

Si ya existe un controlador en el nodo de administración, siga los siguientes pasos para configurarlo mediante `PUT /assets /{asset_id} /controllers /{controller_id}`.

Pasos

1. Acceda a la interfaz de usuario de la API del servicio mnode en el nodo de administración:

<https://<ManagementNodeIP>/mnode>

2. Seleccione **Autorizar** e introduzca las credenciales para acceder a las llamadas a la API.
3. Seleccionar GET /assets para obtener el ID del padre.
4. Seleccionar PUT /assets /{asset_id} /controllers /{controller_id} .
 - a. Introduzca las credenciales creadas en la configuración de la cuenta en el cuerpo de la solicitud.

Agregar un activo al nodo de administración

Si necesita agregar manualmente un nuevo recurso después de la instalación, utilice la nueva cuenta de usuario de HCC que creó en [Configurar una nueva cuenta de usuario en vCenter](#) . Para obtener más información, consulte ["Agregar un activo de controlador al nodo de administración"](#).

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Configurar un controlador de interfaz de red (NIC) de almacenamiento

Si está utilizando una NIC adicional para almacenamiento, puede conectarse mediante SSH al nodo de administración o utilizar la consola de vCenter y ejecutar un comando curl para configurar una interfaz de red etiquetada o no etiquetada.

Antes de empezar

- Conoces tu dirección IP eth0.
- Su versión de clúster ejecuta el software NetApp Element 11.3 o posterior.
- Has implementado un nodo de administración versión 11.3 o posterior.

Opciones de configuración

Elige la opción que sea relevante para tu entorno:

- [Configure un controlador de interfaz de red \(NIC\) de almacenamiento para una interfaz de red sin etiquetar.](#)
- [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 etiquetar.

Pasos

1. Abra una consola SSH o vCenter.
2. Sustituya los valores en la siguiente plantilla de comando y ejecute el comando:



Los valores están representados por \$ para cada uno de los parámetros requeridos para su nueva interfaz de red de almacenamiento. El `cluster` El objeto de la siguiente plantilla es obligatorio y se puede utilizar para cambiar el nombre del host del nodo de administración. `--insecure` o `-k` Estas opciones no deben utilizarse 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 en la siguiente plantilla de comando y ejecute el comando:



Los valores están representados por \$ para cada uno de los parámetros requeridos para su nueva interfaz de red de almacenamiento. El `cluster` El objeto de la siguiente plantilla es obligatorio y se puede utilizar para cambiar el nombre del host del nodo de administración. `--insecure` o `-k` Estas opciones no deben utilizarse 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"
}
'

```

Encuentra más información

- ["Agregar un activo de controlador al nodo de administración"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Recuperar un nodo de administración

Puede recuperar y volver a implementar manualmente el nodo de administración para su clúster que ejecuta el software NetApp Element si su nodo de administración anterior utilizaba volúmenes persistentes.

Puede implementar un nuevo OVA y ejecutar un script de reimplementación para extraer datos de configuración de un nodo de administración previamente instalado que ejecute la versión 11.3 o posterior.

Lo que necesitarás

- Su nodo de administración anterior ejecutaba el software NetApp Element versión 11.3 o posterior con "[Volúmenes persistentes](#)" Funcionalidad activada.
- Conoces la MVIP y la SVIP del clúster que contiene los volúmenes persistentes.
- Su versión de clúster ejecuta el software NetApp Element 11.3 o posterior.
- Su instalación utiliza IPv4. El nodo de gestión 11.3 no admite IPv6.
- Tiene usted permiso para descargar software del sitio de soporte de NetApp .
- Has identificado el tipo de imagen de nodo de administración correcto para tu plataforma:

Plataforma	tipo de imagen de instalación
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

Pasos

1. [Descarga la ISO o el archivo OVA e implementa la máquina virtual.](#)
2. [Configurar la red](#)
3. [Configurar la sincronización horaria](#)
4. [Configurar el nodo de administración](#)

Descarga la ISO o el archivo OVA e implementa la máquina virtual.

1. Descarga el archivo OVA o ISO para tu instalación desde el "[Software Element](#)" página en el sitio de soporte de NetApp .
 - a. Seleccione **Descargar la última versión** y acepte el CLUF.
 - b. Seleccione la imagen del nodo de administración que desea descargar.
2. Si descargaste el archivo OVA, sigue estos pasos:
 - a. Despliegue el OVA.
 - b. Si su clúster de almacenamiento está en una subred separada de su nodo de administración (eth0) y desea utilizar volúmenes persistentes, agregue un segundo controlador de interfaz de red (NIC) a la máquina virtual en la subred de almacenamiento (por ejemplo, eth1) o asegúrese de que la red de administración pueda enrutar a la red de almacenamiento.
3. Si descargaste la imagen ISO, sigue estos pasos:
 - a. Cree una nueva máquina virtual de 64 bits desde su hipervisor con la siguiente configuración:
 - Seis CPU virtuales
 - 24 GB de RAM
 - Disco virtual de 400 GB, aprovisionamiento ligero
 - Una interfaz de red virtual con acceso a Internet y acceso al almacenamiento MVIP.
 - (Opcional para el almacenamiento all-flash SolidFire) Una interfaz de red virtual con acceso de red de administración al clúster de almacenamiento. Si su clúster de almacenamiento está en una

subred separada de su nodo de administración (eth0) y desea utilizar volúmenes persistentes, agregue un segundo controlador de interfaz de red (NIC) a la máquina virtual en la subred de almacenamiento (eth1) o asegúrese de que la red de administración pueda enrutar a la red de almacenamiento.



No encienda la máquina virtual antes del paso que indica que debe hacerlo más adelante en este procedimiento.

b. Adjunte la imagen ISO a la máquina virtual e inicie desde la imagen de instalación .iso.



La instalación de un nodo de administración utilizando la imagen podría provocar una demora de 30 segundos antes de que aparezca la pantalla de inicio.

4. Encienda la máquina virtual del nodo de administración una vez finalizada la instalación.

Configurar la red

1. Utilizando la interfaz de usuario de terminal (TUI), cree un usuario administrador de nodo de gestión.



Para desplazarse por las opciones del menú, pulse las teclas de flecha arriba o abajo. Para desplazarse por los botones, pulse Tab. Para pasar de los botones a los campos, pulse Tab. Para navegar entre los campos, pulse las teclas de flecha arriba o abajo.

2. Configure la red del nodo de administración (eth0).



Si necesita una NIC adicional para aislar el tráfico de almacenamiento, consulte las instrucciones para configurar otra NIC: "[Configurar un controlador de interfaz de red \(NIC\) de almacenamiento](#)".

Configurar la sincronización horaria

1. Verifique que la hora esté sincronizada entre el nodo de administración 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 administración 12.3.1 o posterior, continúe con [subpaso \(f\)](#) para completar la configuración de sincronización horaria.

1. Inicie sesión en el nodo de administración mediante SSH o la consola proporcionada por su hipervisor.

2. Detengan a NTPD:

```
sudo service ntpd stop
```

3. Edita el archivo de configuración NTP /etc/ntp.conf :

a. Comenta las líneas de los servidores predeterminados.(server 0.gentoo.pool.ntp.org) añadiendo un # Delante de cada uno.

b. Agregue una nueva línea por cada servidor de hora predeterminado que desee agregar. Los servidores de hora predeterminados deben ser los mismos servidores NTP que se utilizan en el clúster

de almacenamiento que 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 haya terminado.

4. Fuerza una sincronización NTP con el servidor recién agregado.

```
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 de VMware, por ejemplo, desde la imagen .iso en un entorno Openstack, consulte la documentación del hipervisor para obtener los comandos equivalentes.

a. Desactivar la sincronización horaria periódica:

```
vmware-toolbox-cmd timesync disable
```

b. Mostrar y confirmar el estado actual del servicio:

```
vmware-toolbox-cmd timesync status
```

c. En vSphere, verifique que el Synchronize guest time with host La casilla está desmarcada en las opciones de la máquina virtual.



No habilite esta opción si va a realizar cambios en la máquina virtual en el futuro.



No edite el NTP después de completar la configuración de sincronización horaria, ya que esto afecta al NTP cuando se ejecuta. [comando de redesplicue](#) en el nodo de gestión.

Configurar el nodo de administración

1. Cree un directorio de destino temporal para el contenido del paquete de servicios de administración:

```
mkdir -p /sf/etc/mnode/mnode-archive
```

2. Descargue el paquete de servicios de administración (versión 2.15.28 o posterior) que se instaló previamente en el nodo de administración existente y guárdelo en el `/sf/etc/mnode/` directorio.
3. Extraiga el paquete descargado utilizando el siguiente comando, reemplazando el valor entre corchetes `[]` (incluidos los corchetes) con el nombre del archivo del paquete:

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle file]
```

4. Extraiga el archivo resultante a la `/sf/etc/mnode-archive` directorio:

```
tar -C /sf/etc/mnode/mnode-archive -xvf /sf/etc/mnode/services_deploy_bundle.tar.gz
```

5. Cree 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. Reemplace el valor entre corchetes `[]` (incluidos los corchetes) para cada uno de los siguientes parámetros obligatorios:

- **[dirección IP mvip]:** La dirección IP virtual de administración del clúster de almacenamiento. Configure el nodo de administración con el mismo clúster de almacenamiento que utilizó durante ["Configuración de servidores NTP"](#).
- **[nombre de cuenta de volumen persistente]:** El nombre de la cuenta asociada con todos los volúmenes persistentes en este clúster de almacenamiento.

1. Configure y ejecute el comando de reimplementación del nodo de administración para conectarse a los volúmenes persistentes alojados en el clúster e iniciar los servicios con los datos de configuración del nodo de administración anterior:



Se le solicitará que introduzca las contraseñas en una ventana segura. Si su clúster está detrás de un servidor proxy, debe configurar los ajustes del proxy para poder acceder a una red pública.

```
sudo /sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
```

- a. Reemplace el valor entre corchetes [] (incluidos los corchetes) con el nombre de usuario de la cuenta de administrador del nodo de administración. Es probable que este sea el nombre de usuario de la cuenta de usuario que utilizó para iniciar sesión en el nodo de administración.



Puedes añadir el nombre de usuario o permitir que el script te solicite la información.

- b. Ejecutar el `redploy-mnode` dominio. El script muestra un mensaje de éxito cuando se completa el redesplicue.
- c. Si accede a las interfaces web de Element (como el nodo de administración o NetApp Hybrid Cloud Control) utilizando el nombre de dominio completo (FQDN) del sistema, ["reconfigurar la autenticación para el nodo de administración"](#).



Capacidad 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 administración que ejecutan servicios de administración 2.18 y posteriores. Si previamente habías habilitado la funcionalidad SSH en el nodo de administración, es posible que necesites ["Deshabilitar SSH nuevamente"](#) en el nodo de gestión recuperado.

Encuentra más información

- ["Volúmenes persistentes"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Acceda al nodo de administración

A partir de la versión 11.3 del software NetApp Element, el nodo de administración contiene dos interfaces de usuario: una interfaz de usuario para administrar servicios basados en REST y una interfaz de usuario por nodo para administrar la configuración de red y clúster, así como las pruebas y utilidades del sistema operativo.

Para clústeres que ejecutan la versión 11.3 o posterior del software Element, puede utilizar una de las dos interfaces siguientes:

- Mediante la interfaz de usuario del nodo de administración. ([https:// \[mNode IP\]:442](https://[mNode IP]:442)), puede realizar cambios en la configuración de red y clúster, ejecutar pruebas del sistema o utilizar utilidades del sistema.
- Mediante la interfaz de usuario de la API REST integrada. ([https:// \[mNode IP\]/mnode](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 del nivel de servicio o la administración de activos.

Acceda a la interfaz de usuario de administración por nodo.

Desde la interfaz de usuario de cada nodo, puede acceder a la configuración de red y clúster, y utilizar pruebas y utilidades del sistema.

Pasos

1. Acceda a la interfaz de usuario por nodo para el nodo de administración ingresando la dirección IP del nodo de administración seguida de :442.

```
https://[IP address]:442
```

NetApp

Support and Documentation Enable Debug Info: Requests Responses Logout

Network Settings Cluster Settings System Tests System Utilities

Management

Network Settings - Management

Method : static

Link Speed : 1000

IPv4 Address : 10.117.148.201

IPv4 Subnet Mask : 255.255.248.0

IPv4 Gateway Address : 10.117.131.234

IPv6 Address :

IPv6 Gateway Address :

MTU : 1500

DNS Servers : 10.117.20.40, 10.116.133.40

Search Domains : den.sclloffe.net, ora.den.sclloffe

Status : UpAndRunning

Routes

+ Add

Reset Changes Save Changes

2. Introduzca el nombre de usuario y la contraseña del nodo de administración cuando se le solicite.

Acceda a la interfaz de usuario de la API REST del nodo de administración.

Desde la interfaz de usuario de la API REST, puede acceder a un menú de API relacionadas con el servicio que controlan los servicios de administración en el nodo de administración.

Pasos

1. Para acceder a la interfaz de usuario de la API REST para los servicios de administración, ingrese la dirección IP del nodo de administración seguida de `/mnode` :

```
https://[IP address]/mnode
```

MANAGEMENT SERVICES API ^{4.0}

[Base URL: /mnode]
https://10.117.1.100/mnode/swagger/json

The configuration REST service for MANAGEMENT SERVICES

NetApp - Website

NetApp Commercial Software License

Authorize 

logs Log service

GET /logs Get logs from the MNODE service(s)

assets Asset service

POST /assets Add a new asset

GET /assets Get all assets

GET /assets/compute-nodes Get all compute nodes

GET /assets/compute-nodes/{compute_node_id} Get a specific compute node by ID

GET /assets/controllers Get all controllers

GET /assets/controllers/{controller_id} Get a specific controller by ID

GET /assets/storage-clusters Get all storage clusters

GET /assets/storage-clusters/{storage_cluster_id} Get a specific storage cluster by ID

PUT /assets/{asset_id} Modify an asset with a specific ID

DELETE /assets/{asset_id} Delete an asset with a specific ID

GET /assets/{asset_id} Get an asset by it's ID

POST /assets/{asset_id}/compute-nodes Add a compute asset

GET /assets/{asset_id}/compute-nodes Get compute assets

PUT /assets/{asset_id}/compute-nodes/{compute_id} Update a specific compute node asset

DELETE /assets/{asset_id}/compute-nodes/{compute_id} Delete a specific compute node asset

2. Seleccione **Autorizar** o cualquier icono de candado e introduzca las credenciales de administrador del clúster para obtener permisos para usar las API.

Encuentra más información

- ["Habilitar Active IQ y la monitorización de NetApp"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Cambiar el certificado SSL predeterminado del nodo de administración

Puede cambiar el certificado SSL y la clave privada predeterminados del nodo de administración mediante la API de NetApp Element .

Cuando configura un nodo de administración, se crea un certificado Secure Sockets Layer (SSL) autofirmado

único y una clave privada que se utiliza para toda la comunicación 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 emitidos y verificados por una Autoridad de Certificación (CA) de confianza.

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

- **Obtener certificado SSL del nodo**

Puedes usar el "[Método GetNodeSSLCertificate](#)" Para recuperar información sobre el certificado SSL actualmente instalado, incluyendo todos los detalles del certificado.

- **Configurar certificado SSL del nodo**

Puedes usar el "[Método SetNodeSSLCertificate](#)" para configurar los certificados SSL del clúster y por nodo con el certificado y la clave privada que usted proporcione. El sistema valida el certificado y la clave privada para evitar que se aplique un certificado no válido.

- **Eliminar certificado SSL del nodo**

Este "[Método RemoveNodeSSLCertificate](#)" Elimina el certificado SSL y la clave privada actualmente instalados. A continuación, el clúster genera un nuevo certificado autofirmado y una clave privada.

Encuentra más información

- "[Cambiar el certificado SSL predeterminado del software Element](#)"
- "[¿Cuáles son los requisitos para configurar certificados SSL personalizados en Element Software?](#)"
- "[Documentación del software SolidFire y Element](#)"
- "[Plugin de NetApp Element para vCenter Server](#)"

Trabajar con la interfaz de usuario del nodo de administración

Descripción general de la interfaz de usuario del nodo de administración

Con la interfaz de usuario del nodo de administración(<https://<ManagementNodeIP>:442>), puede realizar cambios en la configuración de red y clúster, ejecutar pruebas del sistema o utilizar utilidades del sistema.

Tareas que puedes realizar con la interfaz de usuario del nodo de administración:

- "[Configurar la monitorización de alertas](#)"
- "[Modifique y pruebe la configuración de la red, el clúster y el sistema del nodo de administración.](#)"
- "[Ejecutar utilidades del sistema desde el nodo de administración](#)"

Encuentra más información

- "[Acceda al nodo de administración](#)"

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Configurar la monitorización de alertas

Las herramientas de monitorización de alertas están configuradas para la monitorización de alertas de NetApp HCI . Estas herramientas no están configuradas ni se utilizan para el almacenamiento all-flash SolidFire . Al ejecutar las herramientas para estos clústeres se produce el siguiente error 405, lo cual es de esperar dada la configuración:

```
webUIParseError : Invalid response from server. 405
```

Para obtener más información sobre la configuración de la supervisión de alertas para NetApp HCI, consulte ["Configurar la monitorización de alertas"](#)

Modifique y pruebe la configuración de la red, el clúster y el sistema del nodo de administración.

Puede modificar y probar la red del nodo de administración, el clúster y la configuración del sistema.

- [Configuración de red del nodo de administración de actualizaciones](#)
- [Configuración del clúster del nodo de administración de actualizaciones](#)
- [Prueba la configuración del nodo de administración](#)

Configuración de red del nodo de administración de actualizaciones

En la pestaña Configuración de red de la interfaz de usuario del nodo de administración por nodo, puede modificar los campos de la interfaz de red del nodo de administración.

1. Abra la interfaz de usuario del nodo de administración por nodo.
2. Seleccione la pestaña **Configuración de red**.
3. Consulte o introduzca la siguiente información:
 - a. **Método:** Elija uno de los siguientes métodos para configurar la interfaz:
 - **loopback:** Se utiliza para definir la interfaz de bucle invertido IPv4.
 - **manual:** Se utiliza para definir interfaces para las que no se realiza ninguna configuración por defecto.
 - **dhcp:** Se utiliza para obtener una dirección IP mediante 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 para la red eth0.
 - d. **Máscara de subred IPv4:** Subdivisiones de direcciones de la red IPv4.
 - e. **Dirección de puerta de enlace IPv4:** Dirección de red del enrutador para enviar paquetes fuera de la red local.
 - f. **Dirección IPv6:** La dirección IPv6 para 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 la versión 11.3 ni con versiones posteriores del nodo de administración.

- h. **MTU:** Tamaño máximo de paquete que un protocolo de red puede transmitir. Debe ser mayor o igual a 1500. Si agrega una segunda NIC de almacenamiento, el valor debería ser 9000.
- i. **Servidores DNS:** Interfaz de red utilizada para la comunicación del clúster.
- j. **Búsqueda de dominios:** Busca direcciones MAC adicionales disponibles para el sistema.
- k. **Estado:** Valores posibles:
- UpAndRunning
 - Down
 - Up
- l. **Rutas:** Rutas estáticas a hosts o redes específicas a través de la interfaz asociada que las rutas están configuradas para usar.

Configuración del clúster del nodo de administración de actualizaciones

En la pestaña Configuración del clúster de la interfaz de usuario por nodo para el nodo de administración, puede modificar los campos de la interfaz del clúster cuando un nodo se encuentra en los estados Disponible, Pendiente, PendienteActivo y Activo.

1. Abra la interfaz de usuario del nodo de administración por nodo.
2. Seleccione la pestaña **Configuración del clúster**.
3. Consulte o introduzca la siguiente información:
 - **Rol:** Rol que el nodo de gestión tiene en el clúster. Valor posible: `Management`.
 - **Versión:** Versión del software Element que se ejecuta en el clúster.
 - **Interfaz predeterminada:** Interfaz de red predeterminada utilizada para la comunicación del nodo de administración con el clúster que ejecuta el software Element.

Prueba la configuración del nodo de administración

Después de modificar la configuración de administración y de red del nodo de administración y confirmar los cambios, puede ejecutar pruebas para validar los cambios realizados.

1. Abra la interfaz de usuario del nodo de administración por nodo.
2. En la interfaz de usuario del nodo de administración, seleccione **Pruebas del sistema**.
3. Complete cualquiera de las siguientes opciones:
 - a. Para verificar que la configuración de red que configuró es válida para el sistema, seleccione **Probar configuración de red**.
 - b. Para probar la conectividad de red a todos los nodos del clúster en las interfaces de 1G y 10G utilizando paquetes ICMP, seleccione **Probar ping**.
4. Vea o ingrese lo siguiente:
 - **Hosts:** Especifique una lista de direcciones o nombres de host de dispositivos a los que hacer ping,

separados por comas.

- **Intentos:** Especifique el número de veces que el sistema debe repetir el ping de prueba. Valor predeterminado: 5.
- **Tamaño del 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 en milisegundos:** Especifique el número de milisegundos que se esperarán para cada respuesta de ping individual. Valor predeterminado: 500 ms.
- **Tiempo de espera total en segundos:** Especifique el tiempo en segundos que el ping debe esperar una respuesta del sistema antes de realizar el siguiente intento de ping o finalizar el proceso. Valor predeterminado: 5.
- **Prohibir la fragmentación:** Habilite la bandera DF (no fragmentar) para los paquetes ICMP.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Ejecutar utilidades del sistema desde el nodo de administración

Puede utilizar la interfaz de usuario por nodo para el nodo de administración para crear o eliminar paquetes de soporte de clúster, restablecer la configuración del nodo o reiniciar la red.

Pasos

1. Abra la interfaz de usuario del nodo de administración por nodo utilizando las credenciales de administrador del nodo de administración.
2. Seleccione **Utilidades del sistema**.
3. Seleccione el botón de la utilidad que desea ejecutar:
 - a. **Control de energía:** Reinicia, apaga o desconecta el nodo. Especifique cualquiera de las siguientes opciones.



Esta operación provoca una pérdida temporal de la 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 en un clúster. Especifique las siguientes opciones:
 - **Nombre del paquete:** Nombre único para cada paquete de soporte creado. Si no se proporciona ningún nombre, se utilizará "supportbundle" y el nombre del nodo como nombre de archivo.
 - **Mvip:** El Mvip del clúster. Los paquetes se recopilan de todos los nodos del clúster. Este parámetro es obligatorio si no se especifica el parámetro Nodos.
 - **Nodos:** Las direcciones IP de los nodos desde los que se recopilarán los paquetes. Utilice Nodos o Mvip, pero no ambos, para especificar los nodos desde los que recopilar 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 el script continúe ejecutándose si no se pueden recopilar paquetes de uno o más de los nodos.
 - **Argumentos adicionales:** Este parámetro se pasa al `sf_make_support_bundle` guion. Este parámetro solo debe utilizarse a petición del soporte de NetApp .
- c. **Eliminar todos los paquetes de soporte:** Elimina todos los paquetes de soporte actuales en el nodo de administración.
- d. **Restablecer nodo:** Restablece el nodo de administración a una nueva imagen de instalación. Esto restablece todos los ajustes, excepto la configuración de red, al estado predeterminado. Especifique las siguientes opciones:
- **Compilación:** La URL a una imagen de software Element remota a la que se reiniciará el nodo.
 - **Opciones:** Especificaciones para ejecutar las operaciones de reinicio. Si fuera necesario, el soporte de NetApp proporcionará los detalles.



Esta operación provoca una pérdida temporal de la conectividad de red.

- e. **Reiniciar red:** Reinicia todos los servicios de red en el nodo de administración.



Esta operación provoca una pérdida temporal de la conectividad de red.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Trabajar con la API REST del nodo de administración

Descripción general de la interfaz de usuario de la API REST del nodo de administración

Mediante la interfaz de usuario de la API 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 del nivel de servicio o la administración de activos.

Tareas que puedes realizar con las API REST:

Autorización

- ["Obtén autorización para usar las API REST"](#)

Configuración de activos

- ["Habilitar Active IQ y la monitorización de NetApp"](#)

- "Configurar un servidor proxy para el nodo de administración"
- "Configurar NetApp Hybrid Cloud Control para varios vCenters"
- "Agregar un activo de controlador al nodo de administración"
- "Crear y administrar activos de clúster de almacenamiento"

Gestión de activos

- "Ver o editar los recursos del controlador existentes"
- "Crear y administrar activos de clúster de almacenamiento"
- "Utilice la API REST para recopilar los registros del sistema Element."
- "Verifique las versiones del sistema operativo y los servicios del nodo de administración."
- "Obtención de registros de los servicios de administración"

Encuentra más información

- "Acceda al nodo de administración"
- "Plugin de NetApp Element para vCenter Server"
- "Documentación del software SolidFire y Element"

Obtén autorización para usar las API REST

Debe autorizar el uso de las API para servicios de gestión en la interfaz de usuario de la API REST. Esto se consigue obteniendo un token de acceso.

Para obtener un token, debe proporcionar las credenciales de administrador del clúster y un ID de cliente. Cada ficha dura aproximadamente diez minutos. Una vez que un token caduque, podrá autorizar nuevamente un nuevo token de acceso.

La funcionalidad de autorización se configura automáticamente durante la instalación y el despliegue del nodo de gestión. El servicio de tokens se basa en el clúster de almacenamiento que definió durante la configuración.

Antes de empezar

- Su versión de clúster debe ejecutar el software NetApp Element 11.3 o posterior.
- Deberías haber implementado un nodo de administración 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 de la interfaz de usuario de la API REST

1. Acceda a la interfaz de usuario de la API REST del servicio introduciendo la dirección IP del nodo de administración seguida del nombre del servicio, por ejemplo: /mnode/ :

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

2. Seleccione **Autorizar**.



Alternativamente, puede seleccionar un icono de candado junto a cualquier API de servicio.

3. Complete lo siguiente:

- Introduzca el nombre de usuario y la contraseña del clúster.
- Introduzca el ID del cliente como `mnode-client`.
- No introduzca ningún valor para la clave secreta del cliente.
- Seleccione **Autorizar** para iniciar una sesión.

4. Cierre el cuadro de diálogo **Autorizaciones disponibles**.



Si intentas ejecutar un comando después de que caduque el token, `401 Error: UNAUTHORIZED` Aparece un mensaje. Si ve esto, autorice de nuevo.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Habilitar Active IQ y la monitorización de NetApp

Puede habilitar la supervisión de almacenamiento Active IQ si no lo hizo durante la instalación o actualización. Es posible que deba utilizar este procedimiento si no configuró SolidFire Active IQ durante la instalación de un sistema de almacenamiento SolidFire all-flash.

El servicio de recopilación Active IQ reenvía datos de configuración y métricas de rendimiento del clúster basadas en software Element a SolidFire Active IQ para la generación de informes históricos y la monitorización del rendimiento casi en tiempo real. El servicio de monitorización de NetApp permite reenviar los fallos del clúster de almacenamiento a vCenter para la notificación de alertas.

Antes de empezar

- Algunas funciones de Active IQ, por ejemplo, la calidad de servicio (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:
 - Su clúster de almacenamiento ejecuta el software NetApp Element 11.3 o posterior.
 - Has implementado un nodo de administración que ejecuta la versión 11.3 o posterior.
- Tienes acceso a internet. El servicio de recopilación Active IQ no se puede utilizar desde sitios web oscuros que no tengan conectividad externa.

Pasos

- Obtenga el ID del recurso base para la instalación:

- a. Abra la interfaz de usuario de la API REST del servicio de inventario en el nodo de administración:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Seleccione **Autorizar** y complete lo siguiente:
- Introduzca el nombre de usuario y la contraseña del clúster.
 - Introduzca el ID del cliente como `mnode-client`.
 - Seleccione **Autorizar** para iniciar una sesión.
 - Cerrar la ventana.
- c. Desde la interfaz de usuario de la API REST, seleccione **GET /installations**.
- d. Seleccione **Probarlo**.
- e. Seleccione **Ejecutar**.
- f. Del cuerpo de la respuesta con 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 actualización.

2. Activar telemetría:

- a. Acceda a la interfaz de usuario de la API del servicio `mnode` en el nodo de administración introduciendo la dirección IP del nodo de administración seguida de `/mnode`:

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

- b. Seleccione **Autorizar** o cualquier icono de candado y complete lo siguiente:
- Introduzca el nombre de usuario y la contraseña del clúster.
 - Introduzca el ID del cliente como `mnode-client`.
 - Seleccione **Autorizar** para iniciar una sesión.
 - Cerrar la ventana.

c. Configurar el recurso base:

- i. Seleccione **PUT /assets/{asset_id}**.
- ii. Seleccione **Probarlo**.
- iii. Introduzca lo siguiente en la carga útil 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 siempre que se modifican los activos. La modificación de los recursos produce una breve demora antes de que se apliquen los ajustes.

3. Si aún no lo ha hecho, agregue un recurso de controlador de vCenter para NetApp Hybrid Cloud Control a los recursos conocidos del nodo de administración:



Se requiere un controlador para los servicios de monitorización de NetApp .

- a. Seleccione **POST /assets/{asset_id}/controllers** para agregar un sub-recurso de controlador.
- b. Seleccione **Probarlo**.
- c. Introduzca el ID del recurso base principal que copió al portapapeles en el campo **asset_id**.
- d. Introduzca los valores de carga útil requeridos con `type` como `vCenter` y las credenciales de vCenter.

```
{
  "username": "string",
  "password": "string",
  "ip": "string",
  "type": "vCenter",
  "host_name": "string",
  "config": {}
}
```



`ip`` es la dirección IP de vCenter.

e. Seleccione **Ejecutar**.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Configurar NetApp Hybrid Cloud Control para varios vCenters

Puede configurar NetApp Hybrid Cloud Control para administrar activos de dos o más vCenters que no utilizan el modo vinculado.

Debe utilizar este proceso después de su instalación inicial cuando necesite agregar recursos para una instalación recientemente escalada o cuando los nuevos recursos no se hayan agregado automáticamente a su configuración. Utilice estas API para agregar recursos que se hayan añadido recientemente a su instalación.

Lo que necesitarás

- Su versión de clúster ejecuta el software NetApp Element 11.3 o posterior.
- Has implementado un nodo de administración que ejecuta la versión 11.3 o posterior.

Pasos

1. ["Agregar nuevos vCenters como activos de controlador"](#) a la configuración del nodo de administración.
2. Actualizar la API del servicio de inventario en el nodo de administración:

```
https://<ManagementNodeIP>/inventory/1/
```



Como alternativa, puede esperar 2 minutos para que se actualice el inventario en la interfaz de usuario de NetApp Hybrid Cloud Control.

- a. Seleccione **Autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID del cliente como `mnode-client`.
 - iii. Seleccione **Autorizar** para iniciar una sesión.
 - iv. Cerrar la ventana.
 - b. Desde la interfaz de usuario de la API REST, seleccione **GET /installations**.
 - c. Seleccione **Probarlo**.
 - d. Seleccione **Ejecutar**.
 - e. Copie el ID del recurso de instalación de la respuesta. ("id").
 - f. Desde la interfaz de usuario de la API REST, seleccione **GET /installations/{id}**.
 - g. Seleccione **Probarlo**.
 - h. Configurar la actualización a `True`.
 - i. Pegue el ID del activo de instalación en el campo **id**.
 - j. Seleccione **Ejecutar**.
3. Actualice el navegador de NetApp Hybrid Cloud Control para ver los cambios.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Agregar un activo de controlador al nodo de administración

Puede agregar un recurso de controlador a la configuración del nodo de administración mediante la interfaz de usuario de la API REST.

Es posible que necesites agregar un recurso si recientemente has escalado tu instalación y los nuevos recursos no se agregaron automáticamente a tu configuración. Utilice estas API para agregar recursos que se hayan añadido recientemente a su instalación.

Lo que necesitarás

- Su versión de clúster ejecuta el software NetApp Element 11.3 o posterior.
- Has implementado un nodo de administración que ejecuta la versión 11.3 o posterior.
- Has creado un nuevo rol de NetApp HCC en vCenter para limitar la vista de servicios del nodo de administración a activos exclusivos de NetApp. Ver ["Cree un rol de NetApp HCC en vCenter."](#)

Pasos

1. Obtenga el ID del recurso base para la instalación:
 - a. Abra la interfaz de usuario de la API REST del servicio de inventario en el nodo de administración:

```
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 del cliente como `mnode-client`.
 - iii. Seleccione **Autorizar** para iniciar una sesión.
 - iv. Cerrar la ventana.
- c. Desde la interfaz de usuario de la API REST, seleccione **GET /installations**.
- d. Seleccione **Probarlo**.
- e. Seleccione **Ejecutar**.
- f. Del cuerpo de la respuesta con 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 actualización.

- g. Desde la interfaz de usuario de la API REST, seleccione **GET /installations/{id}**.
- h. Seleccione **Probarlo**.
- i. Pegue el ID del activo de instalación en el campo **id**.
- j. Seleccione **Ejecutar**.
- k. A partir de la respuesta, copie y guarde el ID del controlador del clúster. ("controllerId") para su uso en un paso posterior.

2. Para agregar un subactivo de controlador a un activo base existente, seleccione:

```
POST /assets/{asset_id}/controllers
```

- a. Abra la interfaz de usuario de la API REST del servicio mNode en el nodo de administración:

```
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 del cliente como `mnode-client`.
 - iii. Seleccione **Autorizar** para iniciar una sesión.
 - iv. Cerrar la ventana.
- c. Seleccione **POST /assets/{asset_id}/controllers**.
- d. Seleccione **Probarlo**.
- e. Introduzca el ID del activo base principal en el campo **asset_id**.
- f. Añada los valores requeridos a la carga útil.
- g. Seleccione **Ejecutar**.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Crear y administrar activos de clúster de almacenamiento

Puede agregar nuevos recursos del clúster de almacenamiento al nodo de administración, editar las credenciales almacenadas para los recursos del clúster de almacenamiento conocidos y eliminar recursos del clúster de almacenamiento del nodo de administración mediante la API REST.

Lo que necesitarás

- Asegúrese de que la versión de su clúster de almacenamiento esté ejecutando el software NetApp Element 11.3 o posterior.
- Asegúrese de haber implementado un nodo de administración que ejecute la versión 11.3 o posterior.

Opciones de gestión de activos de clústeres de almacenamiento

Elige una de las siguientes opciones:

- [Recuperar el ID de instalación y el ID de clúster de un recurso de clúster de almacenamiento](#)
- [Agregar un nuevo recurso de clúster de almacenamiento](#)
- [Edite las credenciales almacenadas para un activo de clúster de almacenamiento.](#)
- [Eliminar un recurso de clúster de almacenamiento](#)

Recuperar el ID de instalación y el ID de clúster de un recurso de clúster de almacenamiento

Puede utilizar la API REST para obtener el ID de instalación y el ID del clúster de almacenamiento. Necesita el ID de instalación para agregar un nuevo recurso de clúster de almacenamiento y el ID del clúster para modificar o eliminar un recurso de clúster de almacenamiento específico.

Pasos

1. Acceda a la interfaz de usuario de la API REST para el servicio de inventario introduciendo la dirección IP del nodo de administración seguida de `/inventory/1/`:

```
https://<ManagementNodeIP>/inventory/1/
```

2. Seleccione **Autorizar** o cualquier icono de candado y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID del cliente como `mnode-client`.
 - c. Seleccione **Autorizar** para iniciar una sesión.
 - d. Cerrar la ventana.
3. Seleccione **GET /installations**.
4. Seleccione **Probarlo**.
5. Seleccione **Ejecutar**.

La API devuelve una lista de todas las instalaciones conocidas.

6. A partir del cuerpo de la respuesta con código 200, guarde el valor en el `id` campo, que puedes encontrar en la lista de instalaciones. 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 la API REST para el servicio de almacenamiento introduciendo la dirección IP del nodo de administración seguida de `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

8. Seleccione **Autorizar** o cualquier icono de candado y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID del cliente como `mnode-client`.
 - c. Seleccione **Autorizar** para iniciar una sesión.
 - d. Cerrar la ventana.
9. Seleccione **GET /clusters**.
10. Seleccione **Probarlo**.
11. Introduzca el ID de instalación que guardó anteriormente en el `installationId` parámetro.
12. Seleccione **Ejecutar**.

La API devuelve una lista de todos los clústeres de almacenamiento conocidos en esta instalación.

13. A partir del cuerpo de la respuesta con código 200, encuentre el clúster de almacenamiento correcto y guarde el valor en el clúster. `storageId` campo. Este es el ID del clúster de almacenamiento.

Agregar un nuevo recurso de clúster de almacenamiento

Puede utilizar la API REST para agregar uno o más activos nuevos del clúster de almacenamiento al inventario del nodo de administración. Cuando se agrega un nuevo recurso de clúster de almacenamiento, este se registra automáticamente en el nodo de administración.

Lo que necesitarás

- Has copiado el [ID del clúster de almacenamiento e ID de instalación](#) para cualquier clúster de almacenamiento que desee agregar.
- Si está agregando más de un nodo de almacenamiento, ha leído y comprendido las limitaciones de ["grupo autoritario"](#) y soporte para múltiples clústeres de almacenamiento.



Todos los usuarios definidos en el clúster autoritativo se definen como usuarios en todos los demás clústeres vinculados a la instancia de NetApp Hybrid Cloud Control.

Pasos

1. Acceda a la interfaz de usuario de la API REST para el servicio de almacenamiento introduciendo la dirección IP del nodo de administración seguida de `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Seleccione **Autorizar** o cualquier icono de candado y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID del cliente como `mnode-client`.
 - c. Seleccione **Autorizar** para iniciar una sesión.
 - d. Cerrar la ventana.
3. Seleccione **POST /clusters**.
4. Seleccione **Probarlo**.
5. Introduzca la información del nuevo clúster de almacenamiento en los siguientes parámetros del 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 se añadirá el nuevo clúster de almacenamiento. Introduzca en este parámetro el ID de instalación que guardó anteriormente.
mvip	cadena	La dirección IP virtual de gestión IPv4 (MVIP) del clúster de almacenamiento.
password	cadena	La contraseña utilizada para comunicarse con el clúster de almacenamiento.

Parámetro	Tipo	Descripción
userId	cadena	El ID de usuario utilizado para comunicarse con el clúster de almacenamiento (el usuario debe tener privilegios de administrador).

6. Seleccione **Ejecutar**.

La API devuelve un objeto que contiene información sobre el recurso de clúster de almacenamiento recién agregado, como el nombre, la versión y la información de la dirección IP.

Edite las credenciales almacenadas para un activo de clúster de almacenamiento.

Puede editar las credenciales almacenadas que el nodo de administración utiliza para iniciar sesión en un clúster de almacenamiento. El usuario que elija debe tener acceso de administrador del clúster.



Asegúrese de haber seguido los pasos en [Recuperar el ID de instalación y el ID de clúster de un recurso de clúster de almacenamiento](#) antes de continuar.

Pasos

1. Acceda a la interfaz de usuario de la API REST para el servicio de almacenamiento introduciendo la dirección IP del nodo de administración seguida de `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Seleccione **Autorizar** o cualquier icono de candado y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID del cliente como `mnode-client`.
 - c. Seleccione **Autorizar** para iniciar una sesión.
 - d. Cerrar la ventana.
3. Seleccione **PUT /clusters/{storageId}**.
4. Seleccione **Probarlo**.
5. Pegue el ID del clúster de almacenamiento que copió anteriormente en el `storageId` parámetro.
6. Modifique uno o ambos de los siguientes parámetros en el campo **Cuerpo de la solicitud**:

```
{
  "password": "adminadmin",
  "userId": "admin"
}
```

Parámetro	Tipo	Descripción
password	cadena	La contraseña utilizada para comunicarse con el clúster de almacenamiento.
userId	cadena	El ID de usuario utilizado para comunicarse con el clúster de almacenamiento (el usuario debe tener privilegios de administrador).

7. Seleccione **Ejecutar**.

Eliminar un recurso de clúster de almacenamiento

Puede eliminar un recurso de clúster de almacenamiento si el clúster de almacenamiento ya no está en servicio. Cuando se elimina un recurso de clúster de almacenamiento, este se anula automáticamente en el nodo de administración.



Asegúrese de haber seguido los pasos en [Recuperar el ID de instalación y el ID de clúster de un recurso de clúster de almacenamiento](#) antes de continuar.

Pasos

1. Acceda a la interfaz de usuario de la API REST para el servicio de almacenamiento introduciendo la dirección IP del nodo de administración seguida de `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Seleccione **Autorizar** o cualquier icono de candado y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID del cliente como `mnode-client`.
 - c. Seleccione **Autorizar** para iniciar una sesión.
 - d. Cerrar la ventana.
3. Seleccione **DELETE /clusters/{storageId}**.
4. Seleccione **Probarlo**.
5. Introduzca el ID del clúster de almacenamiento que copió anteriormente en el `storageId` parámetro.
6. Seleccione **Ejecutar**.

En caso de éxito, la API devuelve una respuesta vacía.

Encuentra más información

- ["grupo autoritario"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Ver o editar los recursos del controlador existentes

Puede ver información sobre los controladores VMware vCenter existentes y editarlos en la configuración del nodo de administración mediante la API REST. Los controladores son instancias de VMware vCenter registradas en el nodo de administración de su instalación de NetApp SolidFire .

Antes de empezar

- Asegúrese de que su versión de clúster esté ejecutando el software NetApp Element 11.3 o posterior.
- Asegúrese de haber implementado un nodo de administración que ejecute la versión 11.3 o posterior.

Acceda a la API REST de los servicios de gestión.

Pasos

1. Acceda a la interfaz de usuario de la API REST para los servicios de administración introduciendo la dirección IP del nodo de administración seguida de `/vcenter/1/` :

```
https://<ManagementNodeIP>/vcenter/1/
```

2. Seleccione **Autorizar** o cualquier icono de candado y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID del cliente como `mnode-client` .
 - c. Seleccione **Autorizar** para iniciar una sesión.
 - d. Cerrar la ventana.

Ver información almacenada sobre los controladores existentes

Puede listar los controladores de vCenter existentes que están registrados con el nodo de administración y ver la información almacenada sobre ellos mediante la API REST.

Pasos

1. Seleccione **GET /compute/controllers**.
2. Seleccione **Probarlo**.
3. Seleccione **Ejecutar**.

La API devuelve una lista de todos los controladores vCenter conocidos, junto con la dirección IP, el ID del controlador, el nombre de host y el ID de usuario utilizados para comunicarse con cada controlador.

4. Si desea conocer el estado de conexión de un controlador específico, copie el ID del controlador desde el `id` Copia el campo de ese controlador a tu portapapeles y observa [Consulta el estado de un controlador existente](#) .

Consulta el estado de un controlador existente.

Puede consultar el estado de cualquiera de los controladores vCenter existentes registrados en el nodo de administración. La API devuelve un estado que indica si NetApp Hybrid Cloud Control puede conectarse con el controlador vCenter, así como el motivo de dicho estado.

Pasos

1. Seleccione **GET /compute/controllers/{controller_id}/status**.
2. Seleccione **Probarlo**.
3. Introduzca el ID del controlador que copió anteriormente en el `controller_id` parámetro.
4. Seleccione **Ejecutar**.

La API devuelve el estado de este controlador vCenter en particular, junto con el motivo de dicho estado.

Edita las propiedades almacenadas de un controlador

Puede editar el nombre de usuario o la contraseña almacenados para cualquiera de los controladores vCenter existentes registrados con el nodo de administración. No se puede editar la dirección IP almacenada de un controlador vCenter existente.

Pasos

1. Seleccione **PUT /compute/controllers/{controller_id}**.
2. Introduzca el ID del controlador de un controlador de vCenter en el `controller_id` parámetro.
3. Seleccione **Probarlo**.
4. Modifique cualquiera de los siguientes parámetros en el campo **Cuerpo de la solicitud**:

Parámetro	Tipo	Descripción
<code>userId</code>	cadena	Cambie el ID de usuario utilizado para comunicarse con el controlador de vCenter (el usuario debe tener privilegios de administrador).
<code>password</code>	cadena	Cambie la contraseña utilizada para comunicarse con el controlador vCenter.

5. Seleccione **Ejecutar**.

La API devuelve información actualizada del controlador.

Encuentra más información

- ["Agregar un activo de controlador al nodo de administración"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Configurar un servidor proxy

Si su clúster está detrás de un servidor proxy, debe configurar los ajustes del proxy para poder acceder a una red pública.

Se utiliza un servidor proxy para los recopiladores de telemetría y las conexiones de túnel inverso. Puede habilitar y configurar un servidor proxy mediante la interfaz de usuario de la API REST si no configuró un

servidor proxy durante la instalación o actualización. También puede modificar la configuración del servidor proxy existente o deshabilitar un servidor proxy.

El comando para configurar un servidor proxy se actualiza y luego devuelve la configuración actual del proxy para el nodo de administración. La configuración del proxy es utilizada por Active IQ, el servicio de monitorización de NetApp , y otras utilidades de software de Element que están instaladas en el nodo de gestión, incluido el túnel de soporte inverso para el Soporte de NetApp .

Antes de empezar

- Debes conocer la información del host y las credenciales del servidor proxy que estás configurando.
- Asegúrese de que su versión de clúster esté ejecutando el software NetApp Element 11.3 o posterior.
- Asegúrese de haber implementado un nodo de administración que ejecute la versión 11.3 o posterior.
- (Nodo de administración 12.0 y posteriores) Ha actualizado NetApp Hybrid Cloud Control a la versión 2.16 de los servicios de administración antes de configurar un servidor proxy.

Pasos

1. Acceda a la interfaz de usuario de la API REST en el nodo de administración introduciendo la dirección IP del nodo de administración seguida de `/mnode` :

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

2. Seleccione **Autorizar** o cualquier icono de candado y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID del cliente como `mnode-client` .
 - c. Seleccione **Autorizar** para iniciar una sesión.
 - d. Cerrar la ventana.
3. Seleccione **PUT /settings**.
4. Seleccione **Probarlo**.
5. Para habilitar un servidor proxy, debe configurar `use_proxy` Es cierto. Introduzca la dirección IP o el nombre de host y los puertos de destino del proxy.

El nombre de usuario del proxy, la contraseña del proxy y el puerto SSH son opcionales y deben omitirse si no se utilizan.

```
{
  "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**.



Dependiendo de su entorno, es posible que deba reiniciar su nodo de administración.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Verifique las versiones del sistema operativo y los servicios del nodo de administración.

Puede verificar los números de versión del sistema operativo del nodo de administración, del paquete de servicios de administración y de los servicios individuales que se ejecutan en el nodo de administración mediante la API REST del nodo de administración.

Lo que necesitarás

- Su clúster ejecuta el software NetApp Element versión 11.3 o posterior.
- Has implementado un nodo de administración que ejecuta la versión 11.3 o posterior.

Opciones

- [Comandos API](#)
- [Pasos de la interfaz de usuario de la API REST](#)

Comandos API

- Obtenga información sobre la versión del sistema operativo del nodo de administración, el paquete de servicios de administración y el servicio de la API del nodo de administración (mnode-api) que se ejecutan en el nodo de administración:

```
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 administración:

```
curl -X GET "https://<ManagementNodeIP>/mnode/services?status=running" -H "accept: */*" -H "Authorization: ${TOKEN}"
```



Puedes encontrar al portador `${TOKEN}` utilizado por el comando de la API cuando usted ["autorizar"](#). El portador `${TOKEN}` está en la respuesta curl.

Pasos de la interfaz de usuario de la API REST

1. Acceda a la interfaz de usuario de la API REST del servicio introduciendo la dirección IP del nodo de administración seguida de `/mnode/`:

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

2. Debe realizar una de las siguientes acciones:

- Obtenga información sobre la versión del sistema operativo del nodo de administración, el paquete de servicios de administración y el servicio de la API del nodo de administración (mnode-api) que se ejecutan en el nodo de administración:
 - i. Seleccione **GET /about**.
 - ii. Seleccione **Probarlo**.
 - iii. Seleccione **Ejecutar**.

La versión del paquete de servicios de gestión("mnode_bundle_version"), versión del sistema operativo del nodo de administración("os_version"), y versión de la API del nodo de administración("version") se indican en el cuerpo de la respuesta.

- Obtenga información de versión sobre los servicios individuales que se ejecutan en el nodo de administración:
 - i. Seleccione **GET /services**.
 - ii. Seleccione **Probarlo**.
 - 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 la respuesta.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Obtención de registros de los servicios de administración

Puede recuperar los registros de los servicios que se ejecutan en el nodo de administración mediante la API REST. Puede obtener registros de todos los servicios públicos o especificar servicios concretos y utilizar parámetros de consulta para definir mejor los resultados devueltos.

Lo que necesitarás

- Su versión de clúster ejecuta el software NetApp Element 11.3 o posterior.
- Has implementado un nodo de administración que ejecuta la versión 11.3 o posterior.

Pasos

1. Abra la interfaz de usuario de la API REST en el nodo de administración.
 - Comenzando con los servicios de gestión 2.21.61:

```
https://<ManagementNodeIP>/mnode/4/
```

- Para servicios de gestión 2.20.69 o anteriores:

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

2. Seleccione **Autorizar** o cualquier icono de candado y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID del cliente como mnode-client si el valor no está ya rellenado.
 - c. Seleccione **Autorizar** para iniciar una sesión.
 - d. Cerrar la ventana.
3. Seleccione **GET /logs**.
4. Seleccione **Probarlo**.
5. Especifique los siguientes parámetros:
 - ``Lines`` Introduzca el número de líneas que desea que devuelva el registro. Este parámetro es un número entero que por defecto es 1000.

 Evite solicitar todo el historial del contenido del registro configurando Líneas en 0.
 - `since`: Agrega una marca de tiempo ISO-8601 para el punto de inicio de los registros de servicio.

 Utilice un criterio razonable `since` parámetro al recopilar registros de períodos de tiempo más amplios.
 - ``service-name`` Introduzca un nombre de servicio.

 Utilice el `GET /services` comando para listar los servicios en el nodo de administración.
 - `stopped`: Configurado a `true` Recuperar los registros de los servicios detenidos.
6. Seleccione **Ejecutar**.
7. En el cuerpo de la respuesta, seleccione **Descargar** para guardar el registro de salida.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Gestionar conexiones de soporte

Acceso a nodos de almacenamiento mediante SSH para la resolución de problemas básicos

A partir de Element 12.5, puede utilizar la cuenta del sistema `sfireadonly` en los nodos de almacenamiento para la resolución de problemas básicos. También puede habilitar y abrir el acceso al túnel de soporte remoto para el Soporte de NetApp para la resolución

de problemas avanzados.

La cuenta de sistema `sftreadonly` permite ejecutar comandos básicos de solución de problemas de sistema y red de Linux, incluyendo `ping`.



Salvo indicación expresa del Soporte de NetApp, cualquier modificación de este sistema no está soportada, anulará su contrato de soporte y podría provocar inestabilidad o inaccesibilidad de los datos.

Antes de empezar

- **Permisos de escritura:** Verifique que tiene permisos de escritura en el directorio de trabajo actual.
- **(Opcional) Genera tu propio par de claves:** Ejecutar `ssh-keygen` Desde Windows 10, MacOS o distribución Linux. Esta es una acción única para crear un par de claves de usuario y se puede reutilizar para futuras sesiones de solución de problemas. También podrías usar certificados asociados a las cuentas de los empleados, que también funcionarían en este modelo.
- **Habilitar la funcionalidad SSH en el nodo de administración:** Para habilitar la funcionalidad de acceso remoto en el modo de administración, consulte ["este tema"](#). Para los servicios de administración 2.18 y posteriores, la capacidad de acceso remoto está deshabilitada en el nodo de administración de forma predeterminada.
- **Habilitar la funcionalidad SSH en el clúster de almacenamiento:** Para habilitar la funcionalidad de acceso remoto en los nodos del clúster de almacenamiento, consulte ["este tema"](#).
- **Configuración del firewall:** Si su nodo de administración se encuentra detrás de un servidor proxy, se requieren los siguientes puertos TCP en el archivo `sshd.config`:

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

Opciones de solución de problemas

- [Solucionar problemas de un nodo del clúster](#)
- [Solucione problemas de un nodo de clúster con el soporte de NetApp](#)
- [Solucionar problemas de un nodo que no forma parte del clúster](#)

Solucionar problemas de un nodo del clúster

Puede realizar tareas básicas de solución de problemas utilizando la cuenta de sistema `sftreadonly`:

Pasos

1. Conéctese al nodo de administración mediante SSH utilizando las credenciales de inicio de sesión de la cuenta que seleccionó al instalar la máquina virtual del nodo de administración.
2. En el nodo de administración, vaya a `/sf/bin`.

3. Encuentra el script adecuado para tu sistema:

- SignSshKeys.ps1
- SignSshKeys.py
- SignSshKeys.sh



SignSshKeys.ps1 depende de PowerShell 7 o posterior y SignSshKeys.py depende de Python 3.6.0 o posterior. ["módulo de solicitudes"](#) .

El SignSshKeys El script escribe user , user.pub , y user-cert.pub archivos en el directorio de trabajo actual, que luego son utilizados por el ssh dominio. Sin embargo, cuando se proporciona un archivo de clave pública al script, solo se utiliza un archivo de clave pública. <public_key> archivo (con <public_key> (reemplazado con el prefijo del archivo de clave pública pasado al script) se escribe en el directorio.

4. Ejecuta el script en el nodo de administración para generar el llavero SSH. El script habilita el acceso SSH utilizando la cuenta de sistema sfreadonly en todos los nodos del clúster.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--publickey [public key path]
```

a. Reemplace el valor entre corchetes [] (incluidos los corchetes) para cada uno de los siguientes parámetros:



Puede utilizar tanto la forma abreviada como la completa del parámetro.

- **--ip | -i [dirección IP]:** Dirección IP del nodo de destino contra el que se ejecutará la API.
 - **--user | -u [nombre de usuario]:** Usuario del clúster utilizado para ejecutar la llamada a la API.
 - **(Opcional) --duration | -d [horas]:** La duración durante la cual una clave firmada debe permanecer válida como un entero en horas. El valor predeterminado es 24 horas.
 - **(Opcional) --publickey | -k [ruta de la clave pública]:** La ruta a una clave pública, si el usuario elige proporcionar una.
- b. Compara tu entrada con el siguiente comando de ejemplo. En este ejemplo, 10.116.139.195 es la IP del nodo de almacenamiento, admin es el nombre de usuario del clúster y la duración de la validez de la clave es de dos horas:

```
sh /sf/bin/SignSshKeys.sh --ip 10.116.139.195 --user admin --duration
2
```

c. Ejecuta el comando.

5. Conexión SSH a las direcciones IP de los nodos:

```
ssh -i user sfreadonly@[node_ip]
```

Podrás ejecutar comandos básicos de solución de problemas de sistemas y redes Linux, tales como:

ping , y otros comandos de solo lectura.

6. (Opcional) Desactivar ["funcionalidad de acceso remoto"](#) nuevamente después de que se complete la resolución de problemas.



SSH permanecerá habilitado en el nodo de administración si no lo deshabilita. La configuración habilitada para SSH persiste en el nodo de administración a través de actualizaciones y mejoras hasta que se deshabilita manualmente.

Solucione problemas de un nodo de clúster con el soporte de NetApp

El soporte de NetApp puede realizar diagnósticos avanzados con una cuenta de sistema que permite a un técnico ejecutar diagnósticos Element más profundos.

Pasos

1. Conéctese al nodo de administración mediante SSH utilizando las credenciales de inicio de sesión de la cuenta que seleccionó al instalar la máquina virtual del nodo de administración.
2. Ejecute el comando rst con el número de puerto enviado por el Soporte de NetApp para abrir el túnel de soporte:

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

El soporte de NetApp iniciará sesión en su nodo de administración utilizando el túnel de soporte.

3. En el nodo de administración, vaya a `/sf/bin`.
4. Encuentra el script adecuado para tu sistema:
 - SignSshKeys.ps1
 - SignSshKeys.py
 - SignSshKeys.sh



SignSshKeys.ps1 depende de PowerShell 7 o posterior y SignSshKeys.py depende de Python 3.6.0 o posterior. ["módulo de solicitudes"](#).

El SignSshKeys El script escribe `user` , `user.pub` , y `user-cert.pub` archivos en el directorio de trabajo actual, que luego son utilizados por el `ssh` dominio. Sin embargo, cuando se proporciona un archivo de clave pública al script, solo se utiliza un archivo de clave pública. `<public_key>` archivo (con `<public_key>` (reemplazado con el prefijo del archivo de clave pública pasado al script) se escribe en el directorio.

5. Ejecuta el script para generar el llavero SSH con el `--sfadmin` bandera. El script habilita SSH en todos los nodos.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]  
--sfadmin
```


Para SSH como `--sfadmin` Para conectarte a un nodo en clúster, debes generar el llavero SSH usando un `--user` con `supportAdmin` acceso en el clúster.

Para configurar `supportAdmin` Para acceder a las cuentas de administrador del clúster, puede usar la interfaz de usuario de Element o las API:



- "Configure el acceso "supportAdmin" mediante la interfaz de usuario de Element."
- Configurar `supportAdmin` acceso mediante el uso de API y agregando "supportAdmin" como el "access" Tipo de solicitud a la API:
 - "Configure el acceso "supportAdmin" para una nueva cuenta."
 - "Configure el acceso "supportAdmin" para una cuenta existente."

Para obtener el `clusterAdminID`, puedes usar el "Lista de administradores de clúster" API.

Para agregar `supportAdmin` Para acceder, debe tener privilegios de administrador de clúster o de administrador.

- a. Reemplace el valor entre corchetes [] (incluidos los corchetes) para cada uno de los siguientes parámetros:



Puede utilizar tanto la forma abreviada como la completa del parámetro.

- `--ip` | `-i` [dirección IP]: Dirección IP del nodo de destino contra el que se ejecutará la API.
 - `--user` | `-u` [nombre de usuario]: Usuario del clúster utilizado para ejecutar la llamada a la API.
 - (Opcional) `--duration` | `-d` [horas]: La duración durante la cual una clave firmada debe permanecer válida como un entero en horas. El valor predeterminado es 24 horas.
- b. Compara tu entrada con el siguiente comando de ejemplo. En este ejemplo, `192.168.0.1` es la IP del nodo de almacenamiento, `admin` es el nombre de usuario del clúster, la duración de la validez de la clave es de dos horas, y `--sfadmin` Permite el acceso del nodo de soporte de NetApp para la resolución de problemas:

```
sh /sf/bin/SignSshKeys.sh --ip 192.168.0.1 --user admin --duration 2 --sfadmin
```

- c. Ejecuta el comando.

6. Conexión SSH a las direcciones IP de los nodos:

```
ssh -i user sfadmin@[node_ip]
```

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

```
rst --killall
```

8. (Opcional) Desactivar "funcionalidad de acceso remoto" nuevamente después de que se complete la

resolución de problemas.



SSH permanecerá habilitado en el nodo de administración si no lo deshabilita. La configuración habilitada para SSH persiste en el nodo de administración a través de actualizaciones y mejoras hasta que se deshabilita manualmente.

Solucionar problemas de un nodo que no forma parte del clúster

Puede realizar la resolución de problemas básicos de un nodo que aún no se ha agregado a un clúster. Puede utilizar la cuenta de sistema sfreadonly para este propósito con o sin la ayuda del soporte de NetApp . Si tiene configurado un nodo de administración, puede usarlo para SSH y ejecutar el script proporcionado para esta tarea.

1. Desde un ordenador Windows, Linux o Mac que tenga instalado un cliente SSH, ejecute el script apropiado para su sistema proporcionado por el soporte de NetApp .
2. Conexión SSH a la IP del nodo:

```
ssh -i user sfreadonly@[node_ip]
```

3. (Opcional) Desactivar "[funcionalidad de acceso remoto](#)" nuevamente después de que se complete la resolución de problemas.



SSH permanecerá habilitado en el nodo de administración si no lo deshabilita. La configuración habilitada para SSH persiste en el nodo de administración a través de actualizaciones y mejoras hasta que se deshabilita manualmente.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación de NetApp HCI"](#)

Inicie una sesión de soporte remoto de NetApp

Si necesita asistencia técnica 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 obtener acceso remoto, el soporte de NetApp puede abrir una conexión Secure Shell (SSH) inversa a su entorno.

Puede abrir un puerto TCP para una conexión de túnel inverso SSH con el soporte de NetApp . Esta conexión permite al soporte de NetApp iniciar sesión en su nodo de administración.

Antes de empezar

- Para los servicios de administración 2.18 y posteriores, la capacidad de acceso remoto está deshabilitada en el nodo de administración de forma predeterminada. Para habilitar la funcionalidad de acceso remoto, consulte ["Gestionar la funcionalidad SSH en el nodo de administración"](#) .
- Si su nodo de administración se encuentra detrás de un servidor proxy, se requieren los siguientes puertos TCP en el archivo sshd.config:

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

Pasos

- Inicie sesión en su nodo de administración y abra una sesión de terminal.
- Cuando se le solicite, ingrese 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) Desactivar ["funcionalidad de acceso remoto"](#) de nuevo.



SSH permanecerá habilitado en el nodo de administración si no lo deshabilita. La configuración habilitada para SSH persiste en el nodo de administración a través de actualizaciones y mejoras hasta que se deshabilita manualmente.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Gestionar la funcionalidad SSH en el nodo de administración

Puede deshabilitar, volver a habilitar o determinar el estado de la capacidad SSH en el nodo de administración (mNode) utilizando la API REST. Capacidad 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 administración que ejecutan servicios de administración 2.18 o posterior.

A partir de Management Services 2.20.69, puede habilitar y deshabilitar la capacidad SSH en el nodo de administración mediante la interfaz de usuario de NetApp Hybrid Cloud Control.

Lo que necesitarás

- *** Permisos de NetApp Hybrid Cloud Control*:** Usted tiene permisos como administrador.
- **Permisos de administrador del clúster:** Usted tiene permisos como administrador en el clúster de almacenamiento.
- **Software Element:** Su clúster ejecuta el software NetApp Element 11.3 o posterior.

- **Nodo de administración:** Ha implementado un nodo de administración que ejecuta la versión 11.3 o posterior.
- **Actualizaciones de servicios de gestión:**
 - Para usar la interfaz de usuario de NetApp Hybrid Cloud Control, debe actualizar su ["paquete de servicios de gestión"](#) a la versión 2.20.69 o posterior.
 - Para usar la interfaz de usuario de la API REST, debe actualizar su ["paquete de servicios de gestión"](#) a la versión 2.17.

Opciones

- [Habilite o deshabilite la funcionalidad SSH en el nodo de administración mediante la interfaz de usuario de NetApp Hybrid Cloud Control.](#)

Puedes realizar cualquiera de las siguientes tareas después de...["autenticar"](#) :

- [Habilite o deshabilite la funcionalidad SSH en el nodo de administración mediante API.](#)
- [Determinar el estado de la capacidad SSH en el nodo de administración mediante API.](#)

Habilite o deshabilite la funcionalidad SSH en el nodo de administración mediante la interfaz de usuario de NetApp Hybrid Cloud Control.

Puede deshabilitar o volver a habilitar la funcionalidad SSH en el nodo de administración. Capacidad 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 administración que ejecutan servicios de administración 2.18 o posterior. Deshabilitar SSH no finaliza ni desconecta las sesiones de cliente SSH existentes con el nodo de administración. Si deshabilita SSH y decide volver a habilitarlo más adelante, puede hacerlo mediante la interfaz de usuario de NetApp Hybrid Cloud Control.



Para habilitar o deshabilitar el acceso de soporte mediante SSH para un clúster de almacenamiento, debe usar el ["página de configuración del clúster de Element UI"](#) .

Pasos

1. Desde el Panel de control, seleccione el menú de opciones en la parte superior derecha y seleccione **Configurar**.
2. En la pantalla **Administrar acceso para el nodo de administración**, active el interruptor para habilitar SSH para el nodo de administración.
3. Una vez finalizada la resolución de problemas, en la pantalla **Acceso de soporte para el nodo de administración**, active el interruptor para deshabilitar el SSH del nodo de administración.

Habilite o deshabilite la funcionalidad SSH en el nodo de administración mediante API.

Puede deshabilitar o volver a habilitar la funcionalidad SSH en el nodo de administración. Capacidad 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 administración que ejecutan servicios de administración 2.18 o posterior. Deshabilitar SSH no finaliza ni desconecta las sesiones de cliente SSH existentes con el nodo de administración. Si deshabilita SSH y decide volver a habilitarlo más adelante, puede hacerlo utilizando la misma API.

Comando API

Para 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 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}"
```



Puedes encontrar al portador `${TOKEN}` utilizado por el comando de la API cuando usted ["autorizar"](#). El portador `${TOKEN}` está en la respuesta curl.

Pasos de la interfaz de usuario de la API REST

1. Acceda a la interfaz de usuario de la API REST para el servicio de API del nodo de administración introduciendo la dirección IP del nodo de administración 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 del cliente como `mnode-client`.
 - c. Seleccione **Autorizar** para iniciar una sesión.
 - d. Cerrar la ventana.
3. Desde la interfaz de usuario de la API REST, seleccione **PUT /settings/ssh**.
 - a. Seleccione **Probarlo**.
 - b. Configure el parámetro **habilitado** para `false` para deshabilitar SSH o `true` para volver a habilitar la funcionalidad SSH que había sido previamente deshabilitada.
 - c. Seleccione **Ejecutar**.

Determinar el estado de la capacidad SSH en el nodo de administración mediante API.

Puede determinar si la capacidad SSH está habilitada o no en el nodo de administración mediante una API de servicio de nodo de administración. SSH está deshabilitado de forma predeterminada en los nodos de administración que ejecutan servicios de administración 2.18 o posterior.

Comando API

Para 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 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}"
```



Puedes encontrar al portador `${TOKEN}` utilizado por el comando de la API cuando usted ["autorizar"](#). El portador `${TOKEN}` está en la respuesta del curl...

Pasos de la interfaz de usuario de la API REST

1. Acceda a la interfaz de usuario de la API REST para el servicio de API del nodo de administración introduciendo la dirección IP del nodo de administración 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 del cliente como `mnode-client`.
 - c. Seleccione **Autorizar** para iniciar una sesión.
 - d. Cerrar la ventana.
3. Desde la interfaz de usuario de la API REST, seleccione **GET /settings/ssh**.
 - a. Seleccione **Probarlo**.
 - b. Seleccione **Ejecutar**.

Encuentra más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación del software SolidFire y Element"](#)

Actualice su sistema de almacenamiento totalmente flash NetApp SolidFire

Descripción general de la secuencia de actualización

Puede mantener actualizado su sistema de almacenamiento SolidFire Element después de la implementación actualizando secuencialmente todos los componentes de almacenamiento de NetApp .

Estos componentes incluyen servicios de administración, NetApp Hybrid Cloud Control, software Element, nodo de administración y (dependiendo de su instalación) el complemento Element para vCenter Server.

- A partir de noviembre de 2023, no podrá iniciar una actualización de componentes utilizando NetApp Hybrid Cloud Control o la API REST porque los certificados de clave de firma (privada y pública) caducaron el 5 de noviembre de 2023. Puedes solucionar este problema mediante ["Realizar una actualización in situ del nodo de gestión"](#) a la versión 12.8 antes de utilizar NetApp Hybrid Cloud Control o la API REST para actualizar los servicios de administración, el software Element y el firmware de almacenamiento.

Si va a implementar un nuevo nodo de administración con la versión 12.8, puede usar NetApp Hybrid Cloud Control o la API REST para realizar las actualizaciones de componentes en el orden que se indica en la documentación. [secuencia de actualización del sistema](#) .



- Los siguientes nodos no son compatibles. Si intenta actualizar uno de estos nodos a una versión de Element no compatible, verá un error que indica que el nodo no es compatible con Element 12.x:
 - Comenzando con los nodos de almacenamiento Element 12.8, SF4805, SF9605, SF19210 y SF38410.
 - Comenzando con los nodos de almacenamiento Element 12.7, SF2405 y SF9608 y los nodos FC FC0025 y SF-FCN-01.
- A partir de Element 12.5, NetApp HealthTools ya no es compatible con las actualizaciones de software de Element. Si está utilizando Element 11.0 o 11.1, primero debe ["Actualizar a Element 12.3 usando HealthTools"](#) y luego actualice a Element 12.5 o posterior utilizando NetApp Hybrid Cloud Control.

El [secuencia de actualización del sistema](#) El contenido describe las tareas necesarias para completar una actualización del sistema de almacenamiento all-flash SolidFire . Lo ideal es que estos procedimientos se realicen como parte de una secuencia de actualización más amplia y no de forma aislada. Si se necesita una actualización o mejora basada en componentes, consulte los requisitos previos del procedimiento para garantizar que se aborden las complejidades adicionales.

El ["secuencia de actualización de vSphere"](#) El contenido que incluye el complemento Element para vCenter Server describe los pasos adicionales previos y posteriores a la actualización necesarios para reinstalar el complemento Element para vCenter Server.

Antes de empezar

- Está ejecutando el nodo de administración 11.3 o posterior. Las versiones más recientes del nodo de gestión tienen una arquitectura modular que proporciona servicios individuales.



Para comprobar la versión, inicie sesión en su nodo de administración y consulte el número de versión de Element en el banner de inicio de sesión. Si no tiene la versión 11.3, consulte ["Actualiza tu nodo de administración"](#).

- Has actualizado tus servicios de gestión al menos a la versión 2.1.326.

Las actualizaciones que utilizan NetApp Hybrid Cloud Control no están disponibles en versiones anteriores del paquete de servicios.

- Te has asegurado de que la hora del sistema en todos los nodos esté sincronizada y de que NTP esté configurado correctamente para el clúster de almacenamiento y los nodos. Cada nodo debe configurarse con un servidor de nombres DNS en la interfaz web de cada nodo. (`https://[IP address]:442`) sin fallos de clúster sin resolver relacionados con la asimetría temporal.
- Has programado tiempo suficiente para tu ["Software Element"](#) y ["firmware de almacenamiento"](#) mejoras. Al actualizar al software Element 12.5 o posterior, el tiempo del proceso de actualización varía según la versión del software Element y las actualizaciones de firmware.

Secuencia de actualización del sistema

Puede utilizar la siguiente secuencia para actualizar su sistema de almacenamiento all-flash NetApp SolidFire a Element 12.5 o posterior.

Pasos

1. ["Ejecute comprobaciones del estado del almacenamiento de Element antes de actualizarlo"](#).
2. ["\(Opcional\) Actualiza tu nodo de administración"](#).



Ya no es necesario actualizar el sistema operativo del nodo de administración para actualizar el software Element en el clúster de almacenamiento. Si el nodo de administración es la versión 11.3 o posterior, puede actualizar los servicios de administración a la última versión para realizar actualizaciones de Element mediante NetApp Hybrid Cloud Control. Siga el procedimiento de actualización del nodo de administración para su caso particular si necesita actualizar el sistema operativo del nodo de administración por otras razones, como la corrección de problemas de seguridad.

3. ["Actualizaciones de los servicios de gestión desde el control de la nube híbrida"](#).



- El paquete de servicios de administración 2.27 incluye el complemento Element para vCenter Server 5.5, que solo es compatible con el nodo de administración 12.8. Cuando actualiza a los servicios de administración 2.27, debe cambiar la secuencia de actualización y actualizar el paquete de servicios de administración *después* de actualizar a Element 12.8 para tener compatibilidad entre el nodo de administración y los servicios de administración.
- Si está actualizando a los servicios de administración 2.21.61 a 2.26.40, debe actualizar el paquete de servicios de administración *antes* de actualizar a Element 12.8.



Si está actualizando los servicios de administración a la versión 2.16 o posterior y está ejecutando un nodo de administración 11.3 a 11.8, deberá aumentar la RAM de la máquina virtual de su nodo de administración antes de actualizar los servicios de administración.

4. ["Actualiza el software y el firmware de almacenamiento de tu Element."](#)

5. "(Opcional) Actualice únicamente el firmware de almacenamiento de su Element".



Es posible que realice esta tarea cuando haya disponible una nueva actualización de firmware de almacenamiento fuera de una versión principal.

6. "Actualiza tu complemento Element para vCenter Server".

Encuentra más información

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

Procedimientos de actualización del sistema

Ejecute las comprobaciones de estado del almacenamiento de Element antes de actualizar el almacenamiento.

Debe ejecutar comprobaciones de estado antes de actualizar el almacenamiento de Element para garantizar que todos los nodos de almacenamiento de su clúster estén listos para la próxima actualización del almacenamiento de Element.

Lo que necesitarás

- **Servicios de administración:** Ha actualizado al último paquete de servicios de administración (2.10.27 o posterior).



Debe actualizar al paquete de servicios de administración más reciente antes de actualizar su software Element.

- **Nodo de administración:** Estás ejecutando el nodo de administración 11.3 o posterior.
- **Software Element:** Su versión de clúster ejecuta el software NetApp Element 11.3 o posterior.
- **Acuerdo de licencia de usuario final (EULA):** A partir de los servicios de administración 2.20.69, debe aceptar y guardar el EULA antes de utilizar la interfaz de usuario o la API de NetApp Hybrid Cloud Control para ejecutar comprobaciones del estado del almacenamiento de Element:
 - a. Abra la dirección IP del nodo de administración en un navegador web:

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

- b. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento.
- c. Seleccione **Actualizar**, situado en la parte superior derecha de la interfaz.
- d. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto las actualizaciones actuales y futuras** y seleccione **Guardar**.

opciones de chequeo de salud

Puede ejecutar comprobaciones de estado utilizando la interfaz de usuario de NetApp Hybrid Cloud Control o la API de NetApp Hybrid Cloud Control:

- [Utilice NetApp Hybrid Cloud Control para ejecutar comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento.](#) (Método preferido)

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 NetApp Hybrid Cloud Control para ejecutar comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento.

Con NetApp Hybrid Cloud Control, puede verificar que un clúster de almacenamiento esté listo para ser actualizado.

Pasos

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

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

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar**, situado en la parte superior derecha de la interfaz.
4. En la página **Actualizaciones**, seleccione la pestaña **Almacenamiento**.
5. Seleccione la revisión de salud  para el clúster que desea comprobar para determinar si está listo para la actualización.
6. En la página **Comprobación del estado del almacenamiento**, seleccione **Ejecutar comprobación del estado**.
7. Si hay algún problema, haga lo siguiente:
 - a. Consulte el artículo de la base de conocimientos específico que se indica para cada problema o realice la solución indicada.
 - b. Si se especifica un KB, complete el proceso descrito en el artículo KB correspondiente.
 - c. Una vez resueltos los problemas del clúster, seleccione **Volver a ejecutar la comprobación de estado**.

Una vez finalizada la comprobación de estado sin errores, el clúster de almacenamiento estará listo para actualizarse. Consulte la actualización del nodo de almacenamiento. ["instrucciones"](#) para continuar.

Utilice la API para ejecutar comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento.

Puede utilizar la API REST para verificar que un clúster de almacenamiento esté listo para ser actualizado. La comprobación del estado verifica que no existan obstáculos para la actualización, como nodos pendientes, problemas de espacio en disco y fallos del clúster.

Pasos

1. Localice el ID del clúster de almacenamiento:
 - a. Abra la interfaz de usuario de la API REST del nodo de administración en el nodo de administración:

```
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 del cliente como `mnode-client` si el valor no está ya asignado.
 - iii. Seleccione **Autorizar** para iniciar una sesión.
 - iv. Cierre la ventana de autorización.
- c. Desde la interfaz de usuario de la API REST, seleccione `GET /assets`.
- d. Seleccione **Probarlo**.
- e. Seleccione **Ejecutar**.
- f. De la respuesta, copie el "id" desde "storage" Sección del clúster que pretende comprobar para verificar su preparación para la actualización.



No utilice el "parent" El valor en esta sección se debe a que se trata del ID del nodo de administración, no del 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. Ejecutar comprobaciones de estado en el clúster de almacenamiento:

- a. Abra la interfaz de usuario de la API REST de almacenamiento en el nodo de administración:

```
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 del cliente como `mnode-client` si el valor no está ya asignado.
 - iii. Seleccione **Autorizar** para iniciar una sesión.
 - iv. Cierre la ventana de autorización.
- c. Seleccione **POST /health-checks**.
- d. Seleccione **Probarlo**.
- e. En el campo de parámetros, ingrese el ID del clúster de almacenamiento obtenido en el paso 1.

```
{
  "config": {},
  "storageId": "123a45b6-1a2b-12a3-1234-1a2b34c567d8"
}
```

- f. Seleccione **Ejecutar** para realizar una comprobación de 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. Copia el `healthCheckId` Eso forma parte de la respuesta.

3. Verifique los resultados de los controles de salud:

- Seleccione **GET /health-checks/{healthCheckId}**.
- Seleccione **Probarlo**.
- Introduzca el ID de comprobación de estado en el campo de parámetros.
- Seleccione **Ejecutar**.
- Desplácese hasta el final del cuerpo de la respuesta.

Si todas las comprobaciones de estado son correctas, el resultado es similar al siguiente ejemplo:

```
"message": "All checks completed successfully.",
"percent": 100,
"timestamp": "2020-03-06T00:03:16.321621Z"
```

4. Si el message El error indica que hubo problemas con el estado del clúster; haga lo siguiente:
 - a. Seleccione **GET /health-checks/{healthCheckId}/log**
 - b. Seleccione **Probarlo**.
 - c. Introduzca el ID de comprobación de estado en el campo de parámetros.
 - d. Seleccione **Ejecutar**.
 - e. Revise cualquier error específico y obtenga los enlaces a los artículos de la base de conocimientos correspondientes.
 - f. Consulte el artículo de la base de conocimientos específico que se indica para cada problema o realice la solución indicada.
 - g. Si se especifica un KB, complete el proceso descrito en el artículo KB correspondiente.
 - h. Después de haber resuelto los problemas del clúster, ejecute **GET /health-checks/{healthCheckId}/log** nuevamente.

Comprobaciones del estado del almacenamiento realizadas por el servicio

Las comprobaciones del estado del almacenamiento realizan las siguientes comprobaciones por clúster.

Nombre de la verificación	Nodo/Clúster	Descripción
comprobar_resultados_asíncronos	Grupo	Verifica que el número de resultados asíncronos en la base de datos esté por debajo de un umbral.
comprobar_fallos_del_clúster	Grupo	Verifica que no haya fallos de clúster que bloqueen la actualización (tal como se define en la fuente de elementos).
comprobar_velocidad_de_carga	Node	Mide la velocidad de carga entre el nodo de almacenamiento y el nodo de gestión.
comprobación de velocidad de conexión	Node	Verifica que los nodos tengan conectividad con el nodo de administración que proporciona los paquetes de actualización y estima la velocidad de conexión.
comprobar_núcleos	Node	Comprueba si hay volcados de memoria del kernel y archivos core en el nodo. La comprobación falla si se ha producido algún fallo en un período de tiempo reciente (umbral de 7 días).
comprobar_espacio_disco_raíz	Node	Verifica que el sistema de archivos raíz tenga suficiente espacio libre para realizar una actualización.

Nombre de la verificación	Nodo/Clúster	Descripción
check_var_log_disk_space	Node	Verifica que <code>/var/log</code> El espacio libre cumple con un determinado umbral de porcentaje de espacio libre. Si no lo hace, la comprobación rotará y eliminará los registros más antiguos para que queden por debajo del umbral. La comprobación falla si no consigue crear suficiente espacio libre.
comprobar_nodos_pendientes	Grupo	Verifica que no haya nodos pendientes en el clúster.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Actualizar un nodo de administración

Puede actualizar su nodo de administración a la versión 12.5 o posterior desde la versión 12.3.x o posterior.

Ya no es necesario actualizar el sistema operativo del nodo de administración para actualizar el software Element en el clúster de almacenamiento. Puede actualizar fácilmente los servicios de administración a la última versión para realizar actualizaciones de Element utilizando NetApp Hybrid Cloud Control. Siga el procedimiento de actualización del nodo de administración para su caso particular si desea actualizar el sistema operativo del nodo de administración por otros motivos, como la corrección de problemas de seguridad.



Si necesita información sobre la actualización de nodos de administración a la versión 12.2 o anterior, consulte la ["Documentación de actualización del nodo de administración de Element 12.3.x"](#).

Paso 1: Actualizar la versión del hardware de la máquina virtual en un nodo de administración

Si va a realizar una actualización in situ de un nodo de administración existente a Element 12.8, antes de actualizar, debe asegurarse de que la versión del hardware de la máquina virtual en el nodo de administración sea compatible con ESXi 6.7 (versión de hardware de la máquina virtual 14) o posterior, según su entorno.

Pasos

1. Inicie sesión en vSphere Web Client como administrador de vCenter.
2. Desde el menú del cliente vSphere, seleccione **Máquinas virtuales y plantillas**.
3. Haz clic con el botón derecho en la máquina virtual (VM) y selecciona **Encendido > Apagar sistema operativo invitado**.

Espere hasta que la máquina virtual se apague.

4. Haz clic con el botón derecho en la máquina virtual y selecciona **Compatibilidad > Actualizar compatibilidad de la máquina virtual**.

5. Seleccione **Sí**.
6. Seleccione ESXi 6.7 o una versión posterior, según la versión de su entorno vSphere.
7. Seleccione **OK**.
8. Una vez finalizada la actualización, haga clic con el botón derecho en la máquina virtual y seleccione **Encender > Activar**.
9. Seleccione **Actualización del cliente vSphere** y verifique que la compatibilidad de la máquina virtual esté en la versión deseada.

Paso 2: Actualice un nodo de administración a Element 12.5 o posterior.

Elige una de las siguientes opciones de actualización:

- [Actualizar un nodo de administración a la versión 12.5 o posterior desde la versión 12.3.x o posterior.](#)
- [Reconfigurar la autenticación mediante la API REST del nodo de administración](#)

Elija esta opción si ha actualizado **secuencialmente** (1) la versión de sus servicios de administración y (2) la versión de su almacenamiento Element y desea **mantener** su nodo de administración existente:



Si no actualiza secuencialmente sus servicios de administración seguidos del almacenamiento de Element, no podrá reconfigurar la reautenticación utilizando este procedimiento. Siga el procedimiento de actualización correspondiente.

Actualizar un nodo de administración a la versión 12.5 o posterior desde la versión 12.3.x o posterior.

Puede realizar una actualización in situ del nodo de administración de la versión 12.3.x o posterior a la versión 12.5 o posterior sin necesidad de aprovisionar una nueva máquina virtual de nodo de administración.



El nodo de administración Element 12.5 o posterior es una actualización opcional. No es necesario para las implementaciones existentes.

Antes de empezar

- La memoria RAM de la máquina virtual del nodo de administración es de 24 GB.
- El nodo de administración que pretende actualizar es la versión 12.0 y utiliza redes IPv4. La versión 12.5 o posterior del nodo de administración no admite IPv6.



Para comprobar la versión de su nodo de administración, inicie sesión en su nodo de administración y consulte el número de versión de Element en el banner de inicio de sesión.

- Has actualizado tu paquete de servicios de administración a la última versión utilizando NetApp Hybrid Cloud Control. Puede acceder a NetApp Hybrid Cloud Control desde la siguiente IP:
`https://<ManagementNodeIP>`
- Si está actualizando su nodo de administración a la versión 12.5 o posterior, necesita los servicios de administración 2.21.61 o posterior para continuar.
- Ha configurado un adaptador de red adicional (si es necesario) siguiendo las instrucciones para ["Configurar una NIC de almacenamiento adicional"](#).



Los volúmenes persistentes podrían requerir un adaptador de red adicional si eth0 no puede enrutarse 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 12.3.x o posterior.

Pasos

1. Inicie sesión en la máquina virtual del nodo de administración mediante SSH o acceso a la consola.
2. Descarga el "[nodo de gestión ISO](#)" para el software Element desde el sitio de soporte de NetApp a la máquina virtual del nodo de administración.



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 ejecutando md5sum en el archivo descargado y compare el resultado con el 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 administración y copie el contenido al sistema de archivos utilizando 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 de inicio y desmonte el archivo ISO desde /mnt :

```
sudo umount /mnt
```

6. Elimine la imagen ISO para ahorrar espacio en el nodo de administración:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

7. En el nodo de administración que está actualizando, ejecute el siguiente comando para actualizar la versión del sistema operativo del nodo de administración. El script conserva todos los archivos de configuración necesarios después de la actualización, como la configuración del compilador y el proxy de

Active IQ .

```
sudo /sf/rtfi/bin/sfrtfi_inplace  
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

El nodo de gestión se reinicia con un nuevo sistema operativo una vez finalizado el proceso de actualización.



Después de ejecutar el comando sudo descrito en este paso, la sesión SSH se finaliza. El acceso a la consola es necesario para continuar la monitorización. 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 inicie sesión, podrá confirmar la nueva versión del sistema operativo en el banner SSH que indica que la actualización se realizó correctamente.

8. En el nodo de administración, ejecute el `redploy-mnode` Script para conservar la configuración anterior de los servicios de administración:



El script conserva la configuración anterior de los servicios de administración, incluida la configuración del servicio recopilador Active IQ , los controladores (vCenters) o el proxy, según su configuración.

```
sudo /sf/packages/mnode/redploy-mnode -mu <mnode user>
```



Si previamente habías deshabilitado la funcionalidad SSH en el nodo de administración, necesitas ["Deshabilitar SSH nuevamente"](#) en el nodo de gestión recuperado. Capacidad SSH que proporciona ["Acceso a la sesión del túnel de soporte remoto \(RST\) de NetApp Support"](#) Está habilitado en el nodo de administración de forma predeterminada.

Reconfigurar la autenticación mediante la API REST del nodo de administración

Puede conservar su nodo de administración existente si ha actualizado secuencialmente (1) los servicios de administración y (2) el almacenamiento de elementos. Si ha seguido un orden de actualización diferente, consulte los procedimientos para las actualizaciones de nodos de administración in situ.

Antes de empezar

- Has actualizado tus servicios de gestión a la versión 2.20.69 o posterior.
- Su clúster de almacenamiento ejecuta Element 12.3 o posterior.
- Has actualizado secuencialmente tus servicios de gestión y, posteriormente, has actualizado tu almacenamiento Element. No podrá reconfigurar la autenticación mediante este procedimiento a menos que haya completado las actualizaciones en la secuencia descrita.

Pasos

1. Abra la interfaz de usuario de la API REST del nodo de administración en el nodo de administración:

```
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 del cliente como `mnode-client` si el valor no está ya asignado.
 - c. Seleccione **Autorizar** para iniciar una sesión.
3. Desde la interfaz de usuario de la API REST, seleccione **POST /services/reconfigure-auth**.
4. Seleccione **Probarlo**.
5. Para el parámetro **load_images**, seleccione `true`.
6. Seleccione **Ejecutar**.

El cuerpo de la respuesta indica que la reconfiguración fue exitosa.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Servicios de gestión de actualizaciones

Puede actualizar sus servicios de administración a la última versión del paquete después de haber instalado el nodo de administración 11.3 o posterior.

A partir del lanzamiento del nodo de gestión Element 11.3, el diseño del nodo de gestión se ha modificado basándose en una nueva arquitectura modular que proporciona servicios individuales. Estos servicios modulares proporcionan una funcionalidad de gestión centralizada y extendida para un sistema de almacenamiento all-flash SolidFire. Los servicios de gestión incluyen telemetría del sistema, registro y servicios de actualización, el servicio QoSSIOC para el complemento Element para vCenter Server, NetApp Hybrid Cloud Control y más.

Acerca de esta tarea

El paquete de servicios de administración 2.27 incluye el complemento Element para vCenter Server 5.5, que solo es compatible con el nodo de administración 12.8. Cuando actualiza a los servicios de administración 2.27, debe cambiar la secuencia de actualización y actualizar el paquete de servicios de administración *después* de actualizar a Element 12.8 para tener compatibilidad entre el nodo de administración y los servicios de administración.

Si está actualizando a los servicios de administración 2.21.61 a 2.26.40, debe actualizar el paquete de servicios de administración *antes* de actualizar a Element 12.8.



- Los servicios de administración 2.22.7 incluyen el complemento Element para vCenter Server 5.0, que contiene el complemento remoto. Si utiliza el complemento Element, debe actualizar a los servicios de administración 2.22.7 o posterior para cumplir con la directiva de VMware que elimina la compatibilidad con complementos locales. ["Más información"](#).
- Para consultar las notas de la versión más reciente de los servicios de administración, que describen los servicios principales, las nuevas funciones, las correcciones de errores y las soluciones alternativas para cada paquete de servicios, consulte ["Notas de lanzamiento de los servicios de gestión"](#)

Lo que necesitarás

A partir de los servicios de administración 2.20.69, debe aceptar y guardar el Acuerdo de licencia de usuario final (EULA) antes de utilizar la interfaz de usuario o la API de NetApp Hybrid Cloud Control para actualizar los servicios de administración:

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

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

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar**, situado en la parte superior derecha de la interfaz.
4. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto las actualizaciones actuales y futuras** y seleccione **Guardar**.

Opciones de actualización

Puede actualizar los servicios de administración mediante la interfaz de usuario de NetApp Hybrid Cloud Control o la API REST del nodo de administración:

- [Servicios de gestión de actualizaciones mediante Hybrid Cloud Control](#)(Método recomendado)
- [Actualizar los servicios de administración mediante la API del nodo de administración](#).

Servicios de gestión de actualizaciones mediante Hybrid Cloud Control

Puede actualizar sus servicios de administración de NetApp mediante NetApp Hybrid Cloud Control.

Los paquetes de servicios de administración proporcionan funcionalidades mejoradas y correcciones para su instalación fuera de las versiones principales.

Antes de empezar

- Está ejecutando el nodo de administración 11.3 o posterior.
- Si está actualizando los servicios de administración a la versión 2.16 o posterior y está ejecutando un nodo de administración de la versión 11.3 a la 11.8, deberá aumentar la RAM de la máquina virtual de su nodo de administración antes de actualizar los servicios de administración:
 - a. Apague la máquina virtual del nodo de administración.
 - b. Cambie la RAM de la máquina virtual del nodo de administración de 12 GB a 24 GB de RAM.
 - c. Encienda la máquina virtual del nodo de administración.
- Su versión de clúster ejecuta el software NetApp Element 11.3 o posterior.
- Has actualizado tus servicios de gestión al menos a la versión 2.1.326. Las actualizaciones de NetApp Hybrid Cloud Control no están disponibles en paquetes de servicios anteriores.



Para obtener una lista de los servicios disponibles para cada versión del paquete de servicios, consulte la ["Notas de la versión de los servicios de gestión"](#) .

Pasos

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

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

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar**, situado en la parte superior derecha de la interfaz.
4. En la página de Actualizaciones, seleccione la pestaña **Servicios de administración**.
5. Siga las instrucciones de la página para descargar y guardar un paquete de actualización de servicios de administración en su computadora.
6. Seleccione **Examinar** para localizar el paquete que guardó y cárguelo.

Una vez cargado el paquete, la actualización se inicia automáticamente.

Una vez iniciada la actualización, podrá consultar su estado 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.

Actualizar los servicios de administración mediante la API del nodo de administración.

Lo ideal es que los usuarios realicen las actualizaciones de los servicios de gestión desde NetApp Hybrid Cloud Control. Sin embargo, puede cargar, extraer e implementar manualmente una actualización del paquete de servicios para los servicios de administración en el nodo de administración mediante la API REST. Puedes ejecutar cada comando desde la interfaz de usuario de la API REST para el nodo de administración.

Antes de empezar

- Ha implementado un nodo de administración de software NetApp Element versión 11.3 o posterior.
- Si está actualizando los servicios de administración a la versión 2.16 o posterior y está ejecutando un nodo de administración de la versión 11.3 a la 11.8, deberá aumentar la RAM de la máquina virtual de su nodo de administración antes de actualizar los servicios de administración:
 - a. Apague la máquina virtual del nodo de administración.
 - b. Cambie la RAM de la máquina virtual del nodo de administración de 12 GB a 24 GB de RAM.
 - c. Encienda la máquina virtual del nodo de administración.
- Su versión de clúster ejecuta el software NetApp Element 11.3 o posterior.
- Has actualizado tus servicios de gestión al menos a la versión 2.1.326. Las actualizaciones de NetApp Hybrid Cloud Control no están disponibles en paquetes de servicios anteriores.



Para obtener una lista de los servicios disponibles para cada versión del paquete de servicios, consulte la ["Notas de la versión de los servicios de gestión"](#).

Pasos

1. Abra la interfaz de usuario de la API REST en el nodo de administración:
<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 del cliente como `mnode-client` si el valor no está ya asignado.

- c. Seleccione **Autorizar** para iniciar una sesión.
- d. Cerrar la ventana.
3. Cargue y extraiga el paquete de servicios en el nodo de administración utilizando este comando: `PUT /services/upload`
4. Implemente los servicios de administración en el nodo de administración: `PUT /services/deploy`
5. Supervise el estado de la actualización: `GET /services/update/status`

Una actualización exitosa devuelve un resultado similar al siguiente ejemplo:

```
{
  "current_version": "2.10.29",
  "details": "Updated to version 2.17.52",
  "status": "success"
}
```

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Actualizar el software Element

Para actualizar el software NetApp Element , puede utilizar la interfaz de usuario de NetApp Hybrid Cloud Control o la API REST. Ciertas operaciones se suprimen durante una actualización de software de Element, como agregar y quitar nodos, agregar y quitar unidades y comandos asociados con iniciadores, grupos de acceso a volúmenes y redes virtuales, entre otros.



El paquete de servicios de administración 2.27 incluye el complemento Element para vCenter Server 5.5, que solo es compatible con el nodo de administración 12.8. Cuando actualiza a los servicios de administración 2.27, debe cambiar la secuencia de actualización y actualizar el paquete de servicios de administración *después* de actualizar a Element 12.8 para tener compatibilidad entre el nodo de administración y los servicios de administración.

Si está actualizando a los servicios de administración 2.21.61 a 2.26.40, debe actualizar el paquete de servicios de administración *antes* de actualizar a Element 12.8.

Antes de empezar

- **Privilegios de administrador:** Usted tiene permisos de administrador del clúster de almacenamiento para realizar la actualización.
- **Ruta de actualización válida:** Ha comprobado la información de la ruta de actualización para la versión de Element a la que está actualizando y ha verificado 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 el software NetApp Element ."]

A partir de Element 12.5, NetApp HealthTools ya no es compatible con las actualizaciones de software de Element. Si está utilizando Element 11.0 o 11.1, primero debe ["Actualizar a Element 12.3.x usando HealthTools"](#) y luego actualice a Element 12.5 o posterior utilizando NetApp Hybrid Cloud Control.

- **Sincronización de la hora del sistema:** Se ha asegurado de que la hora del sistema en todos los nodos esté sincronizada y de que NTP esté configurado correctamente para el clúster de almacenamiento y los nodos. Cada nodo debe configurarse con un servidor de nombres DNS en la interfaz web de cada nodo. ([https://\[IP address\]:442](#)) sin fallos de clúster sin resolver relacionados con la asimetría temporal.
- **Puertos del sistema:** Si utiliza NetApp Hybrid Cloud Control para las actualizaciones, se ha asegurado de que los puertos necesarios estén abiertos. Ver ["puertos de red"](#) Para más información.
- **Nodo de administración:** Para la interfaz de usuario y la API de NetApp Hybrid Cloud Control, el nodo de administración de su entorno ejecuta la versión 11.3.
- **Estado del clúster:** Ha verificado que el clúster está listo para actualizarse. Ver ["Ejecute las comprobaciones de estado del almacenamiento de Element antes de actualizar el almacenamiento."](#) .
- **Controlador de administración de placa base (BMC) actualizado para nodos de almacenamiento H610S:** Ha actualizado la versión del BMC para sus nodos H610S. Ver el ["Notas de la versión e instrucciones de actualización"](#) .
- **Tiempo del proceso de actualización:** Ha programado tiempo suficiente para realizar su actualización. Cuando actualice al software Element 12.5 o posterior, el tiempo del proceso de actualización variará según su versión actual del software Element y las actualizaciones de firmware.

Nodo de almacenamiento	Versión actual del software Element	Tiempo aproximado de instalación de software y firmware por nodo ¹	Tiempo aproximado de sincronización de datos por nodo ²	Tiempo total aproximado de actualización por nodo
Todos los nodos SolidFire y NetApp de la serie H con firmware actualizado ³	12.x	15 minutos	De 10 a 15 minutos	De 20 a 30 minutos
H610S y H410S	12.x y 11.8	60 minutos	De 30 a 60 minutos	De 90 a 120 minutos
H610S	11.7 y anteriores	90 minutos	De 40 a 70 minutos	De 130 a 160 minutos También debes "Realizar un apagado completo del nodo y una desconexión de la alimentación" para cada nodo H610S.

¹Para obtener una matriz completa de firmware y firmware de controladores para su hardware, consulte ["Versiones de firmware de almacenamiento compatibles para nodos de almacenamiento SolidFire"](#) .

²Si se combina un clúster con una carga de IOPS de escritura elevada con un tiempo de actualización de

firmware más largo, el tiempo de sincronización de datos aumentará.

³ Los siguientes nodos no son compatibles. Si intenta actualizar uno de estos nodos a una versión de Element no compatible, verá un error que indica que el nodo no es compatible con Element 12.x:

- Comenzando con los nodos de almacenamiento Element 12.8, SF4805, SF9605, SF19210 y SF38410.
- Comenzando con los nodos de almacenamiento Element 12.7, SF2405 y SF9608 y los nodos FC FC0025 y SF-FCN-01.
- **Acuerdo de licencia de usuario final (EULA):** A partir de los servicios de administración 2.20.69, debe aceptar y guardar el EULA antes de utilizar la interfaz de usuario o la API de NetApp Hybrid Cloud Control para actualizar el software Element:
 - a. Abra la dirección IP del nodo de administración en un navegador web:

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

- b. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento.
- c. Seleccione **Actualizar**, situado en la parte superior derecha de la interfaz.
- d. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto las actualizaciones actuales y futuras** y seleccione **Guardar**.

Opciones de actualización

Elija una de las siguientes opciones de actualización de software de Element:

- [Utilice la interfaz de usuario de NetApp Hybrid Cloud Control para actualizar el almacenamiento de Element.](#)
- [Utilice la API de NetApp Hybrid Cloud Control para actualizar el almacenamiento de Element.](#)



Si está actualizando un nodo de la serie H610S a Element 12.5 o posterior y el nodo ejecuta una versión de Element anterior a la 11.8, deberá realizar los pasos de actualización adicionales que se describen en este documento. ["Artículo de la base de conocimientos"](#) para cada nodo de almacenamiento. Si está utilizando Element 11.8 o posterior, no se requieren pasos de actualización adicionales.

Utilice la interfaz de usuario de NetApp Hybrid Cloud Control para actualizar el almacenamiento de Element.

Mediante la interfaz de usuario de NetApp Hybrid Cloud Control, puede actualizar un clúster de almacenamiento.



Para conocer los posibles problemas que puedan surgir al actualizar clústeres de almacenamiento mediante NetApp Hybrid Cloud Control y sus soluciones alternativas, consulte este documento. ["Artículo de la base de conocimientos"](#).

Pasos

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

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

-
2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar**, situado en la parte superior derecha de la interfaz.
4. En la página **Actualizaciones**, seleccione **Almacenamiento**.

La pestaña **Almacenamiento** muestra los clústeres de almacenamiento que forman parte de su instalación. Si un clúster es inaccesible para NetApp Hybrid Cloud Control, no se mostrará en la página **Actualizaciones**.

-
-
-
-
5. Elija entre las siguientes opciones y realice el conjunto de pasos que correspondan 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 descargó. b. Espere a que finalice la carga. Una barra de progreso muestra el estado de la carga.  Si abandona la ventana del navegador, se perderá la carga del archivo. Aparece un mensaje en pantalla una vez que el archivo se ha cargado y validado correctamente. La validación puede tardar varios minutos. Si abandona la ventana del navegador en este momento, la carga del archivo se conservará. c. Seleccione Iniciar actualización.  El Estado de actualización cambia durante la actualización para reflejar el estado del proceso. También cambia en respuesta a las acciones que realice, como pausar la actualización, o si la actualización devuelve un error. Ver Cambios en el estado de la actualización .  Mientras la actualización está en curso, puede abandonar la página y volver a ella más tarde para continuar supervisando el progreso. La página no actualiza dinámicamente el estado ni la versión actual si la fila del clúster está contraída. Para actualizar la tabla, debe expandir la fila del clúster o bien actualizar la página. Podrá descargar los registros una vez finalizada la actualización.

Opción	Pasos
Estás actualizando un clúster H610S que ejecuta una versión de Element anterior a la 11.8.	a. Seleccione la flecha desplegable junto al clúster que está actualizando y seleccione una de las versiones de actualización disponibles. b. Seleccione Iniciar actualización. Una vez finalizada la actualización, la interfaz de usuario le solicitará que realice pasos de actualización adicionales. c. Complete los pasos adicionales requeridos en el "Artículo de la base de conocimientos" , y confirmar en la interfaz de usuario que ha completado la fase 2. Podrá descargar los registros una vez finalizada la actualización. Para obtener información sobre los distintos cambios en el estado de las actualizaciones, consulte Cambios en el estado de la actualización .

Cambios en el estado de la actualización

Aquí están los diferentes estados que muestra la columna **Estado de actualización** en la interfaz de usuario antes, durante y después del proceso de actualización:

Estado de actualización	Descripción
A hoy	El clúster se actualizó a la última versión disponible de Element.
Versiones disponibles	Hay disponibles versiones más recientes del firmware de Element y/o del almacenamiento 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 fallos a nivel de nodo y el ID de cada nodo del clúster a medida que avanza la actualización. Puede supervisar el estado de cada nodo utilizando la interfaz de usuario de Element o el complemento NetApp Element para la interfaz de usuario de vCenter Server.
Pausa de actualización	Puedes optar por pausar la actualización. Dependiendo del estado del proceso de actualización, la operación de pausa puede tener éxito o fracasar. Verás una ventana emergente en la interfaz de usuario que te pedirá que confirmes la operación de pausa. Para garantizar que el clúster se encuentre en un lugar seguro antes de pausar una actualización, la operación de actualización puede tardar hasta dos horas en pausarse por completo. Para reanudar la actualización, seleccione Reanudar .

Estado de actualización	Descripción
Paused	Has pausado la actualización. Seleccione Reanudar para reanudar el proceso.
Error	Se ha producido un error durante la actualización. Puede descargar el registro de errores y enviarlo al soporte de NetApp . Una vez resuelto el error, puede volver a la página y seleccionar Reanudar . Al reanudar la actualización, la barra de progreso retrocede durante unos minutos mientras el sistema realiza la comprobación de estado y verifica el estado actual de la actualización.
Completo con seguimiento	Solo para nodos H610S que se actualicen desde una versión de Element anterior a la 11.8. Una vez completada la fase 1 del proceso de actualización, este estado le solicita que realice pasos de actualización adicionales (consulte la sección correspondiente). "Artículo de la base de conocimientos"). Después de completar la fase 2 y confirmar que la ha completado, el estado cambia a Actualizado .

Utilice la API de NetApp Hybrid Cloud Control para actualizar el almacenamiento de Element.

Puede utilizar las API para actualizar los nodos de almacenamiento de un clúster a la última versión del software Element. Puedes utilizar la herramienta de automatización que prefieras para ejecutar las API. El flujo de trabajo de la API que se documenta aquí utiliza como ejemplo la interfaz de usuario de la API REST disponible en el nodo de administración.

Pasos

1. Descargue el paquete de actualización de almacenamiento en un dispositivo que sea accesible para el nodo de administración.

Acceda al software Element. ["página de descargas"](#) y descarga la última imagen del nodo de almacenamiento.

2. Cargue el paquete de actualización de almacenamiento al nodo de administración:

- a. Abra la interfaz de usuario de la API REST del nodo de administración en el nodo de administración:

```
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 del cliente como `mnode-client` .
- iii. Seleccione **Autorizar** para iniciar una sesión.
- iv. Cierre la ventana de autorización.

- c. Desde la interfaz de usuario de la API REST, seleccione **POST /packages**.

- d. Seleccione **Probarlo**.

- e. Seleccione **Examinar** y elija el paquete de actualización.
 - f. Seleccione **Ejecutar** para iniciar la carga.
 - g. A partir de la respuesta, copie y guarde el ID del paquete.("id") para su uso en un paso posterior.
3. Verifique el estado de la carga.
- a. Desde la interfaz de usuario de la API REST, seleccione **GET /packages/{id}/status**.
 - b. Seleccione **Probarlo**.
 - c. Introduzca el ID del paquete que copió en el paso anterior en **id**.
 - d. Seleccione **Ejecutar** para iniciar la solicitud de estado.

La respuesta indica `state` como `SUCCESS` cuando esté completo.

4. Localice el ID del clúster de almacenamiento:

- a. Abra la interfaz de usuario de la API REST del nodo de administración en el nodo de administración:

```
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 del cliente como `mnode-client`.
 - iii. Seleccione **Autorizar** para iniciar una sesión.
 - iv. Cierre la ventana de autorización.
 - c. Desde la interfaz de usuario de la API REST, seleccione **GET /installations**.
 - d. Seleccione **Probarlo**.
 - e. Seleccione **Ejecutar**.
 - f. Copie el ID del recurso de instalación de la respuesta.("id").
 - g. Desde la interfaz de usuario de la API REST, seleccione **GET /installations/{id}**.
 - h. Seleccione **Probarlo**.
 - i. Pegue el ID del activo de instalación en el campo **id**.
 - j. Seleccione **Ejecutar**.
 - k. A partir de la respuesta, copie y guarde el ID del clúster de almacenamiento.("id") del clúster que pretende actualizar para su uso en un paso posterior.
5. Ejecutar la actualización de almacenamiento:

- a. Abra la interfaz de usuario de la API REST de almacenamiento en el nodo de administración:

```
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 del cliente como `mnode-client`.
- iii. Seleccione **Autorizar** para iniciar una sesión.
- iv. Cierre la ventana de autorización.
- c. Seleccione **POST /actualizaciones**.
- d. Seleccione **Probarlo**.
- e. Introduzca el ID del paquete de actualización en el campo de parámetros.
- f. Introduzca el ID del clúster de almacenamiento en el campo de parámetros.

La carga útil debería ser 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 forma parte de la respuesta.
6. Verifique el progreso y los resultados de la actualización:
- a. Seleccione **GET /upgrades/{upgradeld}**.
 - b. Seleccione **Probarlo**.
 - c. Introduzca el ID de actualización del paso anterior en **upgradeld**.
 - d. Seleccione **Ejecutar**.
 - e. Realice una de las siguientes acciones si surgen problemas o requisitos especiales durante la actualización:

Opción	Pasos
Debe corregir los problemas de salud del clúster debido a <code>failedHealthChecks</code> mensaje en el cuerpo de la respuesta.	i. Consulte el artículo de la base de conocimientos específico que se indica para cada problema o realice la solución indicada. ii. Si se especifica un KB, complete el proceso descrito en el artículo KB correspondiente. iii. Después de haber resuelto los problemas del clúster, vuelva a autenticarse si es necesario y seleccione PUT /upgrades/{upgradeld}. iv. Seleccione Probarlo. v. Introduzca el ID de actualización del paso anterior en upgradeld. vi. Ingresar <code>"action": "resume"</code> en el cuerpo de la solicitud. <pre>{ "action": "resume" }</pre> vii. Seleccione Ejecutar.
Debe pausar la actualización porque la ventana de mantenimiento está finalizando o por otro motivo.	i. Vuelva a autenticarse si es necesario y seleccione PUT /upgrades/{upgradeld}. ii. Seleccione Probarlo. iii. Introduzca el ID de actualización del paso anterior en upgradeld. iv. Ingresar <code>"action": "pause"</code> en el cuerpo de la solicitud. <pre>{ "action": "pause" }</pre> v. Seleccione Ejecutar.

Opción	Pasos
Si está actualizando un clúster H610S que ejecuta una versión de Element anterior a la 11.8, verá el estado <code>finishedNeedsAck</code> en el cuerpo de la respuesta. Debe realizar pasos de actualización adicionales para cada nodo de almacenamiento H610S.	i. Complete los pasos de actualización adicionales en este "Artículo de la base de conocimientos" para cada nodo. ii. Vuelva a autenticarse si es necesario y seleccione PUT /upgrades/{upgradeld}. iii. Seleccione Probarlo. iv. Introduzca el ID de actualización del paso anterior en upgradeld. v. Ingresar <code>"action": "acknowledge"</code> en el cuerpo de la solicitud. <pre>{ "action": "acknowledge" }</pre> vi. Seleccione Ejecutar.

f. Ejecute la API **GET /upgrades/{upgradeld}** varias veces, según sea necesario, hasta que el proceso esté completo.

Durante la actualización, `status` indica `running` si no se producen errores. A medida que se actualiza cada nodo, el `step` cambia de valor a `NodeFinished`.

La actualización finalizó correctamente cuando `percent` El valor es 100 y el `state` indica `finished`.

¿Qué ocurre si falla una actualización utilizando NetApp Hybrid Cloud Control?

Si una unidad o un nodo falla durante una actualización, la interfaz de usuario de Element mostrará fallos del clúster. El proceso de actualización no pasa al siguiente nodo y espera a que se resuelvan los fallos del clúster. La barra de progreso en la interfaz de usuario muestra que la actualización está esperando a que se resuelvan los fallos del clúster. En esta etapa, seleccionar **Pausar** en la interfaz de usuario no funcionará, porque la actualización espera a que el clúster esté en buen estado. Deberá ponerse en contacto con el soporte de NetApp para que le ayuden con la investigación del fallo.

NetApp Hybrid Cloud Control tiene un período de espera preestablecido de tres horas, durante el cual puede ocurrir uno de los siguientes escenarios:

- Los fallos del clúster se resuelven en un plazo de tres horas y se reanuda la actualización. En este caso, no es necesario que tome ninguna medida.
- El problema persiste después de tres horas y el estado de la actualización muestra **Error** con un banner rojo. Puede reanudar la actualización seleccionando **Reanudar** una vez resuelto el problema.
- El soporte de NetApp ha determinado que es necesario interrumpir temporalmente la actualización para tomar medidas correctivas antes de que transcurran las tres horas. El soporte técnico utilizará la API para cancelar la actualización.



Si se interrumpe la actualización del clúster mientras se está actualizando un nodo, es posible que las unidades se extraigan del nodo de forma incorrecta. Si las unidades se extraen de forma incorrecta, volver a agregarlas durante una actualización requerirá la intervención manual del soporte de NetApp. Es posible que el nodo esté tardando más en realizar las actualizaciones de firmware o las 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.

Encuentra más información

- ["Documentación del software SolidFire y 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 administración, puede realizar actualizaciones solo de firmware en sus nodos de almacenamiento utilizando la interfaz de usuario de NetApp Hybrid Cloud Control y la API REST. Este procedimiento no actualiza el software Element y le permite actualizar el firmware de almacenamiento fuera de una versión principal de Element.

Lo que necesitarás

- **Privilegios de administrador:** Usted tiene permisos de administrador del clúster de almacenamiento para realizar la actualización.
- **Sincronización de la hora del sistema:** Se ha asegurado de que la hora del sistema en todos los nodos esté sincronizada y de que NTP esté configurado correctamente para el clúster de almacenamiento y los nodos. Cada nodo debe configurarse con un servidor de nombres DNS en la interfaz web de cada nodo. ([https://\[IP address\]:442](https://[IP address]:442)) sin fallos de clúster sin resolver relacionados con la asimetría temporal.
- **Puertos del sistema:** Si utiliza NetApp Hybrid Cloud Control para las actualizaciones, se ha asegurado de que los puertos necesarios estén abiertos. Ver ["puertos de red"](#) Para más información.
- **Nodo de administración:** Para la interfaz de usuario y la API de NetApp Hybrid Cloud Control, el nodo de administración de su entorno ejecuta la versión 11.3.
- **Servicios de gestión:** Ha actualizado su paquete de servicios de gestión a la última versión.



Para los nodos de almacenamiento H610S que ejecutan la versión 12.0 del software Element, debe aplicar el parche D 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 D antes de actualizar. Ver ["Notas de la versión 2.27 del paquete de firmware de almacenamiento"](#).



Debe actualizar al paquete de servicios de administración más reciente antes de actualizar el firmware de sus nodos de almacenamiento. Si está actualizando su software Element a la versión 12.2 o posterior, necesita los servicios de administración 2.14.60 o posterior para continuar.

- **Estado del clúster:** Ha ejecutado comprobaciones de estado. Ver ["Ejecute las comprobaciones de estado del almacenamiento de Element antes de actualizar el almacenamiento."](#)
- **Controlador de administración de placa base (BMC) actualizado para nodos H610S:** Ha actualizado

la versión del BMC para sus nodos H610S. Ver ["Notas de la versión e instrucciones de actualización"](#) .



Para obtener una matriz completa de firmware y firmware de controladores para su hardware, consulte ["Versiones de firmware de almacenamiento compatibles para nodos de almacenamiento SolidFire"](#) .

- **Tiempo del proceso de actualización:** Ha programado tiempo suficiente para realizar su actualización. Cuando actualice al software Element 12.5 o posterior, el tiempo del proceso de actualización variará según su versión actual del software Element y las actualizaciones de firmware.

Nodo de almacenamiento	Versión actual del software Element	Tiempo aproximado de instalación de software y firmware por nodo ¹	Tiempo aproximado de sincronización de datos por nodo ²	Tiempo total aproximado de actualización por nodo
Todos los nodos SolidFire y NetApp de la serie H con firmware actualizado ³	12.x	15 minutos	De 10 a 15 minutos	De 20 a 30 minutos
H610S y H410S	12.x y 11.8	60 minutos	De 30 a 60 minutos	De 90 a 120 minutos
H610S	11.7 y anteriores	90 minutos	De 40 a 70 minutos	De 130 a 160 minutos También debes "Realizar un apagado completo del nodo y una desconexión de la alimentación" para cada nodo H610S.

¹Para obtener una matriz completa de firmware y firmware de controladores para su hardware, consulte ["Versiones de firmware de almacenamiento compatibles para nodos de almacenamiento SolidFire"](#) .

²Si se combina un clúster con una carga de IOPS de escritura elevada con un tiempo de actualización de firmware más largo, el tiempo de sincronización de datos aumentará.

³ Los siguientes nodos no son compatibles. Si intenta actualizar uno de estos nodos a una versión de Element no compatible, verá un error que indica que el nodo no es compatible con Element 12.x:

- Comenzando con los nodos de almacenamiento Element 12.8, SF4805, SF9605, SF19210 y SF38410.
- Comenzando con los nodos de almacenamiento Element 12.7, SF2405 y SF9608 y los nodos FC FC0025 y SF-FCN-01.

- **Acuerdo de licencia de usuario final (EULA):** A partir de los servicios de administración 2.20.69, debe aceptar y guardar el EULA antes de utilizar la interfaz de usuario o la API de NetApp Hybrid Cloud Control para actualizar el firmware del almacenamiento:
 - a. Abra la dirección IP del nodo de administración en un navegador web:

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

- b. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento.
- c. Seleccione **Actualizar**, situado en la parte superior derecha de la interfaz.
- d. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto las actualizaciones actuales y futuras** y seleccione **Guardar**.

Opciones de actualización

Elija una de las siguientes opciones de actualización del firmware de almacenamiento:

- [Utilice la interfaz de usuario de NetApp Hybrid Cloud Control para actualizar el firmware del almacenamiento.](#)
- [Utilice la API de NetApp Hybrid Cloud Control para actualizar el firmware del almacenamiento.](#)

Utilice la interfaz de usuario de NetApp Hybrid Cloud Control para actualizar el firmware del almacenamiento.

Puede utilizar la interfaz de usuario de NetApp Hybrid Cloud Control para actualizar el firmware de los nodos de almacenamiento de su clúster.

Lo que necesitarás

- Si su nodo de administración no está conectado a Internet, usted tiene ["Descargué el paquete de firmware de almacenamiento"](#).



Para conocer los posibles problemas que puedan surgir al actualizar clústeres de almacenamiento mediante NetApp Hybrid Cloud Control y sus soluciones alternativas, consulte la documentación. ["Artículo de la base de conocimientos"](#).



El proceso de actualización tarda aproximadamente 30 minutos por nodo de almacenamiento. Si está actualizando un clúster de almacenamiento Element a un firmware de almacenamiento más reciente que la versión 2.76, los nodos de almacenamiento individuales solo se reiniciarán durante la actualización si se escribió un nuevo firmware en el nodo.

Pasos

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

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

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar**, situado en la parte superior derecha de la interfaz.
4. En la página **Actualizaciones**, seleccione **Almacenamiento**.



La pestaña **Almacenamiento** muestra los clústeres de almacenamiento que forman parte de su instalación. Si un clúster es inaccesible para NetApp Hybrid Cloud Control, no se mostrará en la página **Actualizaciones**. Si tiene clústeres que ejecutan Element 12.0 o posterior, verá la versión actual del paquete de firmware indicada para estos clústeres. Si los nodos de un mismo clúster tienen diferentes versiones de firmware o a medida que avanza la actualización, verá **Múltiple** en la columna **Versión actual del paquete de firmware**. Puede seleccionar **Múltiple** para navegar a la página **Nodos** y comparar las versiones de firmware. Si todos sus clústeres ejecutan versiones de Element anteriores a la 12.0, no verá ninguna información sobre los números de versión del paquete de firmware.

Si el clúster está actualizado y/o no hay paquetes de actualización disponibles, las pestañas **Elemento** y **Solo firmware** no se muestran. Estas pestañas tampoco se muestran cuando hay una actualización en curso. Si se muestra la pestaña **Elemento**, pero no la pestaña **Solo firmware**, no hay paquetes de firmware disponibles.

5. Seleccione la flecha desplegable situada junto al clúster que está actualizando.
6. Seleccione **Examinar** para cargar el paquete de actualización que descargó.
7. Espere a que finalice la carga. Una barra de progreso muestra el estado de la carga.



Si abandona la ventana del navegador, se perderá la carga del archivo.

Aparece un mensaje en pantalla una vez que el archivo se ha cargado y validado correctamente. La validación puede tardar varios minutos. Si abandona la ventana del navegador en este momento, la carga del archivo se conservará.

8. Seleccione **Solo firmware** y elija entre las versiones de actualización disponibles.
9. Seleccione **Iniciar actualización**.



El **Estado de actualización** cambia durante la actualización para reflejar el estado del proceso. También cambia en respuesta a las acciones que realice, como pausar la actualización, o si la actualización devuelve un error. Ver [Cambios en el estado de la actualización](#).



Mientras la actualización está en curso, puede abandonar la página y volver a ella más tarde para continuar supervisando el progreso. La página no actualiza dinámicamente el estado ni la versión actual si la fila del clúster está contraída. Para actualizar la tabla, debe expandir la fila del clúster o bien actualizar la página.

Podrá descargar los registros una vez finalizada la actualización.

Cambios en el estado de la actualización

Aquí están los diferentes estados que muestra la columna **Estado de actualización** en la interfaz de usuario antes, durante y después del proceso de actualización:

Estado de actualización	Descripción
A hoy	El clúster se actualizó a la última versión de Element disponible o el firmware se actualizó a la última versión.

Estado de actualización	Descripción
No se pudo detectar	Este estado se muestra cuando la API del servicio de almacenamiento devuelve un estado de actualización que no se encuentra en la lista enumerada de posibles estados de actualización.
Versiones disponibles	Hay disponibles versiones más recientes del firmware de Element y/o del almacenamiento 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 fallos a nivel de nodo y el ID de cada nodo del clúster a medida que avanza la actualización. Puede supervisar el estado de cada nodo utilizando la interfaz de usuario de Element o el complemento NetApp Element para la interfaz de usuario de vCenter Server.
Pausa de actualización	Puedes optar por pausar la actualización. Dependiendo del estado del proceso de actualización, la operación de pausa puede tener éxito o fracasar. Verás una ventana emergente en la interfaz de usuario que te pedirá que confirmes la operación de pausa. Para garantizar que el clúster se encuentre en un lugar seguro antes de pausar una actualización, la operación de actualización puede tardar hasta dos horas en pausarse por completo. Para reanudar la actualización, seleccione Reanudar .
Paused	Has pausado la actualización. Seleccione Reanudar para reanudar el proceso.
Error	Se ha producido un error durante la actualización. Puede descargar el registro de errores y enviarlo al soporte de NetApp . Una vez resuelto el error, puede volver a la página y seleccionar Reanudar . Al reanudar la actualización, la barra de progreso retrocede durante unos minutos mientras el sistema realiza la comprobación de estado y verifica el estado actual de la actualización.

¿Qué ocurre si falla una actualización utilizando NetApp Hybrid Cloud Control?

Si una unidad o un nodo falla durante una actualización, la interfaz de usuario de Element mostrará fallos del clúster. El proceso de actualización no pasa al siguiente nodo y espera a que se resuelvan los fallos del clúster. La barra de progreso en la interfaz de usuario muestra que la actualización está esperando a que se resuelvan los fallos del clúster. En esta etapa, seleccionar **Pausar** en la interfaz de usuario no funcionará, porque la actualización espera a que el clúster esté en buen estado. Deberá ponerse en contacto con el soporte de NetApp para que le ayuden con la investigación del fallo.

NetApp Hybrid Cloud Control tiene un período de espera preestablecido de tres horas, durante el cual puede ocurrir uno de los siguientes escenarios:

- Los fallos del clúster se resuelven en un plazo de tres horas y se reanuda la actualización. En este caso,

no es necesario que tome ninguna medida.

- El problema persiste después de tres horas y el estado de la actualización muestra **Error** con un banner rojo. Puede reanudar la actualización seleccionando **Reanudar** una vez resuelto el problema.
- El soporte de NetApp ha determinado que es necesario interrumpir temporalmente la actualización para tomar medidas correctivas antes de que transcurran las tres horas. El soporte técnico utilizará la API para cancelar la actualización.



Si se interrumpe la actualización del clúster mientras se está actualizando un nodo, es posible que las unidades se extraigan del nodo de forma incorrecta. Si las unidades se extraen de forma incorrecta, volver a agregarlas durante una actualización requerirá la intervención manual del soporte de NetApp. Es posible que el nodo esté tardando más en realizar las actualizaciones de firmware o las 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 NetApp Hybrid Cloud Control para actualizar el firmware del almacenamiento.

Puede utilizar las API para actualizar los nodos de almacenamiento de un clúster a la última versión del software Element. Puedes utilizar la herramienta de automatización que prefieras para ejecutar las API. El flujo de trabajo de la API que se documenta aquí utiliza como ejemplo la interfaz de usuario de la API REST disponible en el nodo de administración.

Pasos

1. Descargue el paquete de actualización del firmware de almacenamiento a un dispositivo accesible para el nodo de administración; acceda al software Element. "[página de descargas](#)" y descarga la última imagen de firmware de almacenamiento.
2. Cargue el paquete de actualización del firmware de almacenamiento al nodo de administración:
 - a. Abra la interfaz de usuario de la API REST del nodo de administración en el nodo de administración:

```
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 del cliente como `mnode-client`.
 - iii. Seleccione **Autorizar** para iniciar una sesión.
 - iv. Cierre la ventana de autorización.
 - c. Desde la interfaz de usuario de la API REST, seleccione **POST /packages**.
 - d. Seleccione **Probarlo**.
 - e. Seleccione **Examinar** y elija el paquete de actualización.
 - f. Seleccione **Ejecutar** para iniciar la carga.
 - g. A partir de la respuesta, copie y guarde el ID del paquete.(`"id"`) para su uso en un paso posterior.
3. Verifique el estado de la carga.
 - a. Desde la interfaz de usuario de la API REST, seleccione **GET /packages/{id}/status**.
 - b. Seleccione **Probarlo**.

- c. Introduzca el ID del paquete de firmware que copió en el paso anterior en **id**.
- d. Seleccione **Ejecutar** para iniciar la solicitud de estado.

La respuesta indica `state` como `SUCCESS` cuando esté completo.

4. Localice el ID del activo de instalación:

- a. Abra la interfaz de usuario de la API REST del nodo de administración en el nodo de administración:

```
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 del cliente como `mnode-client`.
 - iii. Seleccione **Autorizar** para iniciar una sesión.
 - iv. Cierre la ventana de autorización.
- c. Desde la interfaz de usuario de la API REST, seleccione **GET /installations**.
- d. Seleccione **Probarlo**.
- e. Seleccione **Ejecutar**.
- f. Copie el ID del recurso de instalación de la respuesta.(`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. Desde la interfaz de usuario de la API REST, seleccione **GET /installations/{id}**.
- h. Seleccione **Probarlo**.
 - i. Pegue el ID del activo de instalación en el campo **id**.
 - j. Seleccione **Ejecutar**.
- k. A partir de la respuesta, copie y guarde el ID del clúster de almacenamiento.(`"id"`) del clúster que pretende actualizar para su uso en un paso posterior.

```

"storage": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterUuid": "a1bd1111-4f1e-46zz-ab6f-0a1111b1111x",
        "id": "a1bd1111-4f1e-46zz-ab6f-a1a1a111b012",

```

5. Ejecutar la actualización del firmware de almacenamiento:

- a. Abra la interfaz de usuario de la API REST de almacenamiento en el nodo de administración:

```
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 del cliente como `mnode-client`.
- iii. Seleccione **Autorizar** para iniciar una sesión.
- iv. Cerrar la ventana.

- c. Seleccione **POST /actualizaciones**.

- d. Seleccione **Probarlo**.

- e. Introduzca el ID del paquete de actualización en el campo de parámetros.

- f. Introduzca el ID del clúster de almacenamiento en el campo de parámetros.

- 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 forma parte de la respuesta.
6. Verifique el progreso y los resultados de la actualización:
- a. Seleccione **GET /upgrades/{upgradeld}**.
 - b. Seleccione **Probarlo**.
 - c. Introduzca el ID de actualización del paso anterior en **upgradeld**.
 - d. Seleccione **Ejecutar**.
 - e. Realice una de las siguientes acciones si surgen problemas o requisitos especiales durante la actualización:

Opción	Pasos
Debe corregir los problemas de salud del clúster debido a <code>failedHealthChecks</code> mensaje en el cuerpo de la respuesta.	i. Consulte el artículo de la base de conocimientos específico que se indica para cada problema o realice la solución indicada. ii. Si se especifica un KB, complete el proceso descrito en el artículo KB correspondiente. iii. Después de haber resuelto los problemas del clúster, vuelva a autenticarse si es necesario y seleccione PUT /upgrades/{upgradeld}. iv. Seleccione Probarlo. v. Introduzca el ID de actualización del paso anterior en upgradeld. vi. Ingresar <code>"action": "resume"</code> en el cuerpo de la solicitud. <pre>{ "action": "resume" }</pre> vii. Seleccione Ejecutar.
Debe pausar la actualización porque la ventana de mantenimiento está finalizando o por otro motivo.	i. Vuelva a autenticarse si es necesario y seleccione PUT /upgrades/{upgradeld}. ii. Seleccione Probarlo. iii. Introduzca el ID de actualización del paso anterior en upgradeld. iv. Ingresar <code>"action": "pause"</code> en el cuerpo de la solicitud. <pre>{ "action": "pause" }</pre> v. Seleccione Ejecutar.

f. Ejecute la API **GET /upgrades/{upgradeld}** varias veces, según sea necesario, hasta que el proceso esté completo.

Durante la actualización, `status` indica `running` si no se producen errores. A medida que se actualiza cada nodo, el `step` cambia de valor a `NodeFinished`.

La actualización finalizó correctamente cuando `percent` El valor es 100 y el `state` indica `finished`.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Actualizar el complemento Element para vCenter Server

Para los entornos vSphere existentes con un complemento NetApp Element registrado para VMware vCenter Server, puede actualizar el registro de su complemento después de actualizar primero el paquete de servicios de administración que contiene el servicio del complemento.

Puede actualizar el registro del complemento en vCenter Server Virtual Appliance (vCSA) o Windows mediante la utilidad de registro. Debe cambiar su registro para el complemento de vCenter en cada servidor vCenter donde necesite utilizar el complemento.



El paquete de servicios de administración 2.27 incluye el complemento Element para vCenter Server 5.5, que solo es compatible con el nodo de administración 12.8. Cuando actualiza a los servicios de administración 2.27, debe cambiar la secuencia de actualización y actualizar el paquete de servicios de administración *después* de actualizar a Element 12.8 para tener compatibilidad entre el nodo de administración y los servicios de administración.

El paquete de servicios de administración 2.22.7 incluye el complemento Element para vCenter Server 5.0, que contiene el complemento remoto. Si utiliza el complemento Element, debe actualizar a los servicios de administración 2.22.7 o posterior para cumplir con la directiva de VMware que elimina la compatibilidad con complementos locales. ["Más información"](#).

Complemento Element vCenter versión 5.0 o posterior

Este procedimiento de actualización abarca los siguientes escenarios de actualización:

- Está actualizando al complemento Element para vCenter Server 5.5, 5.4, 5.3, 5.2, 5.1 o 5.0.
- Está actualizando a un cliente web vSphere HTML5 8.0 o 7.0.



El complemento Element para vCenter 5.0 o posterior no es compatible con vCenter Server 6.7 y 6.5.



Al actualizar de Element Plug-in para vCenter Server 4.x a 5.x, los clústeres ya configurados con el complemento se pierden, ya que los datos no se pueden copiar de una instancia de vCenter a un complemento remoto. Debe volver a agregar los clústeres al complemento remoto. Esta operación solo se realiza una vez al actualizar de un complemento local a uno remoto.

Complemento Element vCenter versión 4.10 o anterior

Este procedimiento de actualización abarca los siguientes escenarios de actualización:

- Está actualizando al complemento Element para vCenter Server 4.10, 4.9, 4.8, 4.7, 4.6, 4.5 o 4.4.
- Está actualizando a un cliente web vSphere HTML5 7.0, 6.7 o 6.5.

- El complemento no es compatible con VMware vCenter Server 8.0 para el complemento Element para VMware vCenter Server 4.x.
- El complemento no es compatible con VMware vCenter Server 6.5 para el complemento Element para VMware vCenter Server 4.6, 4.7 y 4.8.

- Estás actualizando a un cliente web vSphere Flash 6.7.



El complemento es compatible con vSphere Web Client versión 6.7 U2 para Flash, 6.7 U3 (Flash y HTML5) y 7.0 U1. El complemento no es compatible con la versión 6.7 U2 compilación 13007421 del cliente web HTML5 vSphere y otras compilaciones 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 para "[tu versión del complemento](#)".

Lo que necesitarás

- **Privilegios de administrador:** Usted tiene privilegios de rol de administrador de vCenter para instalar un complemento.
- **Actualizaciones de vSphere:** Ha realizado todas las actualizaciones de vCenter necesarias antes de actualizar el complemento NetApp Element para vCenter Server. Este procedimiento presupone que las actualizaciones de vCenter ya se han completado.
- **Servidor vCenter:** Su complemento vCenter versión 4.x o 5.x está registrado con un servidor vCenter. Desde la utilidad de registro(<https://<ManagementNodeIP>:9443>), seleccione **Estado de registro**, complete los campos necesarios y seleccione **Comprobar estado** para verificar que el complemento de vCenter ya esté registrado y el número de versión de la instalación actual.
- **Actualizaciones de servicios de gestión:** Has actualizado tu "[paquete de servicios de gestión](#)" a la última versión. Las actualizaciones del complemento de vCenter se distribuyen mediante actualizaciones de servicios de administración que se publican fuera de las versiones principales de productos para el almacenamiento all-flash NetApp SolidFire .
- **Actualizaciones del nodo de gestión:**

Complemento Element vCenter versión 5.0 o posterior

Estás ejecutando un nodo de administración que ha sido "[actualizado](#)" a la versión 12.3.x o posterior.

Complemento Element vCenter versión 4.10 o anterior

Para el complemento Element vCenter 4.4 a 4.10, está ejecutando un nodo de administración que ha sido "[actualizado](#)" a la versión 11.3 o posterior. El complemento de vCenter 4.4 o posterior requiere un nodo de administración 11.3 o posterior con una arquitectura modular que proporciona servicios individuales. Su nodo de administración debe estar encendido con su dirección IP o dirección DHCP configurada.

- **Mejoras en el almacenamiento de elementos:**
 - A partir del complemento Element vCenter 5.0, tendrá un clúster que ejecute el software NetApp Element 12.3.x o posterior.
 - Para el complemento Element vCenter 4.10 o anterior, tiene un clúster que ejecuta el software NetApp Element 11.3 o posterior.

- **Cliente web de vSphere:** Ha cerrado sesión en el cliente web de vSphere antes de comenzar cualquier actualización de complementos. El cliente web no reconocerá las actualizaciones realizadas durante este proceso en su complemento si no cierra sesión.

Pasos

1. Introduzca la dirección IP de su nodo de administración en un navegador, incluyendo el puerto TCP para el registro:

<https://<ManagementNodeIP>:9443> La interfaz de usuario de la utilidad de registro se abre en la página **Administrar credenciales de servicio QoSSIOC** para el complemento.

 Element Plug-in for vCenter Server Management Node

[QoSSIOC Service Management](#) [vCenter Plug-in Registration](#)

QoSSIOC Management

Manage Credentials

Restart QoSSIOC Service

Manage QoSSIOC Service Credentials

Old Password

Current password

Current password is required

New Password

New password

Must contain at least 8 characters with at least one lower-case and upper-case alphabet, a number and a special character like # \$ % & ' () * + , - . : ;

Confirm Password

Confirm New Password

New and confirm passwords must match

SUBMIT CHANGES

Contact NetApp Support at <http://mysupport.netapp.com>

2. Seleccione **Registro del complemento de vCenter**.

Complemento Element vCenter versión 5.0 o posterior

Aparece la página de registro del complemento de vCenter:

 **NetApp**

Element Plug-in for vCenter Server Management Node

GoSSIOC Service Management

vCenter Plug-in Registration

Manage vCenter Plug-in

Register Plug-in

Update Plug-in

Unregister Plug-in

Registration Status

vCenter Plug-in - Registration

Register version 5.0.0 of the NetApp Element Plug-in for vCenter Server with your vCenter server.
The Plug-in will not be deployed until a fresh vCenter login after registration.

vCenter Address

vCenter Server Address

Enter the IPV4, IPV6 or DNS name of the vCenter server to register plug-in on.

vCenter User Name

vCenter Admin User Name

Ensure this user is a vCenter user that has administrative privileges for registration.

vCenter Password

vCenter Admin Password

The password for the vCenter user name entered.

☐ Customize URL

Select to customize the Zip file URL.

Plug-in Zip URL

https://10.117.227.44:8333/vcp-ui/plugin.json

URL of XML initialization file

REGISTER

Contact NetApp Support at <http://mysupport.netapp.com>

Complemento Element vCenter versión 4.10 o anterior

Aparece la página de registro del complemento de vCenter:

Manage vCenter Plug-in

- Register Plug-in
- Update Plug-in
- Unregister Plug-in
- Registration Status

vCenter Plug-in - Registration

Register version of the NetApp Element Plug-in for vCenter Server with your vCenter server.
The Plug-in will not be deployed until a fresh vCenter login after registration.

vCenter Address vCenter Server Address

Enter the IPv4, IPv6 or DNS name of the vCenter server to register plug-in on.

vCenter User Name vCenter Admin User Name

Ensure this user is a vCenter user that has administrative privileges for registration.

vCenter Password vCenter Admin Password

The password for the vCenter user name entered.

☐ Customize URL

Select to customize the Zip file URL.

Plug-in Zip URL https://10.117.227.12:9443/solidfire-plugin-4.6.0-bin.zip

URL of XML initialization file

REGISTER

Contact NetApp Support at <http://mysupport.netapp.com>

3. Dentro de **Administrar complemento de vCenter**, seleccione **Actualizar complemento**.

4. Confirme o actualice la siguiente información:

- a. La dirección IPv4 o el FQDN del servicio vCenter en el que registrará su complemento.
- b. El nombre de usuario del administrador de vCenter.



Las credenciales de nombre de usuario y contraseña que introduzca deben pertenecer a un usuario con privilegios de rol de administrador de vCenter.

- c. La contraseña de administrador de vCenter.
- d. (Para servidores internos/sitios oscuros) Dependiendo de la versión de su complemento Element para vCenter, una URL personalizada para el archivo JSON del complemento o el archivo ZIP del complemento:

Complemento Element vCenter versión 5.0 o posterior

Una URL personalizada para el archivo JSON del complemento.



Puedes seleccionar **URL personalizada** para personalizar la URL si estás utilizando un servidor HTTP o HTTPS (sitio oscuro) o si has modificado el nombre del archivo JSON o la configuración de red. Para conocer los pasos de configuración adicionales si desea personalizar una URL, consulte la documentación del complemento Element para vCenter Server sobre cómo modificar las propiedades de vCenter para un servidor HTTP interno (sitio oscuro).

Complemento Element vCenter versión 4.10 o anterior

Una URL personalizada para el archivo ZIP del complemento.



Puedes seleccionar **URL personalizada** para personalizar la URL si estás utilizando un servidor HTTP o HTTPS (sitio oscuro) o si has modificado el nombre del archivo ZIP o la configuración de red. Para conocer los pasos de configuración adicionales si desea personalizar una URL, consulte la documentación del complemento Element para vCenter Server sobre cómo modificar las propiedades de vCenter para un servidor HTTP interno (sitio oscuro).

5. Seleccione **Actualizar**.

Cuando el registro se realiza correctamente, aparece un banner en la interfaz de usuario de la utilidad de registro.

6. Inicie sesión en vSphere Web Client como administrador de vCenter. Si ya ha iniciado sesión en vSphere Web Client, primero debe cerrar sesión, esperar de dos a tres minutos y luego volver a iniciarla.



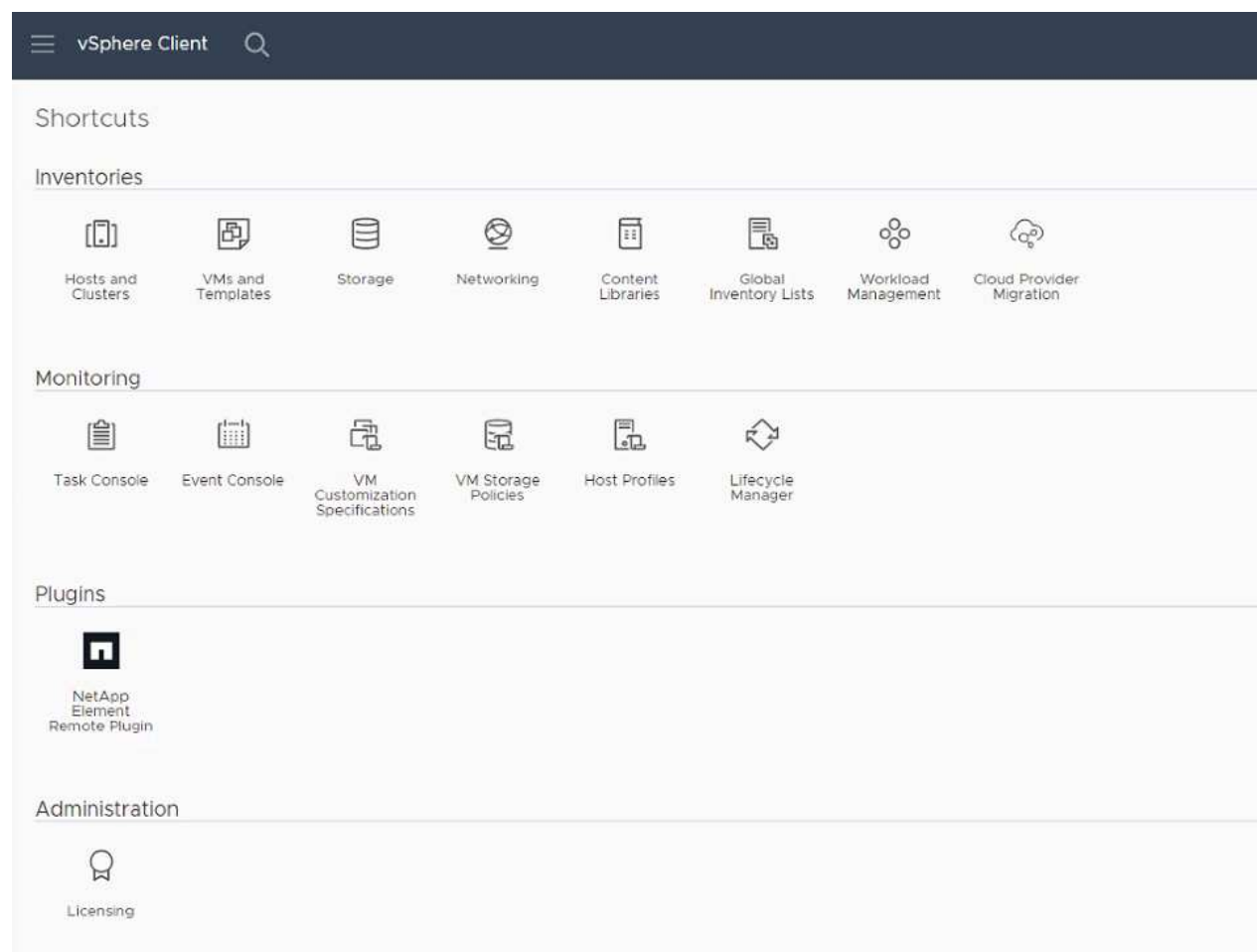
Esta acción crea una nueva base de datos y completa la instalación en el cliente web de vSphere.

7. En vSphere Web Client, busque las siguientes tareas completadas en el monitor de tareas para asegurarse de que la instalación se ha completado: `Download plug-in` y `Deploy plug-in`.

8. Verifique que los puntos de extensión del complemento aparezcan en la pestaña **Accesos directos** del cliente web de vSphere y en el panel lateral.

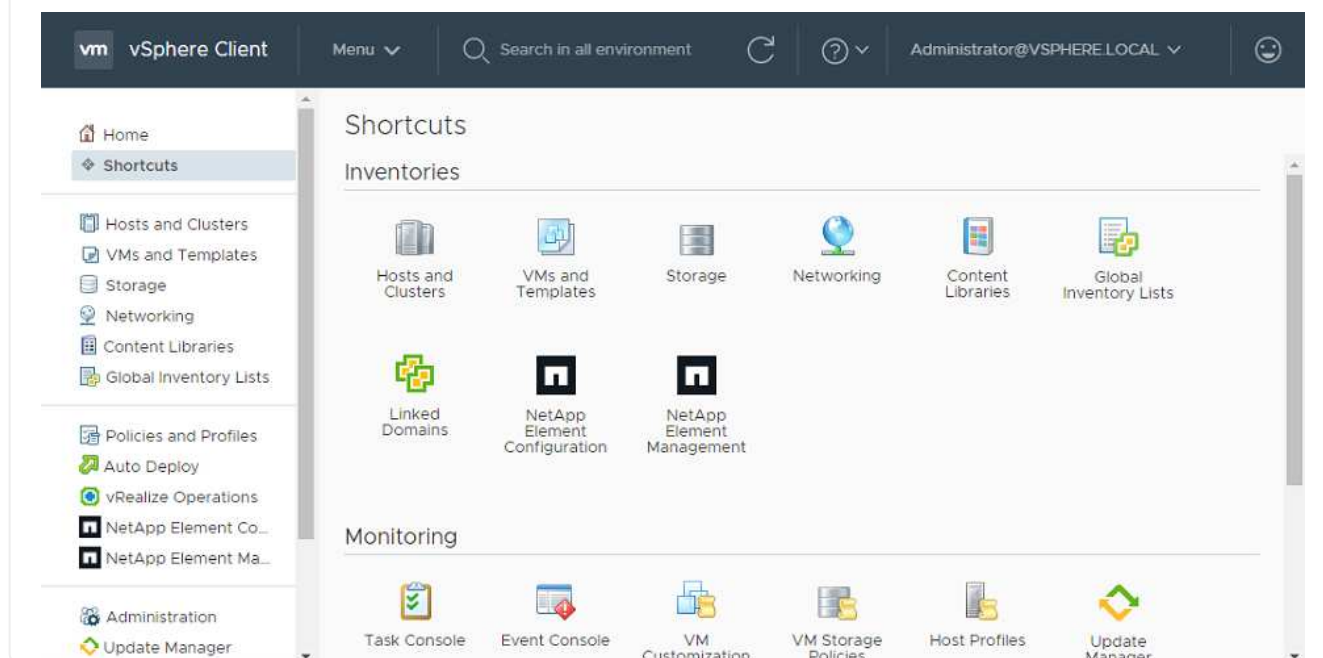
Complemento Element vCenter versión 5.0 o posterior

Aparece el punto de extensión del complemento remoto de NetApp Element :



Complemento Element vCenter versión 4.10 o anterior

Aparecen los puntos de extensión de configuración y administración de NetApp Element :



Si los iconos del complemento de vCenter no están visibles, consulte "[Complemento Element para vCenter Server](#)" Documentación sobre la resolución de problemas del complemento.



Después de actualizar a NetApp Element Plug-in para vCenter Server 4.8 o posterior con VMware vCenter Server 6.7U1, si los clústeres de almacenamiento no aparecen en la lista o se produce un error del servidor en las secciones **Clústeres** y **Configuración de QoSSIOC** de la configuración de NetApp Element, consulte "[Complemento Element para vCenter Server](#)" Documentación sobre la resolución de estos errores.

9. Verifique el cambio de versión en la pestaña **Acerca de** en el punto de extensión *Configuración de NetApp Element * del complemento.

Debería ver los siguientes detalles de la versión:

```
NetApp Element Plug-in Version: 5.5
NetApp Element Plug-in Build Number: 16
```



El complemento de vCenter contiene contenido de ayuda en línea. Para asegurarte de que tu Ayuda contiene el contenido más reciente, borra la caché de tu navegador después de actualizar el complemento.

Encuentra más información

- "[Documentación del software SolidFire y Element](#)"
- "[Plugin de NetApp Element para vCenter Server](#)"

Actualice sus componentes de vSphere para un sistema de almacenamiento NetApp SolidFire con el complemento Element para vCenter Server.

Debe completar pasos adicionales al actualizar los componentes de VMware vSphere. Estos pasos son necesarios para los sistemas con el complemento Element para vCenter Server.

Pasos

1. Para las actualizaciones de vCSA, "[claro](#)" Configuración de QoSSIOC en el complemento (* Configuración de NetApp Element > Configuración de QoSSIOC*). El campo **Estado QoSSIOC** muestra **Not Configured** una vez finalizado el proceso.
2. Para actualizaciones de vCSA y Windows, "[dar de baja](#)" el complemento del servidor vCenter con el que está asociado mediante la utilidad de registro.
3. "[Actualizar vSphere, incluyendo vCenter Server, ESXi, máquinas virtuales y otros componentes de VMware.](#)"



Debe actualizar a NetApp Element Plug-in para vCenter Server 5.0 o posterior para poder implementar el complemento con VMware vCenter 7.0 Update 3 sin tener que aplicar una solución alternativa.

Al actualizar a VMware vCenter Server 7.0 Update 3, el complemento Element para vCenter Server 4.x no se implementa correctamente. Para resolver este problema utilizando Spring Framework 4, consulte ["Este artículo de la base de conocimientos"](#).

4. ["Registro"](#)El complemento Element para vCenter Server vuelve a estar disponible con vCenter.
5. ["Agregar clústeres"](#)usando el complemento.
6. ["Configurar los ajustes de QoSSIOC"](#)usando el complemento.
7. ["Habilitar QoSSIOC"](#)para todos los almacenes de datos controlados por el complemento.

Encuentra más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Documentación de versiones anteriores del software SolidFire y NetApp Element

La documentación de versiones anteriores está disponible en el sitio de soporte de NetApp .

- ["Documentación del elemento 12.2.1"](#)
- ["Documentación del elemento 12.2"](#)
- ["Documentación del elemento 12.0.1"](#)
- ["Documentación del elemento 12.0"](#)
- ["Documentación del elemento 11.8.2"](#)
- ["Documentación del elemento 11.8.1"](#)
- ["Documentación del elemento 11.8"](#)
- ["Documentación del elemento 11.7"](#)
- ["Documentación del elemento 11.5.1"](#)
- ["Documentación del elemento 11.5"](#)
- ["Documentación del elemento 11.3P1"](#)
- ["Documentación del elemento 11.3.2"](#)
- ["Documentación de Element 11.1 y versiones anteriores"](#)

Para más información

- ["Documentación del software SolidFire y Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas comerciales, patentes y más.

Copyright

["https://www.netapp.com/company/legal/copyright/"](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. Otros nombres de empresas y productos pueden ser marcas comerciales de sus respectivos propietarios.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patentes

Puede encontrar una lista actualizada 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/"](https://www.netapp.com/company/legal/privacy-policy/)

Código abierto

Los archivos de aviso proporcionan información sobre derechos de autor y licencias de terceros utilizados en el software de NetApp .

- ["Aviso para el software Element 12.8"](#)
- ["Aviso para el software Element 12.7"](#)
- ["Aviso para Ember OS 12.7"](#)
- ["Aviso para el nodo de administración 12.7"](#)
- ["Aviso para el software Element 12.5"](#)
- ["Aviso para el nodo de administración 12.5"](#)
- ["Aviso para los servicios de administración 2.27.40 \(complemento de NetApp Element para VMware vCenter Server 5.5.16\)"](#)
- ["Aviso para Servicios de administración 2.26.30 \(Complemento NetApp Element para VMware vCenter Server 5.4.1\)"](#)
- ["Aviso para Servicios de administración 2.25.42 \(Complemento NetApp Element para VMware vCenter Server 5.3.9\)"](#)
- ["Aviso para Servicios de administración 2.24.40 \(Complemento NetApp Element para VMware vCenter Server 5.2.12\)"](#)

- "Aviso para Servicios de administración 2.23.64 (Complemento NetApp Element para VMware vCenter Server 5.1.12)"
- "Aviso para Servicios de administración 2.22.7 (Complemento NetApp Element para VMware vCenter Server 5.0.37)"
- "Aviso para Servicios de administración 2.21.61 (Complemento NetApp Element para VMware vCenter Server 4.10.12)"
- "Aviso para Servicios de administración 2.20.69 (Complemento NetApp Element para vCenter Server 4.9.14)"
- "Aviso para Servicios de administración 2.19.48 (Complemento NetApp Element para vCenter Server 4.8.34)"
- "Aviso para Servicios de administración 2.18.91 (Complemento NetApp Element para vCenter Server 4.7.10)"
- "Aviso para Servicios de administración 2.17.56 (Complemento NetApp Element para vCenter Server 4.6.32)"
- "Aviso para Servicios de administración 2.17.52 (Complemento NetApp Element para vCenter Server 4.6.29)"
- "Aviso para Management Services 2.16 (Complemento NetApp Element para vCenter Server 4.6.29)"
- "Aviso para Management Services 2.14 (NetApp Element Plug-in para vCenter Server 4.5.42)"
- "Aviso para Management Services 2.13 (NetApp Element Plug-in para vCenter Server 4.5.42)"
- "Aviso sobre el paquete de firmware de almacenamiento 2.182.0"
- "Aviso sobre el paquete de firmware de almacenamiento 2.175.0"
- "Aviso sobre el paquete de firmware de almacenamiento 2.164.0"
- "Aviso sobre el paquete de firmware de almacenamiento 2.150"
- "Aviso sobre el paquete de firmware de almacenamiento 2.146"
- "Aviso sobre el paquete de firmware de almacenamiento 2.99.2"
- "Aviso sobre el paquete de firmware de almacenamiento 2.76"
- "Aviso sobre 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.