ONTAP y aplicaciones empresariales

Enterprise applications

NetApp
July 31, 2025

This PDF was generated from https://docs.netapp.com/es-es/ontap-apps-dbs/index.html on July 31, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

ONTAP y aplicaciones empresariales . . . 1
Épica . . . 2
Epic en ONTAP . . . 2
Específico . . . 2
Ámbito . . . 2
Destinatarios . . . 3
Epic en ONTAP . . . 3
EPIC en ONTAP . . . 3
Disponibilidad Epic en ONTAP . . . 4
Epic en la consolidación de ONTAP . . . 4
Épica de la eficiencia de ONTAP . . . 5
Rendimiento de ONTAP excepcional . . . 5
Escalabilidad de Epic en ONTAP . . . 7
Configuración épica de la eficiencia del almacenamiento . . . 8
Épica sobre la seguridad de ONTAP . . . 8
Arquitectura y diseño épicos . . . 9
Arquitectura épica . . . 9
Ajuste de tamaño épico . . . 12
Requisitos de almacenamiento de Epic . . . 13
Arquitectura épica con cuatro nodos . . . 14
Arquitectura épica de seis nodos . . . 15
Arquitectura épica de ocho nodos . . . 17
Configuración y prácticas recomendadas . . . 18
Epic en ONTAP - Utilidades de host . . . 18
Configuración de volumen y LUN épica . . . 19
Epic y protocolos de archivo . . . 21
Gestión del rendimiento épico . . . 21
Epic en ONTAP - protocolos . . . 21
Configuración épica de la eficiencia del almacenamiento . . . 22
Configuración épica de la eficiencia del almacenamiento . . . 22
Ajuste del tamaño del almacenamiento para Epic . . . 24
Información adicional sobre Epic en ONTAP . . . 24
Documentos de orientación al cliente épica . . . 24
Hyper-V. . . . 25
Directrices de puesta en marcha y prácticas recomendadas de almacenamiento . . . 25
Descripción general . . . 25
Almacenamiento de NetApp y entorno de Windows Server . . . 26
Aprovisionamiento en entornos SAN . . . 30
Aprovisionamiento en entornos SMB . . . 39
La infraestructura de almacenamiento de Hyper-V en NetApp . . . 42
Eficiencia del almacenamiento . . . 53
Seguridad . . . 56
Implemente Nano server . . . 56

Implemente el cluster de Hyper-V. 60
Implemente Hyper-V Live Migration en un entorno en clúster 61
Implemente Hyper-V Live Migration fuera de un entorno en clúster 62
Implemente Hyper-V Storage Live Migration 63
Implemente la réplica de Hyper-V fuera de un entorno en clúster 64
Implementar la réplica de Hyper-V en un entorno en clúster 65
Dónde encontrar información adicional 67
Microsoft SQL Server 68
Descripción general 68
Cargas de trabajo de Microsoft SQL Server 68
Configuración de la base de datos 69
Configuración de CPU 69
Configuración de memoria 72
Instancia compartida frente a instancia dedicada 75
Archivos tempdb 76
Configuración del almacenamiento en sistemas AFF/FAS 77
Descripción general 77
Archivos de base de datos y grupos de archivos 80
Eficiencia del almacenamiento 84
Protección de datos 89
Recuperación tras siniestros 92
Configuración de almacenamiento en sistemas ASA R2 113
Descripción general 113
Archivos de base de datos y grupos de archivos 115
Protección de datos 120
Recuperación tras siniestros 121
Seguridad de datos 137
Copias Snapshot 137
Snapshots a prueba de manipulación 137
Replicación de SnapMirror 138
Máquinas virtuales de almacenamiento 138
RBAC administrativo 138
Autenticación multifactor (MFA) 139
CONTROL DE ACCESO BASADO EN ROLES API 139
Verificación multi-admin (MAV) 139
MySQL 140
Descripción general 140
Configuración de la base de datos 140
Estructura de archivos 140
Parámetros de configuración 143
innodb_log_file_size 144
innodb_flush_log_at_trx_commit 144
innodb_doublewrite 145
innodb_buffer_pool_size 145
innodb_flush_method 145

innodb_io_capacity . . . 146
innodb_lru_scan_profund . . . 147
open_file_limits . . . 147
Configuración de hosts . . . 147
Colocación de contenedores . . . 148
Mesas de NFSv3 ranuras . . . 148
Programadores de I/O. . . . 148
Descriptores de archivo . . . 149
Configuración del almacenamiento . . . 149
NFS . . . 150
SAN . . . 151
Base de datos Oracle . . . 153
Bases de datos de Oracle en ONTAP . . . 153
Configuración de ONTAP . . . 153
RAID . . . 153
Gestión de la capacidad . . . 154
Máquinas virtuales de almacenamiento . . . 155
Gestión del rendimiento con QoS de ONTAP . . . 155
Eficiencia . . . 157
Aprovisionamiento ligero . . . 161
Recuperación tras fallos y cambio de ONTAP . . . 164
Configuración de la base de datos . . . 165
Tamaños de bloque . . . 165
db_file_multibloque_read_count . . . 166
filesystemio_options . . . 167
Tiempo de espera de RAC . . . 168
Configuración de hosts . . . 169
AIX . . . 169
HP-UX . . . 171
Linux . . . 173
ASMLib/AFD (Controlador de Filtro de ASM) . . . 177
Microsoft Windows . . . 179
Solaris . . . 179
Configuración de red . . . 185
Interfaces lógicas . . . 185
Configuración TCP/IP y ethernet . . . 190
Configuración de SAN FC . . . 191
Red de conexión directa . . . 192
Configuración del almacenamiento . . . 193
FC SAN . . . 193
NFS . . . 197
NVFAIL . . . 210
Utilidad de Reclamación de ASM (ASMRU) . . . 211
Virtualización . . . 211
Compatibilidad . . . 212

Presentación de almacenamiento . . . 212
Controladores paravirtualizados . . . 213
RAM de sobrecompromiso . . . 213
Segmentación de almacenes de datos . . . 214
Organización en niveles . . . 215
Descripción general . . . 215
Políticas de organización en niveles . . . 217
Estrategias de organización en niveles . . . 219
Interrupciones de acceso al almacén de objetos . . . 223
Protección de datos de Oracle . . . 223
Protección de datos con ONTAP . . . 224
Planificación de objetivos de tiempo, objetivos de punto de recuperación y acuerdos de nivel de servicio . . . 224
Disponibilidad de bases de datos . . . 227
Sumas de comprobación e integridad de los datos . . . 229
Conceptos básicos de backup y recuperación . . . 234
Recuperación ante desastres de Oracle . . . 248
Descripción general . . . 248
MetroCluster . . . 249
SnapMirror síncrono activo . . . 269
Migración de bases de datos de Oracle . . . 303
Descripción general . . . 303
Planificación de migración . . . 304
Procedimientos . . . 307
Scripts de ejemplo . . . 413
Notas adicionales . . . 426
Optimización del rendimiento y evaluación comparativa . . . 426
NFSv3 bloqueos obsoletos . . . 429
Verificación de la alineación de WAFL . . . 430
PostgreSQL . . . 436
Descripción general . . . 436
Configuración de la base de datos . . . 436
Arquitectura . . . 436
Parámetros de inicialización . . . 437
Configuración . . . 438
Espacios de tabla . . . 440
Configuración del almacenamiento . . . 440
NFS . . . 440
SAN . . . 442
Protección de datos . . . 444
Protección Ddta nativa . . . 444
Snapshot . . . 445
Software para la protección de datos . . . 446
SAP . . . 447
VMware . . . 448

VMware vSphere con ONTAP . . . 448
VMware vSphere con ONTAP . . . 448
¿Por qué elegir ONTAP para VMware vSphere? . . . 448
Almacenamiento unificado . . . 450
Herramientas de virtualización para ONTAP . . . 452
Volúmenes virtuales (vVols) y gestión basada en políticas de almacenamiento (SPBM) . . . 454
Almacenes de datos y protocolos . . . 455
Configuración de red . . . 470
Clonado de máquinas virtuales y almacenes de datos . . . 473
Protección de datos . . . 475
Calidad de servicio (QoS) . . . 478
Migración al cloud y backup . . . 484
Cifrado para datos de vSphere . . . 485
Active IQ Unified Manager . . . 486
Gestión basada en políticas de almacenamiento y vVols . . . 487
Planificador de recursos distribuidos de almacenamiento de VMware . . . 489
Host ESXi recomendado y otra configuración de ONTAP . . . 490
Virtual Volumes (vVols) con herramientas de ONTAP 10 . . . 494
Descripción general . . . 494
Lista de comprobación . . . 500
Usar vVols con ONTAP . . . 503
Puesta en marcha de vVols en sistemas AFF, ASA, ASA R2 y FAS . . . 508
Protección de vVols . . . 519
Resolución de problemas . . . 524
VMware Site Recovery Manager con ONTAP . . . 525
Recuperación de sitios en vivo de VMware con ONTAP . . . 525
Mejores prácticas de puesta en marcha . . . 527
Mejores prácticas operativas . . . 528
Topologías de replicación . . . 533
Solución de problemas de VLSRM/SRM cuando se usa la replicación de vVols . . . 541
Información adicional . . . 542
Clúster de almacenamiento vSphere Metro con ONTAP . . . 542
Clúster de almacenamiento vSphere Metro con ONTAP . . . 542
Descripción general de la solución de VMware vSphere . . . 545
Directrices de implementación y diseño de VMSC . . . 550
Resiliencia para eventos planificados y no planificados . . . 561
Situaciones de fallo para VMSC con MetroCluster . . . 562
Seguridad de los productos . . . 573
Herramientas de ONTAP para VMware vSphere . . . 573
Complemento de SnapCenter, VMware vSphere . . . 575
Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere . . . 578
Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere 9,13 . . . 578
Verificación de la integridad de las herramientas de ONTAP para los paquetes de instalación de VMware vSphere 9,13 . . . 578
Puertos y protocolos para las herramientas de ONTAP 9,13 . . . 580

Herramientas de ONTAP para puntos de acceso de VMware vSphere 9,13 (usuarios) . . . 581
ONTAP TOOLS 9,13 TLS mutuo (autenticación basada en certificados) . . . 582
Certificado HTTPS de ONTAP TOOLS 9,13 . . . 589
Banner de inicio de sesión de ONTAP tools 9,13 . . . 590
Tiempo de espera de inactividad para las herramientas de ONTAP 9,13 . . . 590
Número máximo de solicitudes simultáneas por usuario (protección de seguridad de red/ataque DOS) herramientas de ONTAP para VMware vSphere 9,13 . . . 590
Configuración del Protocolo de hora de red (NTP) para las herramientas ONTAP 9,13 . . . 591
Políticas de contraseñas para las herramientas de ONTAP 9,13 . . . 591
Avisos legales . . . 594
Derechos de autor . . . 594
Marcas comerciales . . . 594
Estadounidenses . . . 594
Política de privacidad . . . 594
Código abierto . . . 594
ONTAP . . . 594
Mediador de ONTAP para configuraciones IP de MetroCluster . . . 594

ONTAP y aplicaciones empresariales

Épica

Epic en ONTAP

La clave para la transformación digital es hacer más con sus datos.

Esta documentación sustituye al informe técnico *TR-3923 publicado anteriormente: Mejores prácticas de NetApp para Epic*.

Los hospitales necesitan grandes cantidades de datos para iniciar el camino de la transformación digital. Parte del proceso de tratar a los pacientes, gestionar los horarios del personal y los recursos médicos es que la información se recopila y procesa. Sin embargo, muchas acciones todavía se realizan manualmente o a través de sistemas obsoletos. La constante es que la cantidad de datos sigue creciendo de manera exponencial, por lo que se vuelve cada vez más difícil de gestionar.

La causa principal de este problema es que los datos hospitalarios a menudo se almacenan en silos de datos. Se dedica demasiado tiempo a entradas manuales y actualizaciones que conducen a agotamiento y errores. Este documento es sobre una parte de los datos sanitarios, Epic Electronic Health Records (EHR). Sin embargo, la estrategia de gestión de datos que aquí se cubre puede y debe aplicarse a todos los datos de atención médica. NetApp tiene un historial contrastado de modernización y simplificación de la infraestructura digital. Nuestra infraestructura de datos inteligente constituye la base de la transformación digital.

NetApp ofrece una solución de gestión de datos única para todas las necesidades sanitarias y podemos guiar a los hospitales en su viaje hacia la transformación digital. Al construir una base con estructura y soluciones inteligentes, el cuidado de la salud puede extraer todo el valor de esta valiosa información. Este marco puede ayudar a los proveedores médicos a diagnosticar enfermedades más rápidamente y desarrollar planes de tratamiento individualizados para apoyar mejor los procesos de toma de decisiones en situaciones de emergencia. También podrá crear su propia infraestructura de datos inteligente y permitir que su hospital desbloquee los silos de datos, facilite la interoperabilidad de los datos y proteja la información confidencial de los pacientes.

Utilice este documento como guía para construir e implementar correctamente la EHR de Epic. En lugar de crear varios silos de Epic, crea una única infraestructura de datos de Epic y transforma tu hospital.

Específico

Este documento describe las mejores prácticas para integrar el almacenamiento de NetApp en un entorno de software de Epic. Contiene las siguientes secciones:

- Conocimiento técnico del entorno de software Epic y sus requisitos de almacenamiento en varias configuraciones.
- Consideraciones sobre el almacenamiento épico, que describen factores de toma de decisiones importantes para las soluciones Epic.
- Recomendaciones de almacenamiento de NetApp, que describen prácticas recomendadas de configuración del almacenamiento de NetApp para satisfacer los requisitos de almacenamiento de Epic.

Ámbito

Este documento no cubre los siguientes temas:

- Requisitos cuantitativos de rendimiento y directrices sobre tamaño, que se tratan en "TR-3930i: Directrices

de configuración de NetApp para Epic" (se requiere inicio de sesión NetApp)

Destinatarios

NetApp asume que el lector tiene los siguientes conocimientos generales:

- Comprensión sólida de los conceptos DE SAN y NAS
- Familiaridad técnica con los sistemas de almacenamiento ONTAP
- Familiaridad técnica con la configuración y administración de ONTAP

Epic en ONTAP

EPIC en ONTAP

Epic es más fácil con ONTAP.

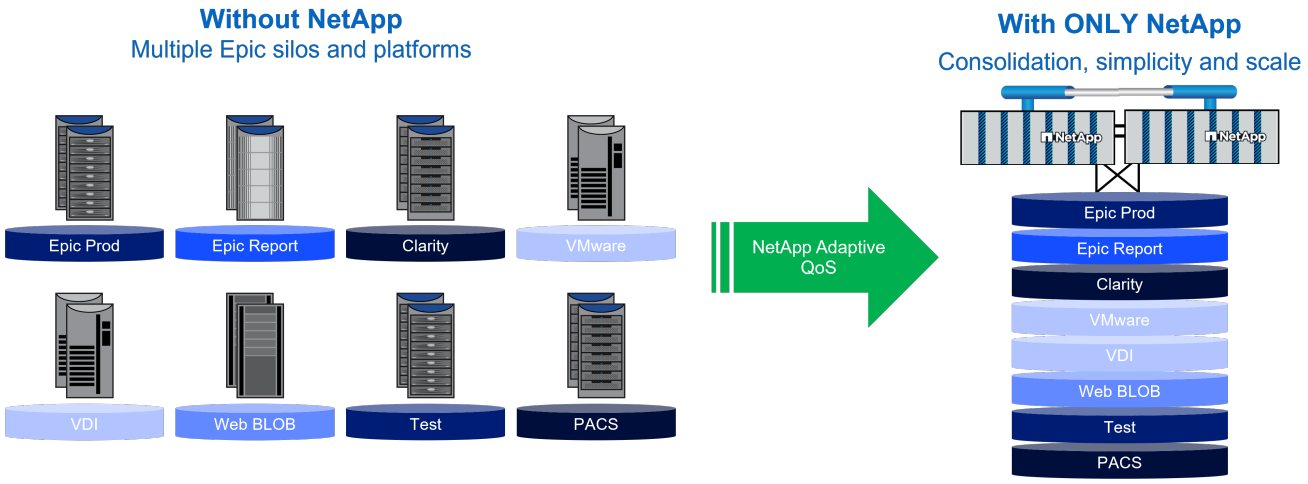
ONTAP es una plataforma de gestión de datos que le permite consolidar las cargas de trabajo de Epic al tiempo que cumple todos sus requisitos de rendimiento, protección de datos y gestión de datos.

Solo en NetApp puede estandarizar todas sus cargas de trabajo del sector sanitario para SAN, NAS y objetos en una única plataforma de gestión de datos de alta disponibilidad. ONTAP es la plataforma de software de almacenamiento con mayor implementación del mundo y cuenta con casi 30 años de innovación constante. Puede hacer frente a todos los retos de Epic con las herramientas nativas de gestión de datos de ONTAP y la integración de aplicaciones. No es necesario adquirir una multitud de herramientas de terceros para llenar las carencias de la solución.

Muchos proveedores de almacenamiento ofrecen un almacenamiento basado en bloques tradicional, fiable y rápido. Funcionan bien, pero normalmente se ponen en marcha en silos para ejecutar una única carga de trabajo, como producción, informes, claridad, VDI, VMware y NAS. Cada uno de estos silos tiene un hardware y herramientas de gestión diferentes, y generalmente están administrados por diferentes grupos de TI. Este enfoque tradicional se suma al mayor problema con la atención sanitaria actual: La complejidad.

Con NetApp, la gestión de datos es más fácil y eficiente. En lugar de destinar dinero a los problemas con los silos de gran tamaño, ONTAP utiliza la innovación y la tecnología para habilitar un acuerdo de nivel de servicio consistente y garantizado para cada carga de trabajo en una única plataforma mediante cualquier protocolo con protección de datos integrada. Estas funcionalidades y herramientas también se extienden al cloud que elija, tal y como se muestra a continuación.

Scale and simplicity for Healthcare



Disponibilidad Epic en ONTAP

El núcleo de ONTAP son las operaciones no disruptivas que permiten evitar costosas interrupciones en las operaciones empresariales.

NetApp ofrece una disponibilidad superior al 99,999999 %, basada en datos de producción, a los que NetApp Active IQ conoce como «casa». Cada par de alta disponibilidad del clúster no tiene ningún único punto de error. ONTAP se remonta a 1992 y es el software de gestión de datos más instalado en el mundo, con una historia excepcional como proveedor de almacenamiento fiable. Ahora, gracias a la supervisión proactiva de Active IQ y a la resolución automática del 97 % de los problemas, la disponibilidad es mayor y tiene mucho menos casos de soporte.

Epic recomienda utilizar sistemas de almacenamiento de alta disponibilidad para mitigar los fallos de los componentes de hardware. Esta recomendación abarca desde hardware básico (como fuentes de alimentación redundantes) hasta redes (como redes multivía).

Si necesita actualizar el almacenamiento, escalar verticalmente, escalar horizontalmente o reequilibrar cargas de trabajo en todo el clúster, la atención al paciente no se ve afectada. Es posible que mueva datos, pero nunca más tendrá que interrumpir la atención a los pacientes mediante migraciones de datos o renovaciones graduales. Cambie a la tecnología de última generación y prepárese para el futuro y evite los bloqueos del hardware. NetApp ofrece incluso una garantía de disponibilidad escrita del 100 %.

En el whitepaper encontrará más información sobre las funciones de fiabilidad, disponibilidad, capacidad de servicio y seguridad de NetApp"Fiabilidad, disponibilidad, capacidad de servicio y seguridad de NetApp ONTAP".

Epic en la consolidación de ONTAP

Uno de los mayores desafíos en la atención sanitaria es la ineficiencia de los entornos aislados.

Varias soluciones puntuales son creadas por varios grupos que impiden el progreso. Tener una estrategia unificada de gestión de datos mejora la eficiencia para acelerar la transformación. Tecnología disruptiva como la digitalización de registros de pacientes, ransomware y la IA generativa son todas las unidades que

necesitan una consolidación.

Con ONTAP puede consolidar archivo/bloque/objeto y cada una de sus cargas de trabajo de nivel 0/1/2/3, en las instalaciones y en el cloud, todas ellas ejecutándose en ONTAP.

Épica de la eficiencia de ONTAP

Epic se ejecuta en cabinas all-flash donde la mayor parte del coste es el disco. Por lo tanto, la eficiencia del almacenamiento es fundamental para reducir los costes.

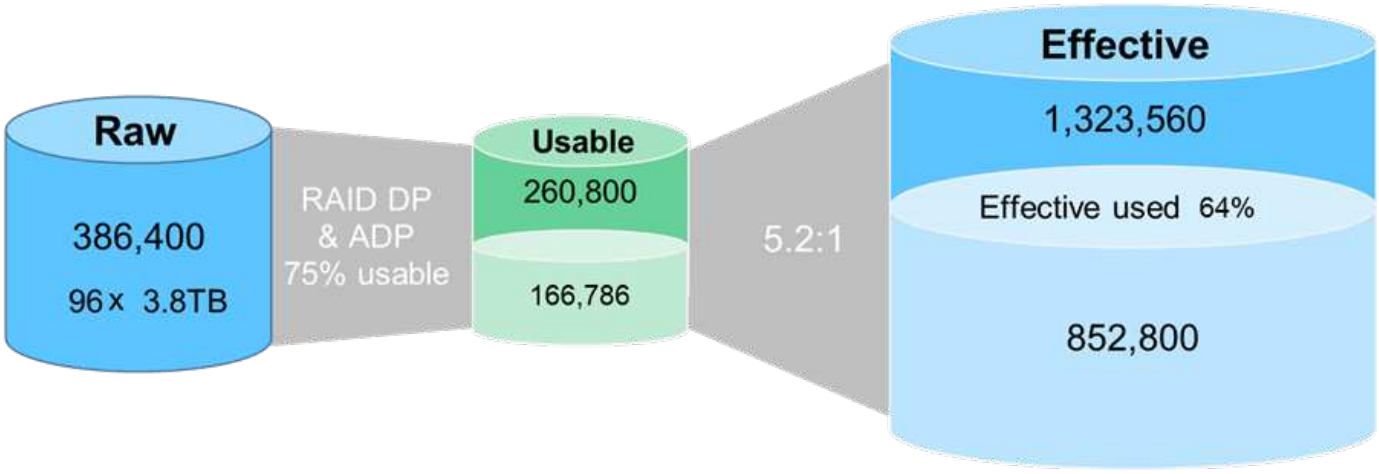
La eficiencia del almacenamiento inline de NetApp consigue unos ahorros de almacenamiento líderes en el sector sin afectar al rendimiento; además, ofrecemos una garantía de eficiencia escrita con las cabinas all-flash.

Al calcular la eficiencia del almacenamiento, es importante medir la capacidad bruta en utilizable para lograr la capacidad efectiva.

- **Capacidad bruta** antes de aplicar cualquier RAID, tamaño del disco por número de discos.
- * Capacidad utilizable * Después de aplicar RAID, cuánto almacenamiento utilizable está disponible.
- * Capacidad efectiva* Cuánto almacenamiento se aprovisiona y se presenta al host o cliente.

La figura siguiente es un cálculo de eficiencia de muestra de una puesta en marcha de Epic típica, que incluye todas las cargas de trabajo que requieren 852TB TB de almacenamiento efectivo y con una eficiencia de 5,2:1 que proporciona 1,32PB PB de datos efectivos totales.

En función del número de discos, la capacidad bruta a utilizable varía ligeramente.



NetApp no utiliza la tecnología Snapshot ni thin provisioning de NetApp para calcular la eficiencia del programa de garantía. Si lo hace, demostraría una eficiencia poco realista de 30-100:1, lo cual no significa nada al ajustar el tamaño de la capacidad de almacenamiento real.

Rendimiento de ONTAP excepcional

ONTAP introdujo las tecnologías flash en 2009 y es compatible con unidades SSD desde 2010. Esta larga experiencia con el almacenamiento flash permite a NetApp ajustar las funciones de ONTAP para optimizar el rendimiento de las unidades de estado sólido y

mejorar la resistencia de los medios flash a la vez que conserva las funcionalidades con gran cantidad de funciones de ONTAP.

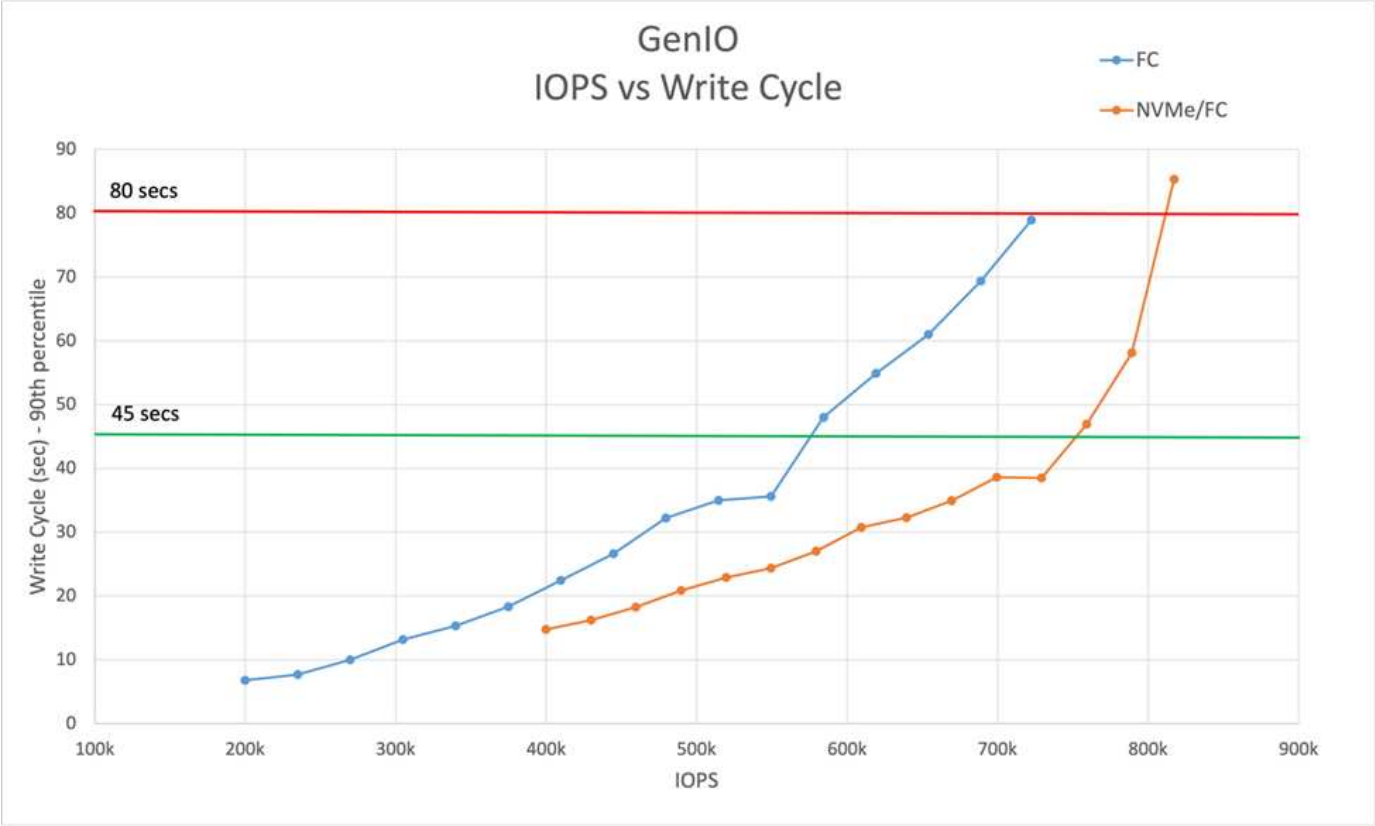
Desde el año 2020, todas las cargas de trabajo de Epic ODB deben estar en almacenamiento all-flash. Las cargas de trabajo de Epic suelen operar a aproximadamente entre 1.000 y 2.000 000 IOPS por terabyte de almacenamiento (bloques de 8k KB, tasa de lectura y escritura del 75 %/25 %, y 100 % aleatorio). Epic es muy sensible a la latencia, y la alta latencia tiene un efecto visible en la experiencia del usuario final, así como tareas operativas como la ejecución de informes, copias de seguridad, comprobaciones de integridad y tiempos de actualización del entorno.

- El factor limitante para las cabinas all-flash no es el de las unidades, sino que es la utilización de las controladoras.
- ONTAP utiliza una arquitectura activa-activa. Para obtener el rendimiento, los dos nodos de la pareja de alta disponibilidad escriben en las unidades.
- Este resultado es una utilización maximizada de la CPU, que es el factor más importante que permite a NetApp publicar el mejor rendimiento de Epic del sector.
- Las tecnologías NetApp RAID DP, Advanced Disk Partitioning (ADP) y WAFL cumplen todos los requisitos de Epic. Todas las cargas de trabajo distribuyen la I/O por todos los discos. Sin cuellos de botella.
- ONTAP está optimizado para escritura; las escrituras se reconocen una vez que se escriben en NVRAM reflejado antes de que se escriban en el disco a la velocidad de la memoria en línea.
- WAFL, NVRAM y la arquitectura modular permiten a NetApp utilizar software para innovar con eficiencias inline, cifrado y rendimiento. También permiten a NetApp introducir nuevas funciones y funcionalidades sin afectar al rendimiento.
- Históricamente, con cada nueva versión de ONTAP, hay un aumento del rendimiento y la eficiencia entre un 30 y un 50 %. El rendimiento es óptimo cuando se mantiene al día con ONTAP.

NVMe

Cuando el rendimiento es primordial, NetApp también admite NVMe/FC, el protocolo SAN FC de nueva generación.

Como se observa en la siguiente figura, en nuestras pruebas GENIO se consiguió un número mucho mayor de IOPS gracias al protocolo NVMe/FC frente al protocolo FC. La solución conectada con NVMe/FC alcanzó más de 700k 000 IOPS antes de superar el umbral del ciclo de escritura de 45 segundos. Al reemplazar comandos SCSI por NVMe, también se reduce significativamente la utilización en el host.



Escalabilidad de Epic en ONTAP

La Guía de configuración de hardware de Epic representa un crecimiento del ~20 % al año durante 3 años. Sin embargo, los entornos también pueden crecer inesperadamente.

NetApp puede escalar sin problemas el rendimiento y la capacidad hasta 12 nodos para clústeres NAS, SAN y de objetos. Como resultado, puede escalar horizontal y verticalmente sin interrupciones a medida que crece su negocio.

Epic Iris aporta más funciones de escalado. Permite a los clientes de mayor tamaño que tienen varias instancias Epic consolidarse en una única instancia. El "Arquitectura verificada de NetApp Epic en SAN moderna" documento demuestra que Epic puede escalar sin problemas cargas de trabajo consolidadas hasta 720K 000 IOPS en una sola alta disponibilidad y escalar horizontalmente hasta más de 4M 000 IOPS en un clúster. Puede escalar verticalmente de forma no disruptiva actualizando las controladoras o añadiendo discos a los clústeres existentes.

Los datos de NAS, SAN y objetos también pueden moverse de forma no disruptiva entre nodos del clúster. Cada pareja de alta disponibilidad del clúster puede ser cualquier combinación de tipos y tamaños de sistemas ONTAP FAS y AFF. Puede equilibrar sus cargas de trabajo en un único clúster para maximizar su inversión en almacenamiento.

ONTAP también ofrece la opción de utilizar el almacenamiento de objetos en StorageGRID o el cloud como destino de backup o destino automático por niveles de almacenamiento en frío. Esta funcionalidad permite liberar automáticamente en Object discos all-flash, snapshots de nivel y datos inactivos costosos.

Como resultado, Epic simplemente funciona mejor con la cartera de productos de NetApp, aprovechando ONTAP, varios protocolos, StorageGRID y el cloud que elija. Estos productos ofrecen opciones para recuperación ante desastres, archivado, análisis, clasificación por niveles, etc.

Configuración épica de la eficiencia del almacenamiento

Una copia de Snapshot es una copia de un momento específico de un volumen de solo lectura.

Una instantánea coloca un bloqueo lógico en todos los bloques del sistema de archivos activo. Las copias de Snapshot de NetApp ONTAP son casi instantáneas y no utilizan almacenamiento adicional.

Write anwhere File Layout, o WAFL, es un sistema de archivos de solo escritura; no realiza E/S adicionales, como copiar los datos de un bloque protegido mediante snapshot antes de sobrescribirlos. Nunca se mueven datos; por lo tanto, las copias Snapshot no afectan a la capacidad de almacenamiento ni al rendimiento. Las copias Snapshot proporcionan un enorme ahorro en almacenamiento, al tiempo que aumentan la solución de backup.

FlexClone

Un volumen NetApp ONTAP FlexClone es un clon de un volumen existente o una copia de Snapshot de un volumen existente. Por lo demás, es un volumen de ONTAP como cualquier otro, y puede clonarse, protegerse con copias Snapshot y configurarse mediante una política de calidad de servicio.

Al igual que sucede con las snapshots, un volumen FlexClone no necesita espacio adicional durante la creación. Solo los cambios en el clon requieren capacidad adicional.

Epic requiere de 10 a 30 copias de las bases de datos de producción para varios requisitos operativos como los backups de streaming, las comprobaciones de integridad y el almacenamiento provisional de los entornos de actualización. Se ha aumentado la necesidad de una solución basada en volúmenes FlexClone con el traslado a actualizaciones más frecuentes.

NetApp proporciona una solución de backup de Epic totalmente automatizada y una solución de actualización de Epic como parte de la solución con las herramientas Ansible y nativas de NetApp.

Épica sobre la seguridad de ONTAP

La seguridad es la principal preocupación para las organizaciones y los ejecutivos de la salud en la actualidad. Nunca ha sido tan difícil gestionar y las organizaciones se enfrentan a retos relacionados con el cumplimiento de normativas, el gobierno de datos, la protección antivirus y ransomware.

Una guía completa sobre Epic y la seguridad del almacenamiento se encuentra fuera del alcance de este documento; sin embargo"Guía de seguridad reforzada de ONTAP", detalla todas las funciones de seguridad completas y avanzadas disponibles en ONTAP.

NetApp Active IQ Unified Manager supervisa las infracciones de seguridad según la información incluida en la "TR-4569"consola y las notifica en ella para simplificar la administración de la seguridad. Estas herramientas pueden ayudar a tu organización a cumplir tus objetivos de seguridad para protegerlos, detectarlos y solucionarlos.

NetApp también se ha asociado con proveedores de seguridad para proporcionar integración a través de "FPolicy de NetApp" software para mejorar su oferta de seguridad. Además, "Autenticación multifactor (MFA)" se puede agregar para proteger su entorno Epic contra el acceso no autorizado con credenciales filtradas.

Por último, las copias Snapshot nativas de ONTAP y las tecnologías de SnapLock inmutables con

"Ciberalmacén de ONTAP", ofrecen una funcionalidad única de aislamiento interno para proteger los registros de pacientes contra el ransomware. Consulte la documentación de NetApp en "La solución de NetApp para ransomware". Para obtener un enfoque más estratégico de la seguridad, consulte "NetApp y Zero Trust".

Arquitectura y diseño épicos

Arquitectura épica

En esta sección se describe el entorno de software Epic y los componentes clave que requieren almacenamiento. Proporciona consideraciones clave para ayudar a guiar el diseño del almacenamiento.

Epic, con sede en Verona, Wisconsin, fabrica software para medianas y grandes grupos médicos, hospitales y organizaciones integradas de atención médica. Los clientes también incluyen hospitales comunitarios, instalaciones académicas, organizaciones de niños, proveedores de redes de seguridad y sistemas multihospitalarios. El software integrado de Epic abarca funciones clínicas, de acceso e ingresos y se extiende al hogar.

Este documento no cubre el amplio abanico de funciones admitidas por el software Epic. Sin embargo, desde el punto de vista del sistema de almacenamiento, todo el software Epic comparte una única base de datos centrada en el paciente para cada puesta en marcha. Epic está realizando la transición de la base de datos de InterSystems Caché a la nueva base de datos de InterSystems Iris. Debido a que los requisitos de almacenamiento son los mismos para Caché e Iris, nos referiremos a la base de datos como Iris a lo largo del resto de este documento. Iris está disponible para los sistemas operativos AIX y Linux.

Iris de InterSystems

InterSystems Iris es la base de datos utilizada por la aplicación Epic. En esta base de datos, el servidor de datos es el punto de acceso para los datos almacenados de forma persistente. El servidor de aplicaciones gestiona las consultas de la base de datos y realiza solicitudes de datos al servidor de datos. En la mayoría de los entornos de software de Epic, el uso de la arquitectura de multiprocesador simétrico (SMP) en un único servidor de base de datos basta para atender las solicitudes de base de datos de aplicaciones de Epic. En implementaciones de gran tamaño, se puede admitir un modelo distribuido mediante el protocolo de caché empresarial (ECP) de InterSystems.

El uso de hardware en clúster habilitado para recuperación tras fallos permite que un servidor de datos en espera acceda al mismo almacenamiento que el servidor de datos primario. También permite que el servidor de datos en espera asuma las responsabilidades de procesamiento durante un fallo de hardware.

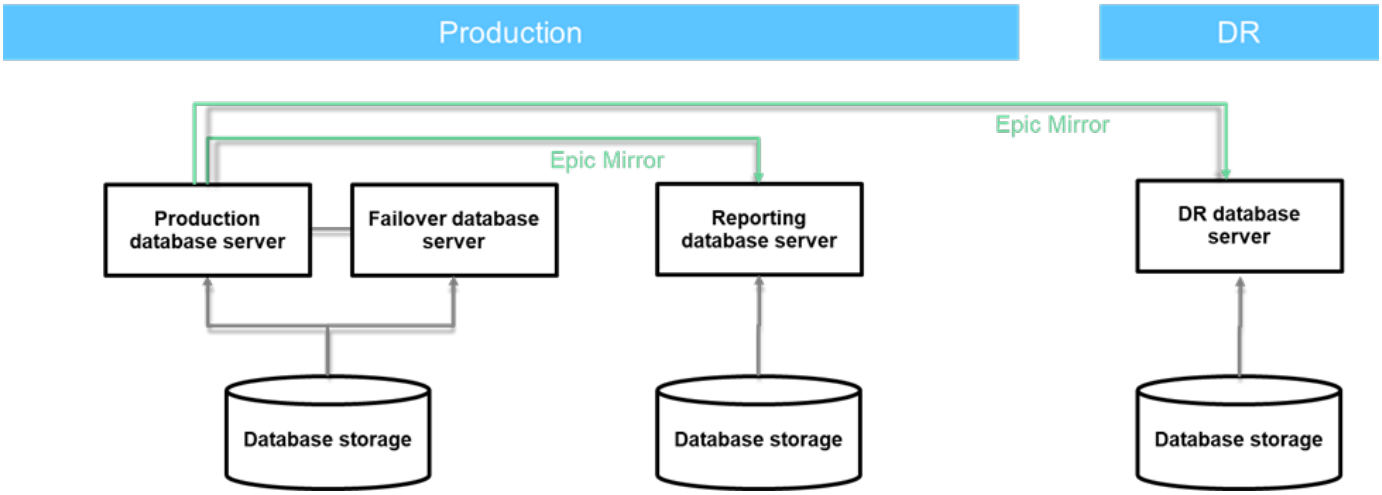
InterSystems también proporciona tecnologías para satisfacer los requisitos de replicación de datos, recuperación ante desastres y alta disponibilidad (HA). La tecnología de replicación de InterSystems se utiliza para replicar una base de datos Iris de forma síncrona o asíncrona desde un servidor de datos primario a uno o más servidores de datos secundarios. NetApp SnapMirror se usa para replicar el almacenamiento de WebBLOB o para backup y recuperación ante desastres.

La base de datos Iris actualizada tiene muchas ventajas:

- Mayor escala y permite que las organizaciones de mayor tamaño con varias instancias Epic se consoliden en una instancia más grande.
- Un período sin licencias en el que los clientes ahora pueden pasar de AIX a Red Hat Enterprise Linux (RHEL) sin tener que pagar por una nueva licencia de plataforma.

Servidores de base de datos Caché y uso del almacenamiento

- **Producción** En entornos de software Epic, se implementa una única base de datos centrada en el paciente. En los requisitos de hardware de Epic, el servidor físico que aloja el servidor de datos primario de lectura/escritura Iris se denomina servidor de bases de datos de producción. Este servidor requiere un almacenamiento all-flash de alto rendimiento para los archivos que pertenecen a la instancia de base de datos primaria. Para una alta disponibilidad, Epic admite el uso de un servidor de base de datos de conmutación por error que tiene acceso a los mismos archivos. Iris utiliza Epic Mirror para replicar en informes de solo lectura, recuperación ante desastres y compatibilidad con copias de solo lectura. Cada tipo de servidor de base de datos se puede cambiar al modo de lectura/escritura por razones de continuidad del negocio.
- **Informe** Un servidor de base de datos de réplica de informes proporciona acceso de solo lectura a los datos de producción. Aloja un servidor de datos Iris configurado como una copia de seguridad del servidor de datos de producción Iris. El servidor de base de datos de informes tiene los mismos requisitos de capacidad de almacenamiento que el servidor de base de datos de producción. Los informes de rendimiento de escritura son iguales que los de producción, pero las características de la carga de trabajo de lectura son diferentes y tienen un tamaño diferente.
- **Soporta solo lectura** Este servidor de base de datos es opcional y no se muestra la figura a continuación. También se puede implementar un servidor de base de datos de réplica para admitir la funcionalidad de solo lectura, en la cual se proporciona acceso a una copia de producción en modo de solo lectura. Este tipo de servidor de base de datos se puede cambiar al modo de lectura/escritura por motivos de continuidad del negocio.
- **Recuperación de desastres** Para cumplir con los objetivos de continuidad del negocio y recuperación ante desastres, un servidor de base de datos de réplica de recuperación ante desastres se implementa comúnmente en un sitio geográficamente separado de los servidores de base de datos de réplica de producción y/o informes. Un servidor de bases de datos duplicado de recuperación ante desastres también aloja un servidor de datos Iris configurado como una copia de seguridad del servidor de datos Iris de producción. Si la ubicación de producción deja de estar disponible durante un tiempo prolongado, este servidor de base de datos de réplica de copia de seguridad se puede configurar para que actúe como instancia de lectura/escritura de reflejo (SRW). El servidor de bases de datos de duplicación de respaldo tiene los mismos requisitos de almacenamiento de archivos que el servidor de bases de datos de producción. En cambio, el almacenamiento de base de datos de réplica de backup tiene el mismo tamaño que el almacenamiento de producción desde una perspectiva del rendimiento a efectos de continuidad del negocio.



- **Test** Las organizaciones de atención médica a menudo implementan entornos de desarrollo, pruebas y puesta en escena. Otros servidores de datos Iris para estos entornos también requieren almacenamiento,

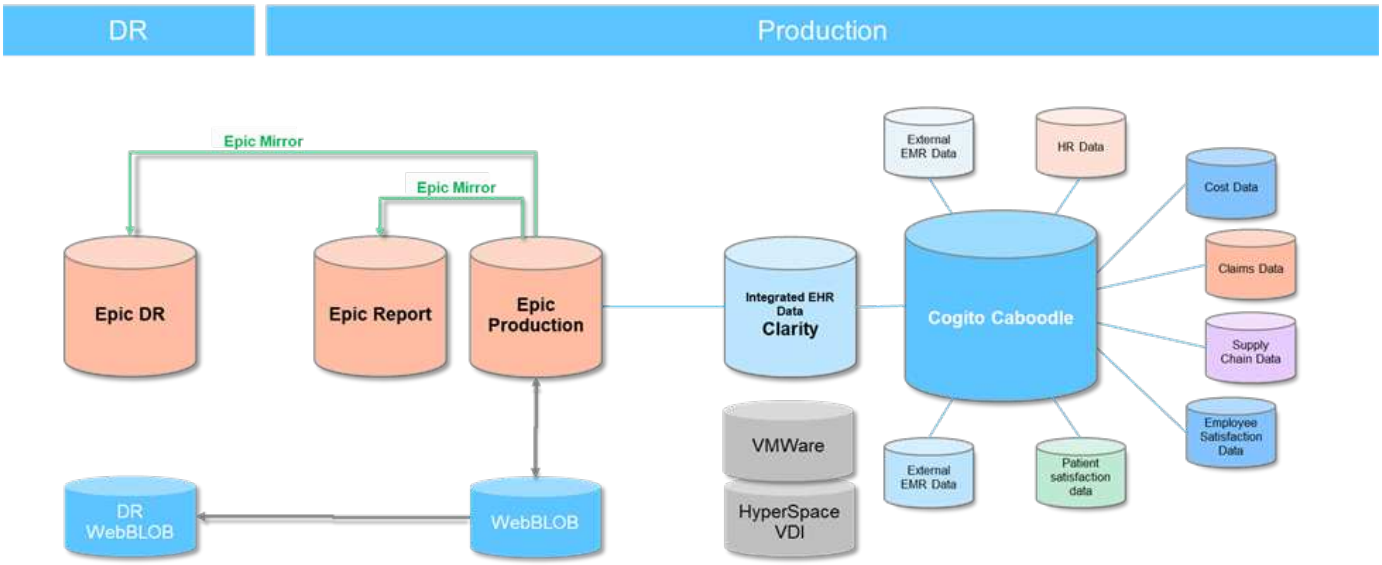
que se puede alojar mediante el mismo sistema de almacenamiento. Epic tiene requisitos y limitaciones específicos para ofrecer almacenamiento adicional a partir de un sistema de almacenamiento compartido. Estos requisitos específicos se abordan genéricamente mediante las mejores prácticas de este documento.

Además de los servidores de datos Iris ODB, los entornos de software Epic suelen incluir otros componentes como los siguientes y como se muestra en la siguiente figura:

- Un servidor de bases de datos de Oracle o Microsoft SQL Server como back-end de las claras herramientas de creación de informes empresariales de Epic

> Clarity se utiliza para generar informes sobre los datos extraídos diariamente de la base de datos Iris de informes.

- Servidor WebBLOB (SMB)
- Servidor de bases de datos multiuso
- Máquinas virtuales de uso múltiple (VM)
- Hiperespacio para el acceso de clientes



Los requisitos de almacenamiento de todas estas diferentes cargas de trabajo, pools, protocolos NAS y SAN se pueden consolidar y alojar en un único clúster de ONTAP. Esta consolidación permite a las organizaciones sanitarias tener una sola estrategia de gestión de datos para todas las cargas de trabajo de Epic y de las que no son de Epic.

Cargas de trabajo de bases de datos operativas

Cada servidor de bases de datos de Epic realiza I/O en los siguientes tipos de archivos:

- Archivos de base de datos
- Archivos de diario
- Archivos de aplicación

La carga de trabajo de un servidor de base de datos individual depende de su papel en el entorno de software de Epic. Por ejemplo, los archivos de la base de datos de producción normalmente conllevan la carga de

trabajo más exigente, que consiste en un 100% de solicitudes de I/O aleatorias. La carga de trabajo de cualquier base de datos reflejada suele ser menos exigente y tiene menos solicitudes de lectura. Las cargas de trabajo de archivos de diarios son principalmente secuenciales.

Epic mantiene un modelo de carga de trabajo para las pruebas de rendimiento del almacenamiento y la carga de trabajo del cliente. Para obtener más información acerca del modelo de carga de trabajo de Epic, los resultados de la prueba de rendimiento y las directrices sobre el uso de herramientas de ajuste de tamaño de NetApp para dimensionar correctamente el almacenamiento para entornos Epic, consulte "TR-3930i: Directrices de configuración de NetApp para Epic" (se requiere inicio de sesión en NetApp).

Epic también proporciona a cada cliente una guía de configuración de hardware personalizada que contiene proyecciones de I/O y los requisitos de capacidad de almacenamiento. Los requisitos de almacenamiento finales pueden incluir entornos de desarrollo, prueba o almacenamiento provisional, así como cualquier otra carga de trabajo complementaria que pueda consolidarse. Los clientes pueden utilizar la guía de configuración de hardware para comunicar los requisitos totales de almacenamiento a NetApp. Esta guía contiene todos los datos necesarios para configurar una puesta en marcha de Epic.

Durante la fase de implementación, Epic proporciona una Guía de distribución de almacenamiento de base de datos, que proporciona detalles más granulares a nivel de LUN que pueden usarse para un diseño de almacenamiento avanzado. Tenga en cuenta que la Guía de diseño de almacenamiento de base de datos es una recomendación de almacenamiento general y no específica de NetApp. Utilice esta guía para determinar el mejor diseño de almacenamiento en NetApp.

Ajuste de tamaño épico

Una de las consideraciones clave de la arquitectura al configurar un entorno de almacenamiento Epic es el tamaño de la base de datos de ODB.

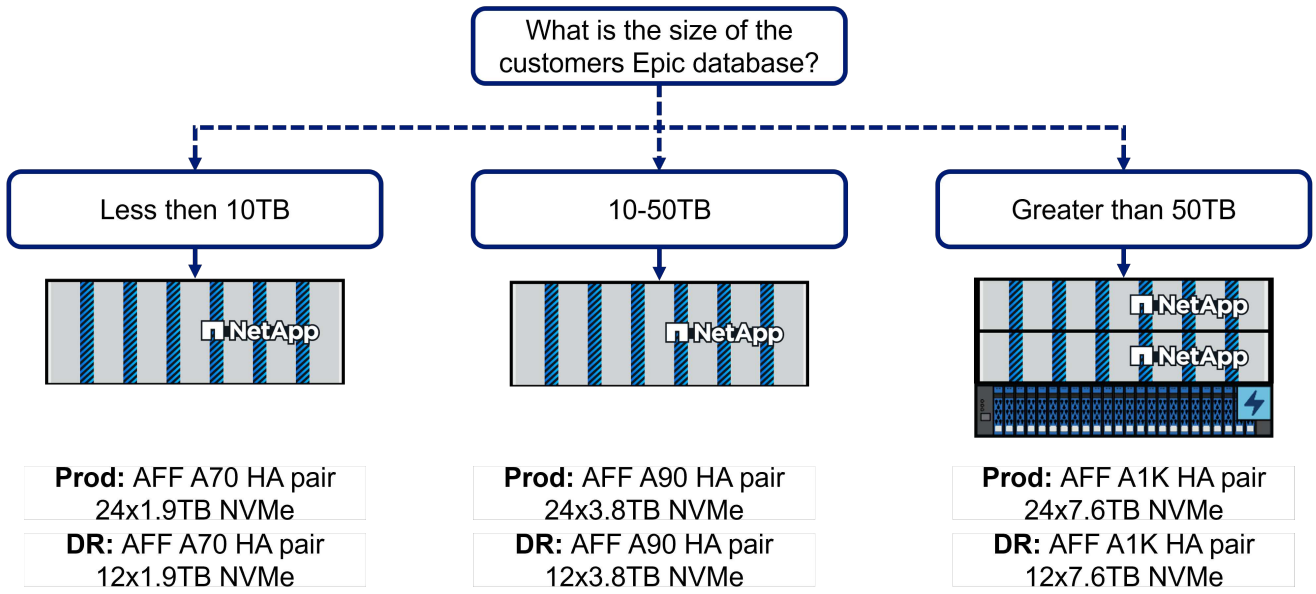
Puede utilizar el diagrama que se muestra a continuación para seleccionar una arquitectura de almacenamiento de Epic pequeña-mediana-grande. Estos diseños incluyen la ejecución de todas las cargas de trabajo enumeradas en la Guía de configuración de hardware. El árbol de tamaño se basa en datos de más de 100 guías de configuración de hardware y debe ser un cálculo casi preciso.

Es importante tener en cuenta que esto es solo un punto de partida. Debe colaborar con nuestro equipo de la alianza de Epic para confirmar cualquier diseño de Epic. Puede ponerse en contacto con el equipo en Epic@NetApp.com. Cada puesta en marcha debe adaptarse a las solicitudes de los clientes a la vez que se cumplen las prácticas recomendadas por Epic y NetApp.

- Arquitectura pequeña de Epic con una base de datos de Epic inferior a 10TB TB
- Arquitectura Epic media con una base de datos Epic de 10TB a 50TB
- Gran arquitectura de Epic con una base de datos de Epic superior a 50TB TB

Epic sizing decision tree

Work with the NetApp Epic alliance team to validate designs



Requisitos de almacenamiento de Epic

Por lo general, los recursos de almacenamiento dedicados se proporcionan para la base de datos de producción, mientras que las instancias de bases de datos replicadas comparten recursos de almacenamiento secundario con otros componentes relacionados con el software de Epic, como las herramientas de generación de informes Clarity.

Otros entornos de almacenamiento de software, como los que se utilizan para archivos del sistema y de aplicaciones, también los proporcionan recursos de almacenamiento secundario.

Más allá de las consideraciones de configuración, Epic tiene las siguientes reglas de distribución del almacenamiento adicionales y consideraciones clave:

- Desde 2020, todas las cargas de trabajo de bases de datos operativas (ODB) deben estar en cabinas all-flash.
- Epic recomienda que cada pool de almacenamiento se encuentre en hardware físico independiente, incluidos pool1, pool2, pool3, NAS1 y NAS2.

> Un nodo de un clúster se puede considerar como un pool de almacenamiento. Con ONTAP 9.4 o posterior y AQoS, puede crear pools protegidos mediante directivas.

- Nueva recomendación de backup de Epic 3-2-1.
  a. Copia ubicada en ubicaciones remotas (recuperación ante desastres)
  b. Una de las copias debe estar en una plataforma de almacenamiento diferente a la copia primaria
  c. Copias de los datos

Los clientes que usan NetApp SnapMirror para realizar backups de NetApp no cumplen las recomendaciones 3-2-1. El motivo es que ONTAP to ONTAP no cumple con el segundo requisito que se indica anteriormente. Puede usar SnapMirror directamente desde ONTAP para almacenar objetos en las instalaciones (por ejemplo, a través de StorageGRID) o en el cloud para cumplir los requisitos de Epic.

Para obtener más información sobre los requisitos de almacenamiento, consulte las siguientes guías épicas disponibles en Galaxy:

- Consideraciones sobre la SAN
- Estado de la tecnología y productos de almacenamiento (SPATS)
- Guía de configuración de hardware

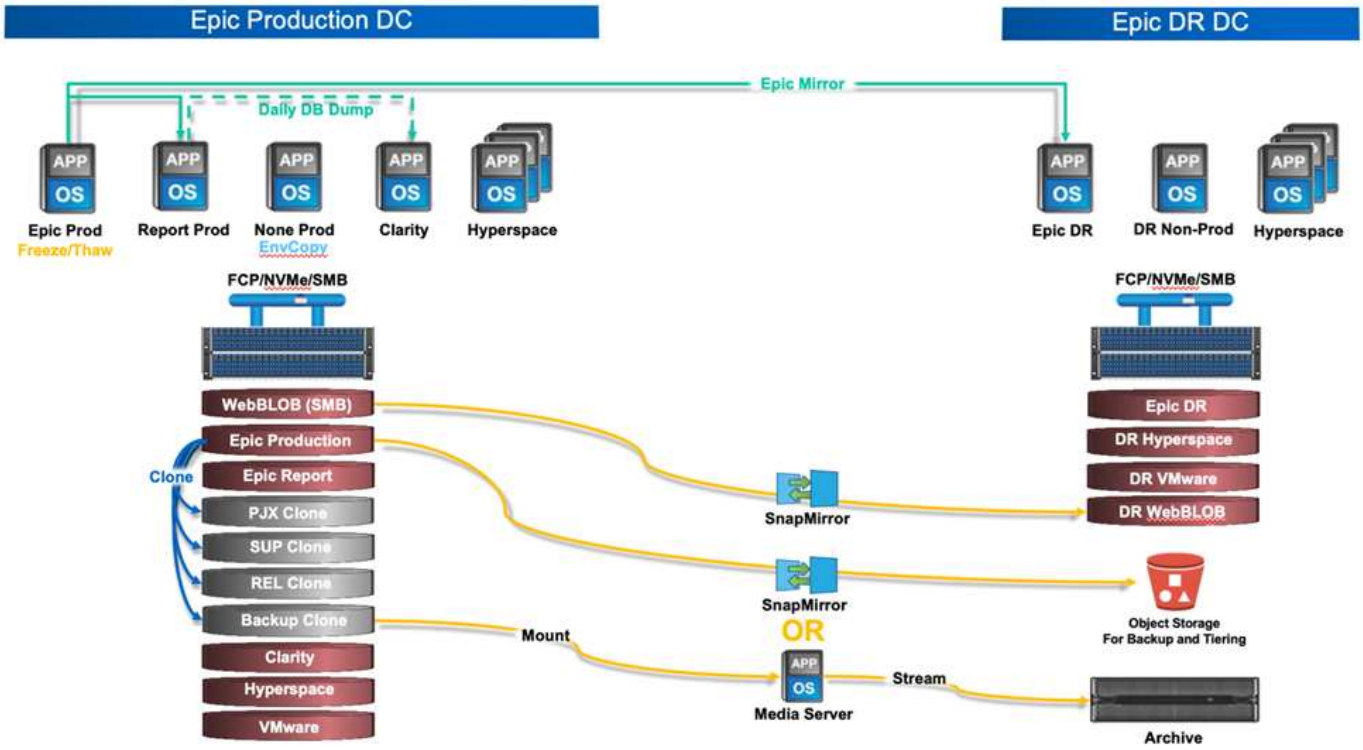
Arquitectura épica con cuatro nodos

Las siguientes figuras muestran la distribución del almacenamiento para una arquitectura de cuatro nodos: Un par de alta disponibilidad en producción y un par de alta disponibilidad en recuperación ante desastres. El tamaño de las controladoras y la cantidad de discos se basa en la última imagen de tamaño.

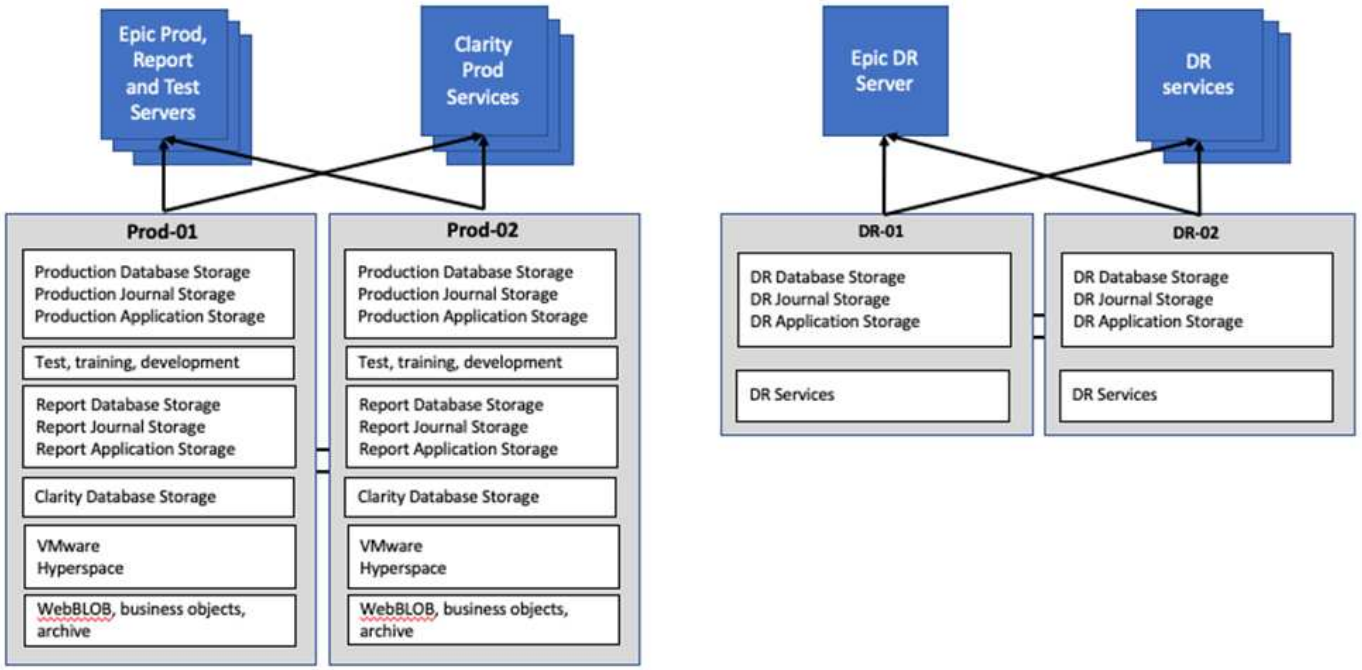
NetApp garantiza un rendimiento mínimo a nivel físico al aceptar las políticas de AQoS recomendadas por SLM. Epic admite la consolidación de pools de almacenamiento basados en ONTAP en un hardware considerablemente menor. Para obtener más información, consulte el documento de CUOTAS trimestrales de Epic. Básicamente, pool1, pool2 y NAS1 (enumerados en la guía de configuración de hardware de Epic) pueden ejecutarse en un solo par de alta disponibilidad con las cargas de trabajo distribuidas uniformemente entre las dos controladoras. En la recuperación ante desastres, Epic Pool 3 y NAS 3 también se dividen entre las dos controladoras del par de alta disponibilidad.

Los entornos de copia completa de prueba (como SUP, REL y PJX) se clonan desde Epic Production, Epic Report o Epic Disaster Recovery. Para obtener información acerca de las copias de seguridad y actualización de Epic, consulte la sección titulada, «Gestión de datos».

Arquitectura con cuatro nodos



Ubicación de cargas de trabajo en cuatro nodos

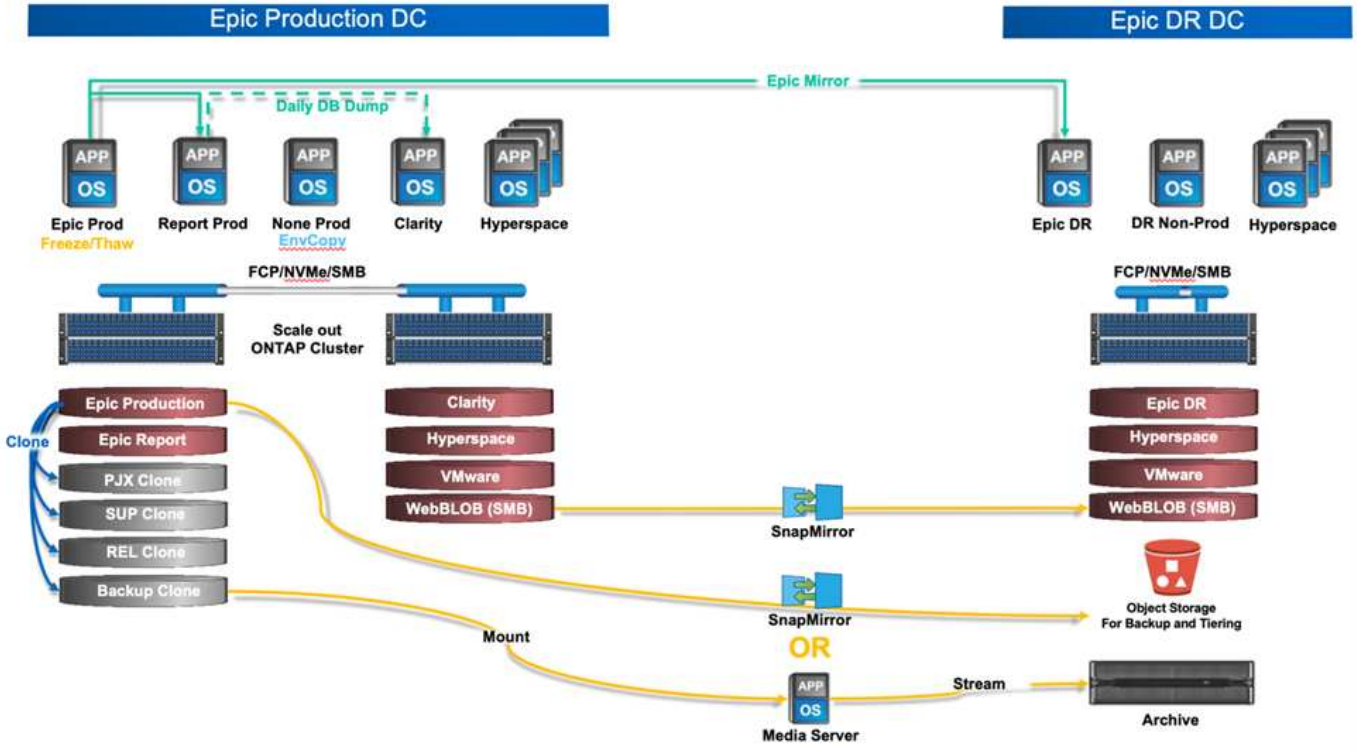


Arquitectura épica de seis nodos

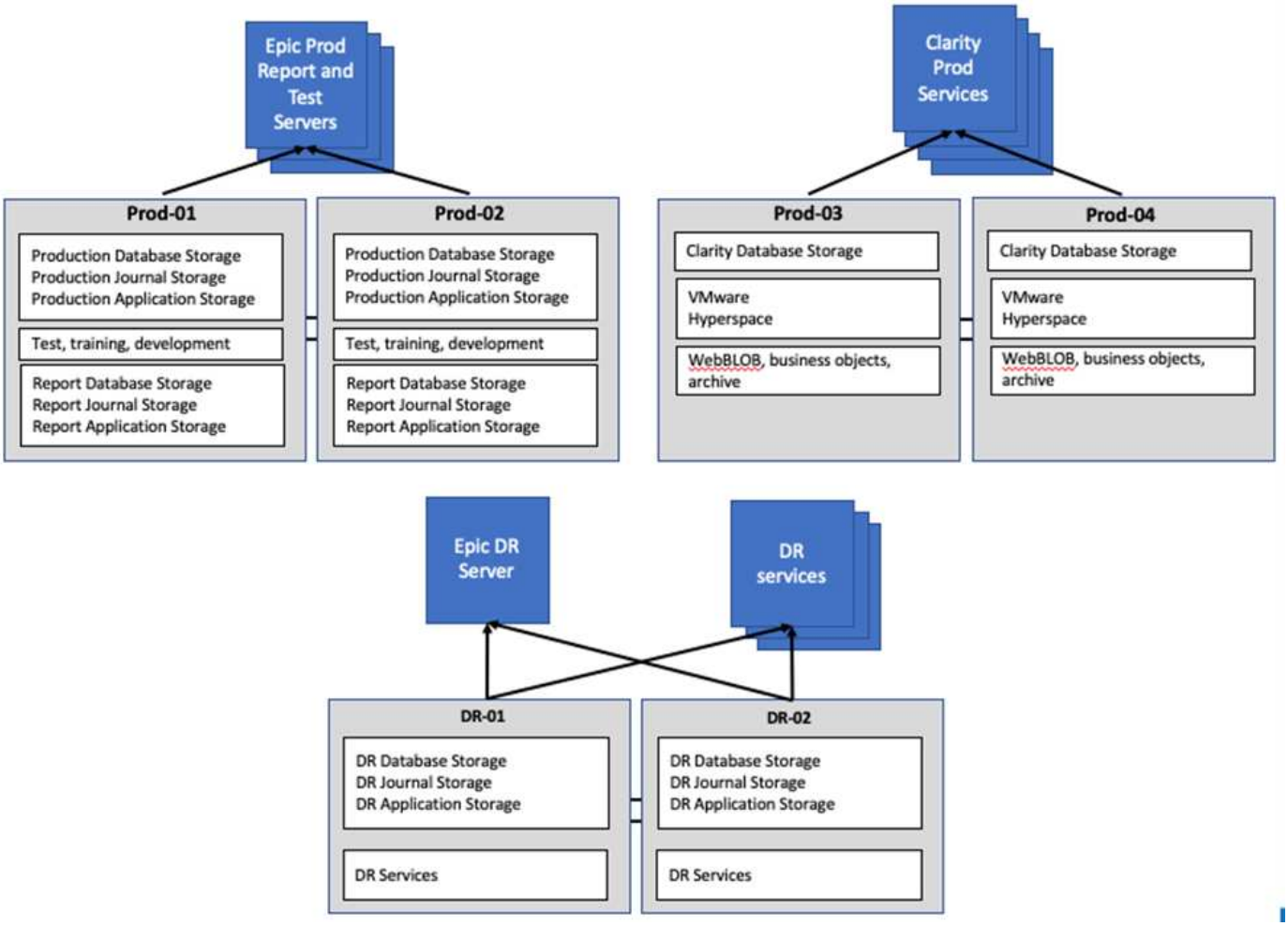
Los clientes pueden querer empezar con un diseño de seis nodos o escalar horizontalmente sin problemas de cuatro a seis nodos con una demanda cada vez mayor. Con el escalado horizontal, puede mover cargas de trabajo entre nodos de forma no disruptiva y reequilibrar en todo el clúster.

Esta arquitectura ofrece el mejor equilibrio de rendimiento y capacidad del clúster. Epic Production, Epic Report y Epic Test se ejecutan todos en el primer par de alta disponibilidad. El segundo par de alta disponibilidad se utiliza para claridad, hiperespacio, VMware, NAS1 y las cargas de trabajo de Epic restantes. La recuperación ante desastres es el mismo que la arquitectura de cuatro nodos de la sección anterior.

Arquitectura de seis nodos



Ubicación de cargas de trabajo de seis nodos

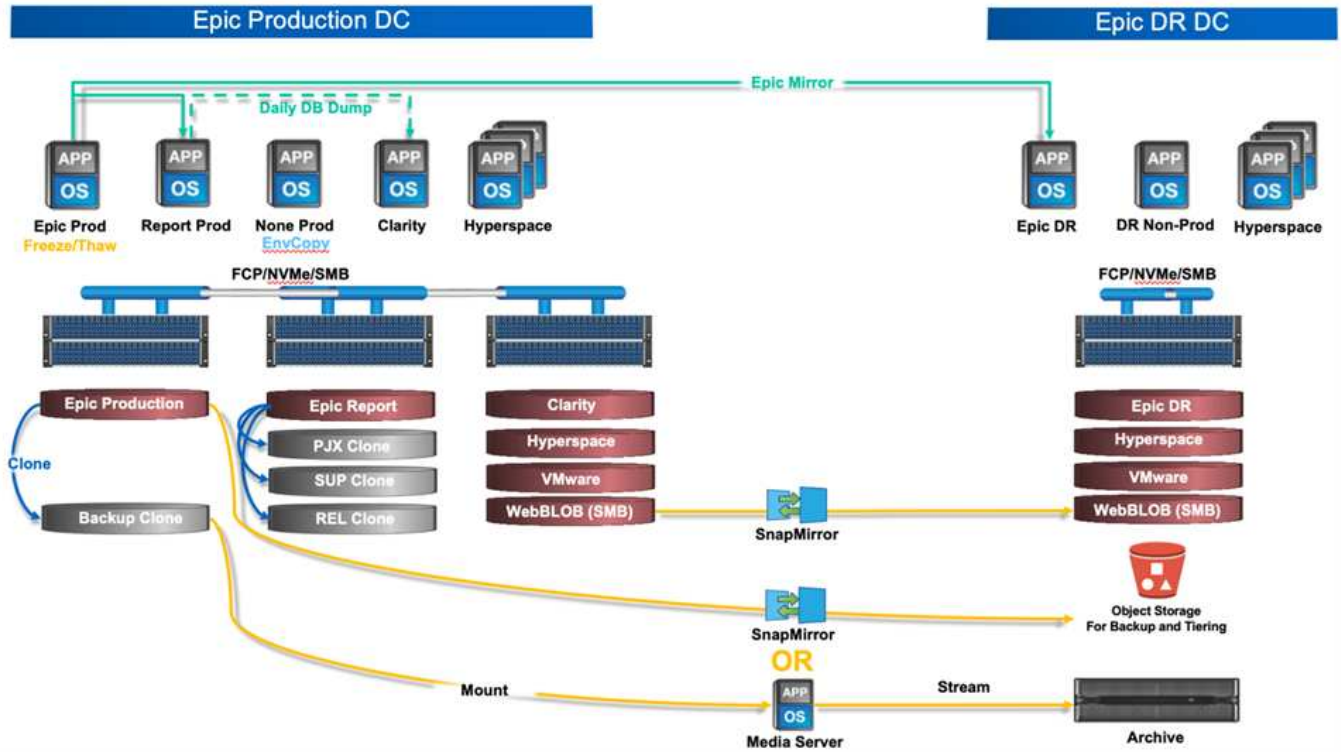


Arquitectura épica de ocho nodos

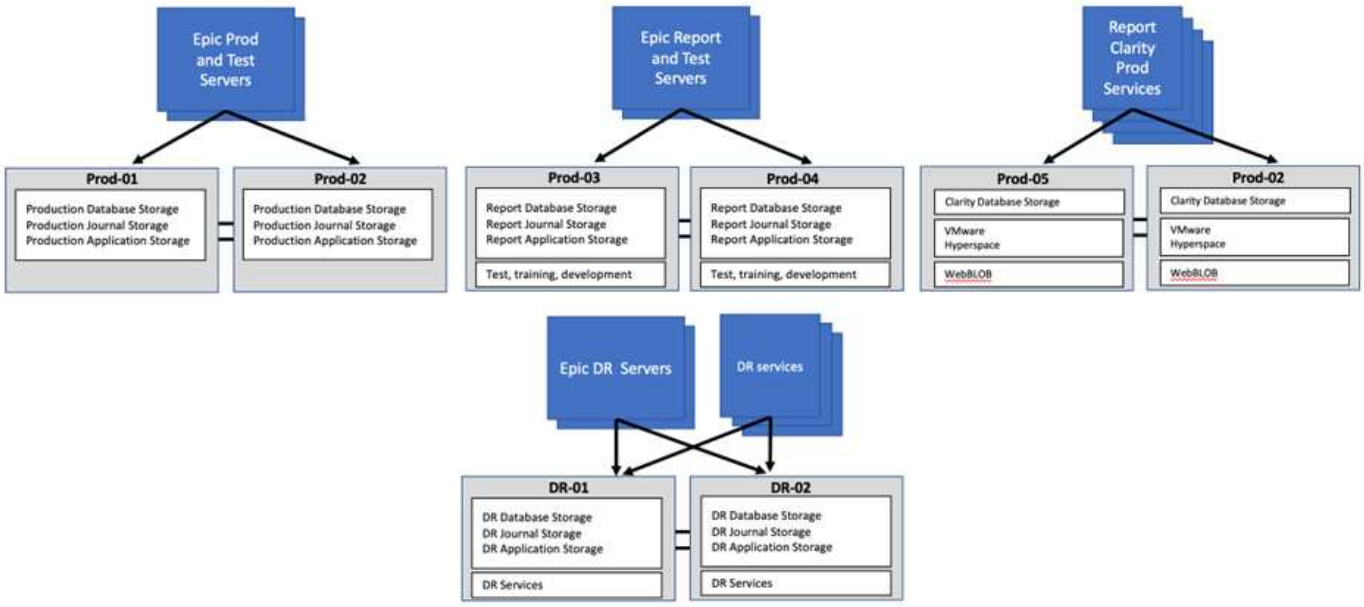
Las siguientes figuras muestran la arquitectura de ocho nodos de escalado horizontal. De nuevo, puede empezar con cuatro nodos y escalar hasta seis nodos, y continuar escalando hasta ocho nodos y superiores. Esta arquitectura ofrece el mejor equilibrio de rendimiento y capacidad en los seis nodos de producción.

Los entornos de prueba se clonan de Report en lugar de Production en este diseño. Esto libera los entornos de prueba y las comprobaciones de integridad de la producción.

Arquitectura de ocho nodos



Ubicación de cargas de trabajo en ocho nodos



Configuración y prácticas recomendadas

Epic en ONTAP - Utilidades de host

Las utilidades de host de NetApp son paquetes de software para varios sistemas operativos que contienen utilidades de gestión como el `sanlun` binario de la CLI, controladores multivía y otros archivos importantes necesarios para realizar correctamente las operaciones de SAN.

NetApp recomienda instalar las utilidades de host de NetApp en los hosts que están conectados y accediendo a los sistemas de almacenamiento de NetApp. Para obtener más información, consulte "Herramienta de matriz de interoperabilidad" y "Hosts SAN" la documentación.

Con AIX, es especialmente importante que se instalen las utilidades de host antes de detectar las LUN. Esto garantiza que el comportamiento de las rutas múltiples de LUN está configurado correctamente. Si la detección se realizó sin las utilidades de host, los LUN deberán desconfigurarse del sistema mediante `rmdev -dl` el comando y a continuación se volverán a detectar mediante `cfgmgr` un reinicio o un reinicio.

Configuración de volumen y LUN épica

El documento de recomendaciones sobre el diseño de bases de datos de Epic proporciona orientación sobre el tamaño y el número de LUN para cada base de datos.

Es importante revisar este documento con el soporte de administrador de bases de datos y Epic de Epic, así como finalizar el número de LUN y tamaños de LUN, ya que deben ajustarse. Estas recomendaciones de almacenamiento son importantes para la profundidad de la cola del adaptador HBA, el rendimiento del almacenamiento, la facilidad de operaciones y la facilidad de expansión.

Para considerar la profundidad de cola del SO del servidor, utilice un mínimo de ocho LUN (una LUN por volumen) para una base de datos. Aumente el número de LUN en función del número de nodos del clúster ONTAP. Por ejemplo, añada 4 LUN cuando se usa un clúster de 4 nodos (2 pareja de alta disponibilidad). Para entornos más grandes, es posible que se necesiten más LUN, use la misma cantidad de volúmenes (ocho total, distribuidos por el nodo de almacenamiento) y añada LUN en múltiplos de dos en los nodos y los volúmenes del clúster. Este enfoque le permite escalar fácilmente su entorno Epic.

Ejemplo 1: Clúster ONTAP de 2 Nodos

2 nodo, 1 parejas de alta disponibilidad, 8 volúmenes, 4 volúmenes por nodo 8 LUN, una LUN por volumen agregando 2 LUN adicionales, una en node01 en volume01, una en node02 en volume02.

Ejemplo 2: Clúster ONTAP de 4 Nodos

Nodo, parejas de alta disponibilidad 8 volúmenes, 2 volúmenes por nodo 8 LUN, una LUN por volumen agregando 4 LUN adicionales, una en node01 en volume01, una en node02 en 4, una en node03 en volume03, una en node04 en 2, una en volume02 en volume04.

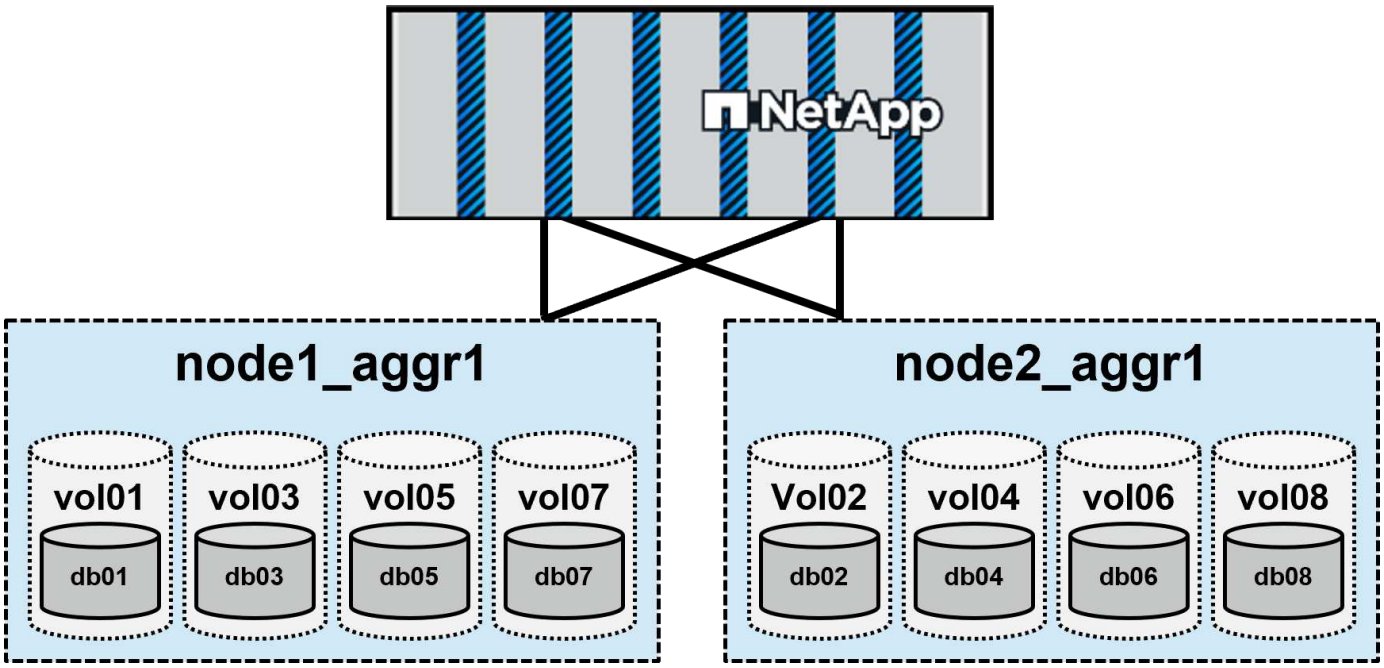
Para maximizar el rendimiento de una carga de trabajo, como la base de datos de Epic o la claridad, cada diseño funciona mejor también para el almacenamiento NetApp. Al usar ocho volúmenes, las operaciones de I/O de escritura se distribuyen de manera uniforme entre las controladoras, con lo que se maximiza la utilización de CPU. Para la replicación y el backup, lo mejor es limitar la cantidad de volúmenes a ocho para simplificar las operaciones.

Opciones de escala

Si el servidor necesita más almacenamiento, la opción más sencilla es hacer crecer las LUN que contienen los volúmenes. La segunda opción es añadir LUN a los grupos de volúmenes en múltiplos de dos a la vez (uno por volumen por nodo).

Ejemplo:

Distribución de volúmenes y 8 LUN



Si en un entorno grande requiere más de 4 nodos o 8 LUN, consulte a nuestro equipo de alianza de Epic para confirmar los diseños de la LUN. Puede ponerse en contacto con el equipo en Epic@NetApp.com.

Mejores prácticas

- Use 8 LUN en volúmenes de 8 para comenzar, añadiendo 2 LUN a la vez en todos los nodos del clúster.
- Equilibre las cargas de trabajo en toda la pareja de alta disponibilidad para maximizar el rendimiento y la eficiencia.
- Cree LUN con el tamaño esperado para 3 años de crecimiento. (Consulte el "Documentación de ONTAP" para obtener el tamaño máximo de LUN.)
- Utilice volúmenes y LUN con thin provisioning.
- Utilice un mínimo de ocho LUN de base de datos, dos LUN de diario y dos LUN de aplicaciones. Esta configuración maximiza el rendimiento del almacenamiento y la profundidad de cola del SO. Se puede usar más si se necesita por capacidad u otros motivos.
- Si necesita añadir LUN a grupos de volúmenes, añada ocho LUN al mismo tiempo.
- Son necesarios los grupos de consistencia (CG) para que el grupo de volúmenes y LUN se realice un backup conjunto.
- No utilice QoS durante el rendimiento de GENIO ni de I/O.
- Tras las pruebas de claridad o genios, NetApp recomienda eliminar el almacenamiento y volver a aprovisionar antes de cargar los datos de producción.
- Es importante que `-space-allocation` habilitado se establezca en las LUN. Si no es así, ONTAP no verá ningún dato eliminado de las LUN y puede dar lugar a problemas de capacidad. Para obtener más información, consulte Guía de referencia rápida de configuración del almacenamiento de Epic.

Epic y protocolos de archivo

Es compatible con la combinación de NAS y SAN en la misma cabina all-flash.

NetApp recomienda usar volúmenes FlexGroup para recursos compartidos NAS, como WebBLOB (cuando esté disponible).

WebBLOB es hasta un 95% de datos inactivos. Otra opción es liberar espacio en su cabina all-flash y organizar en niveles los backups y los datos fríos al almacenamiento de objetos en las instalaciones o en el cloud con "FabricPool"la función de ONTAP. Todo lo cual se puede lograr sin ningún efecto de rendimiento notable. FabricPool es una función incluida de ONTAP. Los clientes pueden generar un informe de datos fríos (o inactivos) para revisar el beneficio que podría obtener si habilita FabricPool. Puede establecer la antigüedad de los datos en niveles mediante la política. Los clientes de Epic han obtenido ahorros significativos con esta función.

Gestión del rendimiento épico

La mayoría de las cabinas all-flash pueden ofrecer el rendimiento necesario para las cargas de trabajo de Epic. El diferenciador de NetApp es su capacidad para establecer políticas de rendimiento a nivel físico y garantizar un rendimiento constante para cada aplicación.

Calidad de servicio (QoS)

NetApp recomienda utilizar la calidad de servicio. La ventaja de la calidad de servicio es la capacidad de consolidar todas las cargas de trabajo de Epic. Todos los protocolos y pools de almacenamiento pueden residir en menos hardware. No es necesario separar pools de almacenamiento.

- NetApp recomienda que todas las cargas de trabajo del clúster se asignen a una política de calidad de servicio para gestionar mejor el margen adicional en el clúster.
- NetApp recomienda equilibrar todas las cargas de trabajo de forma uniforme en toda la pareja de alta disponibilidad.
- No utilice políticas de QoS al realizar cualquier prueba de E/S; de lo contrario, las pruebas de GENIO fallarán. Analiza las distintas cargas de trabajo de producción durante 2-4 semanas antes de asignar cualquier política de calidad de servicio.

Epic en ONTAP - protocolos

FCP es el protocolo preferido para presentar LUN.

NetApp recomienda zonificación de iniciador único: Un iniciador por zona con todos los puertos de destino necesarios en el almacenamiento utilizando nombres de puerto (WWPN) a nivel mundial. Es probable que la presencia de más de un iniciador en una única zona provoque una comunicación entre zonas del HBA intermitente, lo que provoca una interrupción significativa.

Después de crear la LUN, asigne la LUN al igroup que contiene los WWPN del host para habilitar el acceso.

NetApp también admite el uso de NVMe/FC (si dispone de versiones de sistemas operativos AIX y RHEL compatibles) y mejora el rendimiento. FCP y NVMe/FC pueden coexistir en la misma estructura.

Configuración épica de la eficiencia del almacenamiento

Las eficiencias inline de ONTAP son activadas de forma predeterminada y funcionan independientemente del protocolo de almacenamiento, la aplicación o el nivel de almacenamiento.

Las eficiencias reducen la cantidad de datos escritos en almacenamiento flash costoso y el número de unidades necesarias. ONTAP mantiene la eficiencia con la replicación. Cada una de las eficiencias afecta poco o nada al rendimiento, incluso para una aplicación sensible a la latencia como Epic.

NetApp recomienda activar todos los ajustes de eficiencia para maximizar la utilización del disco. Esta configuración está activada de forma predeterminada en los sistemas basados en AFF y ASA.

Las siguientes funciones hacen que esta eficiencia del almacenamiento sea posible:

- La deduplicación ahorra espacio en el almacenamiento primario gracias a la eliminación de las copias redundantes de bloques en un volumen que aloja LUN. Esta opción recomendada está activada de forma predeterminada.
- La compresión en línea reduce la cantidad de datos que se deben escribir en el disco y se consigue un ahorro de espacio considerable con las cargas de trabajo de Epic. Esta opción recomendada está activada de forma predeterminada.
- La compactación inline requiere bloques de 4K KB que están menos de la mitad llenos y los combina en un único bloque. Esta opción recomendada está activada de forma predeterminada.
- Thin replication se encuentra en el centro de la cartera de software de protección de datos de NetApp, que incluye el software NetApp SnapMirror. Thin replication de SnapMirror protege los datos vitales para el negocio a la vez que minimiza los requisitos de capacidad del almacenamiento. **NetApp recomienda** activar esta opción.
- Deduplicación en los agregados. La deduplicación siempre ha estado a nivel de volumen. Con ONTAP 9.2, se hizo disponible la deduplicación de agregado, lo que permite ahorrar más con la reducción de disco. Se ha añadido la deduplicación agregada postprocesamiento con ONTAP 9.3. **NetApp recomienda** activar esta opción.

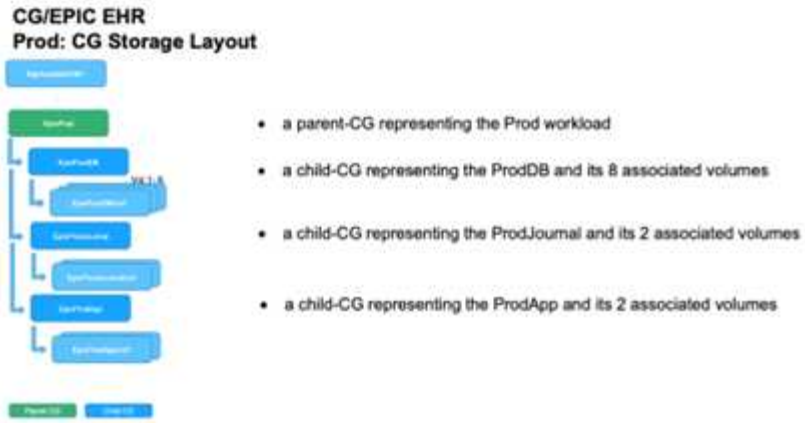
Configuración épica de la eficiencia del almacenamiento

Las aplicaciones con almacenamiento repartidos por más de un volumen con una o varias LUN de las cantidades adecuadas para la carga de trabajo necesitan que se realice un backup conjunto de contenido que garantice que una protección de datos constante requiera CG.

Los grupos de consistencia (CG para abreviar) ofrecen esta funcionalidad y mucho más. Se pueden utilizar todas las noches para crear copias snapshot coherentes bajo demanda o programadas usando una política. Puede usarlo para restaurar, clonar e incluso replicar datos.

Para obtener información adicional acerca de los CG, consulte la "Información general sobre los grupos de consistencia"

Una vez aprovisionados los volúmenes y las LUN tal y como se detallan en las secciones anteriores de este documento, se pueden configurar en un conjunto de CG. Se recomienda configurarlas como se muestra en la siguiente imagen:



Snapshots de grupo de coherencia

Se debe definir una programación de snapshot de CG nocturna en cada uno de los CG secundarios asociados con los volúmenes que proporcionan almacenamiento para la base de datos de producción. Esto dará como resultado un nuevo conjunto de backups consistentes de estos CG cada noche. Estos pueden utilizarse para clonar la base de datos de producción para utilizarlos en entornos distintos a la producción, como desarrollo y pruebas. NetApp ha desarrollado flujos de trabajo Ansible automatizados basados en el CG propio para Epic con el fin de automatizar el backup de bases de datos de producción, así como los entornos de prueba y actualización.

Las instantáneas de CG pueden utilizarse para admitir las operaciones de restauración de la base de datos de producción de Epic.

Para volúmenes SAN, deshabilite la política de snapshots predeterminada en cada volumen que se utiliza para los CG. Estas copias Snapshot normalmente las gestiona la aplicación de backup que se está utilizando o el servicio de automatización Epic Ansible de NetApp.

Para volúmenes SAN, deshabilite la política de Snapshot predeterminada en cada volumen. Estas copias Snapshot normalmente son gestionadas por una aplicación de backup o por la automatización de Epic Ansible[NS2].

WebBLOB y los conjuntos de datos de VMware deben configurarse como volúmenes, no como asociados con los CG. SnapMirror se puede usar para mantener snapshots en sistemas de almacenamiento independientes de producción.

Cuando termine, la configuración sería la siguiente:

Ajuste del tamaño del almacenamiento para Epic

Debe colaborar con nuestro equipo de la alianza de Epic para confirmar cualquier diseño de Epic. Puede ponerse en contacto con el equipo en Epic@NetApp.com. Cada puesta en marcha debe adaptarse a las solicitudes de los clientes a la vez que se cumplen las prácticas recomendadas por Epic y NetApp.

Para obtener información sobre cómo utilizar las herramientas de configuración de NetApp para determinar el tamaño de los grupos de RAID y el número correctos de grupos RAID para las necesidades de almacenamiento de entorno de software Epic, consulte "TR-3930i: Directrices de configuración de NetApp para Epic" (se requiere inicio de sesión en NetApp).

Es necesario acceder a Field Portal de NetApp.

Información adicional sobre Epic en ONTAP

Para obtener más información sobre la información descrita en este documento, consulte los siguientes documentos y/o sitios web:

- "Documentación de productos de NetApp"
- "Documentación de ONTAP 9"
- "Grupos de consistencia"
- "Recursos de documentación de ONTAP y ONTAP System Manager"
- "TR-3930i: Directrices de configuración de NetApp para Epic" (Se requiere inicio de sesión NetApp)

Documentos de orientación al cliente épica

Epic proporciona a los clientes los siguientes documentos para obtener orientación sobre servidores, almacenamiento y redes. Estos documentos se mencionan en este informe técnico.

- Consideraciones sobre la red de área de almacenamiento
- Guía de soluciones técnicas para la continuidad del negocio
- Manual de estrategia de la arquitectura de referencia all-flash
- Estado de productos de almacenamiento y tecnología
- Consideraciones de cloud épicas
- Guía de configuración de hardware (específica del cliente)
- Recomendaciones sobre distribución de almacenamiento de base de datos (específicas del cliente)

Hyper-V.

Directrices de puesta en marcha y prácticas recomendadas de almacenamiento

Descripción general

Microsoft Windows Server es un sistema operativo (SO) de clase empresarial que cubre redes, seguridad, virtualización, cloud privado, cloud híbrido, infraestructura de puestos de trabajo virtuales, protección de acceso, protección de información, servicios web, infraestructura de plataforma de aplicaciones, y mucho más.

Esta documentación sustituye a los informes técnicos publicados anteriormente *TR-4568: Directrices de puesta en funcionamiento de NetApp y mejores prácticas de almacenamiento para Windows Server*

ONTAP se ejecuta en las controladoras de almacenamiento de NetApp. Está disponible en múltiples formatos.

- Arquitectura unificada que admite protocolos de archivos, objetos y bloques. Esto permite a las controladoras de almacenamiento actuar tanto como dispositivos NAS como SAN, así como almacenes de objetos
- Una cabina All SAN (ASA) que se centra únicamente en protocolos de bloque y optimiza los tiempos de reanudación de I/O (IORT) añadiendo accesos múltiples activo-activo simétricos para los hosts de conexión
- Una arquitectura unificada definida por software
  - ONTAP Select ejecutándose en VMware vSphere o KVM
  - Cloud Volumes ONTAP se ejecuta como instancia de cloud nativo
- Primeras ofertas de proveedores de cloud a hiperescala
  - Amazon FSX para ONTAP de NetApp
  - Azure NetApp Files
  - NetApp Volumes para Google Cloud

ONTAP proporciona funcionalidades de eficiencia del almacenamiento de NetApp como la tecnología snapshot de NetApp, clonado, deduplicación, thin provisioning, thin replication, compresión, almacenamiento virtual por niveles y mucho más con un rendimiento y una eficiencia mejorados.

Juntos, Windows Server y ONTAP pueden funcionar en entornos de gran tamaño y aportar un gran valor a la consolidación de centros de datos y las implementaciones de cloud privado o híbrido. Esta combinación también proporciona cargas de trabajo no disruptivas de forma eficiente y admite una escalabilidad fluida.

Audiencia de destino

Este documento está destinado a arquitectos de sistemas y almacenamiento que diseñan soluciones de almacenamiento de NetApp para Windows Server.

En este documento hacemos las siguientes suposiciones:

- El lector tiene un conocimiento general de las soluciones de hardware y software de NetApp. Consulte "Guía de administración del sistema para administradores de clústeres" para obtener más detalles.
- El lector tiene conocimientos generales de protocolos de acceso en bloque, como iSCSI, FC y el protocolo de acceso a archivos SMB/CIFS. Consulte "Gestión de SAN Clustered Data ONTAP" Para obtener información relacionada con SAN. Consulte "Gestión de NAS" Para información relacionada con CIFS/SMB.
- El lector posee conocimientos generales sobre el sistema operativo Windows Server y Hyper-V.

Si quiere obtener una matriz completa y actualizada regularmente de configuraciones SAN y NAS probadas y compatibles, consulte el "Herramienta de matriz de interoperabilidad (IMT)" en el sitio de soporte de NetApp. Con IMT, puede determinar las versiones exactas de producto y funciones compatibles con su entorno concreto. El NetApp IMT define los componentes y las versiones del producto que son compatibles con las configuraciones compatibles con NetApp. Los resultados específicos dependen de la instalación que realice cada cliente de acuerdo con las especificaciones publicadas.

Almacenamiento de NetApp y entorno de Windows Server

Como se menciona en la "Descripción general", Las controladoras de almacenamiento NetApp proporcionan una arquitectura realmente unificada que admite protocolos de archivos, bloques y objetos. Esto incluye SMB/CIFS, NFS, NVMe/TCP, NVMe/FC, iSCSI, FC (FCP) y S3, y crean un acceso unificado a clientes y hosts. El mismo controlador de almacenamiento puede ofrecer simultáneamente un servicio de almacenamiento basado en bloques en forma de LUN SAN y servicio de archivos como NFS y SMB/CIFS. ONTAP también está disponible como cabina All SAN (ASA) que optimiza el acceso del host a través de multivía activo-activo simétrico con iSCSI y FCP, mientras que los sistemas ONTAP unificados utilizan accesos múltiples activo-activo asimétrico. En ambos modos, ONTAP utiliza ANA para la gestión multivía de NVMe over Fabrics (NVMe-oF).

Una controladora de almacenamiento de NetApp que ejecuta ONTAP puede admitir las siguientes cargas de trabajo en un entorno de Windows Server:

- Equipos virtuales alojados en recursos compartidos de SMB 3,0 disponibles continuamente
- Equipos virtuales alojados en LUN de volumen compartido de clúster (CSV) que se ejecutan en iSCSI o FC
- Bases de datos de SQL Server en recursos compartidos de SMB 3,0
- Bases de datos de SQL Server en NVMe-oF, iSCSI o FC
- Otras cargas de trabajo de aplicaciones

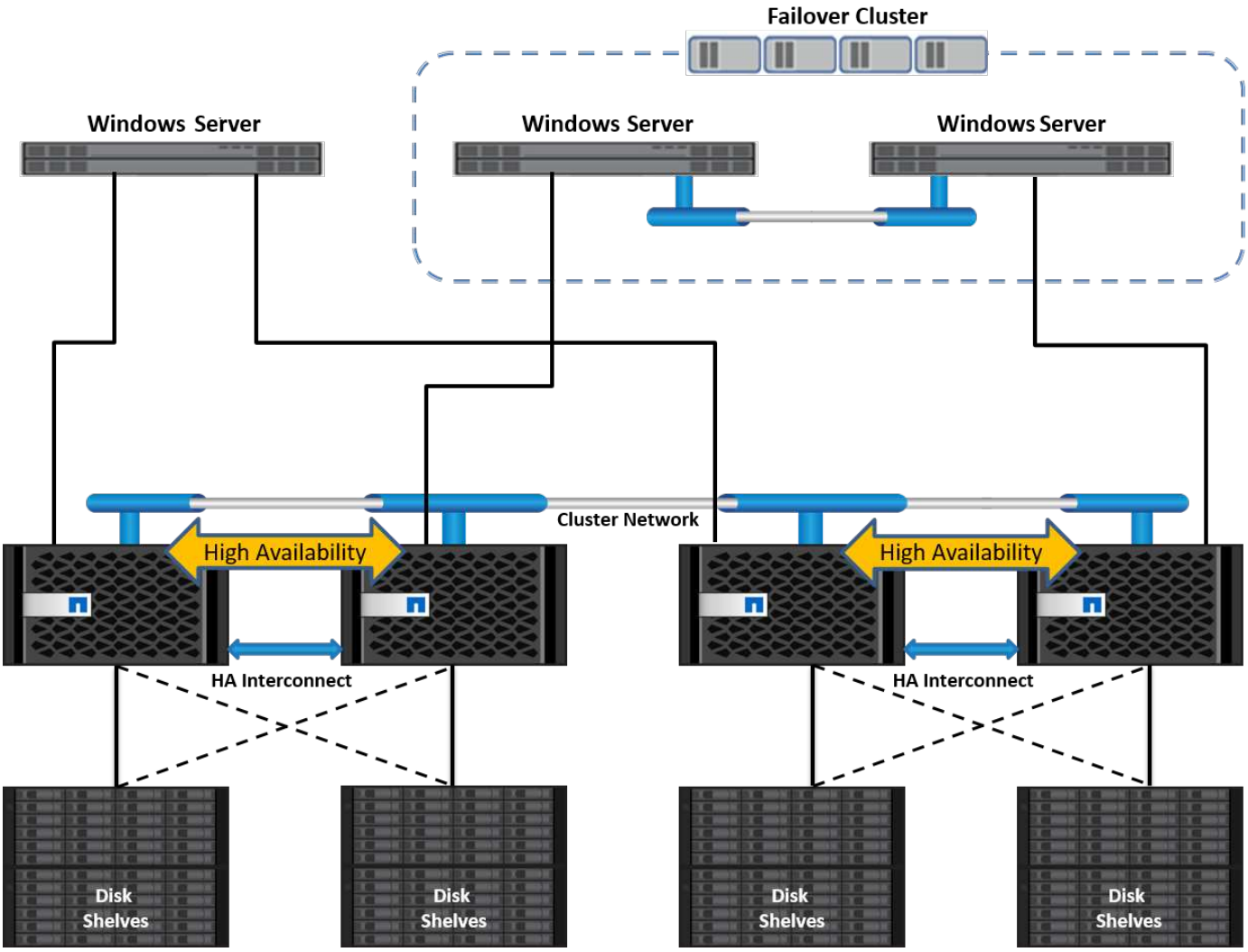
Además, las funciones de eficiencia del almacenamiento de NetApp como la deduplicación, las copias NetApp FlexClone®, la tecnología de snapshots de NetApp, thin provisioning, compresión y almacenamiento por niveles aportan un valor importante a las cargas de trabajo que se ejecutan en Windows Server.

Gestión de datos de ONTAP

ONTAP es un software de gestión que se ejecuta en una controladora de almacenamiento de NetApp. Se conoce como un nodo, una controladora de almacenamiento NetApp es un dispositivo de hardware con un procesador, RAM y NVRAM. El nodo se puede conectar a unidades de disco SATA, SAS o SSD, o a una combinación de dichas unidades.

Varios nodos se agregan en un sistema en clúster. Los nodos del clúster se comunican entre sí continuamente para coordinar las actividades del clúster. Los nodos también pueden mover datos de un nodo a otro de manera transparente mediante rutas redundantes a una interconexión de clúster dedicada que consta de dos switches Ethernet de 10Gb Gb. Los nodos del clúster pueden sustituirse entre sí para proporcionar alta disponibilidad durante cualquier escenario de conmutación por error. Los clústeres se administran en todo el clúster en lugar de por nodo y los datos se proporcionan desde una o varias máquinas virtuales de almacenamiento (SVM). Un clúster debe tener al menos una SVM para suministrar datos.

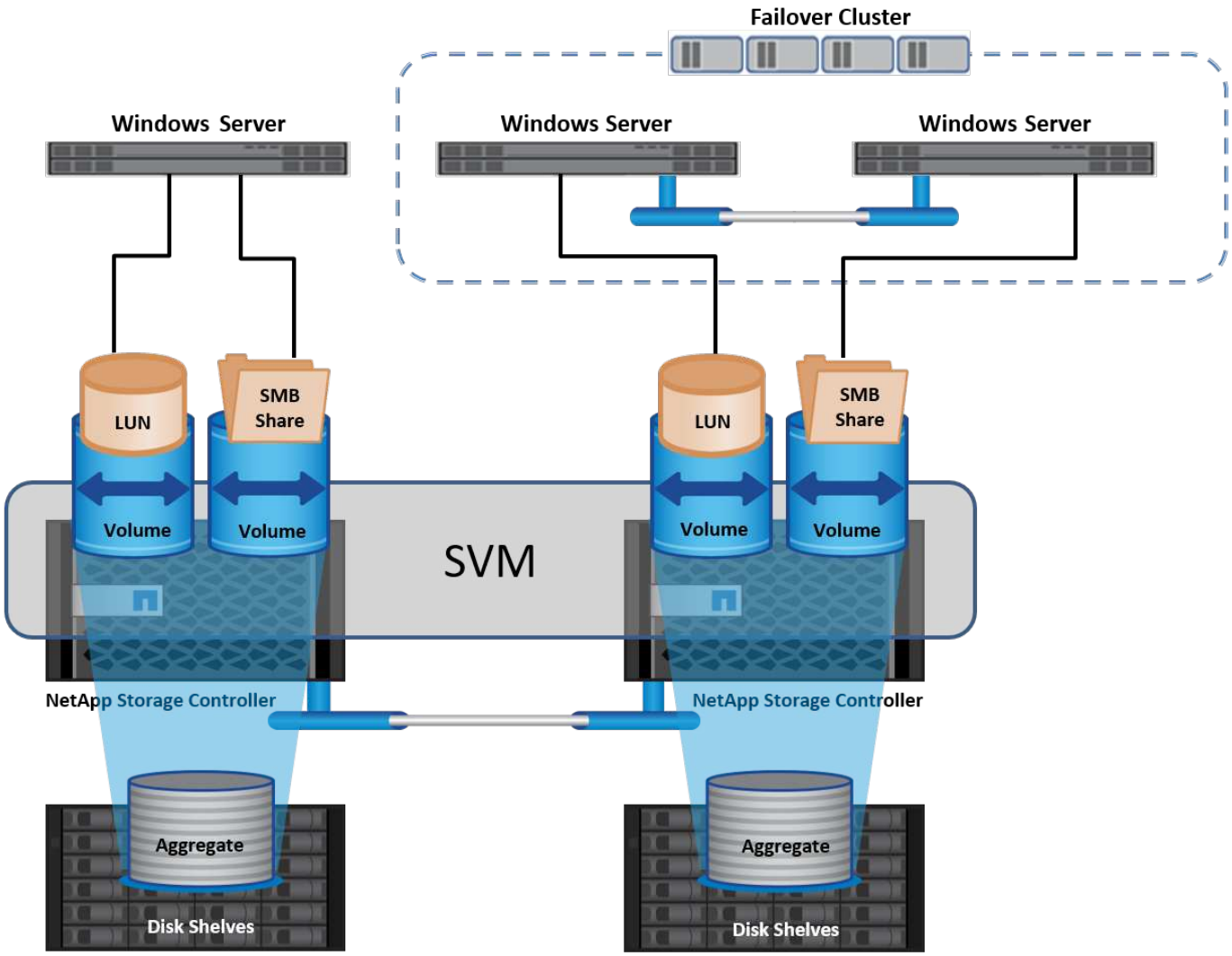
La unidad básica de un clúster es el nodo y los nodos se añaden al clúster como parte de un par de alta disponibilidad (HA). Los pares de ALTA disponibilidad permiten una alta disponibilidad comunicándose entre sí a través de una interconexión de clúster de alta disponibilidad (independiente de la interconexión de clúster dedicada) y al mantener conexiones redundantes a discos del par de alta disponibilidad. Los discos no se comparten entre pares de alta disponibilidad, aunque las bandejas pueden contener discos que pertenecen a cualquier miembro de una pareja de alta disponibilidad. La siguiente figura muestra una instalación de sistemas de almacenamiento de NetApp en un entorno Windows Server.



Máquinas virtuales de almacenamiento

Una SVM de ONTAP es un servidor de almacenamiento lógico que proporciona acceso a datos a LUN y/o un espacio de nombres NAS desde una o más interfaces lógicas (LIF). Por lo tanto, la SVM es la unidad básica de segmentación del almacenamiento que permite una multitenencia segura en ONTAP. Cada SVM se configura para tener volúmenes de almacenamiento aprovisionados desde un agregado físico e interfaces lógicas (LIF) asignados a una red Ethernet física o a puertos de destino FC.

Los discos lógicos (LUN) o los recursos compartidos CIFS se crean dentro de los volúmenes de una SVM y se asignan a hosts y clústeres de Windows para proporcionarles espacio de almacenamiento, como se muestra en la siguiente figura. Las SVM son independientes de nodos y basadas en clústeres; pueden usar recursos físicos, como volúmenes o puertos de red en cualquier lugar del clúster.



Aprovisionar almacenamiento NetApp para Windows Server

El almacenamiento puede aprovisionarse a Windows Server tanto en entornos SAN como NAS. En un entorno SAN, el almacenamiento se proporciona como discos de las LUN del volumen de NetApp como almacenamiento basado en bloques. En un entorno NAS, el almacenamiento se proporciona como recursos compartidos CIFS/SMB en volúmenes NetApp como almacenamiento de archivos. Estos discos y recursos compartidos se pueden aplicar en Windows Server de la siguiente manera:

- Almacenamiento para hosts de Windows Server para cargas de trabajo de aplicaciones
- Almacenamiento para Nano Server y contenedores
- Almacenamiento para hosts Hyper-V individuales para almacenar equipos virtuales
- Almacenamiento compartido para clústeres de Hyper-V en forma de volúmenes compartidos en cluster para almacenar equipos virtuales
- Almacenamiento para bases de datos de SQL Server

Gestión del almacenamiento de NetApp

Para conectar, configurar y administrar el almacenamiento de NetApp desde Windows Server 2016, utilice uno de los siguientes métodos:

- **Shell seguro (SSH).** Utilice cualquier cliente SSH en Windows Server para ejecutar comandos de NetApp CLI.
- **System Manager.** Este es el producto de capacidad de gestión basado en la interfaz gráfica de usuario de NetApp.
- **Kit de herramientas PowerShell de NetApp.** Este es el kit de herramientas PowerShell de NetApp para automatizar e implementar scripts y flujos de trabajo personalizados.

Kit de herramientas PowerShell de NetApp

El kit de herramientas PowerShell de NetApp (PSTK) es un módulo PowerShell que ofrece automatización integral y permite la administración del almacenamiento de ONTAP. El módulo ONTAP contiene más de 2.000 cmdlets y ayuda con la administración de NetApp AFF, FAS, hardware genérico y recursos cloud.

Puntos que debe recordar

- NetApp no es compatible con espacios de almacenamiento de Windows Server. Los espacios de almacenamiento sólo se utilizan para JBOD (solo un montón de discos) y no funcionan con ningún tipo de RAID (almacenamiento de conexión directa [DAS] o SAN).
- ONTAP no admite los pools de almacenamiento en clúster en Windows Server.
- NetApp admite el formato de disco duro virtual compartido (VHDX) para la agrupación en clústeres invitados en entornos SAN de Windows.
- Windows Server no admite la creación de pools de almacenamiento mediante LUN iSCSI o FC.

Más información

- Para obtener más información acerca del kit de herramientas PowerShell de NetApp, visite la "Sitio de soporte de NetApp".
- Para obtener información acerca de las prácticas recomendadas del kit de herramientas PowerShell de NetApp, consulte "TR-4475: Guía de prácticas recomendadas del kit de herramientas PowerShell para NetApp".

Mejores prácticas en red

Las redes Ethernet se pueden separar ampliamente en los siguientes grupos:

- Una red de cliente para las máquinas virtuales
- Una red de almacenamiento más (conexión iSCSI o SMB a los sistemas de almacenamiento)
- Una red de comunicación de clúster (latido del corazón y otra comunicación entre los nodos del clúster)
- Una red de gestión (para supervisar y solucionar problemas del sistema)
- Una red de migración (para la migración dinámica del host)
- Replicación de VM (una réplica de Hyper-V)

Mejores prácticas

- NetApp recomienda tener puertos físicos dedicados para cada una de las funcionalidades anteriores para el rendimiento y el aislamiento de la red.
- Para cada uno de los requisitos de red anteriores (a excepción de los requisitos de almacenamiento), se pueden agregar varios puertos de red físicos para distribuir la carga o proporcionar tolerancia a fallos.
- NetApp recomienda que se haya creado un switch virtual dedicado en el host de Hyper-V para la conexión del almacenamiento invitado en el equipo virtual.
- Asegúrese de que las rutas de datos iSCSI del host Hyper-V y del invitado utilizan diferentes puertos físicos y conmutadores virtuales para lograr un aislamiento seguro entre el invitado y el host.
- NetApp recomienda evitar la agrupación de NIC para los NIC iSCSI.
- NetApp recomienda utilizar ONTAP multipath input/output (MPIO) configurado en el host con fines de almacenamiento.
- NetApp recomienda utilizar MPIO en un equipo virtual invitado si se utilizan iniciadores iSCSI invitados. El uso de MPIO debe evitarse en el invitado si se utilizan discos de paso a través. En este caso, la instalación de MPIO en el host debería ser suficiente.
- NetApp recomienda no aplicar políticas de calidad de servicio al switch virtual asignado a la red de almacenamiento.
- NetApp recomienda no utilizar la dirección IP privada automática (APIPA) en NIC físicas porque APIPA no se puede enrutar y no se ha registrado en el DNS.
- NetApp recomienda activar tramas gigantes para redes CSV, iSCSI y migración dinámica con el fin de aumentar el rendimiento y reducir los ciclos de CPU.
- NetApp recomienda desactivar la opción Permitir que el sistema operativo de gestión comparta este adaptador de red para el conmutador virtual Hyper-V para crear una red dedicada para las máquinas virtuales.
- NetApp recomienda crear rutas de red redundantes (varios switches) para la migración dinámica y la red iSCSI para ofrecer resiliencia y calidad de servicio.

Aprovisionamiento en entornos SAN

Las SVM de ONTAP admiten los protocolos de bloque iSCSI y FC. Cuando se crea una SVM con el protocolo de bloque iSCSI o FC, la SVM obtiene un nombre completo de iSCSI (IQN) o un nombre FC Worldwide (WWN), respectivamente. Este identificador presenta un destino SCSI para los hosts que acceden al almacenamiento en bloques de NetApp.

Aprovisionar LUN de NetApp en Windows Server

Requisitos previos

El uso del almacenamiento de NetApp en entornos SAN en Windows Server tiene los siguientes requisitos:

- Se configura un clúster de NetApp con una o más controladoras de almacenamiento NetApp.
- El clúster de NetApp o las controladoras de almacenamiento tienen una licencia iSCSI válida.
- Hay disponibles los puertos configurados iSCSI y/o FC.
- La división en zonas de FC se realiza en un switch de FC para FC.

- Se crea al menos un agregado.
- Una SVM debería tener un LIF por red Ethernet o una estructura de Fibre Channel en cada controladora de almacenamiento que vaya a servir datos con iSCSI o Fibre Channel.

Puesta en marcha

1. Cree una nueva SVM con el protocolo de bloque iSCSI y/o FC habilitado. Una SVM nueva se puede crear con cualquiera de los siguientes métodos:
   - Comandos de la CLI en almacenamiento de NetApp
   - System Manager de ONTAP
   - Kit de herramientas PowerShell de NetApp
2. Configure el protocolo iSCSI y/o FC.
3. Asigne la SVM con LIF en cada nodo del clúster.
4. Inicie el servicio iSCSI y/o FC en la SVM.

   .

5. Cree conjuntos de puertos iSCSI y/o FC usando los LIF de SVM.
6. Cree un iGroup iSCSI y/o FC para Windows mediante el conjunto de puertos creado.
7. Añada un iniciador al iGroup. El iniciador es el IQN para iSCSI y WWPN para FC. Pueden consultarse desde Windows Server ejecutando el cmdlet de PowerShell Get-InitiatorPort.

```
# Get the IQN for iSCSI
Get-InitiatorPort | Where \{$_.ConnectionType -eq 'iSCSI'} | Select-
Object -Property NodeAddress
```

```
# Get the WWPN for FC
Get-InitiatorPort | Where \{$_.ConnectionType -eq 'Fibre Channel'} |
Select-Object -Property PortAddress
```

```
# While adding initiator to the initiator group in case of FC, make sure
to provide the initiator(PortAddress) in the standard WWPN format
```

El IQN para iSCSI en Windows Server también se puede comprobar en la configuración de las propiedades del iniciador iSCSI.

- Cree una LUN usando el asistente Crear LUN y asócielo con el iGroup creado.

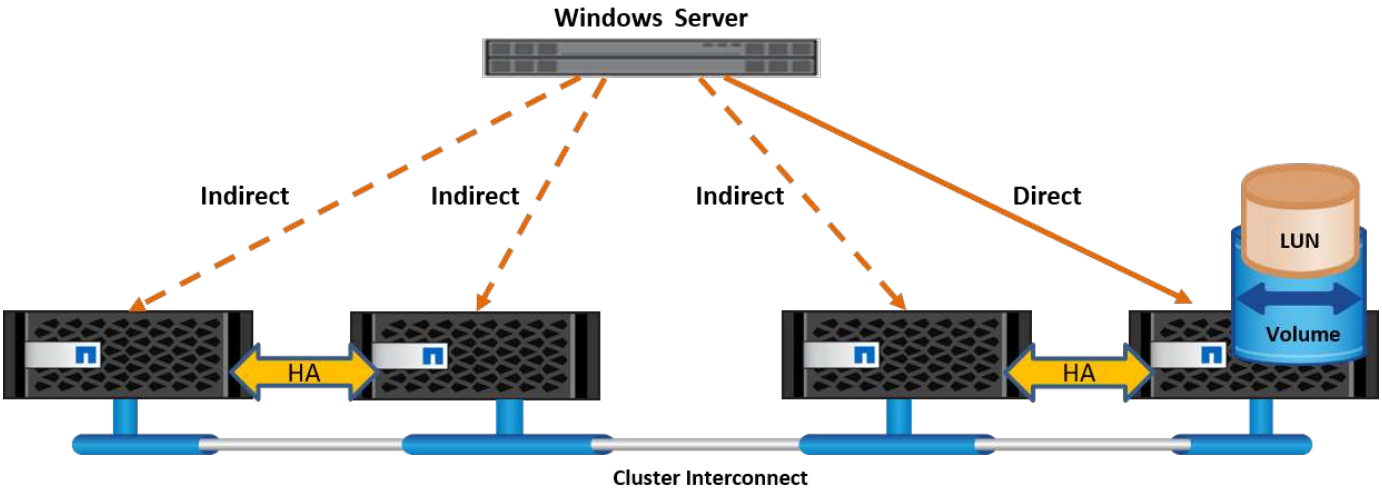
Integración de host

Windows Server utiliza la extensión MPIO de acceso asimétrico a unidad lógica (ALUA) para determinar las rutas directas e indirectas para los LUN. Aunque todas las LIF que son propiedad de una SVM aceptan solicitudes de lectura/escritura para sus LUN, solo uno de los nodos del clúster posee los discos que respaldan ese LUN en un momento dado. Esto divide las rutas disponibles a una LUN en dos tipos, directa o

indirecta, tal y como se muestra en la siguiente figura.

Una ruta directa para una LUN es una ruta en la que las LIF de una SVM y la LUN a la que se accede residen en el mismo nodo. Para pasar de un puerto de destino físico a un disco, no es necesario atravesar la interconexión de clúster.

Las rutas indirectas son rutas de datos en las que los LIF de una SVM y la LUN a la que se accede residen en nodos diferentes. Los datos deben atravesar la interconexión de clúster para pasar de un puerto de destino físico al disco.



MPIO

ONTAP proporciona un almacenamiento de alta disponibilidad en el que pueden existir varias rutas desde la controladora de almacenamiento al servidor de Windows. La multivía es la capacidad de tener varias rutas de datos desde un servidor hasta una cabina de almacenamiento. El multivía protege frente a fallos de hardware (cortes de cable, fallos de switch y adaptador de bus de host [HBA], etc.) y puede proporcionar límites de rendimiento superiores al utilizar el rendimiento agregado de múltiples conexiones. Cuando una ruta o conexión deja de estar disponible, el software de rutas múltiples cambia automáticamente la carga a una de las otras rutas disponibles. La función MPIO combina las distintas rutas físicas del almacenamiento como una única ruta lógica que se utiliza para el acceso a los datos con el fin de ofrecer resiliencia al almacenamiento y balanceo de carga. Para utilizar esta función, la función MPIO debe estar habilitada en Windows Server.

Habilite MPIO

Para activar MPIO en Windows Server, lleve a cabo los siguientes pasos:

1. Inicie sesión en Windows Server como miembro del grupo de administradores.
2. Inicie Server Manager.
3. En la sección Administrar, haga clic en Agregar funciones y características.
4. En la página Seleccionar operaciones, seleccione E/S multirruta

Configurar MPIO

Cuando utiliza el protocolo iSCSI, debe indicar a Windows Server que aplique soporte multivía a los dispositivos iSCSI en las propiedades de MPIO.

Para configurar MPIO en Windows Server, lleve a cabo los siguientes pasos:

1. Inicie sesión en Windows Server como miembro del grupo de administradores.
2. Inicie Server Manager.
3. En la sección Herramientas, haga clic en MPIO.
4. En MPIO Properties on Discover Multi-paths, seleccione Add Support for iSCSI Devices y haga clic en Add. A continuación, se le pedirá que reinicie el equipo.
5. Reinicie Windows Server para ver el dispositivo MPIO que aparece en la sección Dispositivos MPIO de Propiedades de MPIO.

Configure iSCSI

Para detectar el almacenamiento en bloques iSCSI en Windows Server, lleve a cabo los siguientes pasos:

1. Inicie sesión en Windows Server como miembro del grupo de administradores.
2. Inicie Server Manager.
3. En la sección Herramientas, haga clic en Iniciador iSCSI.
4. En la pestaña Discovery, haga clic en Discover Portal.
5. Proporcione la dirección IP de las LIF asociadas con la SVM creada para el almacenamiento de NetApp para el protocolo SAN. Haga clic en Avanzado, configure la información en la ficha General y haga clic en Aceptar.
6. El iniciador iSCSI detecta automáticamente el destino iSCSI y lo muestra en la pestaña Destinos.
7. Seleccione el destino iSCSI en los destinos detectados. Haga clic en Conectar para abrir la ventana Conectar con destino.
8. Debe crear varias sesiones desde el host de Windows Server a los LIF iSCSI de destino en el clúster de almacenamiento de NetApp. Para ello, lleve a cabo los siguientes pasos:
9. En la ventana Conectar a destino, seleccione Habilitar MPIO y haga clic en Avanzado.
10. En Configuración avanzada, en la pestaña General, seleccione el adaptador local como iniciador iSCSI de Microsoft y seleccione la IP de iniciador y la IP de portal de destino.
11. También debe conectarse mediante la segunda ruta. Por lo tanto, repita el paso 5 al paso 8, pero esta vez seleccione la IP del iniciador y la IP del portal de destino para la segunda ruta.
12. Seleccione el destino iSCSI en Discovered Targets en la ventana principal de iSCSI Properties y haga clic en Properties.
13. La ventana Propiedades muestra que se han detectado varias sesiones. Seleccione la sesión, haga clic en Devices y, a continuación, haga clic en MPIO para configurar la política de equilibrio de carga. Se muestran todas las rutas configuradas para el dispositivo y se admiten todas las políticas de equilibrio de carga. NetApp recomienda generalmente round robin con subconjunto, y esta configuración es la predeterminada para las cabinas con ALUA habilitado. Round robin es el valor predeterminado para cabinas activo-activo que no admiten ALUA.

Detectar almacenamiento basado en bloques

Para detectar el almacenamiento en bloques iSCSI o FC en Windows Server, lleve a cabo los siguientes pasos:

1. Haga clic en Administración de equipos en la sección Herramientas del Administrador de servidores.
2. En Administración de equipos, haga clic en la sección Administración de discos en almacenamiento y, a continuación, haga clic en Más acciones y Volver a analizar discos. Al hacerlo se muestran las LUN iSCSI sin configurar.

3. Haga clic en la LUN detectada y conéctela. A continuación, seleccione Inicializar disco con la partición MBR o GPT. Cree un nuevo volumen simple proporcionando el tamaño del volumen y la letra de la unidad y formatéelo usando FAT, FAT32, NTFS o el sistema de archivos resistente (ReFS).

Mejores prácticas

- NetApp recomienda habilitar thin provisioning en los volúmenes que alojan las LUN.
- Para evitar problemas con la multivía, NetApp recomienda usar las 10Gb sesiones o las 1GB sesiones en una LUN determinada.
- NetApp recomienda confirmar que ALUA está habilitado en el sistema de almacenamiento. De forma predeterminada, ALUA está habilitado en ONTAP.
- En el host de Windows Server al que se asigna el LUN de NetApp, habilite el servicio iSCSI (TCP-in) para el servicio entrante y el servicio iSCSI (TCP-out) para saliente en la configuración del firewall. Estos ajustes permiten que el tráfico iSCSI pase hacia y desde el host de Hyper-V y la controladora NetApp.

Aprovisionamiento de LUN de NetApp en Nano Server

Requisitos previos

Además de los requisitos previos mencionados en la sección anterior, el rol de almacenamiento debe estar habilitado desde el lado de Nano Server. Por ejemplo, Nano Server debe implementarse utilizando la opción -Storage. Para implementar Nano Server, consulte la sección ""Implemente Nano Server.""

Puesta en marcha

Para aprovisionar LUN de NetApp en un servidor Nano, realice los siguientes pasos:

1. Conéctese al Nano Server remotamente usando las instrucciones en la sección ""Conéctese a Nano Server"."
2. Para configurar iSCSI, ejecute los siguientes cmdlets de PowerShell en Nano Server:

```
# Start iSCSI service, if it is not already running
Start-Service msiscsi
```

```
# Create a new iSCSI target portal
New-IscsiTargetPortal -TargetPortalAddress <SVM LIF>
```

```
# View the available iSCSI targets and their node address
Get-IscsiTarget
```

```
# Connect to iSCSI target
Connect-IscsiTarget -NodeAddress <NodeAddress>
```

```
# NodeAddress is retrived in above cmdlet Get-IscsiTarget
# OR
Get-IscsiTarget | Connect-IscsiTarget
```

```
# View the established iSCSI session
Get-IscsiSession
```

```
# Note the InitiatorNodeAddress retrieved in the above cmdlet Get-
IscsiSession. This is the IQN for Nano server and this needs to be added
in the Initiator group on NetApp Storage
```

```
# Rescan the disks
Update-HostStorageCache
```

3. Añada un iniciador al iGroup.

```
Add the InitiatorNodeAddress retrieved from the cmdlet Get-IscsiSession
to the Initiator Group on NetApp Controller
```

4. Configurar MPIO.

```
# Enable MPIO Feature
Enable-WindowsOptionalFeature -Online -FeatureName MultipathIo
```

```
# Get the Network adapters and their IPs
Get-NetIPAddress -AddressFamily IPv4 -PrefixOrigin <Dhcp or Manual>
```

```
# Create one MPIO-enabled iSCSI connection per network adapter
Connect-IscsiTarget -NodeAddress <NodeAddress> -IsPersistent $True
-IsMultipathEnabled $True -InitiatorPortalAddress <IP Address of
ethernet adapter>
```

```
# NodeAddress is retrieved from the cmdlet Get-IscsiTarget
# IPs are retrieved in above cmdlet Get-NetIPAddress
```

```
# View the connections
Get-IscsiConnection
```

5. Detectar almacenamiento basado en bloques.

```
# Rescan disks
Update-HostStorageCache
```

```
# Get details of disks
Get-Disk
```

```
# Initialize disk
Initialize-Disk -Number <DiskNumber> -PartitionStyle <GPT or MBR>
```

```
# DiskNumber is retrived in the above cmdlet Get-Disk
# Bring the disk online
Set-Disk -Number <DiskNumber> -IsOffline $false
```

```
# Create a volume with maximum size and default drive letter
New-Partition -DiskNumber <DiskNumber> -UseMaximumSize
-AssignDriveLetter
```

```
# To choose the size and drive letter use -Size and -DriveLetter
parameters
# Format the volume
Format-Volume -DriveLetter <DriveLetter> -FileSystem <FAT32 or NTFS or
REFS>
```

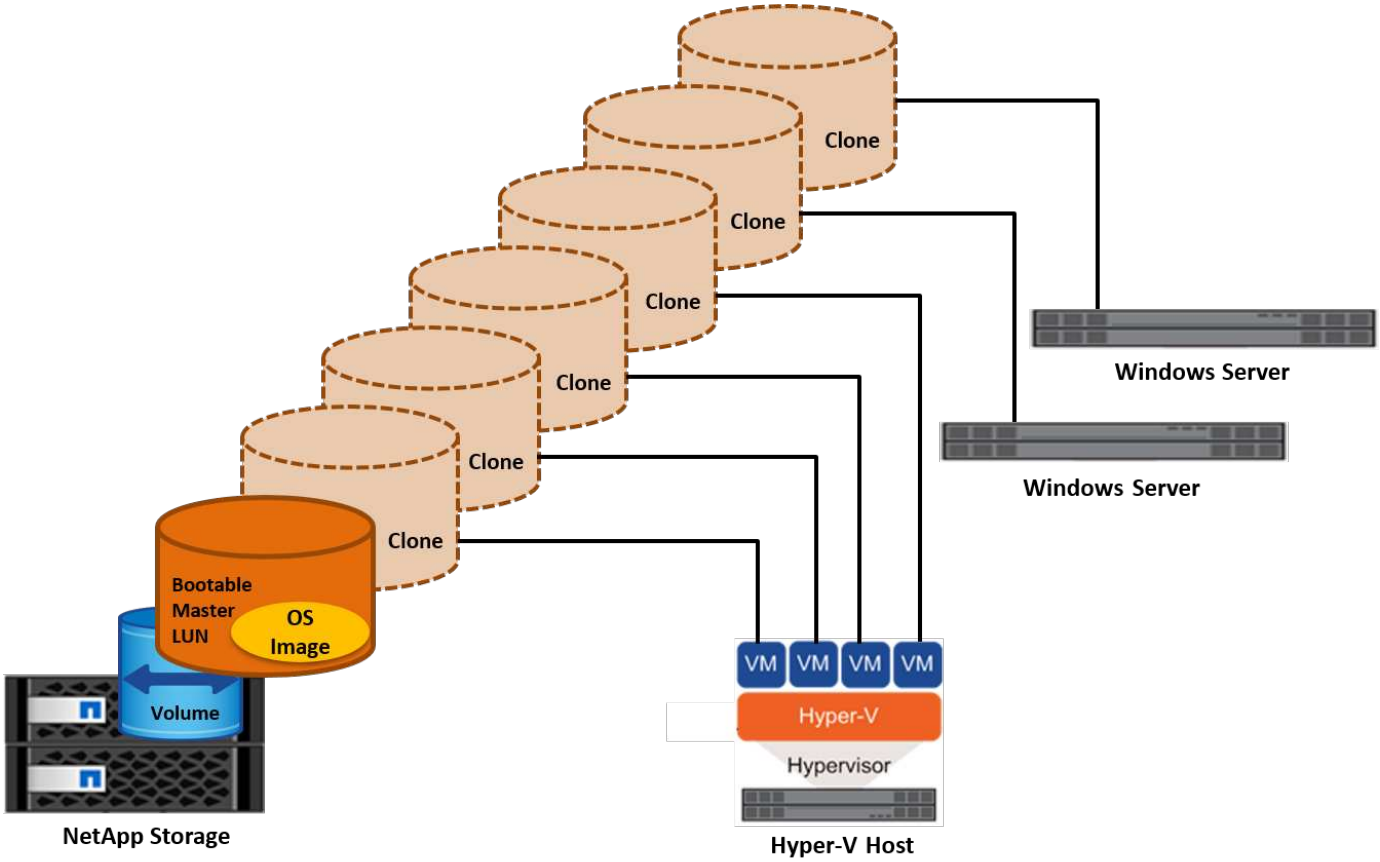
Arranque desde SAN

Un host físico (servidor) o un equipo virtual Hyper-V puede arrancar el SO de Windows Server directamente desde un LUN de NetApp en lugar de su disco duro interno. En el enfoque de arranque desde SAN, la imagen del SO desde la que se arranca reside en una LUN de NetApp conectada a un host físico o equipo virtual. En el caso de un host físico, el HBA del host físico está configurado para usar la LUN de NetApp para arrancar. Para una máquina virtual, la LUN de NetApp se conecta como disco en modo de paso para el arranque.

Enfoque de FlexClone de NetApp

Con la tecnología FlexClone de NetApp, las LUN de arranque con una imagen de SO pueden clonarse al

instante y conectarse a los servidores y máquinas virtuales para proporcionar rápidamente imágenes de sistemas operativos limpios, como se muestra en la siguiente figura.



Arranque desde SAN para host físico

Requisitos previos

- El host físico (servidor) tiene un iSCSI o FC HBA adecuados.
- Ha descargado un controlador de dispositivo HBA adecuado para el servidor compatible con Windows Server.
- El servidor tiene una unidad de CD/DVD o un medio virtual adecuado para insertar la imagen ISO de Windows Server y se ha descargado el controlador del dispositivo HBA.
- Se aprovisiona un iSCSI o un LUN FC de NetApp en la controladora de almacenamiento de NetApp.

Puesta en marcha

Para configurar el arranque desde SAN para un host físico, realice los siguientes pasos:

1. Active BootBIOS en el HBA del servidor.
2. Para los HBA iSCSI, configure la IP de iniciador, el nombre del nodo iSCSI y el modo de inicio del adaptador en los ajustes del BIOS de inicio.
3. Al crear un iGroup para iSCSI y/o FC en una controladora de almacenamiento de NetApp, agregue el iniciador de HBA del servidor al grupo. El iniciador de HBA del servidor es el WWPN para el HBA de FC o el nombre del nodo iSCSI de iSCSI HBA.
4. Cree una LUN en la controladora de almacenamiento de NetApp con un ID de LUN de 0 y asócielo con el

iGroup creado en el paso anterior. Esta LUN actúa como LUN de arranque.

5. Restrinja el HBA a una ruta única al LUN de arranque. Se pueden añadir rutas adicionales después de instalar Windows Server en el LUN de arranque para aprovechar la función de rutas múltiples.
6. Utilice la utilidad BootBIOS del HBA para configurar el LUN como dispositivo de arranque.
7. Reinicie el host e introduzca la utilidad BIOS del host.
8. Configure el BIOS del host para que el LUN de inicio sea el primer dispositivo en el orden de inicio.
9. Desde la ISO de Windows Server, inicie la configuración de instalación.
10. Cuando la instalación le pregunte ¿Dónde desea instalar Windows?, haga clic en Cargar controlador en la parte inferior de la pantalla de instalación para iniciar la página Seleccionar controlador para instalar. Proporcione la ruta del controlador del dispositivo HBA descargado anteriormente y finalice la instalación del controlador.
11. Ahora la LUN de inicio creada anteriormente debe estar visible en la página de instalación de Windows. Seleccione el LUN de inicio para la instalación de Windows Server en el LUN de arranque y finalice la instalación.

Arranque desde SAN para equipos virtuales

Para configurar el arranque desde SAN para una máquina virtual, lleve a cabo los siguientes pasos:

Puesta en marcha

1. Al crear un iGroup para iSCSI o FC en una controladora de almacenamiento de NetApp, agregue el IQN para iSCSI o el WWN para FC del servidor de Hyper-V a la controladora.
2. Cree LUN o clones de LUN en la controladora de almacenamiento de NetApp y asócielo con el iGroup creado en el paso anterior. Estas LUN actúan como LUN de arranque para las máquinas virtuales.
3. Detectar las LUN en el servidor de Hyper-V, conectarlas e inicializarlas.
4. Desconectar las LUN.
5. Cree VM con la opción Adjuntar un Disco Duro Virtual más adelante en la página Conectar Disco Duro Virtual.
6. Añada una LUN como disco en modo de paso a una máquina virtual.
    a. Abra la configuración de la máquina virtual.
    b. Haga clic en Controlador IDE 0, seleccione Disco duro y haga clic en Agregar. Al seleccionar IDE Controller 0, este disco se convierte en el primer dispositivo de inicio para la máquina virtual.
    c. Seleccione Disco duro físico en las opciones de Disco duro y seleccione un disco de la lista como disco de paso. Los discos son LUN configuradas en los pasos anteriores.
7. Instale Windows Server en el disco de paso.

Mejores prácticas

- Asegúrese de que las LUN estén sin conexión. De lo contrario, no se puede agregar el disco como disco en modo de paso a una máquina virtual.
- Cuando haya varias LUN, asegúrese de anotar el número de disco de la LUN en la gestión de discos. Es necesario porque los discos de la máquina virtual aparecen con el número de disco. Además, la selección del disco como disco en modo de paso para la máquina virtual se basa en este número de disco.
- NetApp recomienda evitar la agrupación de NIC para los NIC iSCSI.
- NetApp recomienda usar ONTAP MPIO configurado en el host con fines de almacenamiento.

Aprovisionamiento en entornos SMB

ONTAP proporciona almacenamiento NAS de alto rendimiento y resistente para las máquinas virtuales de Hyper-V que utilizan el protocolo SMB3.

Cuando se crea una SVM con el protocolo CIFS, un servidor CIFS se ejecuta sobre la SVM que forma parte del dominio de Windows Active Directory. Los recursos compartidos de SMB se pueden utilizar para un directorio inicial y para alojar cargas de trabajo de Hyper-V y SQL Server. ONTAP admite las siguientes funciones de SMB 3,0:

- Identificadores persistentes (archivos compartidos disponibles de forma continua)
- Protocolo de observación
- Recuperación tras fallos de cliente en clúster
- Reconocimiento de la escalabilidad horizontal
- ODX
- VSS remoto

Aprovisionamiento de recursos compartidos SMB en Windows Server

Requisitos previos

El uso del almacenamiento de NetApp en entornos NAS en Windows Server tiene los siguientes requisitos:

- El clúster de ONTAP tiene una licencia CIFS válida.
- Se crea al menos un agregado.
- Se crea una interfaz lógica de datos (LIF) y las LIF de datos deben configurarse para CIFS.
- Hay un servidor de dominio de Windows Active Directory y credenciales de administrador de dominio configuradas con DNS.
- Cada nodo del clúster NetApp se sincroniza por hora con la controladora de dominio de Windows.

Controlador de dominio de Active Directory

Una controladora de almacenamiento de NetApp puede unirse y funcionar en un Active Directory similar a un servidor Windows Server. Durante la creación de la SVM, es posible configurar el DNS proporcionando los detalles del nombre de dominio y del servidor de nombres. La SVM intenta buscar una controladora de dominio de Active Directory mediante la consulta del DNS de un servidor de protocolo ligero de acceso a directorios (LDAP)/Active Directory de forma similar a Windows Server.

Para que la configuración de CIFS funcione correctamente, las controladoras de almacenamiento de NetApp deben estar sincronizadas por hora con el controlador de dominio de Windows. NetApp recomienda desfase de tiempo entre la controladora de dominio de Windows y la controladora de almacenamiento de NetApp que no supere los cinco minutos. Se recomienda configurar el servidor de protocolo de tiempo de redes (NTP) para que el clúster de ONTAP se sincronice con un origen de tiempo externo. Para configurar la controladora de dominio de Windows como servidor NTP, ejecute el siguiente comando en su clúster de ONTAP:

```
$domainControllerIP = "<input IP Address of windows domain controller>"
cluster::> system services ntp server create -server $domainControllerIP
```

Puesta en marcha

1. Cree una nueva SVM con el protocolo NAS CIFS habilitado. Una SVM nueva se puede crear con cualquiera de los siguientes métodos:
   - Comandos de la CLI en ONTAP
   - System Manager
   - El kit de herramientas PowerShell de NetApp
2. Configure el protocolo CIFS
   a. Proporcione el nombre del servidor CIFS.
   b. Proporcione el Active Directory al que se debe unir el servidor CIFS. Debe contar con las credenciales de administrador de dominio para unir al servidor CIFS a Active Directory.
3. Asigne la SVM con LIF en cada nodo del clúster.
4. Inicie el servicio CIFS en la SVM.
5. Cree un volumen con el estilo de seguridad NTFS a partir del agregado.
6. Crear un Qtree en el volumen (opcional).
7. Crear recursos compartidos que correspondan al directorio del volumen o qtree para que se pueda acceder a ellos desde Windows Server. Seleccione Enable Continuous Availability for Hyper-V durante la creación del recurso compartido si el recurso compartido se utiliza para el almacenamiento de Hyper-V. Esto permite una alta disponibilidad para los recursos compartidos de archivos.
8. Edite el recurso compartido creado y modifique los permisos según sea necesario para acceder al recurso compartido. Los permisos para el recurso compartido SMB se deben configurar para otorgar acceso a las cuentas de equipo de todos los servidores que acceden a este recurso compartido.

Integración de host

El protocolo NAS CIFS está integrado de manera nativa en ONTAP. Por lo tanto, Windows Server no requiere ningún software cliente adicional para acceder a los datos en ONTAP. Aparece una controladora de almacenamiento de NetApp en la red como servidor de archivos nativo y admite la autenticación de Microsoft Active Directory.

Para detectar el recurso compartido de CIFS creado anteriormente con Windows Server, lleve a cabo los siguientes pasos:

1. Inicie sesión en Windows Server como miembro del grupo de administradores.
2. Vaya a run.exe y escriba la ruta completa del recurso compartido CIFS creado para acceder al recurso compartido.
3. Para asignar de forma permanente el recurso compartido en Windows Server, haga clic con el botón derecho en este equipo, haga clic en Asignar unidad de red y proporcione la ruta del recurso compartido CIFS.
4. Algunas tareas de gestión de CIFS pueden realizarse usando Microsoft Management Console (MMC). Antes de realizar estas tareas, debe conectar el MMC al almacenamiento ONTAP mediante los comandos del menú MMC.
   a. Para abrir MMC en Windows Server, haga clic en Administración de equipos en la sección Herramientas del Administrador del servidor.
   b. Haga clic en Más acciones y Conectarse a otro equipo, lo que abre el cuadro de diálogo Seleccionar equipo.

c. Introduzca el nombre del servidor CIFS o la dirección IP de la LIF de SVM para conectarse al servidor CIFS.

d. Expanda Herramientas del sistema y Carpetas compartidas para ver y administrar archivos abiertos, sesiones y recursos compartidos.

Mejores prácticas

- Para confirmar que no hay tiempo de inactividad cuando un volumen se mueve de un nodo a otro o en caso de fallo de un nodo, NetApp recomienda habilitar la opción de disponibilidad continua en el recurso compartido de archivos.
- Cuando se aprovisionan equipos virtuales para un entorno de Hyper-V a través de SMB, NetApp le recomienda que habilite la copia de datos descargados en el sistema de almacenamiento. De este modo, se reduce el tiempo de aprovisionamiento de las máquinas virtuales.
- Si el clúster de almacenamiento aloja varias cargas de trabajo de SMB como SQL Server, Hyper-V y CIFS, NetApp recomienda alojar diferentes cargas de trabajo de SMB en SVM separadas en agregados separados. Esta configuración es ventajosa porque cada una de estas cargas de trabajo garantiza distribuciones por volúmenes y redes de almacenamiento únicas.
- NetApp recomienda conectar los hosts de Hyper-V y el almacenamiento ONTAP con una red 10GB GbE, si hay alguno disponible. En el caso de la conectividad de red de 1GB GbE, NetApp recomienda crear un grupo de interfaces que consta de varios puertos 1GB GbE.
- Cuando se migran máquinas virtuales de un recurso compartido SMB 3,0 a otro, NetApp recomienda habilitar la funcionalidad de descarga de la copia CIFS en el sistema de almacenamiento para que la migración sea más rápida.

Puntos que debe recordar

- Cuando se aprovisionan volúmenes para entornos SMB, los volúmenes deben crearse con el estilo de seguridad NTFS.
- La configuración de hora de los nodos del clúster debe configurarse según corresponda. Utilice NTP si el servidor CIFS de NetApp debe participar en el dominio de Windows Active Directory.
- Las asas persistentes solo funcionan entre nodos de un par de alta disponibilidad.
- El protocolo testigo solo funciona entre nodos de un par de alta disponibilidad.
- Los recursos compartidos de archivos disponibles continuamente solo son compatibles con las cargas de trabajo de Hyper-V y SQL Server.
- El multicanal SMB es compatible desde ONTAP 9,4 en adelante.
- No se admite RDMA.
- REFS no es compatible.

Aprovisionamiento de recursos compartidos SMB en Nano Server

Nano Server no requiere software de cliente adicional para acceder a los datos del recurso compartido de CIFS en una controladora de almacenamiento de NetApp.

Para copiar archivos de Nano Server a un recurso compartido de CIFS, ejecute los siguientes cmdlets en el servidor remoto:

```
$ip = "<input IP Address of the Nano Server>"
```

```
# Create a New PS Session to the Nano Server
$session = New-PSSession -ComputerName $ip -Credential ~\Administrator
```

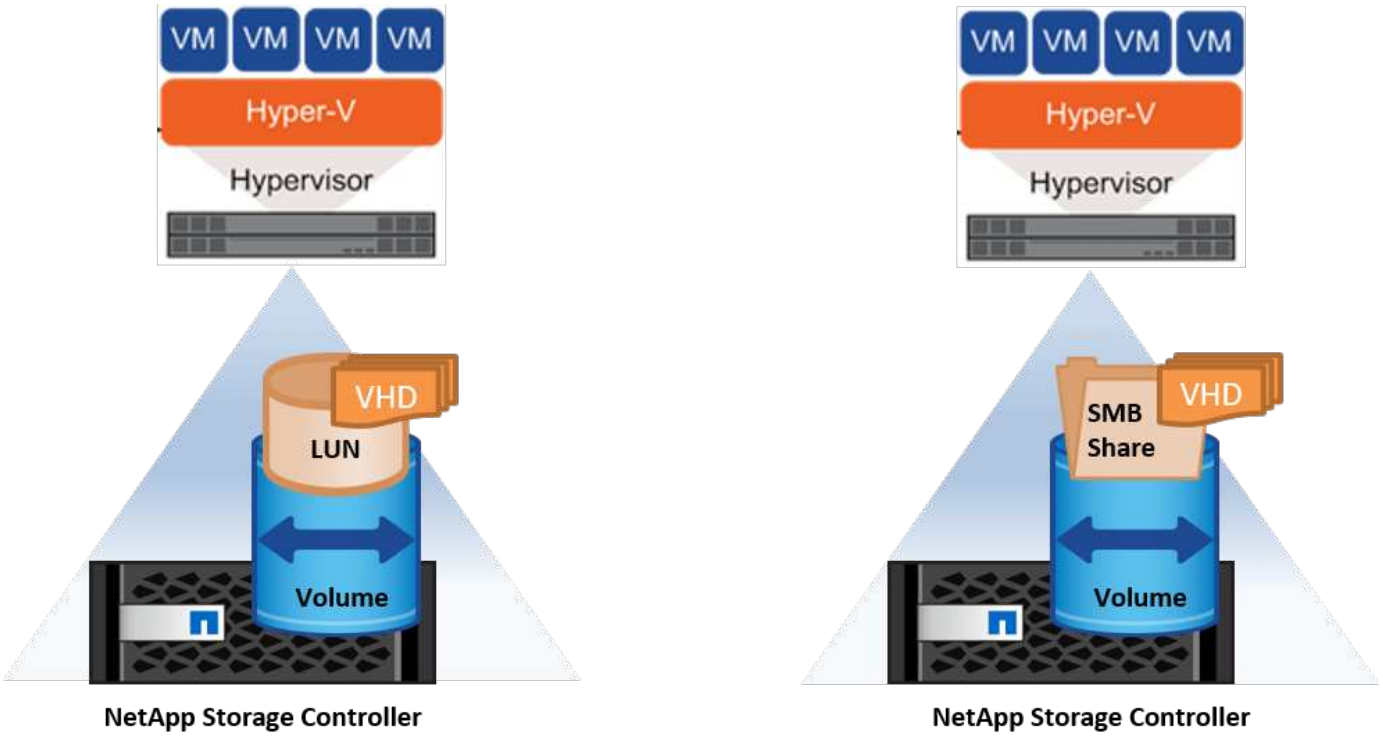
```
 Copy-Item -FromSession $s -Path C:\Windows\Logs\DISM\dism.log
-Destination \\cifsshare
* `cifsshare` Es el recurso compartido de CIFS en la controladora de
almacenamiento de NetApp.
* Para copiar archivos en Nano Server, ejecute el siguiente cmdlet:
```

+
Copy-Item -ToSession $s -Path \\cifsshare\<file> -Destination C:\

Para copiar todo el contenido de una carpeta, especifique el nombre de la carpeta y use el parámetro -Recurse al final del cmdlet.

La infraestructura de almacenamiento de Hyper-V en NetApp

La infraestructura de almacenamiento de Hyper-V se puede alojar en sistemas de almacenamiento de ONTAP. Almacenamiento para Hyper-V para almacenar los archivos de equipos virtuales y sus discos se pueden suministrar usando LUN de NetApp o recursos compartidos CIFS de NetApp, como se muestra en la siguiente figura.



Almacenamiento Hyper-V en LUN de NetApp

- Aprovisionar una LUN de NetApp en la máquina del servidor de Hyper-V. Si quiere más información, consulte la sección «"Aprovisionamiento en entornos SAN"."

- Abra Hyper-V Manager en la sección Herramientas del Administrador de servidores.
- Seleccione el servidor de Hyper-V y haga clic en Configuración de Hyper-V.
- Especifique la carpeta predeterminada para almacenar la máquina virtual y su disco como la LUN. Al hacerlo, se establece la ruta predeterminada como LUN para el almacenamiento de Hyper-V. Si desea especificar la ruta de forma explícita para una máquina virtual, puede hacerlo durante la creación de la máquina virtual.

Almacenamiento de Hyper-V en CIFS de NetApp

Antes de comenzar los pasos enumerados en esta sección, revise la sección “"Aprovisionamiento en entornos SMB".». Para configurar el almacenamiento de Hyper-V en el recurso compartido de CIFS de NetApp, lleve a cabo los siguientes pasos:

1. Abra Hyper-V Manager en la sección Herramientas del Administrador de servidores.
2. Seleccione el servidor de Hyper-V y haga clic en Configuración de Hyper-V.
3. Especifique la carpeta predeterminada para almacenar la máquina virtual y su disco como el recurso compartido de CIFS. Al hacerlo, se define la ruta predeterminada como recurso compartido de CIFS para el almacenamiento de Hyper-V. Si desea especificar la ruta de forma explícita para una máquina virtual, puede hacerlo durante la creación de la máquina virtual.

Cada equipo virtual en Hyper-V puede, a su vez, proporcionarse con los LUN de NetApp y los recursos compartidos de CIFS que se proporcionaban al host físico. Este procedimiento es el mismo que para cualquier host físico. Los siguientes métodos se pueden usar para aprovisionar almacenamiento a una máquina virtual:

- Añadir un LUN de almacenamiento mediante el iniciador FC dentro de la máquina virtual
- Agregar una LUN de almacenamiento mediante el iniciador iSCSI dentro de la máquina virtual
- Agregar un disco físico en modo de paso a una máquina virtual
- Agregar VHD/VHDX a una máquina virtual desde el host

Mejores prácticas

- Cuando un equipo virtual y sus datos se almacenan en el almacenamiento de NetApp, NetApp recomienda ejecutar la deduplicación de NetApp a intervalos regulares a nivel de volumen. Esta práctica provoca un ahorro de espacio considerable cuando se alojan equipos virtuales idénticos en un recurso compartido de CSV o SMB. La deduplicación se ejecuta en la controladora de almacenamiento y no afecta al rendimiento del sistema host ni de los equipos virtuales.
- Cuando utilice LUN iSCSI para Hyper-V, asegúrese de activar 'Servicio iSCSI (TCP-IN) para entrada' y 'Servicio iSCSI (TCP-OUT) para saliente' en la configuración del firewall en el host de Hyper-V. De este modo, se permite que el tráfico iSCSI pase hacia y desde el host de Hyper-V y el controlador de NetApp.
- NetApp recomienda desactivar la opción Permitir que el sistema operativo de gestión comparta este adaptador de red para el conmutador virtual de Hyper-V. Al hacerlo, se crea una red dedicada para las máquinas virtuales.

Puntos que debe recordar

- El aprovisionamiento de un equipo virtual mediante Fibre Channel virtual requiere un HBA FC habilitado para la virtualización N_Port ID. Se admite un máximo de cuatro puertos FC.
- Si el sistema host se configura con varios puertos FC y se presenta a la máquina virtual, debe instalarse MPIO en la máquina virtual para habilitar el acceso multivía.

- Los discos de paso a través no se pueden aprovisionar al host si se está utilizando MPIO en ese host, ya que los discos de paso no son compatibles con MPIO.
- El disco utilizado para los archivos VHD/VHDx debe utilizar el formato 64K para la asignación.

Más información

- Para obtener información sobre los HBA de FC, consulte "Herramienta de matriz de interoperabilidad (IMT)" .
- Para obtener más información acerca de Fibre Channel virtual, consulte Microsoft "Descripción general de Fibre Channel virtual para Hyper-V" página.

Transferencia de datos descargada

Microsoft ODX, también conocido como copia de datos descargados, habilita transferencias de datos directas dentro del dispositivo de almacenamiento o entre dispositivos de almacenamiento compatibles sin transferir los datos a través de la computadora del host. ONTAP admite la función ODX para los protocolos CIFS y SAN. ODX puede mejorar el rendimiento potencialmente si las copias se encuentran en el mismo volumen, reducir la utilización de la CPU y la memoria en el cliente y reducir la utilización de ancho de banda de I/O de la red.

Con ODX, es más rápido y eficiente copiar archivos dentro de los recursos compartidos SMB, dentro de las LUN y entre los recursos compartidos SMB y las LUN si está en el mismo volumen. Este método es más útil en una situación para la que se necesitan varias copias de la imagen maestra de un sistema operativo (VHD/VHDX) en el mismo volumen. Se pueden realizar varias copias de la misma imagen maestra en un tiempo considerablemente menor si las copias se encuentran en el mismo volumen. ODX también se aplica en almacenamiento de Hyper-V para mover almacenamiento de máquinas virtuales.

Si la copia se realiza entre volúmenes, es posible que no haya un aumento significativo del rendimiento en comparación con las copias basadas en host.

Para habilitar la función ODX en CIFS, ejecute los siguientes comandos de la CLI en la controladora de almacenamiento de NetApp:

1. Habilite ODX para CIFS.
   #establecer el nivel de privilegio para el diagnóstico
   cluster::> diagnóstico set -privilege

   ```
   #enable the odx feature
   cluster::> vserver cifs options modify -vserver <vserver_name> -copy
   -offload-enabled true
   ```

   ```
   #return to admin privilege level
   cluster::> set privilege admin
   ```

2. Para habilitar la función ODX en SAN, ejecute los siguientes comandos de la CLI en la controladora de almacenamiento de NetApp:
   #establecer el nivel de privilegio para el diagnóstico
   cluster::> diagnóstico set -privilege

```
#enable the odx feature
cluster::> copy-offload modify -vserver <vserver_name> -scsi enabled
```

```
#return to admin privilege level
cluster::> set privilege admin
```

Puntos que debe recordar

- Para CIFS, ODX solo está disponible cuando el cliente y el servidor de almacenamiento admiten SMB 3,0 y la función ODX.
- En entornos SAN, ODX solo está disponible cuando tanto el cliente como el servidor de almacenamiento admiten la función ODX.

Más información

Para obtener más información acerca de ODX, consulte "Mejora del rendimiento de Microsoft Remote Copy" y.. "Transferencias de datos descargados de Microsoft" .

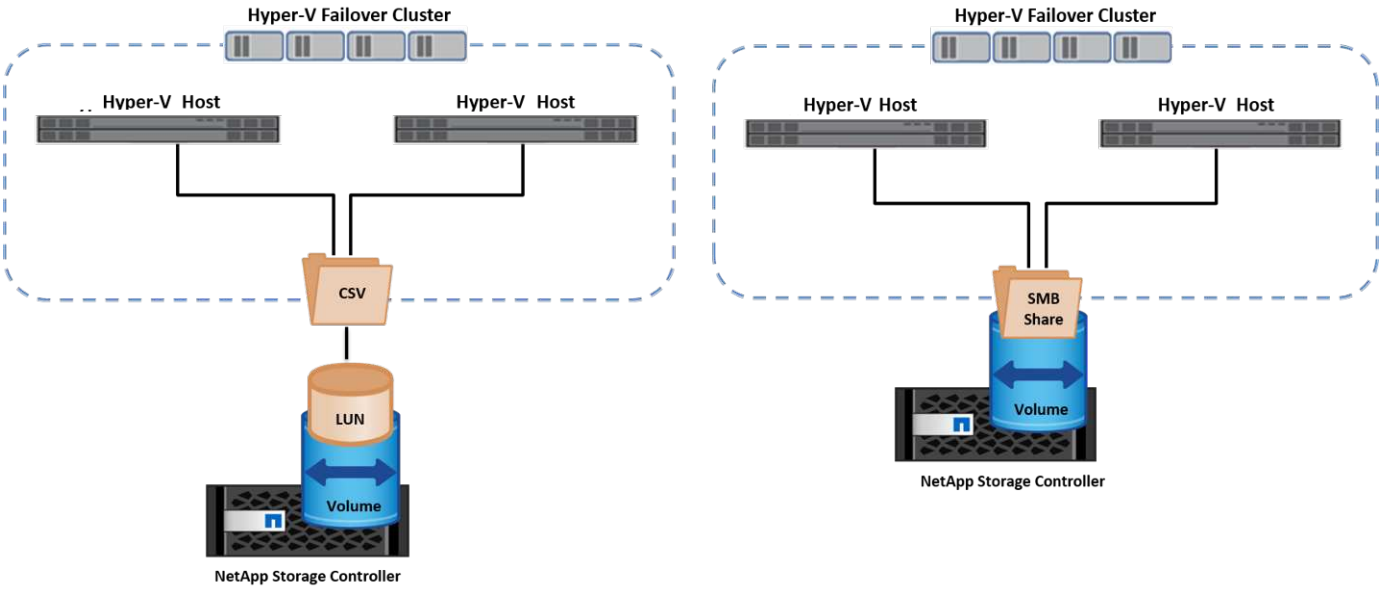
Agrupación en cluster Hyper-V: Alta disponibilidad y escalabilidad para equipos virtuales

Los clusters de conmutación por error proporcionan alta disponibilidad y escalabilidad a los servidores de Hyper-V. Un cluster de recuperación tras fallos es un grupo de servidores Hyper-V independientes que funcionan conjuntamente para aumentar la disponibilidad y la escalabilidad de los equipos virtuales.

Los servidores en clúster de Hyper-V (denominados nodos) están conectados por la red física y por el software de clúster. Estos nodos utilizan almacenamiento compartido para almacenar los archivos de la máquina virtual, lo que incluye los archivos de configuración, disco duro virtual (VHD) y snapshots. El almacenamiento compartido puede ser un recurso compartido SMB/CIFS de NetApp o un volumen compartido en cluster sobre un LUN de NetApp, como se muestra a continuación. Este almacenamiento compartido proporciona un espacio de nombres consistente y distribuido a los que todos los nodos del cluster pueden acceder de forma simultánea. Por lo tanto, si un nodo falla en el clúster, el otro nodo proporciona servicio mediante un proceso llamado conmutación al respaldo. Los clústeres de conmutación por error se pueden gestionar mediante el complemento Administrador de clúster de conmutación por error y los cmdlets de Windows PowerShell de agrupación en clúster de conmutación por error.

Volúmenes compartidos de clúster

Los volúmenes compartidos en cluster permiten que múltiples nodos de un clúster de conmutación por error tengan acceso de lectura/escritura simultáneamente a la misma LUN de NetApp que se aprovisiona como volumen NTFS o ReFS. Con los volúmenes compartidos en cluster, los roles en cluster pueden relevar rápidamente de un nodo a otro sin necesidad de cambiar la propiedad de la unidad, ni de desmontar y montar un volumen. Los volúmenes compartidos en cluster también simplifican la gestión de un número potencialmente grande de LUN en un clúster de recuperación tras fallos. Los CSV proporcionan un sistema de archivos en cluster de uso general que se coloca por encima de NTFS o ReFS.



Mejores prácticas

- NetApp recomienda desactivar la comunicación del clúster en la red iSCSI para evitar que la comunicación del clúster interno y el tráfico de CSV fluyan por la misma red.
- NetApp recomienda tener rutas de red redundantes (varios switches) para ofrecer resiliencia y calidad de servicio.

Puntos que debe recordar

- Los discos utilizados para CSV deben particionarse con NTFS o ReFS. Los discos formateados con FAT o FAT32 no se pueden utilizar para un CSV.
- Los discos utilizados para CSV deben utilizar el formato 64K para la asignación.

Más información

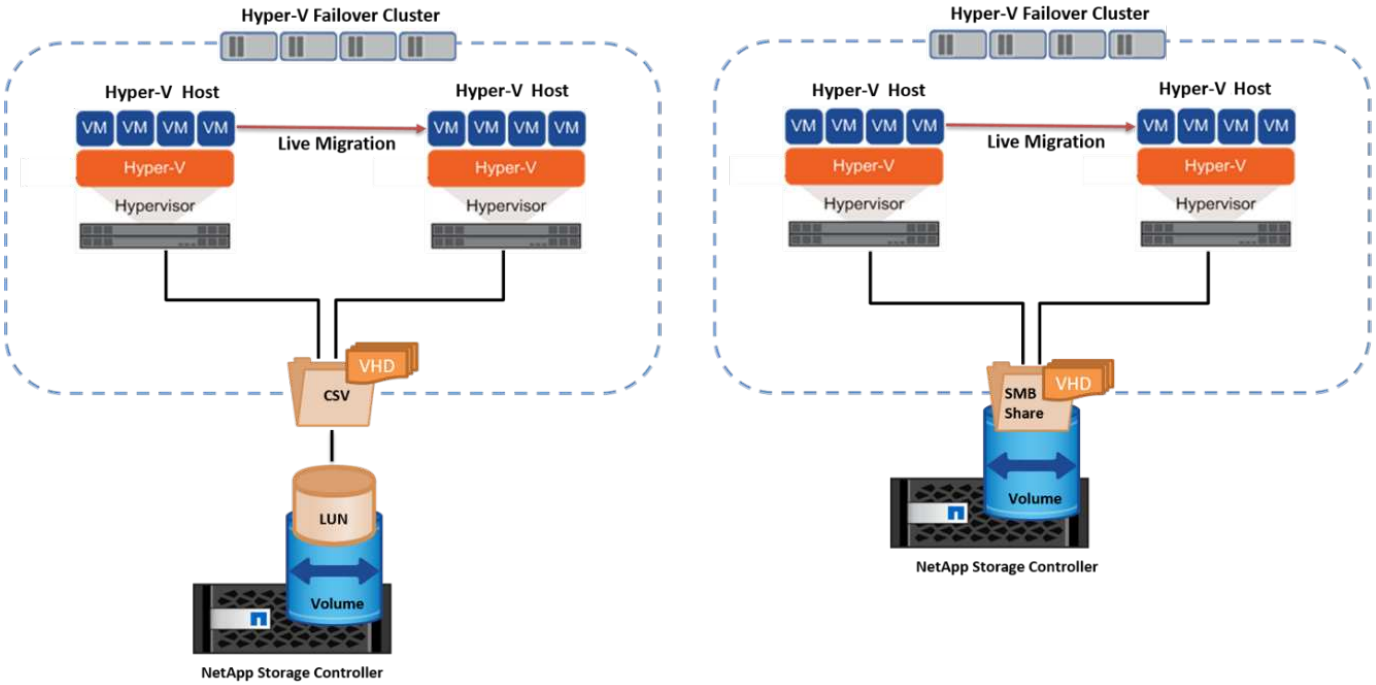
Si desea obtener información sobre la implantación de un cluster de Hyper-V, consulte el apéndice B: "Implemente el cluster Hyper-V".

Migración en vivo de Hyper-V: Migración de equipos virtuales

A veces, es necesario durante la vida útil de las máquinas virtuales para moverlas a un host diferente en el clúster de Windows. Hacerlo puede ser necesario si el host se está quedando sin recursos del sistema o si el host es necesario reiniciarse por razones de mantenimiento. Del mismo modo, podría ser necesario mover un equipo virtual a otro LUN o recurso compartido de SMB. Esto puede ser necesario si el LUN o el recurso compartido actual se está quedando sin espacio o tiene una rentabilidad inferior al rendimiento esperado. La migración en vivo de Hyper-V mueve las máquinas virtuales en ejecución de un servidor Hyper-V físico a otro sin afectar la disponibilidad de las máquinas virtuales a los usuarios. Puede migrar equipos virtuales activos entre servidores de Hyper-V que forman parte de un clúster de conmutación al nodo de respaldo o entre servidores de Hyper-V independientes que no forman parte de ningún cluster.

Migración en vivo en un entorno en clúster

Las máquinas virtuales pueden moverse sin problemas entre los nodos de un clúster. La migración de VM es instantánea porque todos los nodos del clúster comparten el mismo almacenamiento y tienen acceso a la máquina virtual y a su disco. La siguiente figura muestra la migración activa en un entorno en cluster.



Mejor práctica

- Disponga de un puerto dedicado para el tráfico de migración dinámica.
- Disponga de una red de migración activa de host dedicado para evitar problemas relacionados con la red durante la migración.

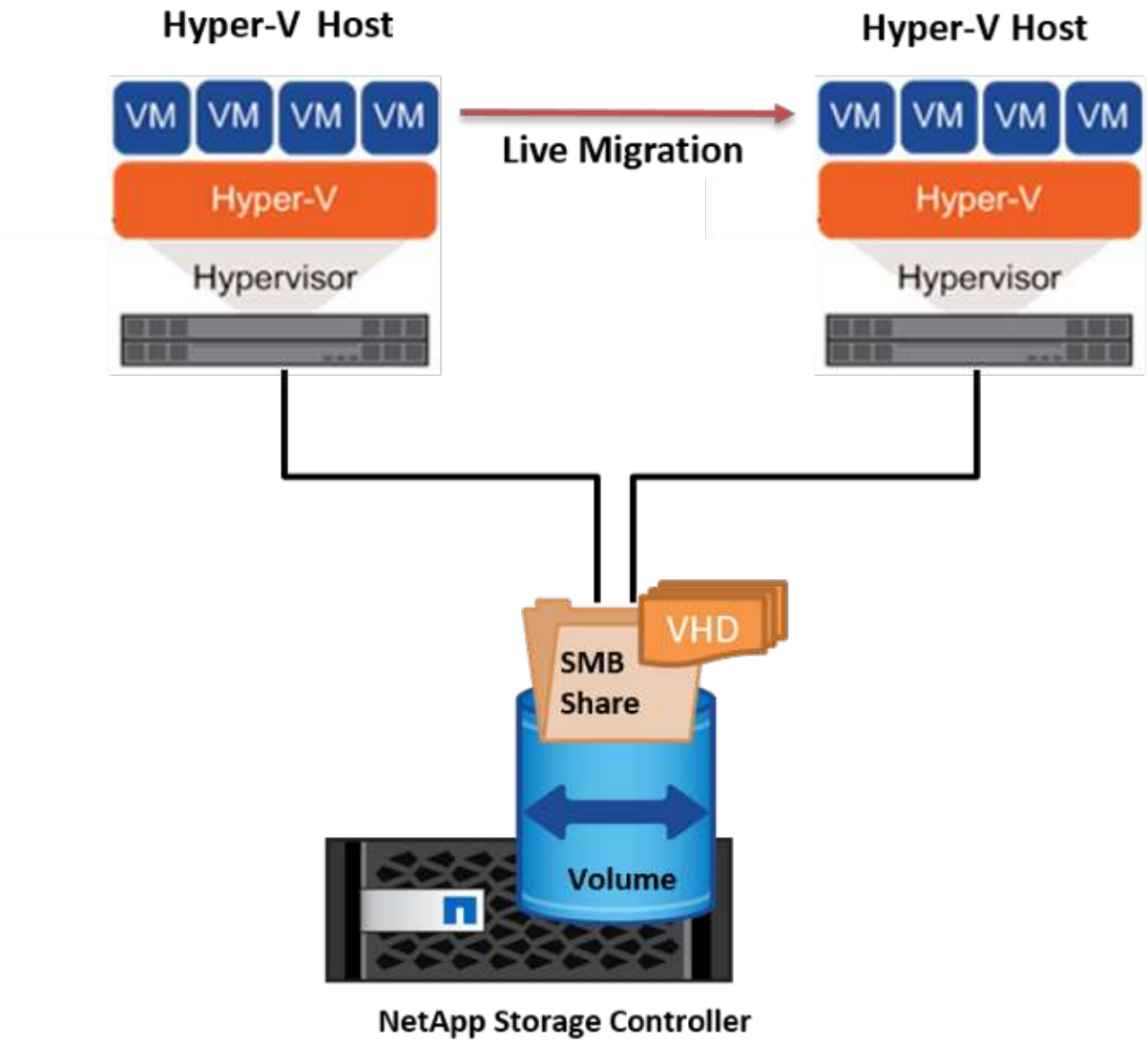
Más información

Para obtener más información sobre la puesta en marcha de la migración en vivo en un entorno en clúster, consulte "Apéndice C: Implementación de la migración en vivo de Hyper-V en un entorno en cluster".

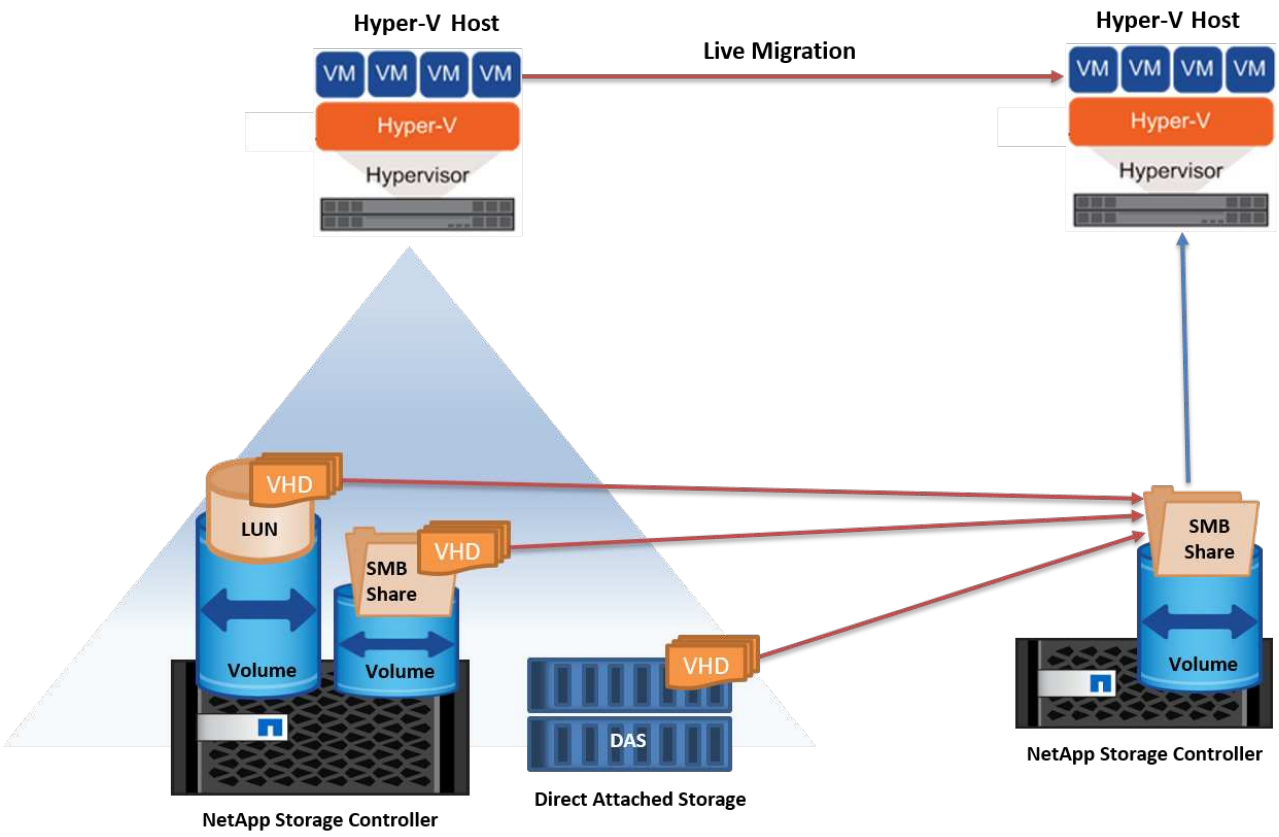
Migración en vivo fuera de un entorno en clúster

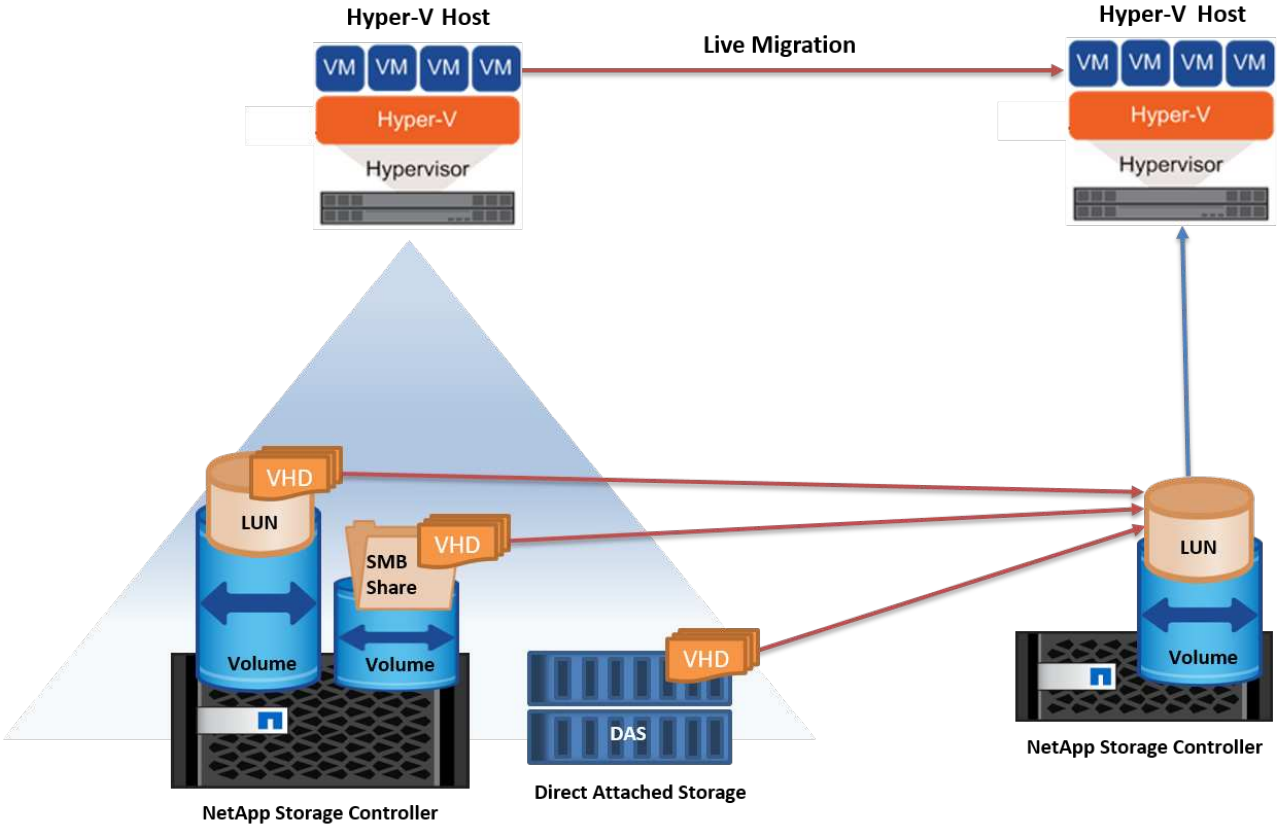
Puede migrar en vivo una máquina virtual entre dos servidores de Hyper-V independientes y no agrupados en clúster. Este proceso puede utilizar una migración dinámica sin uso compartido o sin uso compartido.

- En la migración dinámica compartida, la máquina virtual se almacena en un recurso compartido de SMB. Por lo tanto, cuando migra una máquina virtual en vivo, el almacenamiento de la máquina virtual permanece en el recurso compartido SMB central para que el otro nodo pueda acceder de forma instantánea, como se muestra a continuación.



- En la migración en vivo sin compartir, cada servidor de Hyper-V tiene su propio almacenamiento local (puede ser un recurso compartido SMB, una LUN o DAS) y el almacenamiento del equipo virtual es local en su servidor de Hyper-V. Cuando se migra una máquina virtual activa, el almacenamiento de la máquina virtual se refleja en el servidor de destino a través de la red cliente y, a continuación, se migra la máquina virtual. El equipo virtual almacenado en DAS, un LUN o un recurso compartido de SMB/CIFS puede moverse a un recurso compartido SMB/CIFS en el otro servidor Hyper-V, tal como se muestra en la siguiente figura. También se puede trasladar a una LUN, como se muestra en la segunda figura.





Más información

Para obtener más información sobre la puesta en marcha de la migración en vivo fuera de un entorno en

clúster, consulte "Apéndice D: Implemente Hyper-V Live Migration fuera de un entorno en cluster".

Migración dinámica de almacenamiento de Hyper-V

Durante la vida útil de un equipo virtual, es posible que deba mover el almacenamiento de un equipo virtual (VHD/VHDX) a otro LUN o recurso compartido de SMB. Esto puede ser necesario si el LUN o el recurso compartido actual se está quedando sin espacio o tiene una rentabilidad inferior al rendimiento esperado.

El LUN o el recurso compartido que aloja actualmente el equipo virtual puede quedarse sin espacio, reasignarse o reducir el rendimiento. En estas circunstancias, el equipo virtual se puede mover sin necesidad de sufrir tiempos de inactividad a otro LUN o recurso compartido en un volumen, agregado o clúster diferentes. Este proceso es más rápido si el sistema de almacenamiento tiene capacidad de copia/descarga. Los sistemas de almacenamiento de NetApp son compatibles con la descarga de copias de forma predeterminada para los entornos CIFS y SAN.

La función ODX realiza copias de archivos completos o secundarios entre dos directorios que residen en servidores remotos. Una copia se crea copiando datos entre los servidores (o el mismo servidor si los archivos de origen y de destino están en el mismo servidor). La copia se crea sin que el cliente lea los datos del origen o escriba en el destino. Este proceso reduce el uso de memoria y procesador para el cliente o el servidor y minimiza el ancho de banda de E/S de la red. La copia es más rápida si está dentro del mismo volumen. Si la copia se realiza entre volúmenes, es posible que no haya un aumento significativo del rendimiento en comparación con las copias basadas en host. Antes de continuar con una operación de copia en el host, confirme que los ajustes de descarga de copia estén configurados en el sistema de almacenamiento.

Cuando se inicia la migración activa de almacenamiento de equipos virtuales desde un host, se identifican el origen y el destino, y la actividad de copia se descarga al sistema de almacenamiento. Debido a que el sistema de almacenamiento realiza la actividad, el uso de la CPU, la memoria o la red del host es insignificante.

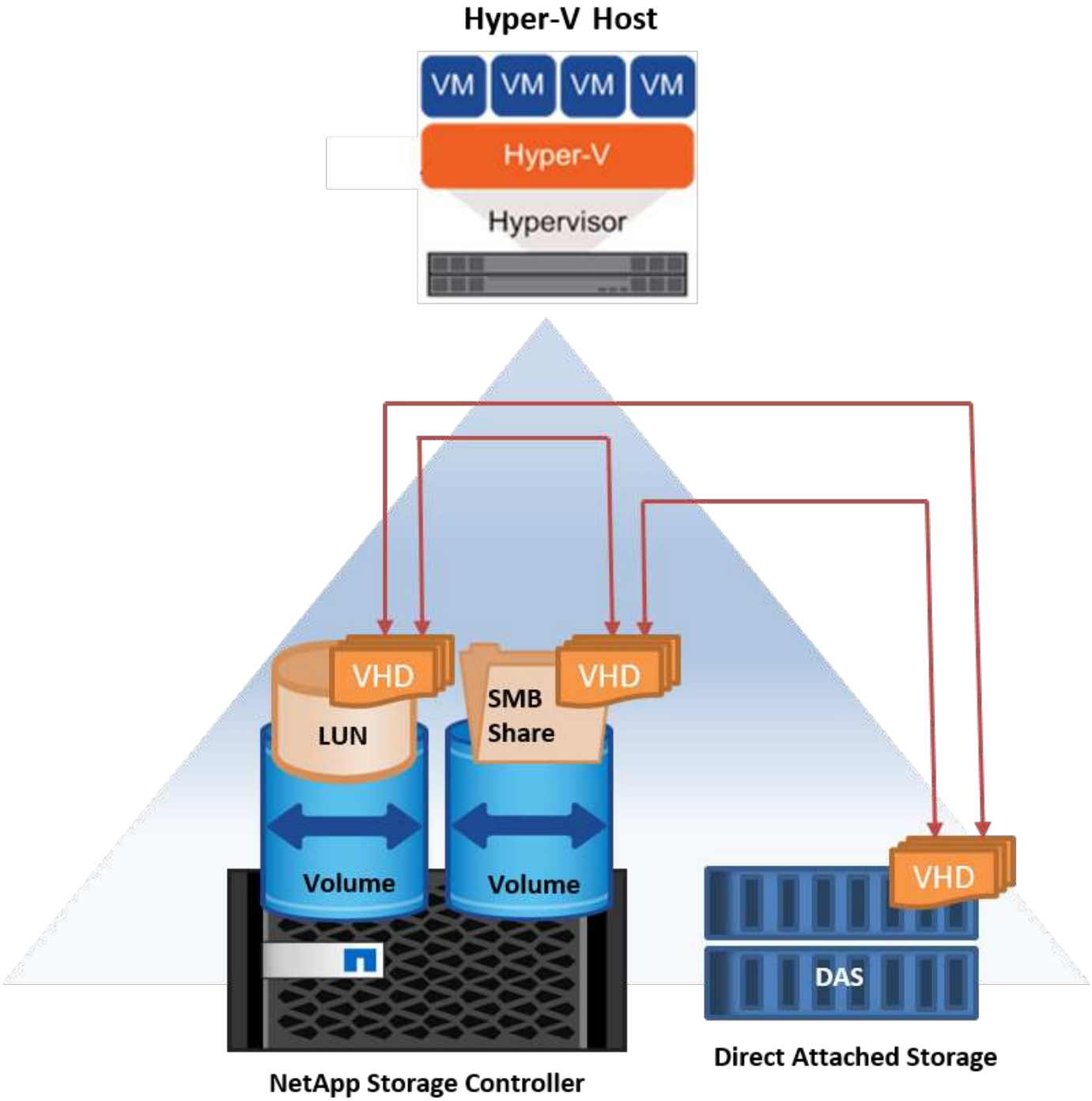
Las controladoras de almacenamiento de NetApp admiten los siguientes escenarios ODX diferentes:

- **IntraSVM.** Los datos son propiedad de la misma SVM:
- **Intravolume, intranode.** Los archivos de origen y destino o LUN residen dentro del mismo volumen. La copia se realiza con la tecnología de archivos FlexClone, lo que proporciona ventajas adicionales de rendimiento de la copia remota.
- **Intervolume, intranode.** Los archivos de origen y destino o LUN están en diferentes volúmenes que están en el mismo nodo.
- **Intervolumen, internodos.** Los archivos de origen y destino o LUN se encuentran en diferentes volúmenes ubicados en diferentes nodos.
- **InterSVM.** Los datos son propiedad de diferentes SVM.
- **Intervolume, intranode.** Los archivos de origen y destino o LUN están en diferentes volúmenes que están en el mismo nodo.
- **Intervolumen, internodos.** Los archivos de origen y destino o LUN están en diferentes volúmenes que están en diferentes nodos.
- **Intercluster.** A partir de ONTAP 9,0, ODX también es compatible con transferencias de LUN de interconexión de clústeres en entornos SAN. ODX entre clústeres solo se admite para protocolos SAN, no para SMB.

Una vez finalizada la migración, las políticas de backup y replicación se deben volver a configurar para reflejar el nuevo volumen que contiene las máquinas virtuales. No se puede utilizar ninguna copia de seguridad anterior realizada.

El almacenamiento VM (VHD/VHDX) se puede migrar entre los siguientes tipos de almacenamiento:

- Das y el recurso compartido de SMB
- Das y LUN
- Un recurso compartido de SMB y un LUN
- Entre las LUN
- Entre recursos compartidos de SMB

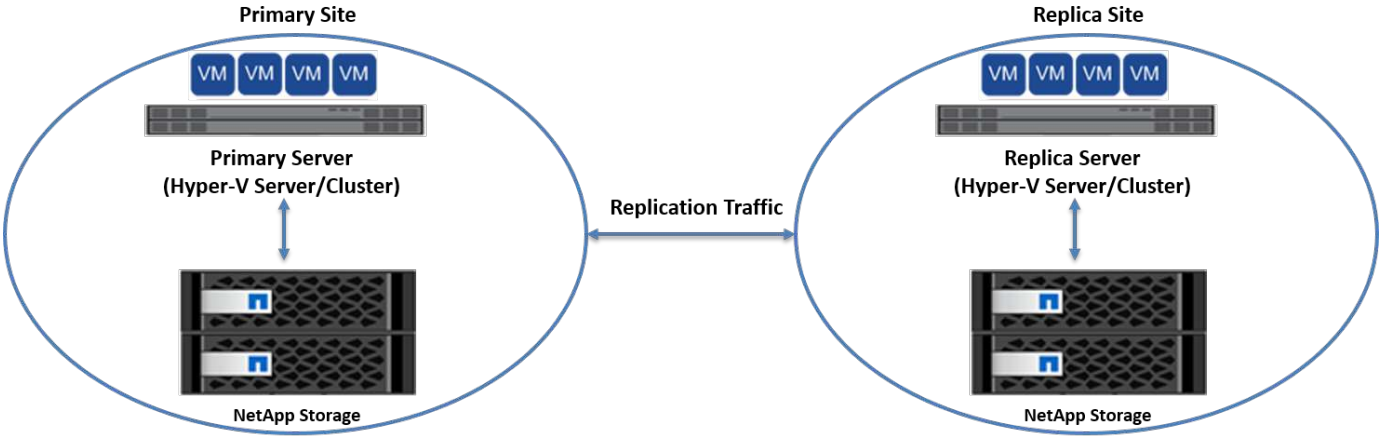


Más información

Para obtener más información sobre la implementación de una migración activa de almacenamiento, consulte "Apéndice E: Implemente Hyper-V Storage Live Migration".

Réplica Hyper-V: Recuperación ante desastres para máquinas virtuales

Hyper-V Replica replica las máquinas virtuales de Hyper-V desde un sitio primario para replicar las máquinas virtuales en un sitio secundario, lo que proporciona de forma asíncrona recuperación ante desastres para las máquinas virtuales. El servidor Hyper-V del centro principal que aloja los equipos virtuales se conoce como servidor primario; el servidor Hyper-V del centro secundario que recibe las máquinas virtuales replicadas se conoce como servidor de réplica. En la siguiente figura se muestra un ejemplo de ejemplo de réplica de Hyper-V. Puede utilizar la réplica de Hyper-V para equipos virtuales entre servidores de Hyper-V que forman parte de un cluster de conmutación por error o entre servidores de Hyper-V independientes que no forman parte de ningún cluster.



Replicación

Después de activar la réplica de Hyper-V para una máquina virtual en el servidor primario, la replicación inicial crea una máquina virtual idéntica en el servidor de réplica. Después de la replicación inicial, Hyper-V Replica mantiene un archivo de registro para los discos duros virtuales de la máquina virtual. El archivo de registro se reproduce en orden inverso al VHD de réplica de acuerdo con la frecuencia de replicación. Este registro y el uso de orden inverso garantizan que los cambios más recientes se almacenan y replican de forma asíncrona. Si la replicación no ocurre en línea con la frecuencia esperada, se emite una alerta.

Replicación ampliada

Hyper-V Replica admite replicación ampliada en la que se puede configurar un servidor de réplica secundario para la recuperación ante desastres. Se puede configurar un servidor de réplica secundario para que el servidor de réplica reciba los cambios en los equipos virtuales de réplica. En un escenario de replicación ampliada, los cambios en los equipos virtuales primarios en el servidor primario se replican en el servidor de réplica. A continuación, los cambios se replican en el servidor de réplicas ampliado. Los equipos virtuales se pueden conmutar por error al servidor de réplica ampliado solo cuando dejan de funcionar los servidores primario y de réplica.

Conmutación al respaldo

La conmutación por error no es automática, el proceso debe activarse manualmente. Existen tres tipos de conmutación al nodo de respaldo:

- **Test failover.** Este tipo se utiliza para verificar que una VM de réplica puede iniciarse correctamente en el

servidor de réplica y se inicia en la VM de réplica. Este proceso crea una VM de prueba duplicada durante la recuperación tras fallos y no afecta a la replicación regular de producción.

- **Failover planificado.** Este tipo se utiliza para conmutar las VM durante el tiempo de inactividad planificado o cortes esperados. Este proceso se inicia en la máquina virtual principal, la cual debe desactivarse en el servidor primario antes de ejecutar una conmutación al respaldo planificada. Después de que la máquina conmute por error, Hyper-V Replica inicia la VM de réplica en el servidor de réplica.
- **Failover no planificado.** Este tipo se utiliza cuando se producen cortes inesperados. Este proceso se inicia en el equipo virtual de réplica y solo se debe usar si falla el equipo primario.

Recuperación

Al configurar la replicación para una máquina virtual, puede especificar el número de puntos de recuperación. Los puntos de recuperación representan puntos temporales a partir del cual se pueden recuperar datos desde una máquina replicada.

Más información

- Para obtener información sobre la implementación de la réplica de Hyper-V fuera de un entorno en clúster, consulte la sección «"Implemente la réplica de Hyper-V fuera de un entorno en clúster"."
- Para obtener información sobre la implementación de la réplica de Hyper-V en un entorno en clúster, consulte la sección «"Implementar la réplica de Hyper-V en un entorno en clúster"."

Eficiencia del almacenamiento

ONTAP proporciona eficiencia de almacenamiento líder del sector para entornos virtualizados incluido Microsoft Hyper-V. NetApp también ofrece programas de garantía de eficiencia del almacenamiento.

Deduplicación NetApp

La deduplicación de NetApp funciona eliminando bloques duplicados en el volumen de almacenamiento, almacenando solo una copia física, independientemente del número de copias lógicas presentes. Por lo tanto, la deduplicación crea la ilusión de que existen numerosas copias de dicho bloque. La deduplicación elimina automáticamente bloques de datos duplicados en bloques de 4KB KB en todo el volumen. Este proceso recupera el almacenamiento para alcanzar ahorros de espacio y rendimiento potencial al reducir el número de escrituras físicas en el disco. La deduplicación puede proporcionar un ahorro de espacio superior al 70% en entornos Hyper-V.

Aprovisionamiento ligero

Thin provisioning es una manera eficiente de aprovisionar almacenamiento, ya que el almacenamiento no se asigna previamente. Es decir, cuando se crea un volumen o LUN mediante thin provisioning, el espacio del sistema de almacenamiento no se utiliza. El espacio sigue sin utilizar hasta que se escriben los datos en la LUN o el volumen y solo se utiliza el espacio necesario para almacenar dichos datos. NetApp recomienda habilitar thin provisioning en el volumen y deshabilitar la reserva de LUN.

Calidad de servicio

La calidad de servicio de almacenamiento en NetApp ONTAP permite agrupar objetos de almacenamiento y establecer límites de rendimiento en el grupo. La calidad de servicio de almacenamiento puede utilizarse para limitar el rendimiento a las cargas de trabajo y supervisar el rendimiento de las cargas de trabajo. Con esta capacidad, un administrador de almacenamiento puede separar las cargas de trabajo por organización,

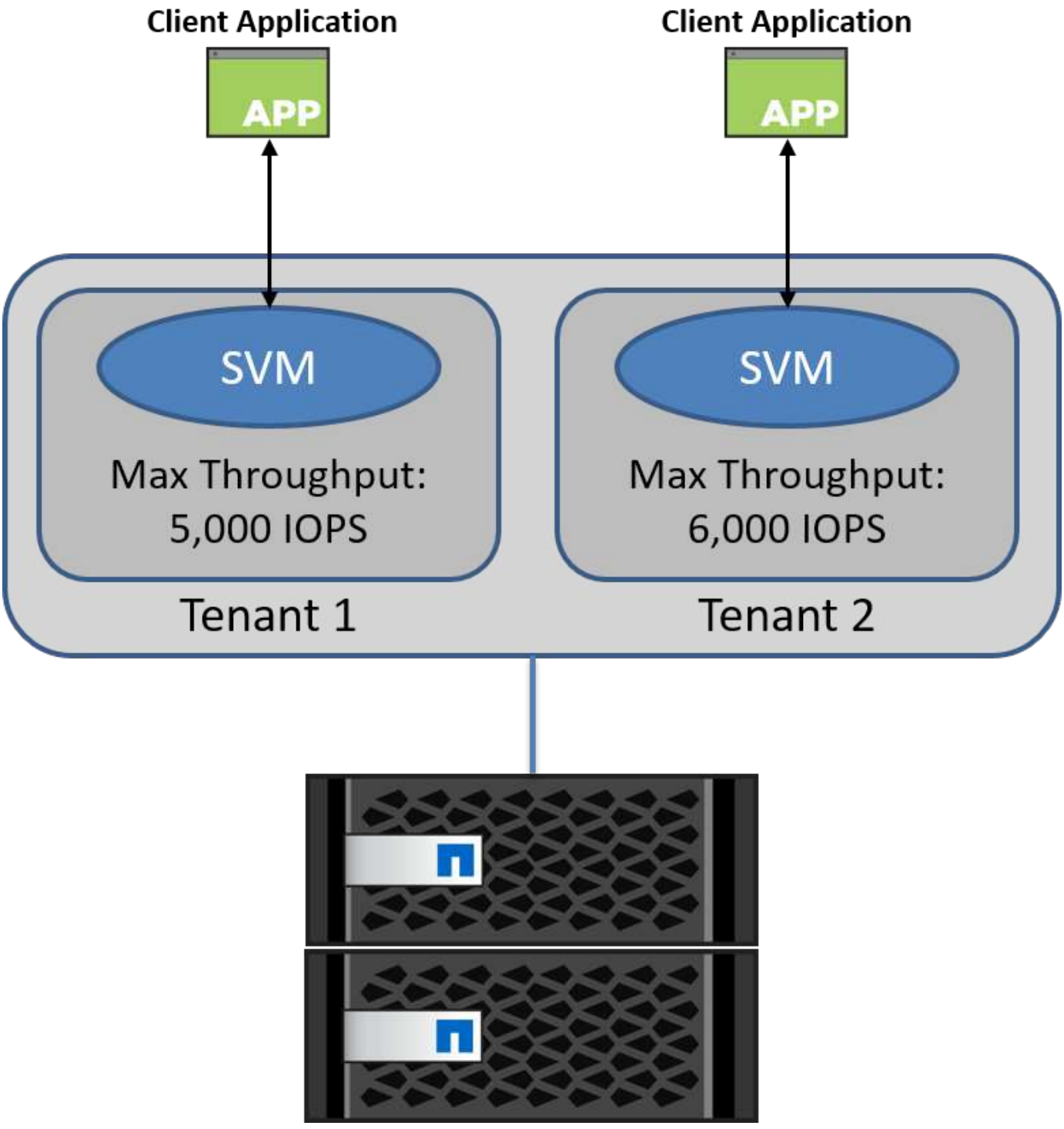
aplicación, unidad empresarial o entornos de producción o desarrollo.

En entornos empresariales, la calidad de servicio del almacenamiento ayuda a conseguir lo siguiente:

- Impide que las cargas de trabajo de los usuarios se afecten entre sí.
- Protege aplicaciones cruciales con tiempos de respuesta específicos que deben satisfacerse en entornos de TECNOLOGÍA como servicio (ITaaS).
- Evita que los clientes se afecten entre sí.
- Evita la degradación del rendimiento con la adición de cada nuevo inquilino.

La calidad de servicio le permite limitar la cantidad de I/O enviada a una SVM, un volumen flexible, una LUN o un archivo. El número de operaciones o el rendimiento bruto pueden limitar las I/O.

La siguiente figura ilustra la SVM con su propia política de calidad de servicio, que aplica un límite máximo de rendimiento.



Para configurar una SVM con su propia política de calidad de servicio y su grupo de políticas de supervisión, ejecute los siguientes comandos en el clúster de ONTAP:

```
# create a new policy group pg1 with a maximum throughput of 5,000 IOPS
cluster::> qos policy-group create pg1 -vserver vs1 -max-throughput
5000iops
```

```
# create a new policy group pg2 without a maximum throughput
cluster::> qos policy-group create pg2 -vserver vs2
```

```
# monitor policy group performance
cluster::> qos statistics performance show
```

```
# monitor workload performance
cluster::> qos statistics workload performance show
```

Seguridad

ONTAP ofrece un sistema de almacenamiento seguro para el sistema operativo Windows.

Antivirus de Windows Defender

Windows Defender es un software antimalware instalado y habilitado en Windows Server de forma predeterminada. Este software protege activamente Windows Server contra malware conocido y puede actualizar regularmente las definiciones antimalware a través de Windows Update. Los LUN de NetApp y los recursos compartidos de SMB se pueden analizar mediante Windows Defender.

Más información

Para obtener más información, consulte "Descripción general de Windows Defender".

BitLocker

El cifrado de la unidad BitLocker es una característica de protección de datos continuada desde Windows Server 2012. Este cifrado protege los discos físicos, las LUN y los volúmenes compartidos en cluster.

Mejor práctica

Antes de habilitar BitLocker, el CSV debe ponerse en modo de mantenimiento. Por lo tanto, NetApp recomienda que las decisiones relativas a la seguridad basada en BitLocker se tomen antes de crear VM en el CSV para evitar tiempos de inactividad.

Implemente Nano server

Obtenga información sobre la implementación de Microsoft Windows Nano Server.

Puesta en marcha

Para implementar un Nano Server como host de Hyper-V, realice los siguientes pasos:

1. Inicie sesión en Windows Server como miembro del grupo de administradores.
2. Copie la carpeta NanoServerImageGenerator de la carpeta \NanoServer de la ISO de Windows Server al disco duro local.

3. Para crear un servidor Nano VHD/VHDX, realice los siguientes pasos:
   a. Inicie Windows PowerShell como administrador, desplácese hasta la carpeta NanoServerImageGenerator copiada en el disco duro local y ejecute el siguiente cmdlet:

```
Set-ExecutionPolicy RemoteSigned
Import-Module .\NanoServerImageGenerator -Verbose
```

   b. Cree un VHD para Nano Server como host de Hyper-V ejecutando el siguiente cmdlet de PowerShell. Este comando solicita una contraseña de administrador para el nuevo disco duro virtual.

```
 New-NanoServerImage -Edition Standard -DeploymentType Guest
-MediaPath <"input the path to the root of the contents of Windows
Server 2016 ISO"> -TargetPath <"input the path, including the
filename and extension where the resulting VHD/VHDX will be created">
-ComputerName <"input the name of the nano server computer you are
about to create"> -Compute
.. En el siguiente ejemplo, creamos un VHD de Nano Server con la
función de host Hyper-V con clustering de conmutación por error
activado. Este ejemplo crea un VHD Nano Server a partir de una ISO
montada en f:\. El VHD recién creado se coloca en una carpeta llamada
NanoServer en la carpeta desde donde se ejecuta el cmdlet. El nombre
del equipo es NanoServer y el VHD resultante contiene la edición
estándar de Windows Server.
```

```
 New-NanoServerImage -Edition Standard -DeploymentType Guest
-MediaPath f:\ -TargetPath .\NanoServer.vhd -ComputerName NanoServer
-Compute -Clustering
.. Con el cmdlet New-NanoServerImage, configure los parámetros que
establecen la dirección IP, la máscara de subred, la puerta de enlace
predeterminada, el servidor DNS, el nombre de dominio, y así
sucesivamente.
```

4. Utilice el VHD en una máquina virtual o en un host físico para implementar Nano Server como host de Hyper-V:
   a. Para la implementación en un equipo virtual, cree un nuevo equipo virtual en Hyper-V Manager y utilice el disco duro virtual creado en el paso 3.
   b. Para la implementación en un host físico, copie el VHD en el equipo físico y configúrelo para arrancar desde este nuevo VHD. Primero, monte el VHD, ejecute bcdboot e:\windows (donde el VHD está montado en E:\), desmonte el VHD, reinicie el equipo físico y arranque en el Nano Server.
5. Unir el Nano Server a un dominio (opcional):
   a. Inicie sesión en cualquier equipo del dominio y cree un blob de datos ejecutando el siguiente cmdlet de PowerShell:

```
$domain = "<input the domain to which the Nano Server is to be
joined>"
$nanoserver = "<input name of the Nano Server>"
```

```
 djoin.exe /provision /domain $domain /machine $nanoserver /savefile
C:\temp\odjblob /reuse
.. Copie el archivo odjblob en Nano Server ejecutando los siguientes
cmdlets de PowerShell en una máquina remota:
```

```
$nanoserver = "<input name of the Nano Server>"
$nanouname = ""<input username of the Nano Server>"
$nanopwd = ""<input password of the Nano Server>"
```

```
$filePath = 'c:\temp\odjblob'
$fileContents = Get-Content -Path $filePath -Encoding Unicode
```

```
$securenanopwd = ConvertTo-SecureString -AsPlainText -Force $nanopwd
$nanosecurecred = new-object management.automation.pscredential
$nanouname, $securenanopwd
```

```
Invoke-Command -VMName $nanoserver -Credential $nanosecurecred
-ArgumentList @($filePath,$fileContents) -ScriptBlock \{
    param($filePath,$data)
    New-Item -ItemType directory -Path c:\temp
    Set-Content -Path $filePath -Value $data -Encoding Unicode
    cd C:\temp
    djoin /requestodj /loadfile c:\temp\odjblob /windowspath
c:\windows /localos
}
```

b. Reinicie Nano Server.

Conéctese a Nano Server

Para conectarse al Nano Server de forma remota mediante PowerShell, realice los siguientes pasos:

1. Agregue Nano Server como un host de confianza en el equipo remoto ejecutando el siguiente cmdlet en el servidor remoto:

```
 Set-Item WSMan:\LocalHost\Client\TrustedHosts "<input IP Address of the
Nano Server>"
. Si el entorno es seguro y desea configurar todos los hosts que se van
a agregar como hosts de confianza en un servidor, ejecute el siguiente
comando:
```

```
 Set-Item WSMan:\LocalHost\Client\TrustedHosts *
. Inicie la sesión remota ejecutando el siguiente cmdlet en el servidor
remoto. Proporcione la contraseña para el servidor Nano cuando se le
solicite.
```

```
Enter-PSSession -ComputerName "<input IP Address of the Nano Server>"
-Credential ~\Administrator
```

Para conectarse al Nano Server de forma remota utilizando las herramientas de administración de GUI desde un Windows Server remoto, complete los siguientes comandos:

1. Inicie sesión en Windows Server como miembro del grupo de administradores.
2. Inicie Server Manager**.**
3. Para administrar un servidor Nano de forma remota desde el Administrador del servidor, haga clic con el botón derecho en Todos los servidores, haga clic en Agregar servidores, proporcione la información del servidor Nano y agréguela. Ahora puede ver el Nano Server en la lista de servidores. Seleccione el Nano Server, haga clic con el botón derecho del ratón y comience a administrarlo con las diversas opciones proporcionadas.
4. Para administrar servicios en un Nano Server de forma remota, complete los siguientes pasos:
   a. Abra Servicios en la sección Herramientas del Administrador del servidor.
   b. Haga clic con el botón derecho del ratón en Servicios (Local).
   c. Haga clic en Conectar al servidor.
   d. Proporcione los detalles de Nano Server para ver y administrar los servicios en Nano Server.
5. Si el rol Hyper-V está habilitado en Nano Server, complete los siguientes pasos para administrarlo de forma remota desde Hyper-V Manager:
   a. Abra Hyper-V Manager en la sección Herramientas del Administrador de servidores.
   b. Haga clic con el botón derecho en Hyper-V Manager.
   c. Haga clic en Conectar al servidor y proporcione los detalles de Nano Server. Ahora el Nano Server se puede administrar como un servidor Hyper-V para crear y administrar VM sobre él.
6. Si el rol de agrupación en clúster de conmutación por error está activado en Nano Server, realice los siguientes pasos para gestionarlo de forma remota desde el administrador de clústeres de conmutación por error:
   a. Abra el Administrador de clústeres de conmutación por error en la sección Herramientas del Administrador del servidor.

b. Realice operaciones relacionadas con la agrupación en clústeres con Nano Server.

Implemente el cluster de Hyper-V.

En este apéndice se describe la puesta en marcha de un clúster Hyper-V.

Requisitos previos

- Existen al menos dos servidores de Hyper-V conectados entre sí.
- Hay al menos un switch virtual configurado en cada servidor de Hyper-V.
- La función de cluster de conmutación por error está activada en cada servidor de Hyper-V.
- Los recursos compartidos de SMB o volúmenes compartidos en cluster se utilizan como almacenamiento compartido para almacenar equipos virtuales y sus discos para la agrupación en cluster de Hyper-V.
- El almacenamiento no se debe compartir entre clústeres diferentes. Solo debe tener un recurso compartido CSV/CIFS por clúster.
- Si el recurso compartido de SMB se utiliza como almacenamiento compartido, se deben configurar los permisos en el recurso compartido de SMB para otorgar acceso a las cuentas de equipo de todos los servidores de Hyper-V del clúster.

Puesta en marcha

1. Inicie sesión en uno de los servidores de Windows Hyper-V como miembro del grupo de administradores.
2. Inicie Server Manager**.**
3. En la sección Herramientas, haga clic en Administrador de clústeres de conmutación por error.
4. Haga clic en el menú Create Cluster from Actions.
5. Proporcione los detalles del servidor Hyper-V que forma parte de este cluster.
6. Valide la configuración del clúster. Seleccione Yes when prompted for cluster configuration validation y seleccione las pruebas necesarias para validar si los servidores de Hyper-V cumplen los requisitos previos para formar parte del cluster.
7. Una vez que la validación se realiza correctamente, se inicia el asistente Create Cluster. En el asistente, proporcione el nombre del clúster y la dirección IP del clúster para el nuevo clúster. A continuación, se crea un nuevo cluster de recuperación tras fallos para el servidor de Hyper-V.
8. Haga clic en el clúster recién creado en el Administrador de clústeres de conmutación al nodo de respaldo y gestiónelo.
9. Defina almacenamiento compartido para que utilice el clúster. Puede ser un recurso compartido de SMB o un volumen compartido en clúster.
10. Si se utiliza un recurso compartido de SMB como almacenamiento compartido, no es necesario realizar pasos especiales.
    - Configurar un recurso compartido de CIFS en una controladora de almacenamiento de NetApp. Para ello, consulte la sección «"Aprovisionamiento en entornos SMB""**"**.
11. Para usar un CSV como almacenamiento compartido, complete los siguientes pasos:
    a. Configure LUN en una controladora de almacenamiento de NetApp. Para ello, consulte la sección «Provisionamiento en entornos SAN».
    b. Asegúrese de que todos los servidores Hyper-V del cluster de recuperación tras fallos pueden ver las LUN de NetApp. Para hacerlo con todos los servidores de Hyper-V que forman parte del cluster de

recuperación tras fallos, asegúrese de que sus iniciadores se hayan añadido al iGroup en el almacenamiento de NetApp. También asegúrese de que se detectan sus LUN y asegúrese de que MPIO está habilitado.

c. En cualquiera de los servidores de Hyper-V del cluster, realice los siguientes pasos:

   i. Ponga el LUN en línea, inicialice el disco, cree un nuevo volumen sencillo y formatee con NTFS o ReFS.

   ii. En el Administrador de clústeres de conmutación por error, expanda el clúster, expanda Almacenamiento, haga clic con el botón derecho en Discos y, a continuación, haga clic en Agregar discos. Al hacerlo, se abre el asistente para agregar discos a un clúster mostrando la LUN como un disco. Haga clic en OK para añadir la LUN como disco.

   iii. Ahora la LUN se denomina 'Disco en cluster' y se muestra como Almacenamiento disponible en Discos.

d. Haga clic con el botón derecho en LUN ('Clustered Disk') y haga clic en Add to Cluster Shared Volumes. Ahora la LUN se muestra como un volumen compartido en clúster.

e. El CSV es visible y accesible simultáneamente desde todos los servidores Hyper-V del cluster de conmutación por error en su ubicación local C:\ClusterStorage\.

12. Crear un equipo virtual de alta disponibilidad:

    a. En el Administrador de clústeres de conmutación por error, seleccione y expanda el clúster que creó anteriormente.

    b. Haga clic en Roles y, a continuación, en Máquinas virtuales en Acciones. Haga clic en New Virtual Machine.

    c. Seleccione el nodo del clúster donde debe residir la máquina virtual.

    d. En el asistente Virtual Machine Creation, proporcione el almacenamiento compartido (recurso compartido de SMB o CSV) como la ruta para almacenar la máquina virtual y sus discos.

    e. Utilice Hyper-V Manager para establecer el almacenamiento compartido (recurso compartido de SMB o CSV) como ruta predeterminada para almacenar el equipo virtual y sus discos para un servidor de Hyper-V.

13. Probar la conmutación al respaldo planificada. Mueva máquinas virtuales a otro nodo mediante una migración dinámica, una migración rápida o una migración de almacenamiento (movimiento). Revisar "Migración activa en un entorno en cluster" para obtener más detalles.

14. Probar la recuperación tras fallos no planificada. Detenga el servicio de clúster en el servidor propietario de la máquina virtual.

Implemente Hyper-V Live Migration en un entorno en clúster

Este apéndice describe la puesta en marcha de la migración en vivo en un entorno en clúster.

Requisitos previos

Para implementar la migración dinámica, es necesario tener los servidores de Hyper-V configurados en un cluster de conmutación por error con almacenamiento compartido. Revisar "Implemente el cluster Hyper-V" para obtener más detalles.

Puesta en marcha

Para utilizar la migración dinámica en un entorno en clúster, complete los siguientes pasos:

1. En el Administrador de clústeres de conmutación por error, seleccione y expanda el clúster. Si el clúster no está visible, haga clic en Administrador de clústeres de conmutación por error, haga clic en Connect to Cluster y proporcione el nombre del clúster.
2. Haga clic en Roles, donde se enumeran todas las máquinas virtuales disponibles en un clúster.
3. Haga clic con el botón derecho en la máquina virtual y haga clic en Move. Esto le proporciona tres opciones:
   - **Migración en vivo.** Puede seleccionar un nodo manualmente o permitir que el clúster seleccione el mejor nodo. En la migración dinámica, el cluster copia la memoria utilizada por la máquina virtual del nodo actual a otro nodo. Por lo tanto, cuando la máquina virtual se migra a otro nodo, la información de memoria y estado que necesita la máquina virtual ya está puesta para la máquina virtual. Este método de migración es casi instantáneo, pero solo se puede migrar en vivo un equipo virtual cada vez.
   - **Migración rápida.** Puede seleccionar un nodo manualmente o permitir que el clúster seleccione el mejor nodo. En una rápida migración, el clúster copia la memoria utilizada por un equipo virtual a un disco del almacenamiento. Por lo tanto, cuando la máquina virtual se migra a otro nodo, la información de memoria y estado que necesita el equipo virtual se puede leer rápidamente desde el disco en el otro nodo. Con una migración rápida, se pueden migrar varios equipos virtuales de forma simultánea.
   - **Migración de almacenamiento de máquinas virtuales.** Este método utiliza el asistente Mover almacenamiento de máquinas virtuales. Con este asistente, puede seleccionar el disco del equipo virtual junto con otros archivos que se moverán a otra ubicación, que puede ser un recurso compartido CSV o de SMB.

Implemente Hyper-V Live Migration fuera de un entorno en clúster

Esta sección describe la puesta en marcha de la migración activa de Hyper-V fuera de un entorno en clúster.

Requisitos previos

- Servidores de Hyper-V independientes con almacenamiento independiente o almacenamiento SMB compartido.
- La función Hyper-V instalada en los servidores de origen y destino.
- Ambos servidores Hyper-V pertenecen al mismo dominio o a dominios que confían entre sí.

Puesta en marcha

Para realizar la migración activa en un entorno no agrupado, configure los servidores Hyper-V de origen y destino para que puedan enviar y recibir operaciones de migración en directo. En ambos servidores de Hyper-V, complete los siguientes pasos:

1. Abra Hyper-V Manager en la sección Herramientas del Administrador de servidores.
2. En Acciones, haga clic en Configuración de Hyper-V.
3. Haga clic en Live Migrations y seleccione Enable Live Migrations entrantes y salientes.
4. Elija si desea permitir el tráfico de migración en vivo en cualquier red disponible o solo en redes específicas.
5. Opcionalmente, puede configurar el protocolo de autenticación y las opciones de rendimiento en la sección Avanzadas de Migración en Directo.
6. Si se utiliza CredSSP como protocolo de autenticación, asegúrese de iniciar sesión en el servidor Hyper-V

de origen desde el servidor Hyper-V de destino antes de mover el equipo virtual.

7. Si Kerberos se utiliza como protocolo de autenticación, configure la delegación restringida. Para hacerlo, es necesario tener acceso al controlador de dominio de Active Directory. Para configurar la delegación, realice los siguientes pasos:
   a. Inicie sesión en el controlador de dominio de Active Directory como administrador.
   b. Inicie Server Manager.
   c. En la sección Herramientas, haga clic en Usuarios y equipos de Active Directory.
   d. Expanda el dominio y haga clic en Equipos.
   e. Seleccione el servidor Hyper-V de origen de la lista, haga clic con el botón derecho en él y haga clic en Propiedades.
   f. En la pestaña Delegación, seleccione Confiar en esta computadora sólo para la delegación a los servicios especificados.
   g. Seleccione Utilizar solo Kerberos.
   h. Haga clic en Agregar, que abre el asistente Agregar servicios.
   i. En Agregar servicios, haga clic en Usuarios y equipos, que abre Seleccionar usuarios o equipos**.**
   j. Proporcione el nombre del servidor Hyper-V de destino y haga clic en Aceptar.
      - Para mover el almacenamiento de equipos virtuales, seleccione CIFS.
      - Para mover máquinas virtuales, seleccione el servicio Microsoft Virtual System Migration.
   k. En la ficha Delegación, haga clic en Aceptar.
   l. En la carpeta Equipos, seleccione el servidor Hyper-V de destino de la lista y repita el proceso. En Seleccionar usuarios o equipos, proporcione el nombre del servidor Hyper-V de origen.
8. Mover la máquina virtual.
   a. Abra Hyper-V Manager.
   b. Haga clic con el botón derecho en una máquina virtual y haga clic en Mover.
   c. Seleccione Move the Virtual Machine.
   d. Especifique el servidor Hyper-V de destino para la máquina virtual.
   e. Seleccione las opciones de movimiento. Para Migración en vivo compartida, seleccione Mover únicamente la máquina virtual. Para Shared Nothing Live Migration, elija cualquiera de las otras dos opciones en función de sus preferencias.
   f. Proporcione la ubicación de la máquina virtual en el servidor Hyper-V de destino en función de sus preferencias.
   g. Revise el resumen y haga clic en OK para mover la máquina virtual.

Implemente Hyper-V Storage Live Migration

Descubre cómo configurar la migración dinámica del almacenamiento de Hyper-V.

Requisitos previos

- Debe tener un servidor de Hyper-V independiente con almacenamiento independiente (DAS o LUN) o almacenamiento SMB (local o compartido entre otros servidores de Hyper-V.
- El servidor de Hyper-V debe configurarse para la migración dinámica. Revise la sección sobre la implementación en "Migración en vivo fuera de un entorno en cluster".

Puesta en marcha

1. Abra Hyper-V Manager.
2. Haga clic con el botón derecho en una máquina virtual y haga clic en Mover.
3. Seleccione Mover el almacenamiento de la máquina virtual.
4. Seleccione opciones para mover el almacenamiento en función de sus preferencias.
5. Proporcione la nueva ubicación para los elementos de la VM.
6. Revise el resumen y haga clic en OK para mover el almacenamiento de la máquina virtual.

Implemente la réplica de Hyper-V fuera de un entorno en clúster

Este apéndice describe la implementación de la réplica de Hyper-V fuera de un entorno en clúster.

Requisitos previos

- Necesita servidores Hyper-V independientes ubicados en las mismas ubicaciones geográficas o independientes que sirvan de servidores primarios y de réplica.
- Si se utilizan sitios separados, el firewall de cada sitio debe configurarse para permitir la comunicación entre los servidores primario y de réplica.
- El servidor de réplica debe tener espacio suficiente para almacenar las cargas de trabajo replicadas.

Puesta en marcha

1. Configure el servidor de réplicas.
   a. Para que las reglas del firewall entrante permitan el tráfico de replicación entrante, ejecute el siguiente cmdlet de PowerShell:

```
 Enable-Netfirewallrule -displayname "Hyper-V Replica HTTP Listener
(TCP-In)"
.. Abra Hyper-V Manager en la sección Herramientas del Administrador
de servidores.
.. Haga clic en Configuración de Hyper-V en Acciones.
.. Haga clic en Configuración de Replicación y seleccione Habilitar
este equipo como servidor de réplica.
.. En la sección Autenticación y puertos, seleccione el método de
autenticación y el puerto.
.. En la sección Autorización y almacenamiento, especifique la
ubicación en la que se almacenarán los equipos virtuales y los
archivos replicados.
```

2. Activar la replicación de equipos virtuales para equipos virtuales en el servidor primario. La replicación de VM se habilita por VM y no para todo el servidor de Hyper-V.
   a. En Hyper-V Manager, haga clic con el botón derecho en una máquina virtual y haga clic en Enable Replication para abrir el asistente Enable Replication.

b. Proporcione el nombre del servidor de réplica en el que se debe replicar la máquina virtual.
c. Proporcione el tipo de autenticación y el puerto del servidor de réplica que se configuró para recibir tráfico de replicación en el servidor de réplica.
d. Seleccione los discos duros virtuales que desea replicar.
e. Seleccione la frecuencia (duración) a la que se envían los cambios al servidor de réplica.
f. Configure los puntos de recuperación para especificar el número de puntos de recuperación que se deben mantener en el servidor de réplica.
g. Seleccione Initial Replication Method para especificar el método para transferir la copia inicial de los datos del equipo virtual al servidor de réplica.
h. Revise el resumen y haga clic en Finish.
i. Este proceso crea una réplica de VM en el servidor de réplica.

Replicación

1. Ejecute una conmutación por error de prueba para asegurarse de que la VM de réplica funciona correctamente en el servidor de réplica. La prueba crea una VM temporal en el servidor de réplica.
   a. Inicie sesión en el servidor de réplicas.
   b. En Hyper-V Manager, haga clic con el botón derecho en una VM de réplica, haga clic en Replicación y, a continuación, en Probar conmutación por error.
   c. Elija el punto de recuperación que desea utilizar.
   d. Este proceso crea una VM con el mismo nombre que se agrega con -Test.
   e. Verificar la máquina virtual para asegurarse de que todo funciona bien.
   f. Después de la conmutación por error, la VM de prueba de réplica se elimina si selecciona Detener failover de prueba para ella.
2. Ejecute una conmutación al respaldo planificada para replicar los cambios más recientes del equipo virtual principal al equipo virtual de réplica.
   a. Inicie sesión en el servidor primario.
   b. Apague el equipo virtual para que se conmute al nodo de respaldo.
   c. En Hyper-V Manager, haga clic con el botón derecho en la máquina virtual desactivada, haga clic en Replication y, a continuación, en Planned Failover.
   d. Haga clic en Failover para transferir los últimos cambios de VM al servidor de réplica.
3. Ejecute una conmutación al respaldo no planificada en caso de un fallo del equipo virtual principal.
   a. Inicie sesión en el servidor de réplicas.
   b. En Hyper-V Manager, haga clic con el botón derecho en una réplica de VM, haga clic en Replication y, a continuación, haga clic en Failover.
   c. Elija el punto de recuperación que desea utilizar.
   d. Haga clic en Failover para conmutar la máquina virtual al nodo de respaldo.

Implementar la réplica de Hyper-V en un entorno en clúster

Aprenda a implementar y configurar la réplica de Hyper-V con el clúster de conmutación por error de Windows Server.

Requisitos previos

- Necesita que haya clústeres de Hyper-V ubicados en la misma ubicación geográfica o en diferentes ubicaciones geográficas que funcionen como clústeres primarios y de réplica. Revisar "Implemente el cluster Hyper-V" para obtener más detalles.
- Si se utilizan sitios separados, se debe configurar el firewall de cada sitio para permitir la comunicación entre los clústeres primario y de réplica.
- El clúster de réplica debe tener suficiente espacio para almacenar las cargas de trabajo replicadas.

Puesta en marcha

1. Active las reglas de firewall en todos los nodos de un clúster. Ejecute el siguiente cmdlet de PowerShell con privilegios de administrador en todos los nodos en los clústeres primario y de réplica.

```
# For Kerberos authentication
get-clusternode | ForEach-Object \{Invoke-command -computername $_.name
-scriptblock \{Enable-Netfirewallrule -displayname "Hyper-V Replica HTTP
Listener (TCP-In)"}}
```

```
# For Certificate authentication
get-clusternode | ForEach-Object \{Invoke-command -computername $_.name
-scriptblock \{Enable-Netfirewallrule -displayname "Hyper-V Replica
HTTPS Listener (TCP-In)"}}
```

2. Configure el cluster de réplicas.
   a. Configure el broker de réplica Hyper-V con un nombre NetBIOS y una dirección IP para utilizarlo como punto de conexión al cluster que se utiliza como cluster de réplica.
      i. Abra el Administrador de clústeres de conmutación por error.
      ii. Expanda el clúster, haga clic en Roles y haga clic en el panel Configurar rol desde Acciones.
      iii. Seleccione Broker de Réplica Hyper-V en la página Seleccionar Rol.
      iv. Proporcione el nombre de NetBIOS y la dirección IP que se utilizarán como punto de conexión al clúster (punto de acceso del cliente).
      v. Este proceso crea un rol de intermediario de réplica Hyper-V. Compruebe que se ha conectado correctamente.
   b. Configurar los ajustes de replicación.
      i. Haga clic con el botón derecho en el broker de réplicas creado en los pasos anteriores y haga clic en Configuración de Replicación.
      ii. Seleccione Activar este cluster como servidor de réplica.
      iii. En la sección Autenticación y puertos, seleccione el método de autenticación y el puerto.
      iv. En la sección Autorización y almacenamiento, seleccione los servidores permitidos para replicar los equipos virtuales en este clúster. Además, especifique la ubicación predeterminada donde se almacenan las máquinas virtuales replicadas.

Replicación

La replicación es similar al proceso descrito en la sección "Réplica fuera de un entorno en clúster".

Dónde encontrar información adicional

Recursos adicionales para Microsoft Windows y Hyper-V.

- Conceptos de ONTAP
  https://docs.netapp.com/us-en/ontap/concepts/introducing-data-management-software-concept.html
- Prácticas recomendadas para SAN modernas
  https://www.netapp.com/media/10680-tr4080.pdf
- Disponibilidad e integridad de datos en la cabina All-SAN de NetApp con NetApp ASA
  https://www.netapp.com/pdf.html?item=/media/85671-tr-4968.pdf
- Documentación de SMB
  https://docs.netapp.com/us-en/ontap/smb-admin/index.html
- Empezando con Nano Server
  https://technet.microsoft.com/library/mt126167.aspx
- Novedades de Hyper-V en Windows Server
  https://technet.microsoft.com/windows-server-docs/compute/hyper-v/what-s-new-in-hyper-v-on-windows

Microsoft SQL Server

Descripción general

ONTAP ofrece una solución de rendimiento y seguridad empresarial para sus bases de datos de Microsoft SQL Server y proporciona herramientas de primera calidad para gestionar su entorno.

Esta documentación sustituye al informe técnico publicado previamente *TR-4590: Guía de mejores prácticas para Microsoft SQL Server con ONTAP*

NetApp asume que el lector tiene conocimiento práctico de lo siguiente:

- ONTAP
- Arquitectura y administración de Microsoft SQL Server
- NetApp SnapCenter como software de backup, que incluye:
  - Plugin de SnapCenter para Microsoft Windows
  - Plugin de SnapCenter para SQL Server

El alcance de esta sección de mejores prácticas se limita al diseño técnico basado en los principios y estándares preferidos que NetApp recomienda para la infraestructura de almacenamiento. La implementación integral está fuera del alcance.

Para obtener información sobre compatibilidad de los productos de NetApp, consulte la "Herramienta de matriz de interoperabilidad de NetApp (IMT)".

Cargas de trabajo de Microsoft SQL Server

Antes de implementar SQL Server, debe entender los requisitos de la carga de trabajo de las aplicaciones que admiten las instancias de bases de datos de SQL Server. Cada aplicación tiene requisitos distintos en cuanto a capacidad, rendimiento y disponibilidad, por lo que cada base de datos debería estar diseñada para satisfacer de forma óptima dichos requisitos. Muchas organizaciones clasifican las bases de datos en varios niveles de gestión utilizando los requisitos de las aplicaciones para definir acuerdos de nivel de servicios. Las cargas de trabajo de SQL Server a menudo se clasifican como se describen a continuación:

- OLTP, que suelen ser las bases de datos más cruciales de una organización. Estas bases de datos, por lo general, generan aplicaciones orientadas al cliente y se consideran esenciales para las operaciones principales de la compañía. Las bases de datos OLTP críticas para la misión y las aplicaciones a las que dan soporte suelen tener SLA que requieren un alto rendimiento, son sensibles a la degradación del rendimiento y requieren una disponibilidad máxima. También pueden ser candidatos para Always On Failover Clusters o Always On Availability Groups. La combinación de I/O en estos tipos de bases de datos suele caracterizarse por un 75 % a un 90 % de las lecturas aleatorias y entre un 25 % y un 10 % de las escrituras.
- Bases de datos del sistema de soporte para la toma de decisiones (DSS), a veces denominadas almacenes de datos. Estas bases de datos son cruciales para el negocio de muchas organizaciones que dependen de los análisis de sus empresas. Estas bases de datos son sensibles al uso de la CPU y a las operaciones de lectura del disco cuando se ejecutan consultas. En muchas organizaciones, las bases de datos de DSS son las más críticas durante el mes, el trimestre y el final del año Esta carga de trabajo suele tener una combinación de I/O de lectura de casi el 100 % y el rendimiento de I/O suele ser más

importante que IOPS.

Configuración de la base de datos

Configuración de CPU

El rendimiento de SQL Server tiene varias dependencias en la configuración de CPU y núcleo.

Hyper-threading

Hyper-threading se refiere a la implementación simultánea de multithreading (SMT), lo que mejora la paralelización de los cálculos realizados en procesadores x86. SMT está disponible en procesadores Intel y AMD.

Hyper-threading genera CPU lógicas que aparecen como CPU físicas en el sistema operativo. SQL Server ve a continuación esas CPU adicionales y las utiliza como si hubiera más núcleos que los presentes físicamente. Esto puede mejorar sustancialmente el rendimiento al aumentar la paralelización.

La advertencia aquí es que cada versión de SQL Server tiene sus propias limitaciones en cuanto a la potencia informática que puede utilizar. Para obtener más información, consulte "Límites de capacidad de cálculo por edición de SQL Server".

Núcleos y licencias

Hay dos opciones para la licencia de SQL Server. El primero se conoce como modelo de licencia de acceso de servidor + cliente (CAL); el segundo es el modelo de núcleo por procesador. Aunque puede acceder a todas las características del producto disponibles en SQL Server con la estrategia server + CAL, hay un límite de hardware de 20 núcleos de CPU por socket. Incluso si tiene SQL Server Enterprise Edition + CAL para un servidor con más de 20 núcleos de CPU por socket, la aplicación no puede utilizar todos esos núcleos a la vez en esa instancia.

La imagen siguiente muestra el mensaje de registro de SQL Server después del inicio que indica la aplicación del límite principal.

```
2017-01-11 07:16:30.71 Server      Microsoft SQL Server 2016
(RTM) - 13.0.1601.5 (X64)
     Apr 29 2016 23:23:58
     Copyright (c) Microsoft Corporation
     Enterprise Edition (64-bit) on Windows Server 2016
Datacenter 6.3 <X64> (Build 14393: )

2017-01-11 07:16:30.71 Server      UTC adjustment: -8:00
2017-01-11 07:16:30.71 Server      (c) Microsoft Corporation.
2017-01-11 07:16:30.71 Server      All rights reserved.
2017-01-11 07:16:30.71 Server      Server process ID is 10176.
2017-01-11 07:16:30.71 Server      System Manufacturer:
'FUJITSU', System Model: 'PRIMERGY RX2540 M1'.
2017-01-11 07:16:30.71 Server      Authentication mode is MIXED.
2017-01-11 07:16:30.71 Server      Logging SQL Server messages
in file 'C:\Program Files\Microsoft SQL Server
\MSSQL13.MSSQLSERVER\MSSQL\Log\ERRORLOG'.
2017-01-11 07:16:30.71 Server      The service account is 'SEA-
TM\FUJIA2R30$'. This is an informational message; no user action
is required.
2017-01-11 07:16:30.71 Server      Registry startup parameters:
     -d C:\Program Files\Microsoft SQL Server
\MSSQL13.MSSQLSERVER\MSSQL\DATA\master.mdf
     -e C:\Program Files\Microsoft SQL Server
\MSSQL13.MSSQLSERVER\MSSQL\Log\ERRORLOG
     -l C:\Program Files\Microsoft SQL Server
\MSSQL13.MSSQLSERVER\MSSQL\DATA\mastlog.ldf
     -T 3502
     -T 834
2017-01-11 07:16:30.71 Server      Command Line Startup
Parameters:
     -s "MSSQLSERVER"
2017-01-11 07:16:30.72 Server      SQL Server detected 2 sockets
with 18 cores per socket and 36 logical processors per socket,
72 total logical processors; using 40 logical processors based
on SQL Server licensing. This is an informational message; no
user action is required.
2017-01-11 07:16:30.72 Server      SQL Server is starting at
```

Por lo tanto, para utilizar todas las CPU, debe utilizar la licencia de núcleo por procesador. Para obtener información detallada sobre las licencias de SQL Server, consulte "SQL Server 2022: Su plataforma de datos moderna".

Afinidad de CPU

Es poco probable que necesite alterar los valores predeterminados de afinidad del procesador a menos que encuentre problemas de rendimiento, pero aún vale la pena entender qué son y cómo funcionan.

SQL Server admite la afinidad del procesador mediante dos opciones:

- Máscara de afinidad de CPU
- Máscara de I/O de afinidad

SQL Server utiliza todas las CPU disponibles en el sistema operativo (si se selecciona la licencia de núcleo por procesador). También crea programadores f0r cada CPU para hacer el mejor uso de los recursos para cualquier carga de trabajo dada. Al realizar varias tareas, el sistema operativo u otras aplicaciones del servidor pueden cambiar los subprocesos de un procesador a otro. SQL Server es una aplicación que consume muchos recursos y el rendimiento puede verse afectado cuando esto ocurre. Para minimizar el impacto, puede configurar los procesadores de modo que toda la carga de SQL Server se dirija a un grupo preseleccionado de procesadores. Esto se logra mediante el uso de la máscara de afinidad de CPU.

La opción de máscara de E/S de afinidad enlaza E/S de disco de SQL Server a un subconjunto de CPU. En

entornos OLTP de SQL Server, esta extensión puede mejorar significativamente el rendimiento de los subprocesos de SQL Server que emiten operaciones de E/S.

Grado máximo de paralelismo (MAXDOP)

De forma predeterminada, SQL Server utiliza todas las CPU disponibles durante la ejecución de la consulta si se elige la licencia central por procesador.

Aunque esto es útil para consultas grandes, puede causar problemas de rendimiento y limitar la simultaneidad. Un mejor enfoque es limitar el paralelismo al número de núcleos físicos en un único socket de CPU. Por ejemplo, en un servidor con dos sockets CPU físicos con 12 núcleos por socket, independientemente de hyper-threading, `MAXDOP` se debe establecer en 12. `MAXDOP` No se puede restringir ni dictar qué CPU se va a utilizar. En su lugar, restringe el número de CPU que puede utilizar una única consulta por lotes.

NetApp recomienda para DSS, como almacenes de datos, comience con `MAXDOP` 50 y explore el ajuste hacia arriba o hacia abajo si es necesario. Asegúrese de medir las consultas críticas de la aplicación al realizar cambios.

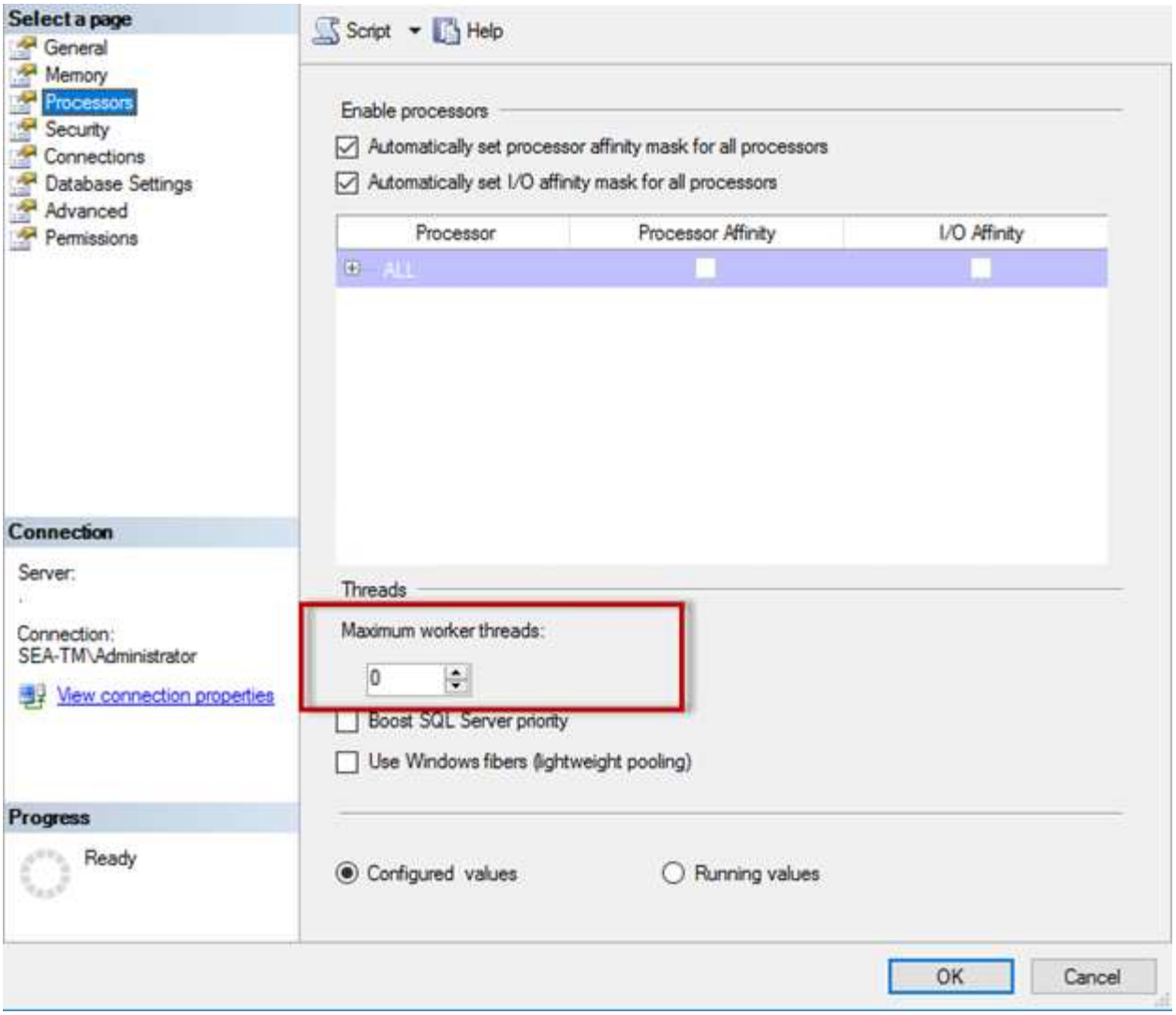
Máximo de Threads de Trabajador

La opción Máximo de Threads de Trabajador ayuda a optimizar el rendimiento cuando un gran número de clientes están conectados a SQL Server.

Normalmente, se crea un thread de sistema operativo independiente para cada consulta. Si se realizan cientos de conexiones simultáneas a SQL Server, la configuración de un subproceso por consulta puede consumir demasiados recursos del sistema. `max worker threads`La opción ayuda a mejorar el rendimiento al permitir que SQL Server cree un pool de threads de trabajo que pueden atender colectivamente un número mayor de solicitudes de consulta.

El valor por defecto es 0, que permite a SQL Server configurar automáticamente el número de threads de trabajador al iniciar. Esto funciona para la mayoría de los sistemas. Max worker threads es una opción avanzada y no se debe modificar sin la ayuda de un administrador de base de datos experimentado (DBA).

¿Cuándo debe configurar SQL Server para que utilice más threads de trabajo? Si la longitud media de la cola de trabajo de cada programador es superior a 1, puede que se beneficie de agregar más threads al sistema, pero sólo si la carga no está vinculada a la CPU o si experimenta otras esperas pesadas. Si cualquiera de estos ocurre, agregar más hilos no ayuda porque terminan esperando otros cuellos de botella del sistema. Para obtener más información sobre el máximo de threads de trabajo, consulte "Configure la opción de configuración del servidor de threads de trabajo máximo".



Configuración de un máximo de threads de trabajador mediante SQL Server Management Studio.

En el siguiente ejemplo se muestra cómo configurar la opción Máximo de Threads de Trabajo mediante T-SQL.

```
EXEC sp_configure 'show advanced options', 1;
GO
RECONFIGURE ;
GO
EXEC sp_configure 'max worker threads', 900 ;
GO
RECONFIGURE;
GO
```

Configuración de memoria

La siguiente sección explica la configuración de memoria de SQL Server necesaria para optimizar el rendimiento de la base de datos.

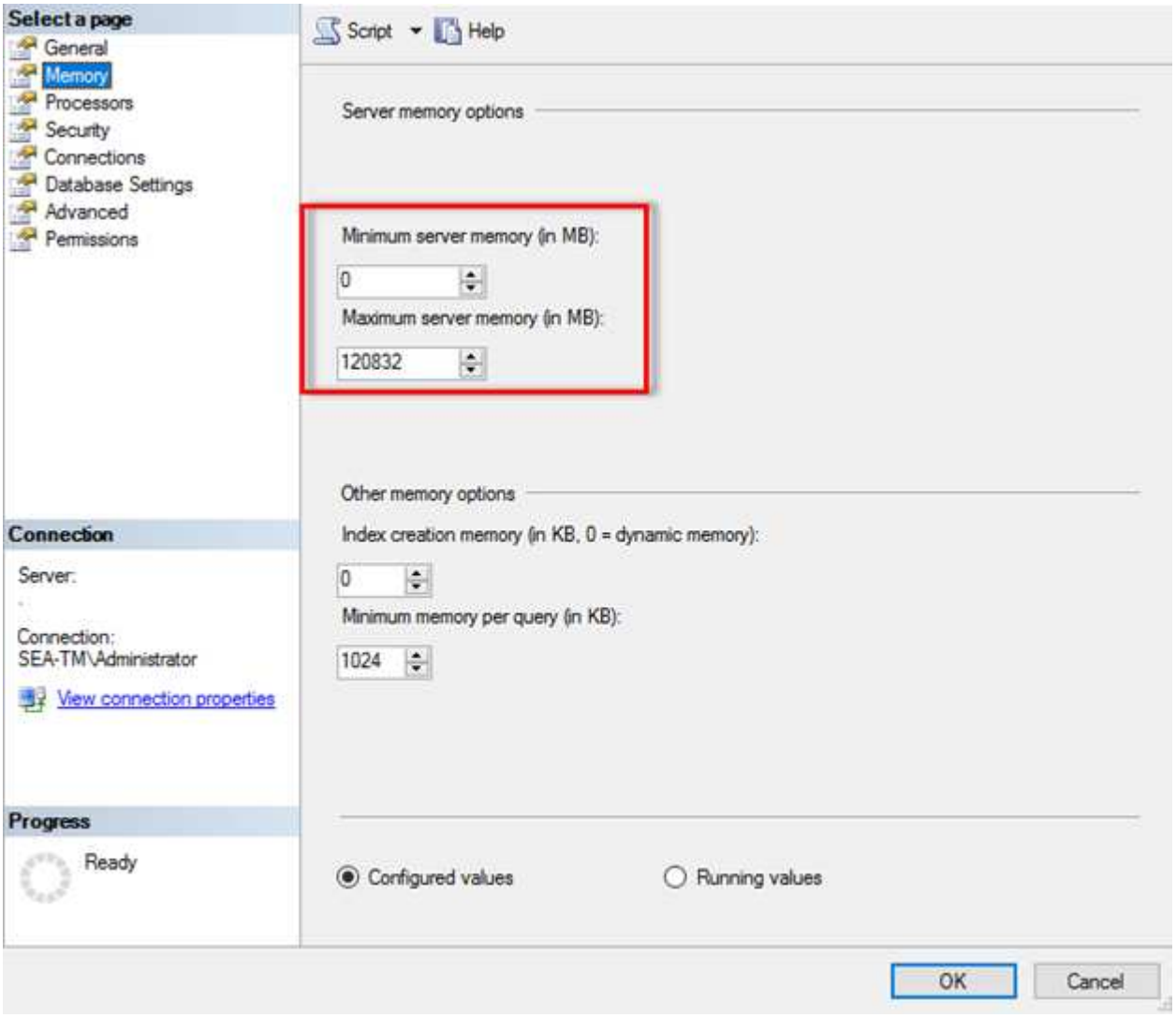
Memoria máxima del servidor

La opción max server memory define la cantidad máxima de memoria que puede utilizar la instancia de SQL Server. Se utiliza generalmente si se ejecutan varias aplicaciones en el mismo servidor donde se ejecuta SQL Server y desea garantizar que estas aplicaciones tengan suficiente memoria para funcionar correctamente.

Algunas aplicaciones solo utilizan la memoria disponible cuando se inician y no solicitan memoria adicional, incluso si están bajo presión de memoria. Aquí es donde entra en juego la configuración de memoria máxima del servidor.

En un clúster de SQL Server con varias instancias de SQL Server, cada instancia podría competir por los recursos. Establecer un límite de memoria para cada instancia de SQL Server puede ayudar a garantizar el mejor rendimiento para cada instancia.

NetApp recomienda dejar al menos 4GB a 6GB de RAM para el sistema operativo para evitar problemas de rendimiento.



Ajuste de la memoria mínima y máxima del servidor mediante SQL Server Management Studio.

El uso de SQL Server Management Studio para ajustar la memoria mínima o máxima del servidor requiere un reinicio del servicio de SQL Server. También puede ajustar la memoria del servidor mediante Transact SQL (T-SQL) usando este código:

```
EXECUTE sp_configure 'show advanced options', 1
GO
EXECUTE sp_configure 'min server memory (MB)', 2048
GO
EXEC sp_configure 'max server memory (MB)', 120832
GO
RECONFIGURE WITH OVERRIDE
```

Acceso a memoria no uniforme

El acceso no uniforme a la memoria (NUMA) es una tecnología de optimización del acceso a la memoria que ayuda a evitar la carga adicional en el bus del procesador.

Si NUMA está configurado en un servidor donde SQL Server está instalado, no se requiere ninguna configuración adicional porque SQL Server tiene en cuenta NUMA y funciona bien en el hardware NUMA.

Index CREATE MEMORIA

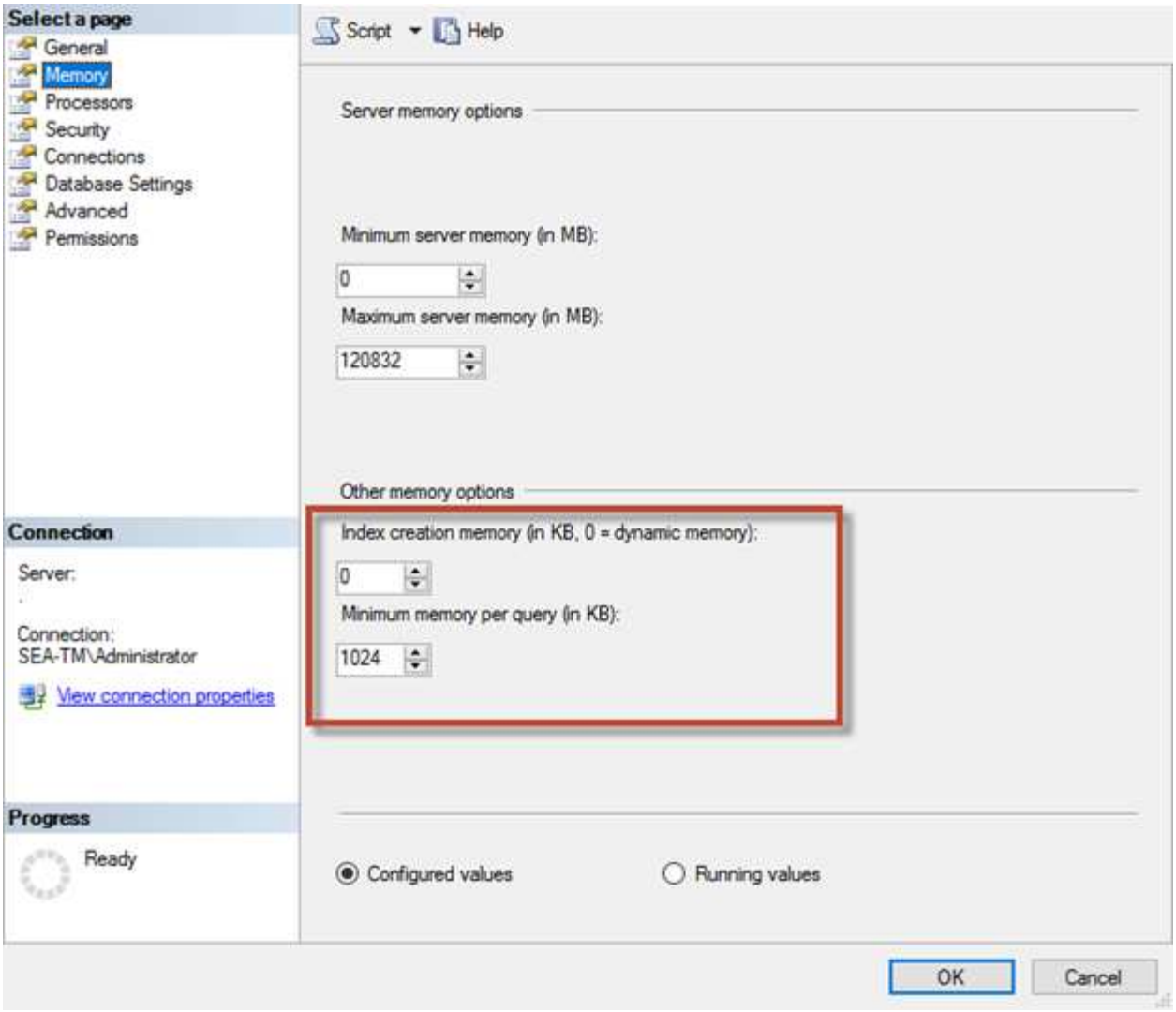
La opción INDEX CREATE MEMORY es otra opción avanzada que normalmente no debe cambiarse de los valores predeterminados.

Controla la cantidad máxima de RAM asignada inicialmente para crear índices. El valor por defecto de esta opción es 0, lo que significa que SQL Server la gestiona automáticamente. Sin embargo, si tiene dificultades para crear índices, considere aumentar el valor de esta opción.

Memoria mínima por consulta

Cuando se ejecuta una consulta, SQL Server intenta asignar la cantidad óptima de memoria para que se ejecute de forma eficiente.

De forma predeterminada, el valor de memoria mínima por consulta asigna >= a 1024KB para cada consulta que se ejecute. Es recomendable dejar este valor en el valor por defecto para permitir que SQL Server gestione dinámicamente la cantidad de memoria asignada para las operaciones de creación de índices. Sin embargo, si SQL Server tiene más RAM de la que necesita para ejecutarse de manera eficiente, el rendimiento de algunas consultas se puede aumentar si aumenta este valor. Por lo tanto, siempre y cuando la memoria esté disponible en el servidor que no esté utilizando SQL Server, ninguna otra aplicación o el sistema operativo, aumentar esta configuración puede ayudar en general al rendimiento de SQL Server. Si no hay memoria libre disponible, aumentar esta configuración puede afectar al rendimiento general.



Instancia compartida frente a instancia dedicada

SQL Server se puede configurar como una única instancia por servidor o como varias instancias. La decisión correcta generalmente depende de factores como si el servidor se va a utilizar para la producción o el desarrollo, si la instancia se considera crítica para las operaciones de negocio y los objetivos de rendimiento.

Las configuraciones de instancias compartidas pueden ser inicialmente más fáciles de configurar, pero pueden provocar problemas en los que los recursos se dividen o bloquean, lo que a su vez provoca problemas de rendimiento para otras aplicaciones que tienen bases de datos alojadas en la instancia compartida de SQL Server.

La solución de problemas de rendimiento puede ser complicada porque debe averiguar qué instancia es la causa raíz. Esta pregunta se compara con los costes de las licencias del sistema operativo y de las licencias de SQL Server. Si el rendimiento de las aplicaciones es primordial, se recomienda encarecidamente utilizar una instancia dedicada.

Microsoft concede licencias de SQL Server por núcleo a nivel de servidor y no por instancia. Por este motivo, los administradores de bases de datos se ven tentados a instalar tantas instancias de SQL Server como el servidor pueda manejar para ahorrar en costes de licencias, lo que puede ocasionar mayores problemas de rendimiento más adelante.

NetApp recomienda elegir instancias dedicadas de SQL Server siempre que sea posible para obtener un rendimiento óptimo.

Archivos tempdb

La base de datos Tempdb se puede utilizar en gran medida. Además de la ubicación óptima de los archivos de base de datos de usuario en ONTAP, la ubicación de los archivos de datos tempdb también es crítica para reducir la contención de asignación. Tempdb debe colocarse en un disco independiente y no compartirse con los archivos de datos de usuario.

La contención de página se puede producir en las páginas de mapa de asignación global (GAM), mapa de asignación global compartida (SGAM) o espacio libre de página (PFS) cuando SQL Server debe escribir en páginas especiales del sistema para asignar nuevos objetos. Los pestillos bloquean estas páginas en la memoria. En una instancia de SQL Server ocupada, puede tardar mucho tiempo en obtener un bloqueo en una página del sistema en tempdb. Esto da como resultado tiempos de ejecución de consultas más lentos y se conoce como contención de bloqueo interno. Consulte las siguientes prácticas recomendadas para crear archivos de datos tempdb:

- Para < or = a 8 núcleos: Archivos de datos tempdb = número de núcleos
- Para > 8 núcleos: 8 archivos de datos tempdb
- El archivo de datos tempdb se debe crear con el mismo tamaño

El siguiente script de ejemplo modifica tempdb creando ocho archivos tempdb de igual tamaño y moviendo tempdb al punto de montaje `C:\MSSQL\tempdb` para SQL Server 2012 y posterior.

```
use master

go

-- Change logical tempdb file name first since SQL Server shipped with
logical file name called tempdev

alter database tempdb modify file (name = 'tempdev', newname =
'tempdev01');



-- Change location of tempdev01 and log file

alter database tempdb modify file (name = 'tempdev01', filename =
'C:\MSSQL\tempdb\tempdev01.mdf');

alter database tempdb modify file (name = 'templog', filename =
'C:\MSSQL\tempdb\templog.ldf');

GO
```

```
-- Assign proper size for tempdev01

ALTER DATABASE [tempdb] MODIFY FILE ( NAME = N'tempdev01', SIZE = 10GB );

ALTER DATABASE [tempdb] MODIFY FILE ( NAME = N'templog', SIZE = 10GB );

GO

-- Add more tempdb files

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev02', FILENAME =
N'C:\MSSQL\tempdb\tempdev02.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev03', FILENAME =
N'C:\MSSQL\tempdb\tempdev03.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev04', FILENAME =
N'C:\MSSQL\tempdb\tempdev04.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev05', FILENAME =
N'C:\MSSQL\tempdb\tempdev05.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev06', FILENAME =
N'C:\MSSQL\tempdb\tempdev06.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev07', FILENAME =
N'C:\MSSQL\tempdb\tempdev07.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev08', FILENAME =
N'C:\MSSQL\tempdb\tempdev08.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

GO
```

A partir de SQL Server 2016, el número de núcleos de CPU visibles para el sistema operativo se detecta automáticamente durante la instalación y, en función de ese número, SQL Server calcula y configura el número de archivos tempdb necesarios para un rendimiento óptimo.

Configuración del almacenamiento en sistemas AFF/FAS

Descripción general

La combinación de las soluciones de almacenamiento de ONTAP y Microsoft SQL Server permite diseñar un almacenamiento de base de datos de nivel empresarial que puede satisfacer los requisitos de aplicaciones más exigentes de hoy en día.

La optimización de una solución SQL Server en ONTAP requiere comprender el patrón y las características de

E/S de SQL Server. Una buena distribución del almacenamiento para una base de datos de SQL Server debe soportar los requisitos de rendimiento de SQL Server y proporcionar la máxima capacidad de gestión de la infraestructura en su conjunto. Una buena distribución de almacenamiento también permite que la puesta en marcha inicial tenga éxito y que el entorno crezca sin problemas con el tiempo a medida que crece el negocio.

Diseño de almacenamiento de datos

Para las bases de datos de SQL Server que no utilizan SnapCenter para realizar backups, Microsoft recomienda colocar los archivos de datos y de registro en unidades independientes. Para las aplicaciones que actualizan y solicitan datos simultáneamente, el archivo de registro tiene un gran consumo de escrituras y el archivo de datos (en función de la aplicación) tiene un gran volumen de lecturas y escrituras. Para la recuperación de datos, el archivo de registro no es necesario. Por lo tanto, las solicitudes de datos pueden satisfacerse desde el archivo de datos ubicado en su propia unidad.

Cuando se crea una nueva base de datos, Microsoft recomienda especificar unidades independientes para los datos y los registros. Para mover archivos después de crear la base de datos, ésta debe desconectarse. Para obtener más recomendaciones de Microsoft, consulte "Coloque los archivos de datos y de registro en unidades separadas".

Agregados

Los agregados son los contenedores de almacenamiento de nivel más bajo para las configuraciones de almacenamiento de NetApp. Existe cierta documentación heredada en Internet, que recomienda separar las operaciones de I/O en diferentes conjuntos de unidades subyacentes. No se recomienda con ONTAP. NetApp ha realizado distintas pruebas de caracterización de las cargas de trabajo de I/O utilizando agregados compartidos y dedicados con archivos de datos y archivos de registro de transacciones separados. Las pruebas muestran que un gran agregado con más grupos RAID y unidades optimiza y mejora el rendimiento del almacenamiento y tiene mayor facilidad de gestión para los administradores por dos motivos:

- Un gran agregado hace que las funcionalidades de I/O de todas las unidades estén disponibles para todos los archivos.
- Un agregado de gran tamaño permite hacer un uso más eficiente del espacio en disco.

Para alta disponibilidad (HA), colocar la réplica síncrona secundaria de SQL Server Always On Availability Group en una máquina virtual de almacenamiento (SVM) independiente del agregado. Para fines de recuperación ante desastres, coloque la réplica asíncrona en un agregado que forma parte de un clúster de almacenamiento separado en el sitio de recuperación ante desastres, con el contenido replicado mediante la tecnología SnapMirror de NetApp. NetApp recomienda tener al menos un 10% de espacio libre disponible en un agregado para un rendimiento del almacenamiento óptimo.

Volúmenes

los volúmenes se crean y residen dentro de los agregados. Este término a veces provoca confusión porque un volumen ONTAP no es una LUN. Un volumen ONTAP es un contenedor de gestión para datos. Un volumen puede contener archivos, LUN o incluso objetos S3. Un volumen no ocupa espacio, solo se utiliza para la gestión de los datos contenidos.

Consideraciones sobre el diseño del volumen

Antes de crear un diseño de volumen de base de datos, es importante comprender cómo los patrones de I/O de SQL Server y las características varían en función de la carga de trabajo y de los requisitos de backup y recuperación. Consulte las siguientes recomendaciones de NetApp para volúmenes flexibles:

- Evite compartir volúmenes entre hosts. Por ejemplo, aunque sería posible crear 2 LUN en un único

volumen y compartir cada LUN en un host diferente, esto debe evitarse porque puede complicar la gestión. En el caso de ejecutar varias instancias de SQL Server en el mismo host, a menos que esté cerca del límite de volúmenes en un nodo, evite el uso compartido de volúmenes y disponga en su lugar de un volumen separado por instancia por host para facilitar la gestión de datos.

- Utilice puntos de montaje NTFS en lugar de letras de unidad para superar la limitación de 26 unidades en Windows. Cuando se usan puntos de montaje de volumen, se recomienda generalmente asignar a la etiqueta de volumen el mismo nombre que el punto de montaje.
- Cuando sea necesario, configure una política de tamaño automático de volúmenes para ayudar a evitar condiciones de falta de espacio.
- Si instala SQL Server en un recurso compartido de SMB, asegúrese de que Unicode esté habilitado en los volúmenes de SMB para crear carpetas.
- Establezca el valor de reserva de instantáneas en el volumen en cero para facilitar la supervisión desde una perspectiva operativa.
- Deshabilite las programaciones de Snapshot y las políticas de retención. En su lugar, utilice SnapCenter para coordinar las copias Snapshot de los volúmenes de datos de SQL Server.
- Coloque las bases de datos del sistema SQL Server en un volumen dedicado.
- Tempdb es una base de datos del sistema utilizada por SQL Server como espacio de trabajo temporal, especialmente para operaciones DBCC CHECKDB intensivas en E/S. Por lo tanto, coloque esta base de datos en un volumen dedicado con un conjunto de discos separado. En entornos grandes en los que el número de volúmenes es un reto, puede consolidar tempdb en menos volúmenes y almacenarlo en el mismo volumen que otras bases de datos del sistema tras una planificación cuidadosa. La protección de datos para tempdb no es una prioridad alta porque esta base de datos se vuelve a crear cada vez que se reinicia SQL Server.
- Colocar archivos de datos de usuario (`.mdf`) en volúmenes separados porque son cargas de trabajo de lectura/escritura aleatorias. Es común crear backups de registros de transacciones con más frecuencia que los backups de bases de datos. Por este motivo, coloque los archivos de registro de transacciones (`.ldf`) en un volumen o VMDK separados de los archivos de datos para que puedan crearse programaciones de backup independientes para cada uno. Esta separación también aísla la E/S de escritura secuencial de los archivos de registro de la E/S de lectura/escritura aleatoria de los archivos de datos y mejora significativamente el rendimiento de SQL Server.

LUN

- Asegúrese de que los archivos de la base de datos del usuario y el directorio de registro para almacenar backup de registros se encuentren en volúmenes independientes para evitar que la política de retención sobrescriba las snapshots cuando estas se usen con la tecnología SnapVault.
- No mezcle archivos de base de datos ni de otro tipo, como archivos relacionados con la búsqueda de texto completo, en el mismo LUN.
- La colocación de archivos secundarios de base de datos (como parte de un grupo de archivos) en volúmenes distintos mejora el rendimiento de la base de datos de SQL Server. Esta separación solo es válida si el archivo de la base de datos `.mdf` no comparte su LUN con ningún otro `.mdf` archivo.
- Si crea LUN con DiskManager u otras herramientas, asegúrese de que el tamaño de unidad de asignación esté establecido en 64K para las particiones al formatear las LUN.
- Consulte "Microsoft Windows e MPIO nativo bajo las prácticas recomendadas de ONTAP para SAN moderna" Para aplicar la compatibilidad con accesos múltiples en Windows a dispositivos iSCSI en las propiedades MPIO.

Archivos de base de datos y grupos de archivos

La ubicación correcta del archivo de la base de datos de SQL Server en ONTAP es crítica durante la etapa de la implementación inicial. Esto garantiza un rendimiento óptimo, gestión del espacio, tiempos de backup y restauración que pueden configurarse para que se ajusten a sus necesidades empresariales.

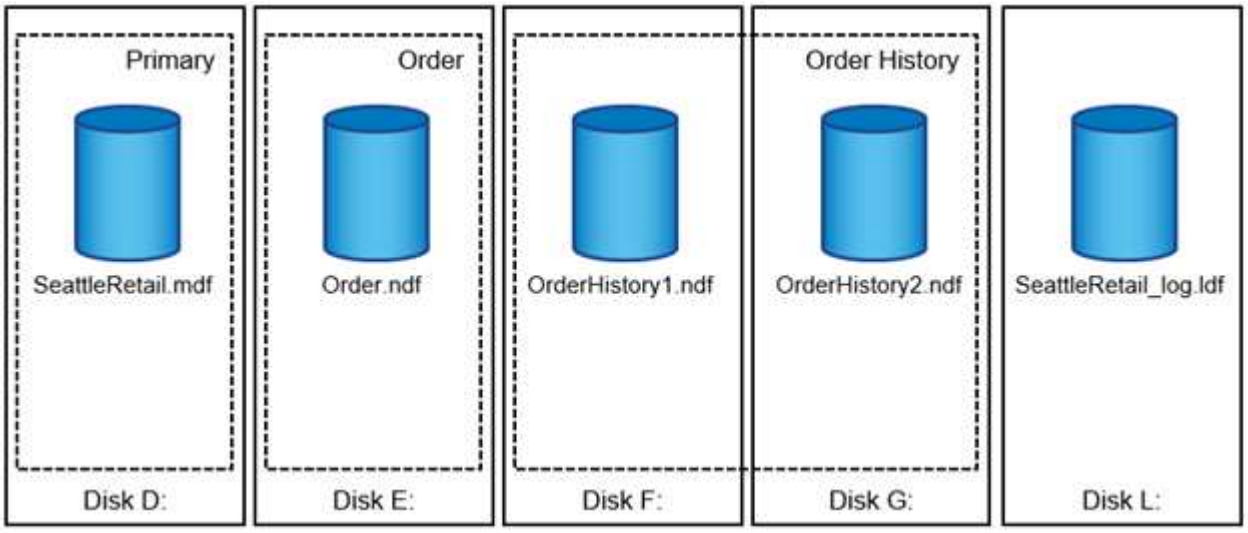
En teoría, SQL Server (64 bits) admite 32.767 bases de datos por instancia y 524.272TB GB de tamaño de base de datos, aunque la instalación típica suele tener varias bases de datos. Sin embargo, el número de bases de datos que SQL Server puede manejar depende de la carga y el hardware. No es raro ver instancias de SQL Server que alojan docenas, cientos o incluso miles de pequeñas bases de datos.

Archivos y grupo de archivos de bases de datos

Cada base de datos consta de uno o más archivos de datos y uno o varios archivos de registro de transacciones. El log de transacciones almacena la información sobre las transacciones de la base de datos y todas las modificaciones de datos realizadas por cada sesión. Cada vez que se modifican los datos, SQL Server almacena suficiente información en el log de transacciones para deshacer (realizar rollback) o rehacer (reproducir) la acción. Un registro de transacciones de SQL Server es una parte esencial de la reputación de SQL Server en cuanto a integridad y solidez de los datos. El registro de transacciones es vital para las capacidades de atomicidad, consistencia, aislamiento y durabilidad (ACID) de SQL Server. SQL Server escribe en el registro de transacciones tan pronto como se producen cambios en la página de datos. Cada sentencia de lenguaje de manipulación de datos (DML) (por ejemplo, SELECT, INSERT, UPDATE o DELETE) es una transacción completa, y el registro de transacciones se asegura de que se realice toda la operación basada en juegos, asegurándose de la atomicidad de la transacción.

Cada base de datos tiene un archivo de datos primario, que, por defecto, tiene la extensión .mdf. Además, cada base de datos puede tener archivos de base de datos secundarios. Esos archivos, por defecto, tienen extensiones .ndf.

Todos los archivos de base de datos se agrupan en grupos de archivos. Un grupo de archivos es la unidad lógica, que simplifica la administración de la base de datos. Permiten la separación entre la ubicación de objetos lógicos y los archivos físicos de la base de datos. Al crear las tablas de objetos de base de datos, especifique en qué grupo de archivos se deben colocar sin preocuparse por la configuración del archivo de datos subyacente.



La capacidad de colocar varios archivos de datos dentro del grupo de archivos permite distribuir la carga entre

diferentes dispositivos de almacenamiento, lo que ayuda a mejorar el rendimiento de I/O del sistema. Por el contrario, el registro de transacciones no se beneficia de los varios archivos, ya que SQL Server escribe en el registro de transacciones de forma secuencial.

La separación entre la ubicación de objetos lógicos en los grupos de archivos y los archivos físicos de la base de datos le permite ajustar el diseño del archivo de la base de datos, aprovechando al máximo el subsistema de almacenamiento. La cantidad de archivos de datos que soportan una carga de trabajo maestra se puede modificar según sea necesario para admitir los requisitos de I/O y la capacidad esperada sin afectar a la aplicación. Esas variaciones en el diseño de la base de datos son transparentes para los desarrolladores de aplicaciones, que colocan los objetos de la base de datos en los grupos de archivos en lugar de en los archivos de la base de datos.

NetApp recomienda evitar el uso del grupo de archivos primario para cualquier cosa excepto objetos del sistema. La creación de un grupo de archivos independiente o un conjunto de grupos de archivos para los objetos de usuario simplifica la administración de la base de datos y la recuperación ante desastres, especialmente en el caso de bases de datos grandes.

Inicialización del archivo de instancia de base de datos

Puede especificar el tamaño inicial del archivo y los parámetros de crecimiento automático en el momento de crear la base de datos o agregar nuevos archivos a una base de datos existente. SQL Server utiliza un algoritmo de relleno proporcional al elegir en qué archivo de datos debe escribir los datos. Escribe una cantidad de datos proporcionalmente al espacio libre disponible en los archivos. Cuanto mayor sea el espacio libre del archivo, más escrituras gestionará.

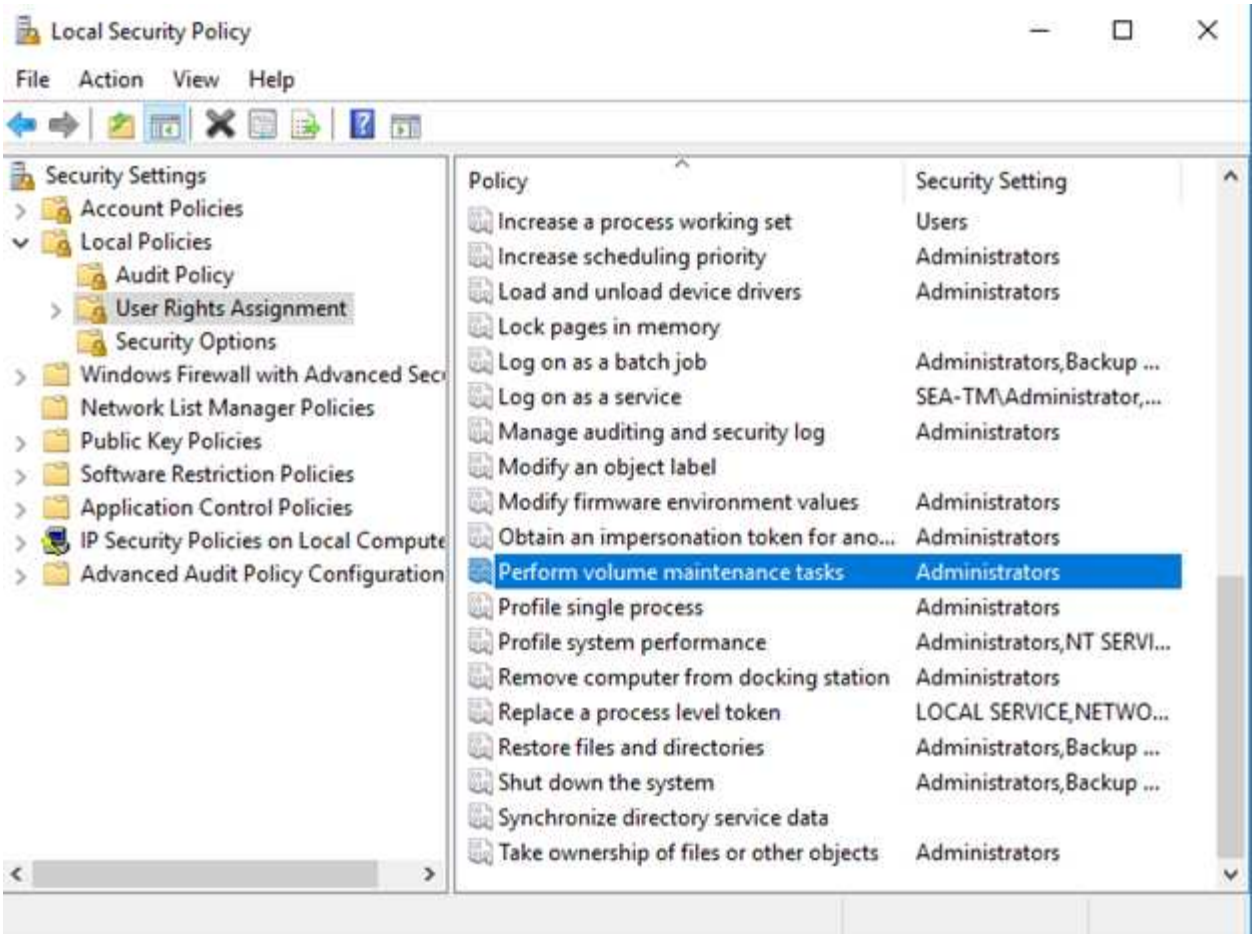
NetApp recomienda que todos los archivos en un solo grupo de archivos tengan los mismos parámetros iniciales de tamaño y crecimiento automático, con el tamaño de crecimiento definido en megabytes en lugar de porcentajes. Esto ayuda al algoritmo de relleno proporcional a equilibrar de forma uniforme las actividades de escritura en los archivos de datos.

Cada vez que SQL Server crece archivos, llena el espacio recién asignado con ceros. Este proceso bloquea todas las sesiones que necesitan escribir en el archivo correspondiente o, en caso de crecimiento del log de transacciones, generar registros de log de transacciones.

SQL Server siempre pone a cero el registro de transacciones y ese comportamiento no se puede cambiar. Sin embargo, puede controlar si los archivos de datos están a cero habilitando o deshabilitando la inicialización instantánea de archivos. La activación de la inicialización instantánea de archivos ayuda a acelerar el crecimiento de los archivos de datos y reduce el tiempo necesario para crear o restaurar la base de datos.

Un pequeño riesgo de seguridad está asociado con la inicialización instantánea de archivos. Cuando esta opción está activada, las partes no asignadas del archivo de datos pueden contener información de los archivos del sistema operativo eliminados anteriormente. Los administradores de bases de datos pueden examinar estos datos.

Puede activar la inicialización instantánea de archivos agregando el permiso SA_MANAGE_VOLUME_NAME, también conocido como “Realizar tarea de mantenimiento de volúmenes”, a la cuenta de inicio de SQL Server. Puede hacerlo en la aplicación de gestión de políticas de seguridad local (secpol.msc), como se muestra en la siguiente figura. Abra las propiedades del permiso “Realizar tarea de mantenimiento de volúmenes” y agregue la cuenta de inicio de SQL Server a la lista de usuarios allí.



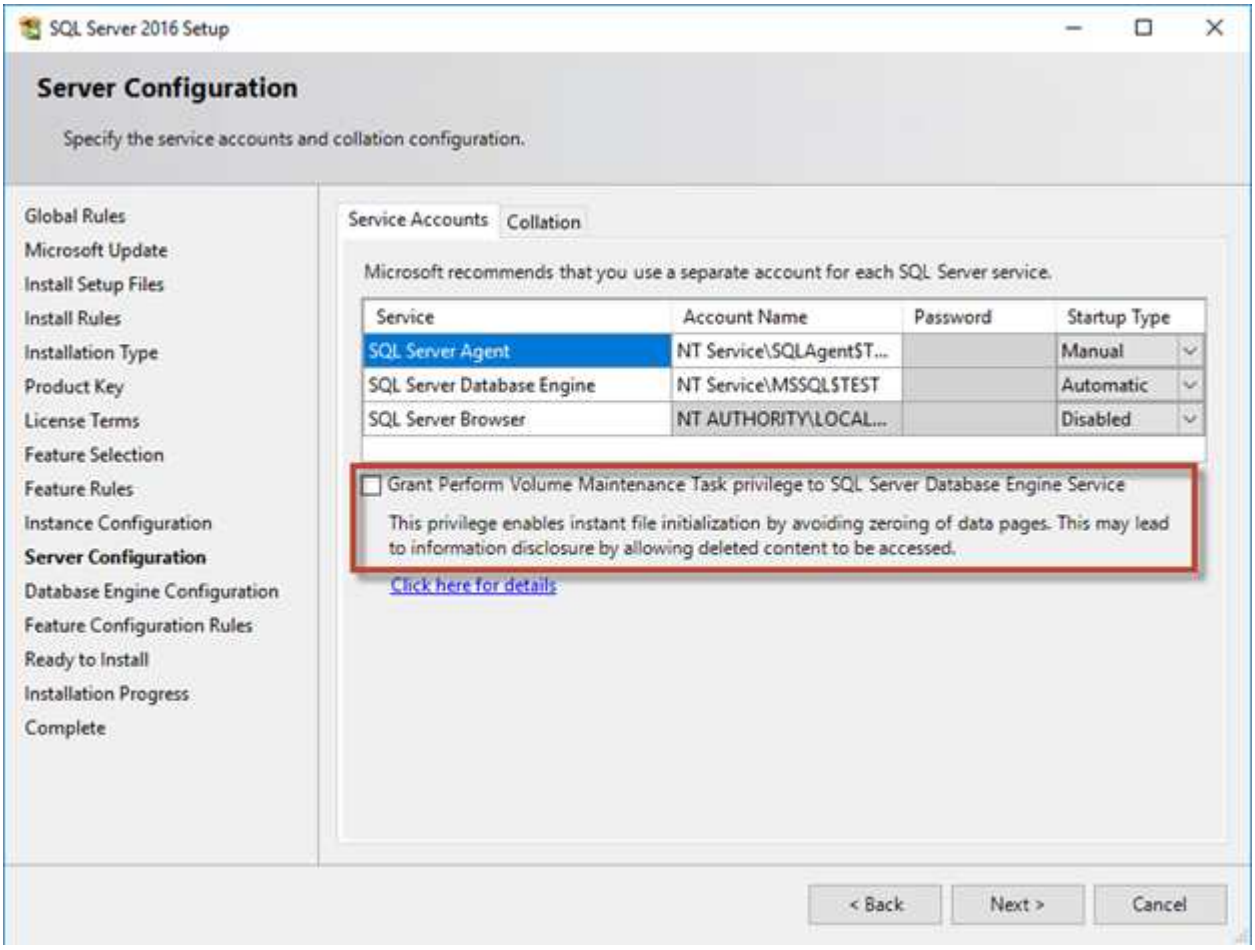
Para comprobar si el permiso está habilitado, puede utilizar el código del siguiente ejemplo. Este código establece dos indicadores de rastreo que obligan a SQL Server a escribir información adicional en el log de errores, crear una base de datos pequeña y leer el contenido del log.

```
DBCC TRACEON(3004,3605,-1)
GO
CREATE DATABASE DelMe
GO
EXECUTE sp_readerrorlog
GO
DROP DATABASE DelMe
GO
DBCC TRACEOFF(3004,3605,-1)
GO
```

Cuando la inicialización instantánea de archivos no está activada, el registro de errores de SQL Server muestra que SQL Server pone a cero el archivo de datos de mdf además de poner a cero el archivo log ldf, como se muestra en el siguiente ejemplo. Cuando se activa la inicialización instantánea del archivo, sólo se muestra la puesta a cero del archivo log.

	LogDate	ProcessInfo	Text
365	2017-02-09 08:10:07.660	spid53	Ckpt dbid 3 flush delta counts.
366	2017-02-09 08:10:07.660	spid53	Ckpt dbid 3 logging active xact info.
367	2017-02-09 08:10:07.750	spid53	Ckpt dbid 3 phase 1 ended (8)
368	2017-02-09 08:10:07.750	spid53	About to log Checkpoint end.
369	2017-02-09 08:10:07.880	spid53	Ckpt dbid 3 complete
370	2017-02-09 08:10:08.130	spid53	Starting up database 'DelMe'.
371	2017-02-09 08:10:08.150	spid53	FixupLogTail(progress) zeroing C:\Program Files\Micros
372	2017-02-09 08:10:08.160	spid53	Zeroing C:\Program Files\Microsoft SQL Server\MSSQ
373	2017-02-09 08:10:08.170	spid53	Zeroing completed on C:\Program Files\Microsoft SQL
374	2017-02-09 08:10:08.710	spid53	Ckpt dbid 6 started
375	2017-02-09 08:10:08.710	spid53	About to log Checkpoint begin.

La tarea Realizar mantenimiento de volumen se simplifica en SQL Server 2016 y, posteriormente, se proporciona como opción durante el proceso de instalación. Esta figura muestra la opción para otorgar al servicio del motor de base de datos SQL Server el privilegio para realizar la tarea de mantenimiento de volúmenes.



Otra opción importante de la base de datos que controla los tamaños de los archivos de la base de datos es la reducción automática. Cuando esta opción está habilitada, SQL Server reduce regularmente los archivos de la base de datos, reduce su tamaño y libera espacio al sistema operativo. Esta operación consume muchos recursos y rara vez es útil porque los archivos de la base de datos vuelven a crecer después de un tiempo cuando llegan nuevos datos al sistema. La reducción automática no debe estar activada en la base de datos.

Directorio de registro

El directorio de registro se especifica en SQL Server para almacenar datos de backup de registros de transacciones en el nivel de host. Si utiliza SnapCenter para realizar backup de archivos de registro, cada host SQL Server que utiliza SnapCenter debe tener un directorio de registro de host configurado para realizar backups de registros. SnapCenter tiene un repositorio de base de datos, por lo que los metadatos relacionados con las operaciones de backup, restauración o clonado se almacenan en un repositorio de base de datos central.

Los tamaños del directorio de registro de host se calculan de la siguiente manera:
Tamaño del directorio de registro de host = ((tamaño máximo de LDF de base de datos x tasa de cambio de registro diario %) x (retención de instantánea) ÷ (1: Porcentaje de espacio de sobrecarga de LUN)
La fórmula de ajuste de tamaño del directorio de registro del host asume una sobrecarga del 10% de las LUN

Coloque el directorio de registro en un volumen o LUN dedicados. La cantidad de datos en el directorio de registro del host depende del tamaño de los backups y de la cantidad de días que se retienen los backups. SnapCenter solo permite un directorio de registro de host por cada host SQL Server. Puede configurar los directorios de registro de host en SnapCenter -→ Host -→ Configurar el plugin.

NetApp recomienda lo siguiente para un directorio de registro de host:

- Asegúrese de que el directorio de registro de host no esté compartido por ningún otro tipo de datos que pueda dañar los datos de la instantánea de backup.
- No coloque bases de datos de usuario ni bases de datos del sistema en un LUN que aloje puntos de montaje.
- Cree el directorio de registro de host en un volumen dedicado al cual SnapCenter copia los registros de transacciones.
- Utilice los asistentes de SnapCenter para migrar bases de datos al almacenamiento NetApp de modo que las bases de datos se almacenen en ubicaciones válidas, lo que permite realizar correctamente las operaciones de backup y restauración de SnapCenter. Tenga en cuenta que el proceso de migración es disruptivo y puede provocar que las bases de datos se desconecten mientras se realiza la migración.
- Deben establecerse las siguientes condiciones para las instancias de clúster de conmutación por error (FCI) de SQL Server:
  - Si va a utilizar una instancia de clúster de conmutación al nodo de respaldo, el LUN del directorio de registro de host debe ser un recurso de disco de clúster en el mismo grupo de clústeres que la instancia de SQL Server que se va a realizar el backup de SnapCenter.
  - Si utiliza una instancia de clúster de conmutación al nodo de respaldo, las bases de datos de usuario deben colocarse en LUN compartidos que sean recursos de clúster de discos físicos asignados al grupo de clústeres asociado con la instancia de SQL Server.

Eficiencia del almacenamiento

La eficiencia del almacenamiento de ONTAP está optimizada para almacenar y gestionar datos de SQL Server de una manera que consuma la menor cantidad de espacio de almacenamiento sin que ello afecte al rendimiento.

Las funciones de eficiencia del espacio, como la compresión, la compactación y la deduplicación están diseñadas para aumentar la cantidad de datos lógicos que se adaptan a una determinada cantidad de almacenamiento físico. El resultado es una reducción de los costes y los gastos generales de gestión.

En un nivel superior, la compresión es un proceso matemático por el cual los patrones en los datos se detectan y codifican de manera que reducen los requisitos de espacio. Por el contrario, la deduplicación detecta bloques de datos repetidos y elimina las copias externas. La compactación permite que varios bloques lógicos de datos compartan el mismo bloque físico en medios.

Consulte las siguientes secciones sobre thin provisioning para obtener una explicación de la interacción entre la eficiencia del almacenamiento y la reserva fraccionaria.

Compresión

Antes de la disponibilidad de sistemas de almacenamiento all-flash, la compresión basada en cabinas era de un valor limitado debido a que la mayoría de las cargas de trabajo con un gran volumen de I/O requerían un gran número de discos para proporcionar un rendimiento aceptable. Los sistemas de almacenamiento contenían invariablemente mucha más capacidad de la necesaria como efecto secundario al gran número de unidades. La situación ha cambiado con el aumento del almacenamiento de estado sólido. Ya no es necesario sobreaprovisionar enormemente las unidades solo para obtener un buen rendimiento. El espacio de las unidades de un sistema de almacenamiento puede coincidir con las necesidades de capacidad reales.

La mayor funcionalidad de IOPS de las unidades de estado sólido (SSD) casi siempre genera ahorro de costes en comparación con las unidades giratorias, pero la compresión puede conseguir un mayor ahorro al aumentar la capacidad efectiva de los medios de estado sólido.

Existen varias formas de comprimir datos. Muchas bases de datos incluyen sus propias funcionalidades de compresión, pero esto se observa muy rara vez en los entornos del cliente. La razón suele ser la penalización de rendimiento para un **cambio** a los datos comprimidos, además con algunas aplicaciones hay altos costos de licencia para la compresión a nivel de base de datos. Por último, existen las consecuencias de rendimiento generales para las operaciones de base de datos. Tiene poco sentido pagar un alto coste de licencia por CPU por una CPU que realiza compresión y descompresión de datos en lugar de trabajo real de base de datos. Una mejor opción es descargar el trabajo de compresión en el sistema de almacenamiento.

Compresión adaptativa

La compresión adaptativa se ha probado minuciosamente en cargas de trabajo empresariales sin que ello afecte al rendimiento, incluso en un entorno all-flash en el que la latencia se mide en microsegundos. Algunos clientes incluso han informado de un aumento del rendimiento con el uso de la compresión, ya que los datos siguen comprimidos en la caché, lo que aumenta efectivamente la cantidad de caché disponible en una controladora.

ONTAP gestiona bloques físicos en 4KB unidades. La compresión adaptativa usa un tamaño de bloque de compresión predeterminado de 8KB KB, lo que significa que los datos se comprimen en 8KB unidades. Esto coincide con el tamaño de bloque de 8KB KB que suelen utilizar las bases de datos relacionales. Los algoritmos de compresión son más eficientes a medida que se comprimen más datos como una sola unidad. Un tamaño de bloque de compresión de 32KB KB haría más eficiente el espacio que una unidad de bloques de compresión de 8KB KB. Esto significa que la compresión adaptativa con el tamaño de bloque de 8KB KB predeterminado conduce a tasas de eficiencia ligeramente más bajas, pero también ofrece una ventaja significativa si se usa un tamaño de bloque de compresión más pequeño. Las cargas de trabajo de bases de datos incluyen una gran cantidad de actividad de sobrescritura. Para sobrescribir un bloque de datos de 8KB GB de 32KB comprimido, es necesario volver a leer los 32KB TB completos de datos lógicos, descomprimirlos, actualizar la región de 8KB requerida, recomprimir y, a continuación, volver a escribir todo el 32KB en las unidades. Esta es una operación muy cara para un sistema de almacenamiento y es el motivo por el que algunas cabinas de almacenamiento de la competencia basadas en bloques de compresión más grandes también incurren en un impacto significativo en el rendimiento con las cargas de trabajo de base de datos.

El tamaño de los bloques utilizado por la compresión adaptativa se puede aumentar hasta 32KB KB. Esto puede mejorar la eficiencia del almacenamiento y debe considerarse en el caso de archivos inactivos, como registros de transacciones y archivos de backup, cuando se almacena una cantidad sustancial de dichos datos en la cabina. En algunas situaciones, las bases de datos activas que usan un tamaño de bloque de 16KB KB o de 32KB KB también pueden beneficiarse de aumentar el tamaño de bloque de la compresión adaptativa para que coincida. Consulte a un representante de NetApp o de su partner para obtener orientación sobre si esto es adecuado para su carga de trabajo.

Los bloques de compresión superiores a los 8KB MB no se deben usar junto a la deduplicación en destinos de backup en streaming. El motivo es que los pequeños cambios en los datos de backup afectan a la ventana de compresión de 32KB:1. Si la ventana cambia, los datos comprimidos resultantes difieren en todo el archivo. La deduplicación ocurre después de la compresión, lo que significa que el motor de deduplicación ve cada backup comprimido de forma diferente. Si se requiere la deduplicación de backups en streaming, solo deberá usarse la compresión adaptativa de 8KB bloques. Es preferible recurrir a la compresión adaptativa, ya que funciona con un tamaño de bloque más pequeño y no interrumpe la eficiencia de la deduplicación. Por motivos similares, la compresión en el lado del host también interfiere con la eficiencia de la deduplicación.

Alineación de la compresión

La compresión adaptativa en un entorno de base de datos requiere tener en cuenta algún tipo de aspecto en la alineación de bloques de compresión. Hacerlo solo es una preocupación para los datos sujetos a sobrescrituras aleatorias de bloques muy específicos. Este enfoque es similar en concepto a la alineación general del sistema de archivos, donde el inicio de un sistema de archivos debe alinearse con un límite de dispositivo 4K y el tamaño de bloque de un sistema de archivos debe ser un múltiplo de 4K.

Por ejemplo, una escritura 8KB en un archivo se comprime solo si se alinea con un límite de 8KB KB en el propio sistema de archivos. Este punto significa que debe caer en los primeros 8KB del archivo, el segundo 8KB del archivo, y así sucesivamente. La forma más sencilla de garantizar una alineación correcta es utilizar el tipo de LUN correcto, cualquier partición creada debe tener un desplazamiento desde el inicio del dispositivo que sea un múltiplo de 8K y usar un tamaño de bloque del sistema de archivos que sea un múltiplo del tamaño del bloque de la base de datos.

Los datos como los backups o los registros de transacciones son operaciones escritas secuencialmente que abarcan varios bloques, todos ellos comprimidos. Por lo tanto, no hay necesidad de considerar la alineación. El único patrón de E/S preocupante es la sobrescritura aleatoria de archivos.

Compactación de datos

La compactación de datos es una tecnología que mejora la eficiencia de la compresión. Como se ha indicado anteriormente, la compresión adaptativa por sí sola puede proporcionar un ahorro de 2:1 KB, ya que se limita a almacenar una I/O de 8KB KB en un bloque de 4KB WAFL. Los métodos de compresión con tamaños de bloque más grandes ofrecen una mejor eficiencia. Sin embargo, no son adecuados para datos sujetos a sobrescrituras de bloques pequeños. La descompresión de 32KB unidades de datos, la actualización de una parte de 8KB, la recompresión y la escritura en las unidades genera una sobrecarga.

La compactación de datos permite almacenar varios bloques lógicos en bloques físicos. Por ejemplo, una base de datos con datos altamente comprimibles, como texto o bloques parcialmente completos, puede comprimirse de 8KB a 1KB. Sin compactación, esos 1KB TB de datos seguirían ocupando un bloque completo de 4KB KB. La compactación de datos inline permite almacenar 1KB TB de datos comprimidos en solo 1KB GB de espacio físico junto con otros datos comprimidos. No es una tecnología de compresión; simplemente es

una forma más eficaz de asignar espacio en las unidades y, por tanto, no debe crear un efecto de rendimiento detectable.

El grado de ahorro obtenido varía. Por lo general, los datos que ya están comprimidos o cifrados no se pueden comprimir aún más y, por lo tanto, estos conjuntos de datos no se benefician de la compactación. Por el contrario, los archivos de datos recién inicializados que contienen poco más que metadatos de bloques y ceros se comprimen hasta 80:1.

Eficiencia de almacenamiento sensible a la temperatura

La eficiencia de almacenamiento sensible a la temperatura (TSSE) está disponible en ONTAP 9, e.8 y posteriores. Se basa en mapas de calor de acceso a bloques para identificar los bloques a los que se accede con poca frecuencia y comprimirlos con mayor eficiencia.

Deduplicación

La deduplicación es eliminar los tamaños de bloques duplicados de un conjunto de datos. Por ejemplo, si existiera el mismo bloque de 4KB KB en 10 archivos diferentes, la deduplicación redirigiría ese bloque de 4KB KB en los 10 archivos al mismo bloque físico de 4KB KB. El resultado sería una mejora de 10:1 veces en eficiencia en esos datos.

Los datos, como las LUN de arranque invitado de VMware, suelen deduplicar muy bien porque constan de varias copias de los mismos archivos del sistema operativo. Se ha observado una eficiencia de 100:1 y mayor.

Algunos datos no contienen datos duplicados. Por ejemplo, un bloque de Oracle contiene una cabecera que es única globalmente para la base de datos y un cola que es casi único. Como resultado, la deduplicación de una base de datos de Oracle rara vez produce un ahorro superior al 1%. La deduplicación con bases de datos de MS SQL es ligeramente mejor, pero los metadatos únicos a nivel de bloque siguen siendo una limitación.

En pocos casos, se ha observado un ahorro de espacio de hasta un 15 % en bases de datos con 16KB KB y tamaños de bloque grandes. El primer 4KB de cada bloque contiene el encabezado único a nivel mundial, y el último bloque de 4KB contiene el remolque casi único. Los bloques internos pueden optar a la deduplicación, aunque en la práctica esto se atribuye casi por completo a la deduplicación de datos puestos a cero.

Muchas cabinas de la competencia afirman la capacidad de deduplicar bases de datos basándose en la presunción de que una base de datos se copia varias veces. En este sentido, la deduplicación de NetApp también podría utilizarse, pero ONTAP ofrece una opción mejor: La tecnología FlexClone de NetApp. El resultado final es el mismo; se crean varias copias de una base de datos que comparten la mayoría de los bloques físicos subyacentes. El uso de FlexClone es mucho más eficiente que tomarse tiempo para copiar archivos de base de datos y después deduplicarlos. Es, de hecho, la no duplicación en lugar de la deduplicación, porque nunca se crea un duplicado.

Eficiencia y thin provisioning

Las funciones de eficiencia son formas de thin provisioning. Por ejemplo, una LUN de 100GB GB que ocupa un volumen de 100GB GB podría comprimirse hasta 50GB 000. Todavía no hay ahorros reales realizados porque el volumen sigue siendo de 100GB GB. Primero se debe reducir el volumen para que el espacio ahorrado se pueda usar en cualquier otro lugar del sistema. Si los cambios realizados en la LUN de 100GB TB más adelante hacen que los datos se puedan comprimir menos, el tamaño de la LUN aumentará y el volumen podría llenarse.

Se recomienda encarecidamente el aprovisionamiento ligero porque puede simplificar la gestión y, al mismo tiempo, proporcionar una mejora considerable en la capacidad utilizable con un ahorro de costes asociado. La razón es simple: Los entornos de bases de datos suelen incluir una gran cantidad de espacio vacío, un gran número de volúmenes y LUN, y datos comprimibles. El aprovisionamiento grueso provoca la reserva de

espacio en el almacenamiento para volúmenes y LUN por si en algún momento llegan a estar llenos un 100 % y contienen un 100 % de datos que no se pueden comprimir. Es poco probable que esto ocurra. El thin provisioning permite reclamar y utilizar ese espacio en otra parte, y permite que la gestión de la capacidad se base en el propio sistema de almacenamiento en lugar de muchos volúmenes y LUN más pequeños.

Algunos clientes prefieren utilizar el aprovisionamiento pesado, ya sea para cargas de trabajo específicas o, por lo general, basándose en prácticas operativas y de adquisición establecidas.

> Si un volumen se aprovisiona en exceso, debe tenerse cuidado desactivar por completo todas las funciones de eficiencia de ese volumen, incluida la descompresión y la eliminación de la deduplicación con `sis undo` el comando. El volumen no debe aparecer en `volume efficiency show` la salida. Si lo hace, el volumen sigue estando parcialmente configurado para las funciones de eficiencia. Como resultado, la sobrescritura garantiza un funcionamiento diferente, lo que aumenta la posibilidad de que las sobretensiones de la configuración hagan que el volumen se quede sin espacio inesperadamente, lo que producirá errores de I/O de la base de datos.

Mejores prácticas de eficiencia

NetApp recomienda lo siguiente:

Valores predeterminados de AFF

Los volúmenes creados en ONTAP en un sistema AFF all-flash son thin provisioning, con todas las funciones de eficiencia inline habilitadas. Aunque por lo general, las bases de datos no se benefician de la deduplicación y pueden incluir datos que no se pueden comprimir, la configuración predeterminada es adecuada para casi todas las cargas de trabajo. ONTAP está diseñado para procesar eficientemente todo tipo de datos y patrones de I/O, independientemente de que generen o no ahorros. Los valores predeterminados solo se deben cambiar si los motivos se entienden por completo y existe un beneficio para desviarse.

Recomendaciones generales

- Si los volúmenes o LUN no son con thin provisioning, debe deshabilitar todas las configuraciones de eficiencia, ya que el uso de estas funciones no proporciona ahorro y la combinación de aprovisionamiento grueso con la eficiencia de espacio habilitada puede provocar un comportamiento inesperado, incluidos errores de falta de espacio.
- Si los datos no están sujetos a sobrescrituras, como con backups o registros de transacciones de base de datos, puede lograr una mayor eficiencia habilitando TSSE con un bajo período de enfriamiento.
- Es posible que algunos archivos contengan una cantidad significativa de datos que no se puedan comprimir, por ejemplo, cuando la compresión ya está activada en el nivel de aplicación de los archivos está cifrada. Si se da alguna de estas situaciones, considere la posibilidad de deshabilitar la compresión para permitir un funcionamiento más eficiente en otros volúmenes que contengan datos comprimibles.
- No utilice la compresión 32KB ni la deduplicación con backups de bases de datos. Consulte la sección Compresión adaptativa para obtener más detalles.

Compresión de base de datos

SQL Server en sí también tiene funciones para comprimir y gestionar datos de forma eficiente. SQL Server soporta actualmente dos tipos de compresión de datos: Compresión de filas y compresión de páginas.

La compresión de filas cambia el formato de almacenamiento de datos. Por ejemplo, cambia los enteros y decimales al formato de longitud variable en lugar de su formato nativo de longitud fija. También cambia las cadenas de caracteres de longitud fija al formato de longitud variable eliminando espacios en blanco. La

compresión de páginas implementa la compresión de filas y otras dos estrategias de compresión (compresión de prefijo y compresión de diccionario). Puede encontrar más detalles sobre la compresión de páginas en "Implantación de Compresión de Página".

Actualmente, la compresión de datos es compatible en las ediciones Enterprise, Developer y Evaluation de SQL Server 2008 y versiones posteriores. Aunque la propia base de datos puede realizar la compresión, esto rara vez se observa en un entorno de SQL Server.

Aquí están las recomendaciones para administrar el espacio para los archivos de datos de SQL Server

- Use thin provisioning en los entornos SQL Server para mejorar el aprovechamiento del espacio y reducir los requisitos generales de almacenamiento cuando se utilice la funcionalidad de garantía de espacio.
  - Use el crecimiento automático para las configuraciones de puesta en marcha más comunes porque el administrador de almacenamiento solo necesita supervisar el uso de espacio en el agregado.
- No active la deduplicación en ningún volumen de FAS que contenga archivos de datos de SQL Server, a menos que se sepa que el volumen contenga varias copias de los mismos datos, como la restauración de la base de datos desde backups en un único volumen.

Recuperación de espacio

La recuperación de espacio se puede iniciar periódicamente para recuperar el espacio no utilizado en una LUN. Con SnapCenter, puede utilizar el siguiente comando de PowerShell para iniciar la recuperación de espacio.

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

Si necesita ejecutar la recuperación de espacio, este proceso debe ejecutarse en períodos de baja actividad porque inicialmente consume ciclos en el host.

Protección de datos

Las estrategias de backup de bases de datos se deben basar en requisitos del negocio identificados, no en capacidades teóricas. Al combinar la tecnología Snapshot de ONTAP y aprovechar las API de Microsoft SQL Server, puede realizar rápidamente backup consistente con las aplicaciones independientemente del tamaño de las bases de datos del usuario. Para obtener requisitos de gestión de datos más avanzados o de escalado horizontal, NetApp ofrece SnapCenter.

SnapCenter

SnapCenter es el software de protección de datos de NetApp para aplicaciones empresariales. Las bases de datos de SQL Server pueden protegerse de forma rápida y fácil con el complemento de SnapCenter para SQL Server y con operaciones de sistema operativo gestionadas por el plugin de SnapCenter para Microsoft Windows.

La instancia de SQL Server puede ser una configuración independiente, una instancia de clúster de conmutación por error o puede estar siempre en un grupo de disponibilidad. El resultado es que, a partir de un solo panel, las bases de datos pueden protegerse, clonarse y restaurarse a partir de copias principales o secundarias. SnapCenter puede gestionar bases de datos de SQL Server tanto en las instalaciones, en el cloud como en configuraciones híbridas.Las copias de bases de datos también se pueden crear en pocos

minutos en el host original o alternativo para fines de desarrollo o generación de informes.

SQL Server también requiere coordinación entre el SO y el almacenamiento para garantizar que los datos correctos están presentes en las snapshots en el momento de la creación. En la mayoría de los casos, el único método seguro para hacerlo es con SnapCenter o T-SQL. Es posible que las instantáneas creadas sin esta coordinación adicional no se puedan recuperar de forma fiable.

Para obtener más detalles sobre el plugin de SQL Server para SnapCenter, consulte "TR-4714: Guía de mejores prácticas para SQL Server con NetApp SnapCenter".

Protección de la base de datos mediante instantáneas de T-SQL

En SQL Server 2022, Microsoft introdujo las copias Snapshot de T-SQL que ofrecen una ruta para el scripting y la automatización de las operaciones de backup. En lugar de realizar copias de tamaño completo, puede preparar la base de datos para instantáneas. Una vez que la base de datos está lista para el backup, se pueden aprovechar las API DE REST DE ONTAP para crear snapshots.

A continuación, se muestra un flujo de trabajo de backup de ejemplo:

1. Congelar una base de datos con el comando ALTER. Esto prepara la base de datos para una instantánea coherente en el almacenamiento subyacente. Después de congelar, puede descongelar la base de datos y registrar la instantánea con el comando BACKUP.
2. Realice copias Snapshot de varias bases de datos en los volúmenes de almacenamiento de forma simultánea con los nuevos comandos DEL GRUPO DE BACKUP y DEL SERVIDOR DE BACKUP.
3. Realice copias de seguridad COMPLETAS o copias de seguridad COMPLETAS COPY_ONLY. Estas copias de seguridad también se registran en msdb.
4. Llevar a cabo una recuperación puntual mediante backups de registro realizados con el método de streaming normal después del backup COMPLETO de la instantánea. Las copias de seguridad diferenciales de transmisión también se admiten si se desea.

Para obtener más información, consulte "Documentación de Microsoft para conocer las instantáneas de T-SQL".

NetApp recomienda usar SnapCenter para crear copias snapshot. También funciona el método T-SQL descrito anteriormente, pero SnapCenter ofrece una automatización completa del proceso de backup, restauración y clonación. También realiza una detección para garantizar que se crean las snapshots correctas. No se necesita ninguna configuración previa.

Grupo de disponibilidad de SQL Server con SnapCenter

SnapCenter admite el backup de la base de datos de grupo de disponibilidad de SQL Server configurada con clúster de conmutación al nodo de respaldo de Windows.

El complemento de SnapCenter para Microsoft SQL Server debe estar instalado en todos los nodos del clúster de conmutación al nodo de respaldo de Windows Server. Consulte "documentación"los requisitos previos de ON y los pasos para configurar los plugins de SnapCenter.

SnapCenter descubre todas las bases de datos, las instancias y los grupos de disponibilidad de hosts y recursos de Windows se enumeran en la página de recursos de SnapCenter.

Protección de bases de datos en un grupo de disponibilidad siempre disponible

Las bases de datos del grupo de disponibilidad se pueden proteger de varias maneras.

- Database level backup: Seleccione la base de datos de disponibilidad para la página de recursos de la base de datos, añadir la política que consta de backup completo/de registros, programar el backup. SnapCenter realiza el backup con independencia del rol de la base de datos, ya sea una réplica primaria o secundaria. La protección también puede configurarse si se añaden bases de datos al grupo de recursos.
- Backup de nivel de instancia: Seleccione la instancia y todas las bases de datos que se ejecutan en la instancia se protegen según la política seleccionada. Se realiza un backup de todas las bases de datos, incluida la base de datos con disponibilidad que se ejecuta como réplica primaria o secundaria, con SnapCenter. La protección también puede configurarse si se añade una instancia al grupo de recursos.
- Backup de nivel de grupo de disponibilidad: Al configurar la política, SnapCenter tiene una opción avanzada para backup de nivel de grupo de disponibilidad. La configuración del grupo de disponibilidad en la política permite a los usuarios seleccionar la preferencia de réplica para backup. Puede seleccionar réplica primaria, secundaria o todas ellas. La opción predeterminada se basa en el conjunto de réplica de backup en la configuración del grupo de disponibilidad de SQL Server.

La configuración del grupo de disponibilidad en la política de SnapCenter se aplica solo si el backup en el nivel de grupo de disponibilidad se utiliza para proteger las bases de datos de grupos de disponibilidad y no se aplica para el backup en el nivel de la base de datos o la instancia.

NetApp recomienda utilizar el respaldo de nivel de disponibilidad para realizar copias de seguridad en toda la réplica que se ejecuta en el almacenamiento de NetApp ONTAP.

Configurar el backup de registros en SnapCenter

Si el grupo de disponibilidad está configurado en la configuración independiente de SQL Server, debe montarse un disco dedicado en cada nodo de un clúster de conmutación al nodo de respaldo del servidor Windows. Se debe utilizar el disco dedicado para configurar el directorio log para guardar las copias de seguridad de log de transacciones.

Si el grupo de disponibilidad está configurado en el clúster de conmutación al nodo de respaldo de SQL Server, el disco almacenado en clúster se debe crear en la instancia de clúster de conmutación por error de SQL Server al directorio de registro de host.

Restaurando base de datos en la configuración del grupo de disponibilidad con SnapCenter

- SnapCenter proporciona la opción de propagación para recuperar automáticamente la base de datos a partir de la última instantánea disponible en la réplica secundaria. La operación de propagación restaurará y unirá automáticamente el backup de la base de datos al grupo de disponibilidad.
- Una forma alternativa de restaurar la base de datos de réplica en el grupo de disponibilidad es romper el grupo de disponibilidad y llevar a cabo la restauración completa y de registros. Utilice SnapCenter para restaurar la base de datos en modo norecovery y, a continuación, utilice SQL Server Management Studio o T-SQL para unir la base de datos al grupo de disponibilidad.
- Para recuperar sólo un subconjunto de datos, la funcionalidad de clonado de SnapCenter se puede usar para crear copias de clones de la base de datos. La copia de la base de datos se crea en pocos minutos con SnapCenter y, a continuación, exporte los datos a la réplica principal mediante las herramientas nativas de SQL Server.

Para conocer las mejores prácticas para configurar el diseño de almacenamiento de base de datos con el fin de cumplir los requisitos de RTO y RPO, consulte "TR-4714 Mejores prácticas para Microsoft SQL Server con

NetApp SnapCenter".

SnapCenter no admite grupos de disponibilidad distribuida ni grupos de disponibilidad contenidos.

Recuperación tras siniestros

Recuperación tras siniestros

Las bases de datos empresariales y las infraestructuras de aplicaciones a menudo requieren la replicación para protegerse de desastres naturales o de la interrupción inesperada del negocio con un tiempo de inactividad mínimo.

La función de replicación de grupos de disponibilidad siempre disponible de SQL Server puede ser una opción excelente, y NetApp ofrece opciones para integrar la protección de datos con disponibilidad permanente. Sin embargo, en algunos casos es posible que desee considerar la tecnología de replicación de ONTAP. Hay tres opciones básicas.

SnapMirror

La tecnología SnapMirror ofrece una solución empresarial rápida y flexible para replicar datos en LAN y WAN. La tecnología SnapMirror solo transfiere los bloques de datos modificados al destino una vez que se creó el reflejo inicial, lo que reduce considerablemente los requisitos de ancho de banda de la red. Puede configurarse tanto en modo síncrono como asíncrono.

Sincronización activa de NetApp MetroCluster y SnapMirror

Para muchos clientes, la recuperación ante desastres requiere algo más que poseer una copia remota de datos, requiere la capacidad para usar rápidamente esos datos. NetApp ofrece dos tecnologías para satisfacer esta necesidad: La sincronización activa de MetroCluster y SnapMirror

MetroCluster se refiere a ONTAP en una configuración de hardware que incluye almacenamiento reflejado sincrónico de bajo nivel y numerosas funciones adicionales. Las soluciones integradas como MetroCluster simplifican las complicadas infraestructuras de bases de datos, aplicaciones y virtualización actuales y de escalado horizontal. Reemplaza múltiples productos y estrategias de protección de datos externa por una cabina de almacenamiento simple y central. También proporciona integración de backup, recuperación, recuperación tras siniestros y alta disponibilidad (HA) en un único sistema de almacenamiento en clúster.

La sincronización activa de SnapMirror se basa en SnapMirror síncrono. Con MetroCluster, cada controladora de ONTAP es responsable de replicar los datos de la unidad en una ubicación remota. Con la sincronización activa de SnapMirror, básicamente cuenta con dos sistemas ONTAP diferentes que mantienen copias independientes de los datos de su unidad lógica, pero que cooperan para presentar una única instancia de esa LUN. Desde el punto de vista del host, se trata de una única entidad de LUN.

Comparación SM-AS y MCC

SM-AS y MetroCluster son similares en cuanto a funcionalidad general, pero hay diferencias importantes en la forma en que se implementó la replicación RPO=0 y cómo se gestiona. La sincronización asíncrona y síncrona de SnapMirror también se puede utilizar como parte de un plan de recuperación ante desastres, pero no están diseñadas como tecnologías de réplica de alta disponibilidad.

- Una configuración de MetroCluster es más como un clúster integrado con nodos distribuidos por todos los sitios. SM-AS se comporta como dos clústeres independientes que cooperan en el servicio de un objetivo de punto de recuperación seleccionado=0 LUN replicadas de forma síncrona.

- Los datos de una configuración MetroCluster solo son accesibles desde un sitio concreto en un momento dado. Una segunda copia de los datos está presente en el sitio opuesto, pero los datos son pasivos. No es posible acceder a ella sin una conmutación por error del sistema de almacenamiento.
- El mirroring de MetroCluster y SM-AS se produce en diferentes niveles. El mirroring de MetroCluster se realiza en la capa de RAID. Los datos de bajo nivel se almacenan en un formato duplicado mediante SyncMirror. El uso del mirroring es prácticamente invisible en las capas de LUN, volumen y protocolo.
- Por el contrario, la duplicación SM-AS se produce en la capa de protocolo. Los dos clústeres son clústeres independientes en general. Una vez que las dos copias de datos están sincronizadas, los dos clústeres solo tienen que reflejar las escrituras. Cuando se produce una escritura en un clúster, se replica en otro clúster. La escritura solo se reconoce en el host cuando la escritura se ha completado en ambos sitios. Aparte de este comportamiento de división del protocolo, los dos clústeres son clústeres ONTAP normales.
- El rol principal de MetroCluster es la replicación a gran escala. Puede replicar toda una cabina con RPO=0 y RTO casi nulo. Esto simplifica el proceso de conmutación al nodo de respaldo porque solo hay una cosa que conmutar al nodo de respaldo y ofrece una escalabilidad extremadamente buena en cuanto a capacidad e IOPS.
- Un caso de uso clave de SM-AS es la replicación granular. En ocasiones, no desea replicar todos los datos como una sola unidad, o debe poder conmutar al nodo de respaldo de forma selectiva ciertas cargas de trabajo.
- Otro caso de uso clave de SM-AS es en las operaciones activo-activo, donde desea que existan copias de datos totalmente utilizables para estar disponibles en dos clústeres diferentes ubicados en dos ubicaciones diferentes con idénticas características de rendimiento y, si lo desea, no es necesario ampliar la SAN entre los sitios. Puede tener sus aplicaciones ya ejecutándose en ambos sitios, lo que reduce el RTO general durante las operaciones de conmutación al respaldo.

SnapMirror

Las siguientes son recomendaciones para SnapMirror para SQL Server:

- Si se usa SMB, la SVM de destino debe ser miembro del mismo dominio de Active Directory al que pertenece la SVM de origen para que las listas de control de acceso (ACL) almacenadas en archivos NAS no se interrumpan durante la recuperación de un desastre.
- No es necesario usar nombres de volúmenes de destino iguales a los nombres de los volúmenes de origen, pero puede simplificar la gestión del proceso de montaje de los volúmenes de destino en el destino. Si se utiliza SMB, debe hacer que el espacio de nombres NAS de destino sea idéntico en rutas y la estructura de directorios para el espacio de nombres de origen.
- Con fines de coherencia, no programe actualizaciones de SnapMirror de las controladoras. En lugar de eso, habilite las actualizaciones de SnapMirror desde SnapCenter para actualizar SnapMirror después de haber completado el backup completo o de registro.
- Distribuya los volúmenes que contienen datos de SQL Server en diferentes nodos del clúster para permitir que todos los nodos del clúster compartan la actividad de replicación de SnapMirror. Esta distribución optimiza el uso de los recursos de los nodos.
- Use la replicación síncrona donde la demanda de recuperación de datos rápida sea mayor y las soluciones asíncronas para obtener flexibilidad en el objetivo de punto de recuperación.

Para obtener más información acerca de SnapMirror, consulte "TR-4015: Guía de configuración de SnapMirror y prácticas recomendadas para ONTAP 9".

MetroCluster

Arquitectura

La puesta en marcha de Microsoft SQL Server con entorno MetroCluster requiere alguna explicación del diseño físico de un sistema MetroCluster.

MetroCluster refleja de forma síncrona los datos y la configuración entre dos clústeres de ONTAP en ubicaciones independientes o en dominios de fallos. MetroCluster proporciona almacenamiento disponible de forma continua para las aplicaciones gestionando automáticamente dos objetivos:

- Objetivo de punto de recuperación cero (RPO) gracias al mirroring síncrono de los datos escritos en el clúster.
- Objetivo de tiempo de recuperación (RTO) casi cero mediante el mirroring de la configuración y la automatización del acceso a los datos en el segundo sitio.

MetroCluster proporciona simplicidad con mirroring automático de datos y configuración entre los dos clústeres independientes ubicados en los dos sitios. A medida que se aprovisiona el almacenamiento en un clúster, se replica automáticamente en el segundo clúster del segundo centro. NetApp SyncMirror® proporciona una copia completa de todos los datos con un RPO cero. Esto significa que las cargas de trabajo de un sitio podrían conmutar en cualquier momento al sitio opuesto y seguir proporcionando datos sin pérdida de datos. MetroCluster gestiona el proceso de switchover de proporcionar acceso a los datos NAS y aprovisionados con SAN en el segundo sitio. El diseño de MetroCluster como solución validada contiene el dimensionamiento y la configuración que permiten realizar una conmutación de sitios dentro de períodos de tiempo de espera del protocolo o antes (normalmente menos de 120 segundos). Esto da como resultado un objetivo de punto de recuperación casi cero, y las aplicaciones pueden seguir accediendo a los datos sin incurrir en fallos. El MetroCluster está disponible en varias variaciones definidas en el entramado de almacenamiento del back-end.

MetroCluster está disponible en 3 configuraciones diferentes

- Pares DE ALTA DISPONIBILIDAD con conectividad IP
- Pares DE ALTA DISPONIBILIDAD con conectividad FC
- Controladora única con conectividad FC

> El término 'conectividad' hace referencia a la conexión de clúster usada para la replicación entre sitios. No hace referencia a los protocolos de host. Todos los protocolos del lado del host se admiten como de costumbre en una configuración de MetroCluster, independientemente del tipo de conexión utilizada para la comunicación entre clústeres.

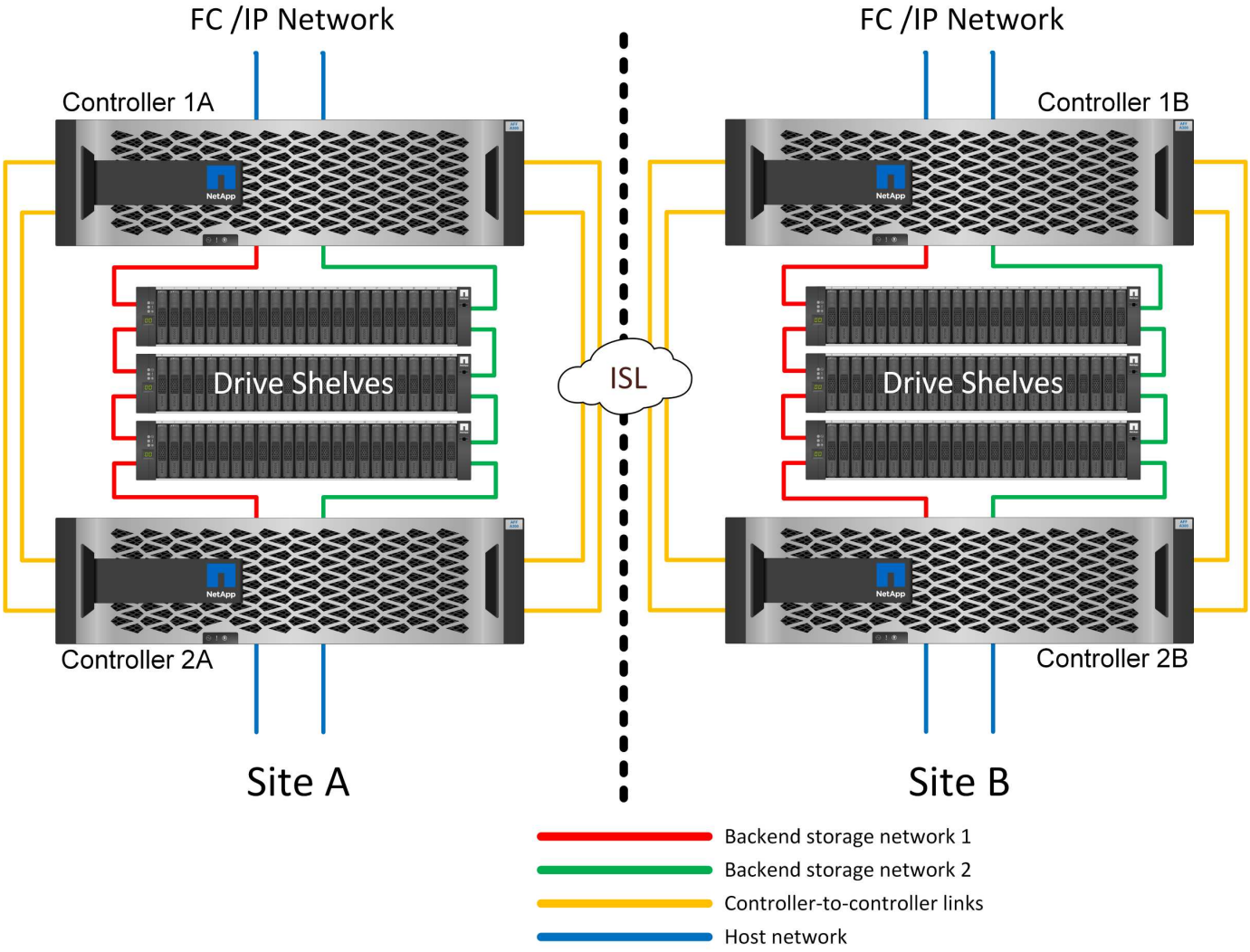
IP de MetroCluster

La configuración IP de MetroCluster para pares de alta disponibilidad utiliza dos o cuatro nodos por sitio. Esta opción de configuración aumenta la complejidad y los costes relacionados con la opción de dos nodos, pero ofrece una ventaja importante: La redundancia dentro del sitio. Un simple fallo de una controladora no requiere acceso a los datos a través de la WAN. El acceso a los datos sigue siendo local a través de la controladora local alternativa.

La mayoría de los clientes eligen la conectividad IP porque los requisitos de infraestructura son más simples. En el pasado, la conectividad entre sitios de alta velocidad solía ser más fácil de aprovisionar mediante switches FC y de fibra oscura; sin embargo, hoy en día los circuitos IP de alta velocidad y baja latencia son más fáciles de obtener.

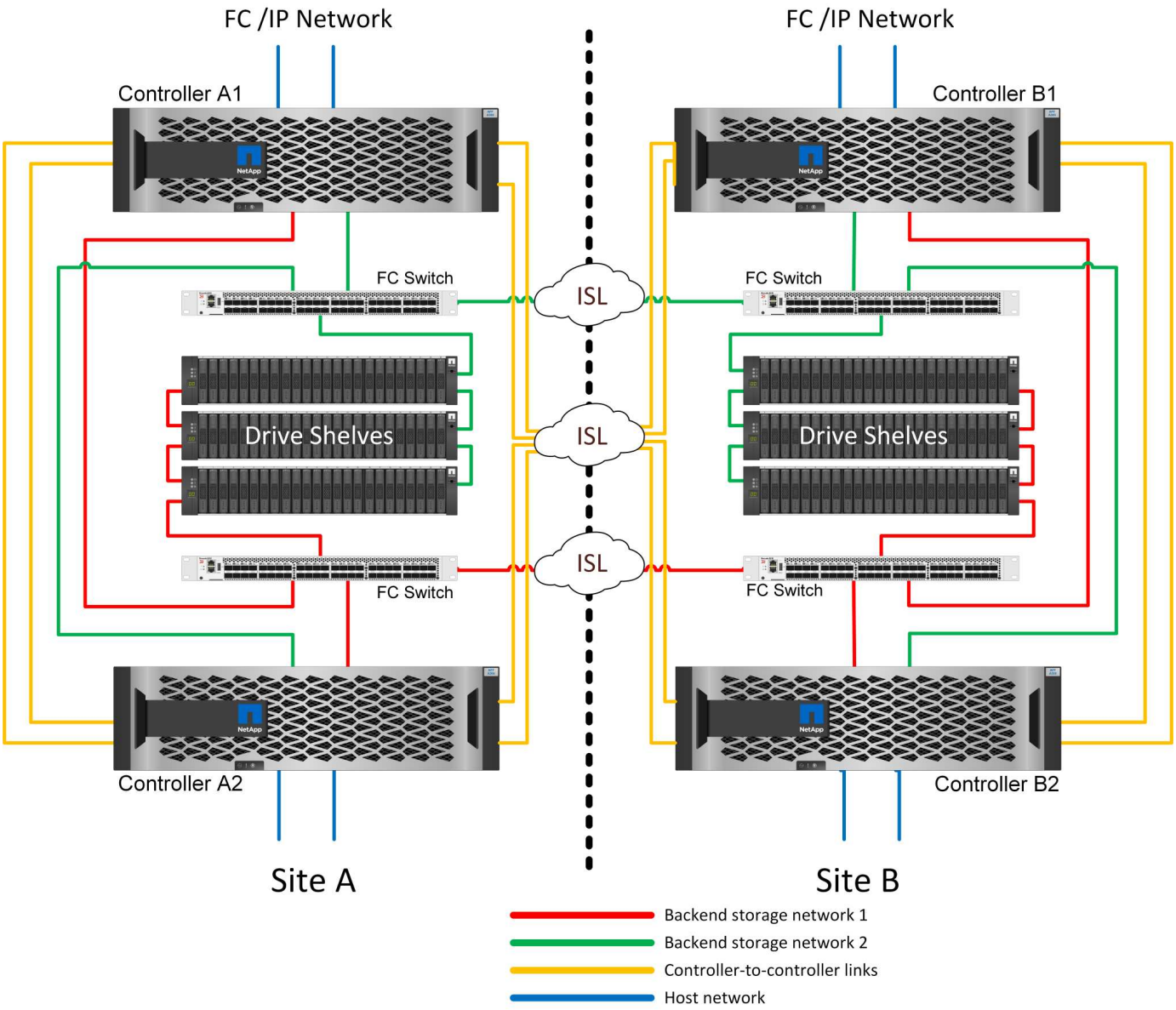
La arquitectura además es más sencilla ya que las únicas conexiones entre sitios son para las controladoras. En MetroCluster conectados a FC SAN, una controladora escribe directamente en las unidades del sitio opuesto y, por lo tanto, requiere conexiones SAN, switches y puentes adicionales. En cambio, una controladora con una configuración IP escribe en las unidades opuestas a través de la controladora.

Para obtener información adicional, consulte la documentación oficial de ONTAP y. "Arquitectura y diseño de la solución MetroCluster IP".



MetroCluster con conexión SAN FC de par de ALTA DISPONIBILIDAD

La configuración MetroCluster FC de par de alta disponibilidad utiliza dos o cuatro nodos por sitio. Esta opción de configuración aumenta la complejidad y los costes relacionados con la opción de dos nodos, pero ofrece una ventaja importante: La redundancia dentro del sitio. Un simple fallo de una controladora no requiere acceso a los datos a través de la WAN. El acceso a los datos sigue siendo local a través de la controladora local alternativa.



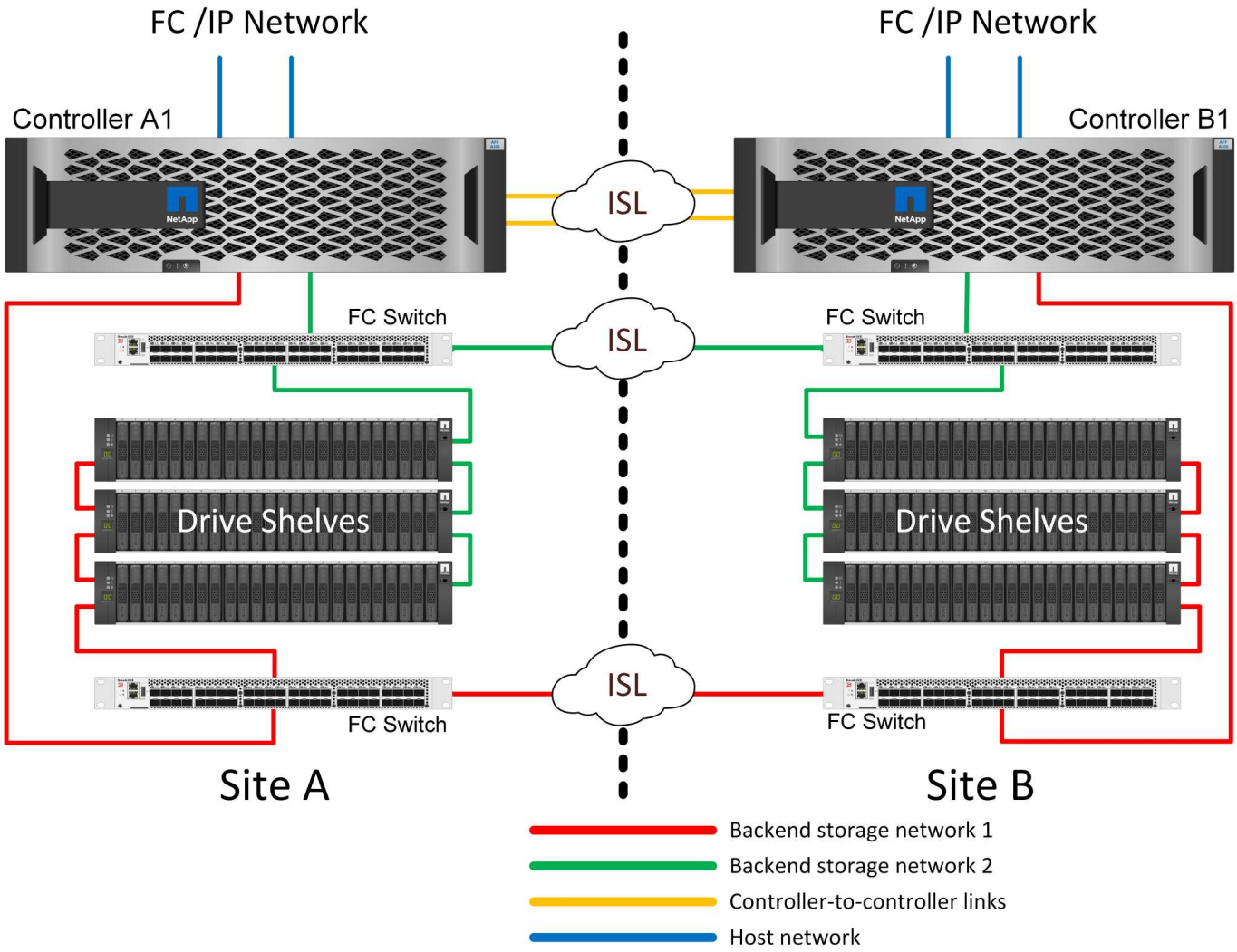
Algunas infraestructuras multisitio no están diseñadas para operaciones activo-activo, sino que se utilizan más como sitio principal y sitio de recuperación de desastres. En esta situación, generalmente es preferible una opción MetroCluster de una pareja de alta disponibilidad por las siguientes razones:

- Aunque un clúster MetroCluster de dos nodos es un sistema de alta disponibilidad, el fallo inesperado de una controladora o de tareas de mantenimiento planificadas requiere que los servicios de datos deban estar online en el sitio opuesto. Si la conectividad de red entre los sitios no puede soportar el ancho de banda requerido, el rendimiento se ve afectado. La única opción sería también conmutar por error los diversos sistemas operativos host y los servicios asociados a la ubicación alternativa. El clúster MetroCluster de la pareja de alta disponibilidad elimina este problema porque la pérdida de una controladora hace que la conmutación al respaldo sea sencilla dentro del mismo sitio.
- Algunas topologías de red no están diseñadas para el acceso entre sitios, sino que utilizan subredes diferentes o SAN FC aisladas. En estos casos, el clúster MetroCluster de dos nodos ya no funciona como un sistema de alta disponibilidad porque la controladora alternativa no puede proporcionar datos a los servidores del sitio opuesto. La opción MetroCluster de par de alta disponibilidad es necesaria para ofrecer una redundancia completa.
- Si se considera una infraestructura de dos sitios como una única infraestructura de alta disponibilidad, la configuración de MetroCluster de dos nodos es adecuada. Sin embargo, si el sistema debe funcionar

durante un largo período de tiempo tras el fallo del sitio, se prefiere un par de alta disponibilidad porque sigue proporcionando alta disponibilidad dentro de un único sitio.

MetroCluster FC de dos nodos conectado a SAN

La configuración de MetroCluster de dos nodos solo utiliza un nodo por sitio. Este diseño es más sencillo que la opción de pareja de alta disponibilidad porque hay menos componentes que configurar y mantener. También ha reducido las demandas de infraestructura en términos de cableado y conmutación FC. Por último, reduce los costes.



El impacto obvio de este diseño es que el fallo de una controladora en un único sitio significa que los datos están disponibles en el sitio opuesto. Esta restricción no es necesariamente un problema. Muchas empresas tienen operaciones de centros de datos multisitio con redes extendidas de alta velocidad y baja latencia que funcionan básicamente como una única infraestructura. En estos casos, la versión de dos nodos de MetroCluster es la configuración preferida. Varios proveedores de servicios utilizan actualmente sistemas de dos nodos a escala de petabytes.

Funcionalidades de resiliencia de MetroCluster

No hay puntos únicos de error en una solución de MetroCluster:

- Cada controladora tiene dos rutas independientes a las bandejas de unidades en el sitio local.

- Cada controladora tiene dos rutas independientes a las bandejas de unidades en el sitio remoto.
- Cada controladora tiene dos rutas independientes a las controladoras del sitio opuesto.
- En la configuración de par de alta disponibilidad, cada controladora tiene dos rutas desde su compañero local.

En resumen, puede eliminarse cualquier componente de la configuración sin poner en riesgo la capacidad de MetroCluster para suministrar datos. La única diferencia en términos de flexibilidad entre las dos opciones es que la versión del par de alta disponibilidad sigue siendo un sistema de almacenamiento de alta disponibilidad global tras un fallo del sitio.

SyncMirror

La protección para SQL Server con MetroCluster se basa en SyncMirror, que ofrece una tecnología de mirroring síncrono con escalabilidad horizontal y máximo rendimiento.

Protección de datos con SyncMirror

En el nivel más sencillo, la replicación síncrona implica que se debe realizar cualquier cambio en ambas partes del almacenamiento reflejado antes de que se reconozca. Por ejemplo, si una base de datos está escribiendo un registro o se está aplicando la revisión a un invitado VMware, no se debe perder nunca una escritura. Como nivel de protocolo, el sistema de almacenamiento no debe reconocer la escritura hasta que se haya comprometido a medios no volátiles en ambos sitios. Solo entonces es seguro proceder sin el riesgo de pérdida de datos.

El uso de una tecnología de replicación síncrona es el primer paso para diseñar y gestionar una solución de replicación síncrona. Lo más importante es comprender qué podría suceder durante varios escenarios de fallos planificados y no planificados. No todas las soluciones de replicación síncrona ofrecen las mismas funcionalidades. Si necesita una solución que proporcione un objetivo de punto de recuperación (RPO) de cero, lo que significa cero pérdida de datos, deben tenerse en cuenta todos los escenarios de fallo. En particular, ¿cuál es el resultado esperado cuando la replicación es imposible debido a la pérdida de conectividad entre sitios?

Disponibilidad de datos SyncMirror

La replicación de MetroCluster se basa en la tecnología de NetApp SyncMirror, que se ha diseñado para alternar eficientemente entre el modo síncrono y este se sale de él. Esta funcionalidad satisface los requisitos de los clientes que demandan replicación síncrona pero que también necesitan una alta disponibilidad para sus servicios de datos. Por ejemplo, si la conectividad con un sitio remoto se interrumpe, generalmente es preferible que el sistema de almacenamiento siga funcionando en un estado sin replicar.

Muchas soluciones de replicación síncrona solo pueden funcionar en modo síncrono. Este tipo de replicación compuesta por todos o nada se denomina a veces modo domino. Este tipo de sistemas de almacenamiento dejan de servir datos en lugar de permitir que las copias locales y remotas de datos se dessincronicen. Si la replicación se interrumpe de forma forzada, la resincronización puede requerir mucho tiempo y puede dejar al cliente expuesto a la pérdida de datos durante el tiempo que se restablece el mirroring.

SyncMirror no solo puede salir del modo síncrono sin problemas si no se puede acceder al sitio remoto, sino que también puede volver a sincronizar rápidamente con un estado RPO = 0 cuando se restaura la conectividad. La copia obsoleta de los datos en el sitio remoto también se puede conservar en estado utilizable durante la resincronización, lo que garantiza la existencia de copias locales y remotas de los datos en todo momento.

Cuando se requiere el modo domino, NetApp ofrece SnapMirror síncrono (SM-S). También existen opciones de nivel de aplicación, como Oracle DataGuard o SQL Server, grupos de disponibilidad Always On. El

mirroring de discos a nivel de sistema operativo puede ser una opción. Consulte con su equipo de cuentas de partner o de NetApp para obtener más información y opciones.

SQL Server con MetroCluster

MetroCluster es una opción para proteger las bases de datos de SQL Server con un objetivo de punto de recuperación cero. MetroCluster es una tecnología de replicación sencilla y de alto rendimiento RPO=0 que le permite replicar fácilmente toda una infraestructura entre sitios.

SQL Server puede ampliar hasta miles de bases de datos en un único sistema MetroCluster. Podría haber instancias independientes de SQL Server o instancias de cluster de conmutación al nodo de respaldo, el sistema MetroCluster no necesariamente agrega o cambia las mejores prácticas para gestionar una base de datos.

Una explicación completa de MetroCluster está más allá del alcance de este documento, pero los principios son simples. MetroCluster puede proporcionar una solución de replicación RPO=0 con una rápida conmutación al respaldo. Lo que construya sobre esta base depende de sus necesidades.

Por ejemplo, un procedimiento básico de DR rápida después de la pérdida repentina del sitio podría seguir los siguientes pasos básicos:

- Forzar una conmutación de MetroCluster
- Detección de LUN FC/iSCSI (solo SAN)
- Montaje de sistemas de archivos
- Inicie SQL Services

El requisito principal de este método es un sistema operativo en ejecución instalado en el sitio remoto. Se debe preconfigurar con la configuración de SQL Server y se debe actualizar con una versión de compilación equivalente. Las bases de datos del sistema SQL Server también pueden duplicarse en el sitio remoto y montarse si se declara un desastre.

Si los volúmenes, los sistemas de archivos y el almacén de datos que alojan bases de datos virtualizadas no se utilizan en el sitio de recuperación ante desastres antes de la conmutación de sitios, no es necesario establecer `dr-force-nvfail` en los volúmenes asociados.

SnapMirror síncrono activo

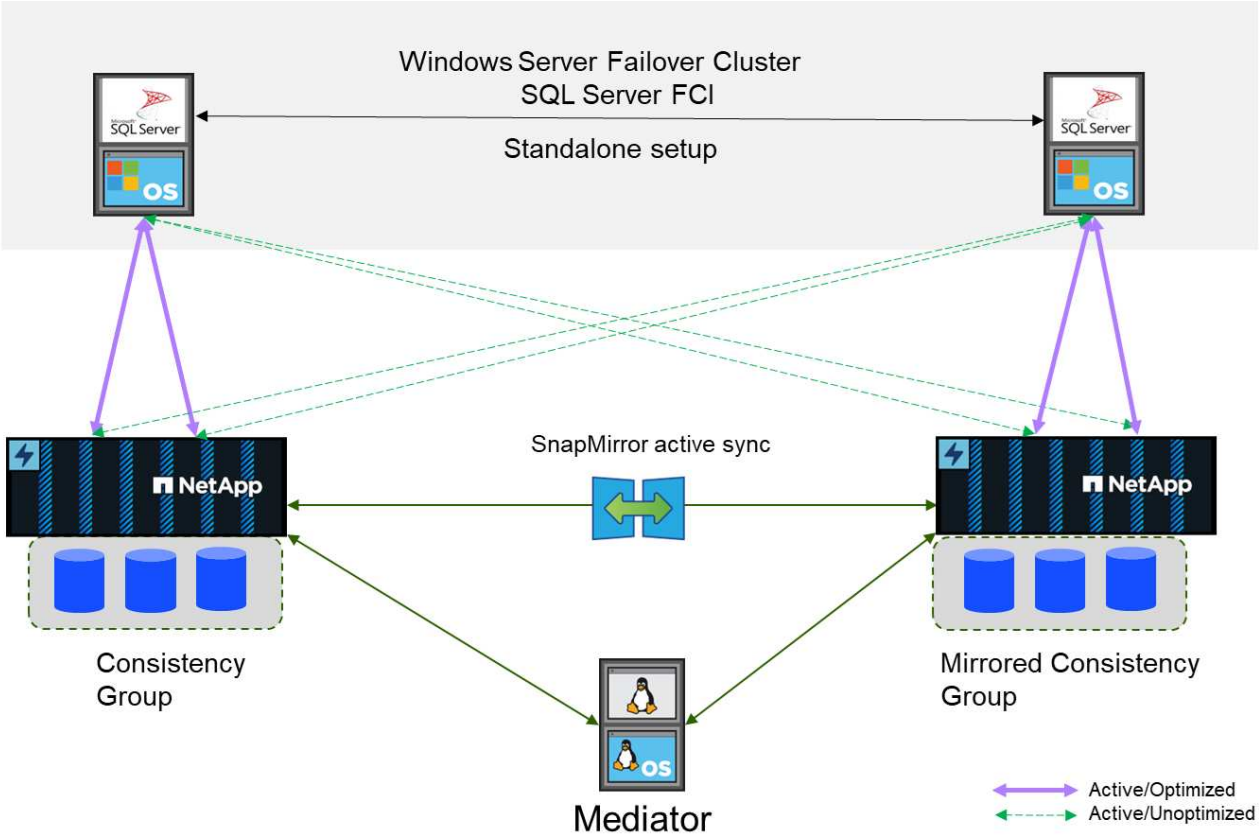
Descripción general

La sincronización activa de SnapMirror permite que las aplicaciones y bases de datos individuales de SQL Server continúen las operaciones durante interrupciones de las redes y el almacenamiento, con conmutación al respaldo transparente del almacenamiento sin intervención manual.

A partir de ONTAP 9.15,1, SnapMirror Active Sync admite arquitectura activo-activo simétrica además de la configuración asimétrica existente. La funcionalidad activo-activo simétrica proporciona replicación bidireccional síncrona para la continuidad del negocio y la recuperación ante desastres. Le ayuda a proteger el acceso a los datos para cargas de trabajo SAN críticas con acceso de lectura y escritura simultáneo a los datos en varios dominios de fallo, lo que garantiza operaciones ininterrumpidas y minimiza el tiempo de inactividad durante desastres o fallos del sistema.

Los hosts SQL Server acceden al almacenamiento a través de LUN de Fibre Channel (FC) o iSCSI. Replicación entre cada clúster que aloja una copia de los datos replicados. Dado que esta función es la replicación de nivel de almacenamiento, las instancias de SQL Server que se ejecutan en instancias de clúster de conmutación por error o host independiente pueden realizar operaciones de lectura/escritura en cualquier clúster. Para obtener información sobre los pasos de planificación y configuración, consulte "Documentación de ONTAP en sincronización activa de SnapMirror" .

Arquitectura de SnapMirror sincronización activa con activo-activo simétrico



Replicación síncrona

En condiciones de funcionamiento normal, cada copia es una réplica síncrona RPO=0 en todo momento, con una excepción. Si los datos no se pueden replicar, ONTAP liberará el requisito para replicar datos y reanudar el servicio de I/O en un sitio mientras las LUN del otro sitio se desconecten.

Hardware de almacenamiento

Al contrario que otras soluciones de recuperación ante desastres del almacenamiento, SnapMirror Active Sync ofrece una flexibilidad de plataforma asimétrica. No es necesario que el hardware de cada sitio sea idéntico. Esta funcionalidad permite ajustar el tamaño adecuado del hardware que se utiliza para dar soporte a SnapMirror de sincronización activa. El sistema de almacenamiento remoto puede ser idéntico al sitio principal si necesita soportar una carga de trabajo de producción completa, pero si un desastre provoca una reducción de I/O, es posible que un sistema más pequeño en el sitio remoto sea más rentable.

Mediador ONTAP

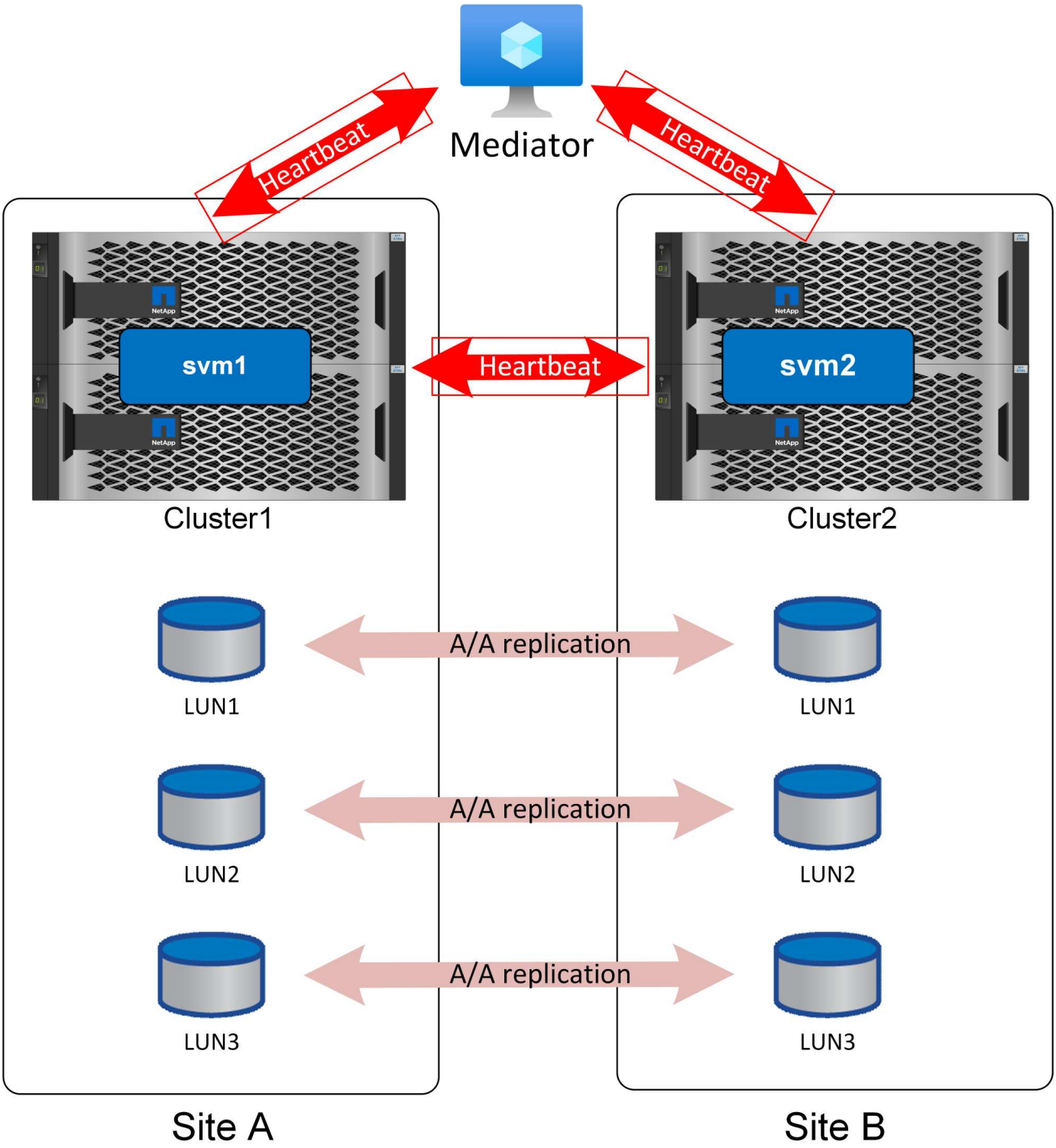
ONTAP Mediator es una aplicación de software que se descarga del soporte técnico de NetApp y que normalmente se implementa en una pequeña máquina virtual. El Mediador ONTAP no es un desempate. Es

un canal de comunicación alternativo para los dos clústeres que participan en la replicación síncrona activa de SnapMirror. Las operaciones automatizadas son impulsadas por ONTAP en función de las respuestas recibidas del partner a través de conexiones directas y a través del mediador.

Mediador ONTAP

Mediator es necesario para automatizar la recuperación tras fallos de forma segura. Lo ideal sería que se ubicara en un sitio 3rd independiente, pero todavía puede funcionar para la mayoría de las necesidades si se ubicara con uno de los clústeres que participan en la replicación.

El mediador no es realmente un desempate, aunque esa es efectivamente la función que proporciona. No realiza ninguna acción, sino que proporciona un canal de comunicación alternativo para la comunicación del clúster al clúster.



El desafío #1 con la conmutación automática por error es el problema de cerebro dividido, y ese problema surge si sus dos sitios pierden conectividad entre sí. ¿Qué debería pasar? No desea que dos sitios diferentes se designen a sí mismos como copias supervivientes de los datos, pero ¿cómo puede un solo sitio diferenciar entre la pérdida real del sitio opuesto y la incapacidad de comunicarse con el sitio opuesto?

Aquí es donde el mediador entra en la imagen. Si se coloca en un sitio 3rd y cada sitio tiene una conexión de red independiente con ese sitio, tiene una ruta adicional para que cada sitio valide el estado del otro. Mire la imagen de arriba otra vez y considere los siguientes escenarios.

- ¿Qué sucede si el mediador falla o es inaccesible desde uno o ambos sitios?
  - Los dos clústeres pueden comunicarse entre sí a través del mismo enlace utilizado para los servicios de replicación.
  - Los datos se siguen ofreciendo con la protección RPO=0
- ¿Qué sucede si falla el sitio A?
  - El sitio B verá que ambos canales de comunicación se caen.
  - El sitio B se hará cargo de los servicios de datos, pero sin el mirroring RPO=0
- ¿Qué sucede si falla el sitio B?
  - El sitio A verá que ambos canales de comunicación se caen.
  - El sitio A se hará cargo de los servicios de datos, pero sin el mirroring RPO=0

Hay otro escenario a considerar: Pérdida del enlace de replicación de datos. Si se pierde el enlace de replicación entre los sitios, obviamente el mirroring RPO=0 se convertirá en imposible. ¿Qué debería pasar entonces?

Esto se controla por el estado de sitio preferido. En una relación SM-AS, uno de los sitios es secundario al otro. Esto no afecta a las operaciones normales y todo el acceso a los datos es simétrico, pero si la replicación se interrumpe, el vínculo tendrá que romperse para reanudar las operaciones. Como resultado, el sitio preferido continuará con las operaciones sin mirroring y el sitio secundario detendrá el procesamiento de I/O hasta que se restaure la comunicación de la replicación.

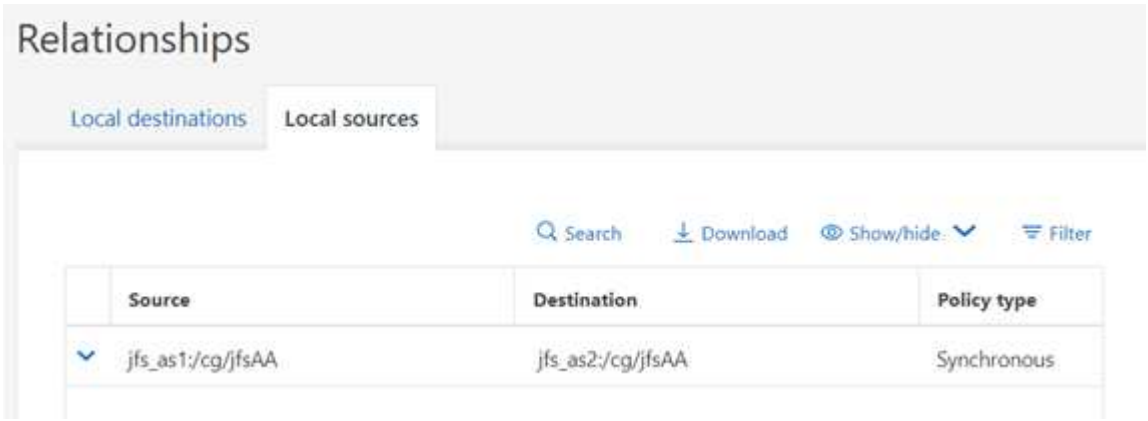
Sitio preferido

El comportamiento de sincronización activa de SnapMirror es simétrico, con una excepción importante: La configuración de sitio preferida.

La sincronización activa de SnapMirror considerará que un sitio es el «origen» y el otro el «destino». Esto implica una relación de replicación unidireccional, pero esto no se aplica al comportamiento de E/S. La replicación es bidireccional y simétrica, y los tiempos de respuesta de I/O son los mismos en cualquier lado del espejo.

La `source` designación controla el sitio preferido. Si se pierde el enlace de replicación, las rutas de LUN en la copia de origen seguirán sirviendo datos mientras las rutas de LUN en la copia de destino dejarán de estar disponibles hasta que se restablezca la replicación y SnapMirror vuelva a entrar en un estado síncrono. A continuación, las rutas reanudarán el servicio de datos.

La configuración de origen/destino se puede ver a través de SystemManager:



O en la CLI:

```
Cluster2::> snapmirror show -destination-path jfs_as2:/cg/jfsAA

                           Source Path: jfs_as1:/cg/jfsAA
                     Destination Path: jfs_as2:/cg/jfsAA
                    Relationship Type: XDP
                Relationship Group Type: consistencygroup
                    SnapMirror Schedule: -
                 SnapMirror Policy Type: automated-failover-duplex
                      SnapMirror Policy: AutomatedFailOverDuplex
                            Tries Limit: -
                      Throttle (KB/sec): -
                           Mirror State: Snapmirrored
                    Relationship Status: InSync
```

La clave es que la fuente es la máquina virtual de almacenamiento SVM en cluster1. Tal como se ha mencionado anteriormente, los términos «origen» y «destino» no describen el flujo de los datos replicados. Ambos sitios pueden procesar una escritura y replicarla en el sitio opuesto. De hecho, ambos clústeres son orígenes y destinos. El efecto de designar un clúster como origen simplemente controla qué clúster sobrevive como sistema de almacenamiento de lectura y escritura si se pierde el enlace de replicación.

Topología de red

Acceso uniforme

La conexión de red de acceso uniforme significa que los hosts pueden acceder a las rutas en ambos sitios (o dominios de fallo dentro del mismo sitio).

Una característica importante de SM-AS es la capacidad de configurar los sistemas de almacenamiento para conocer dónde se encuentran los hosts. Cuando asigna las LUN a un host determinado, puede indicar si son proximales o no a un sistema de almacenamiento determinado.

Ajustes de proximidad

La proximidad se refiere a una configuración por clúster que indica que un ID de iniciador de iSCSI o WWN de host particular pertenece a un host local. Es un segundo paso opcional para configurar el acceso a LUN.

El primer paso es la configuración habitual del igroup. Cada LUN debe asignarse a un igroup que contiene los ID WWN/iSCSI de los hosts que necesitan acceder a ese LUN. Este controla el host que tiene *access* a una LUN.

El segundo paso opcional es configurar la proximidad del host. Esto no controla el acceso, controla *priority*.

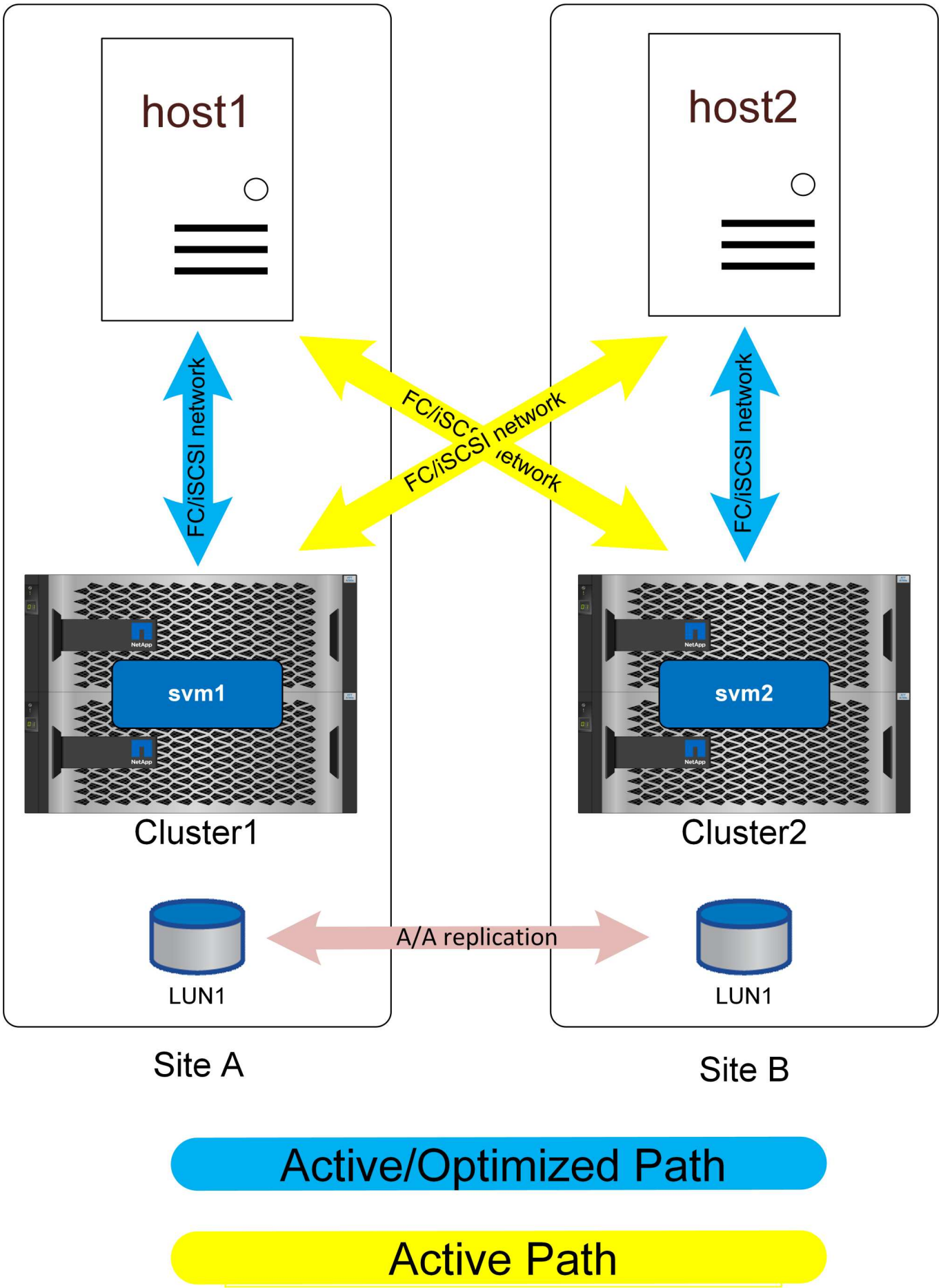
Por ejemplo, se puede configurar un host del sitio A para acceder a una LUN protegida por sincronización activa de SnapMirror y, como la SAN se extiende a través de los sitios, las rutas están disponibles para ese LUN usando el almacenamiento en el sitio A o el almacenamiento del sitio B.

Sin configuración de proximidad, ese host usará ambos sistemas de almacenamiento por igual porque ambos sistemas de almacenamiento anunciarán rutas activas/optimizadas. Si la latencia SAN o el ancho de banda

entre los sitios es limitada, es posible que no sea deseable y puede que desee asegurarse de que durante el funcionamiento normal cada host utilice preferentemente rutas hacia el sistema de almacenamiento local. Esto se configura añadiendo el ID de WWN/iSCSI de host al clúster local como un host proximal. Esto se puede hacer en la CLI o en SystemManager.

AFF

Con un sistema AFF, las rutas aparecerían como se muestra a continuación cuando se configura la proximidad del host.


host1
host2
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
svm1
svm2
Cluster1
Cluster2
A/A replication
LUN1
LUN1
Site A
Site B
Active/Optimized Path
Active Path

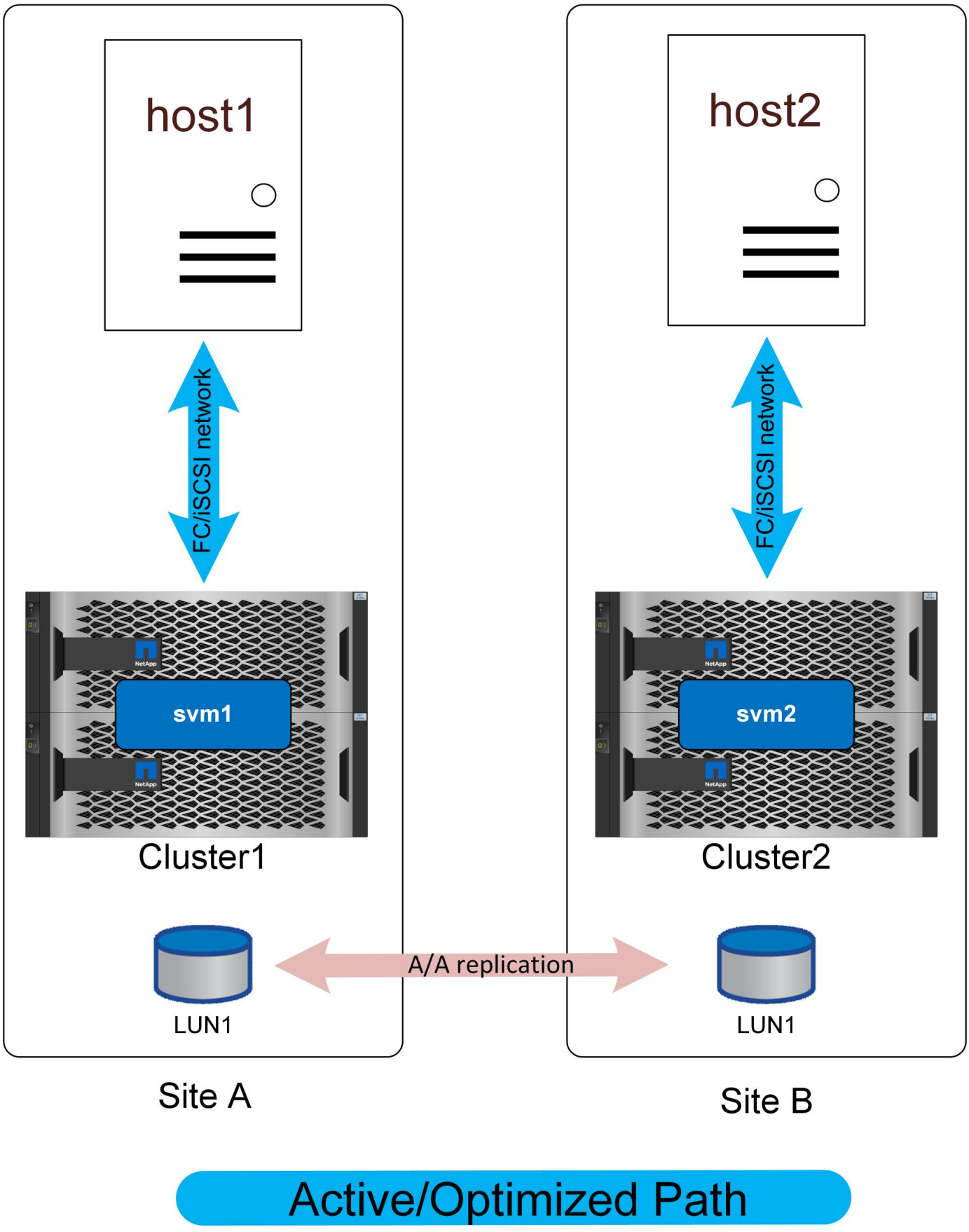
En funcionamiento normal, todas las I/O son locales. Las lecturas y escrituras se sirven desde la cabina de almacenamiento local. Por supuesto, el controlador local también deberá replicar el I/O de escritura en el sistema remoto antes de reconocerlo, pero todas las I/O de lectura se prestarán de servicio local y no incurrirán en latencia adicional atravesando el enlace SAN entre los sitios.

La única vez que se utilizarán las rutas no optimizadas es cuando se pierden todas las rutas activas/optimizadas. Por ejemplo, si se perdiera alimentación toda la cabina en el sitio A, los hosts del sitio A seguirían teniendo acceso a las rutas a la cabina en el sitio B y, por lo tanto, permanecerían operativos, aunque experimentarían una mayor latencia.

Existen rutas redundantes a través del clúster local que no se muestran en estos diagramas para simplificar el proceso. Los sistemas de almacenamiento de ONTAP son por sí mismos de alta disponibilidad, por lo que un fallo de una controladora no debe dar lugar a un fallo del sitio. Simplemente debe dar lugar a un cambio en el que se utilizan las rutas locales en el sitio afectado.

Acceso no uniforme

La red de acceso no uniforme significa que cada host solo tiene acceso a los puertos del sistema de almacenamiento local. La SAN no se extiende entre sitios (o dominios de fallos dentro del mismo sitio).



La principal ventaja de este método es la simplicidad en entornos SAN, eliminando la necesidad de extender una SAN por la red. Algunos clientes no tienen una conectividad de baja latencia suficiente entre los sitios o

no disponen de la infraestructura para túnel el tráfico de SAN FC a través de una red intersitio.

La desventaja del acceso no uniforme es que ciertos escenarios de fallo, incluida la pérdida del enlace de replicación, provocarán que algunos hosts pierdan el acceso al almacenamiento. Las aplicaciones que se ejecutan como instancias únicas, como una base de datos sin cluster que inherentemente solo se ejecuta en un único host en cualquier montaje dado, fallarían si se perdiera la conectividad del almacenamiento local. Los datos seguirían estando protegidos, pero el servidor de la base de datos ya no tendría acceso. Deberá reiniciarse en un sitio remoto, preferiblemente mediante un proceso automatizado. Por ejemplo, VMware HA puede detectar una situación de todas las rutas inactivas en un servidor y reiniciar una máquina virtual en otro servidor donde haya rutas disponibles.

Por el contrario, una aplicación en cluster como Oracle RAC puede ofrecer un servicio que esté disponible al mismo tiempo en dos sitios diferentes. Perder un sitio no significa la pérdida del servicio de la aplicación en su conjunto. Las instancias siguen estando disponibles y en ejecución en el sitio superviviente.

En muchos casos, sería inaceptable que la sobrecarga de latencia adicional derivada de una aplicación que accede al almacenamiento a través de un enlace entre sitio y sitio. Esto significa que la disponibilidad mejorada de una red uniforme es mínima, ya que la pérdida de almacenamiento en un sitio llevaría a la necesidad de apagar los servicios en ese sitio que ha fallado de todos modos.

> Existen rutas redundantes a través del clúster local que no se muestran en estos diagramas para simplificar el proceso. Los sistemas de almacenamiento de ONTAP son por sí mismos de alta disponibilidad, por lo que un fallo de una controladora no debe dar lugar a un fallo del sitio. Simplemente debe dar lugar a un cambio en el que se utilizan las rutas locales en el sitio afectado.

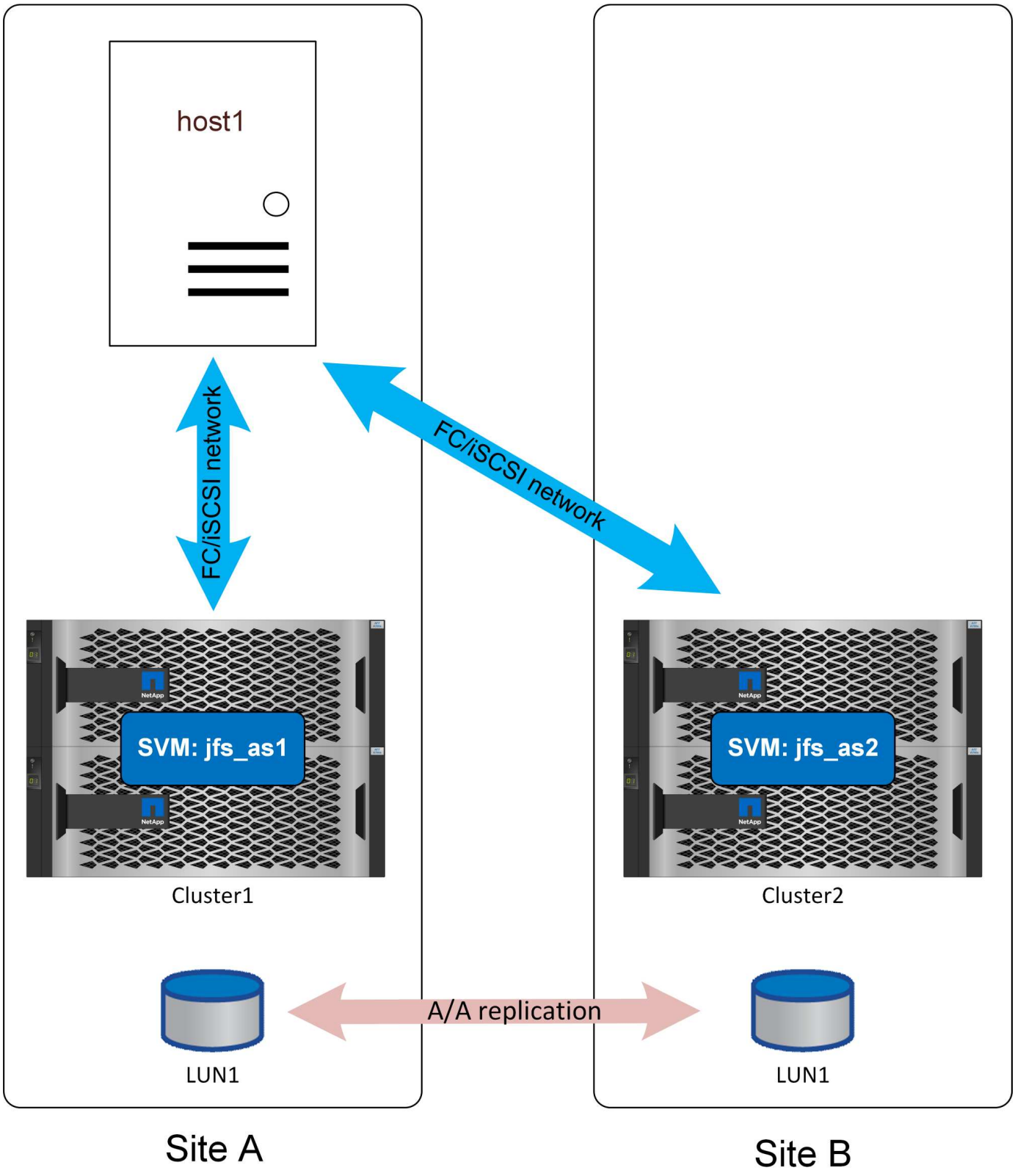
Descripción general

SQL Server se puede configurar para que funcione con la sincronización activa de SnapMirror de varias maneras. La respuesta correcta depende de la conectividad de red disponible, los requisitos de RPO y los requisitos de disponibilidad.

Instancia independiente de SQL Server

Las mejores prácticas para la distribución de archivos y la configuración del servidor son las mismas que se recomiendan en "SQL Server en ONTAP" la documentación.

Con una configuración independiente, SQL Server sólo podría ejecutarse en un sitio. Presumiblemente "uniforme"se utilizaría el acceso.



Gracias a un acceso uniforme, un fallo de almacenamiento en cualquiera de los sitios no interrumpía las operaciones de la base de datos. Un fallo completo del sitio en el sitio que incluyera el servidor de la base de datos, por supuesto, daría lugar a una interrupción del servicio.

Algunos clientes podrían configurar un sistema operativo que se ejecute en el sitio remoto con una configuración de SQL Server preconfigurada, actualizada con una versión de compilación equivalente a la de

la instancia de producción. La conmutación por error requeriría activar esa instancia independiente de SQL Server en la ubicación alternativa, detectar LAS LUN e iniciar la base de datos. El proceso completo puede automatizarse con el cmdlet de Windows PowerShell ya que no es necesario realizar operaciones en el almacenamiento.

"No uniforme" también se podía utilizar el acceso, pero el resultado sería una interrupción en la base de datos si se hubiera producido un error en el sistema de almacenamiento donde se encontraba el servidor de base de datos porque la base de datos no tendría rutas disponibles para el almacenamiento. Esto todavía puede ser aceptable en algunos casos. La sincronización activa de SnapMirror seguiría proporcionando protección de datos con objetivo de punto de recuperación = 0 y, en caso de fallo del sitio, la copia superviviente estaría activa y lista para reanudar las operaciones usando el mismo procedimiento usado con un acceso uniforme como se describió anteriormente.

Un proceso de conmutación por error simple y automatizado puede configurarse más fácilmente con el uso de un host virtualizado. Por ejemplo, si los archivos de datos de SQL Server se replican sincrónicamente en el almacenamiento secundario junto con un VMDK de arranque, entonces, en caso de desastre, el entorno completo podría activarse en el sitio alternativo. Un administrador puede activar manualmente el host en el sitio superviviente o automatizar el proceso mediante un servicio como la alta disponibilidad de VMware.

Instancia de cluster de failover de SQL Server

Las instancias de conmutación por error de SQL Server también se pueden alojar en un clúster de conmutación por error de Windows que se ejecute en un servidor físico o virtual como sistema operativo invitado. Esta arquitectura multihost proporciona flexibilidad de almacenamiento y instancia de SQL Server. Dicha puesta en marcha es útil en entornos con una gran demanda que buscan sólidos procesos de conmutación al respaldo y mantener un rendimiento mejorado. En una configuración de clúster de conmutación al nodo de respaldo, cuando un host o almacenamiento principal se ve afectado, SQL Services realizará una conmutación por error al host secundario; al mismo tiempo, el almacenamiento secundario estará disponible para prestar servicio de I/O. No se requiere ninguna secuencia de comandos de automatización ni intervención del administrador.

Escenarios de fallo

La planificación de una arquitectura completa de aplicaciones de sincronización activa de SnapMirror requiere comprender cómo SM-AS responderá en varias situaciones de conmutación por error planificadas e imprevistas.

Para los siguientes ejemplos, supongamos que el sitio A está configurado como el sitio preferido.

Pérdida de conectividad de replicación

Si se interrumpe la replicación de SM-AS, la E/S de escritura no se puede completar porque sería imposible que un clúster replique los cambios en el sitio opuesto.

Sitio A (Sitio preferido)

El resultado de un fallo del enlace de replicación en el sitio preferido será una pausa de aproximadamente 15 segundos en el procesamiento de I/O de escritura, ya que ONTAP reintenta las operaciones de escritura replicadas antes de que determine que el enlace de replicación es realmente inaccesible. Una vez transcurridos los 15 segundos, el sistema del sitio A reanuda el procesamiento de E/S de lectura y escritura. Las rutas de SAN no se modificarán y los LUN permanecerán en línea.

Centro B

Dado que el sitio B no es el sitio preferido de sincronización activa de SnapMirror, sus rutas de LUN dejarán de estar disponibles después de unos 15 segundos.

Fallo del sistema de almacenamiento

El resultado de un fallo del sistema de almacenamiento es casi idéntico al de perder el enlace de replicación. El sitio superviviente debería experimentar una pausa de IO de aproximadamente 15 segundos. Una vez transcurrido ese período de 15 segundos, IO se reanudará en ese sitio como de costumbre.

Pérdida del mediador

El servicio de mediador no controla directamente las operaciones de almacenamiento. Funciona como una ruta de control alternativa entre los clústeres. Existe principalmente para automatizar la conmutación al nodo de respaldo sin el riesgo de un escenario de cerebro dividido. En un funcionamiento normal, cada clúster está replicando los cambios en su compañero y, por lo tanto, cada clúster puede verificar que el clúster asociado esté en línea y sirviendo datos. Si el enlace de replicación falla, la replicación se detendría.

El motivo por el que se necesita un mediador para una conmutación por error automatizada segura es que, de otro modo, sería imposible que un clúster de almacenamiento pueda determinar si la pérdida de comunicación bidireccional se debió a una interrupción de la red o a un error real de almacenamiento.

El mediador proporciona una ruta alternativa para que cada clúster compruebe el estado de su compañero. Los escenarios son los siguientes:

- Si un clúster puede ponerse en contacto directamente con su socio, los servicios de replicación están operativos. No se requiere ninguna acción.
- Si un sitio preferido no puede ponerse en contacto con su partner directamente o a través del mediador, se asumirá que el partner no está disponible o que se ha aislado y ha desconectado las rutas de LUN. El sitio preferido procederá a liberar el estado RPO=0 y continuará procesando las I/O de lectura y escritura.
- Si un sitio no preferido no puede ponerse en contacto directamente con su socio, pero puede contactarlo a través del mediador, tomará sus rutas fuera de línea y esperará la devolución de la conexión de replicación.
- Si un sitio no preferido no puede contactar a su partner directamente o a través de un mediador operativo, asumirá que el partner no está disponible o que se ha aislado y ha desconectado las rutas de LUN. El sitio no preferido continuará liberando el estado RPO=0 y continuará procesando las I/O de lectura y escritura. Asumirá el rol del origen de replicación y se convertirá en el nuevo sitio preferido.

Si el mediador no está totalmente disponible:

- El fallo en los servicios de replicación por cualquier motivo, incluido el fallo del sitio o del sistema de almacenamiento no preferido, provocará que el sitio preferido libere el estado RPO=0 y reanude el procesamiento de I/O de lectura y escritura. El sitio no preferido desconectará sus rutas.
- Un fallo del sitio preferido provocará una interrupción porque el sitio no preferido no podrá verificar que el sitio opuesto esté realmente fuera de línea y, por lo tanto, no sería seguro para el sitio no preferido reanudar los servicios.

Restauración de servicios

Tras resolver un fallo, como restaurar la conectividad de sitio a sitio o encender un sistema fallido, los extremos de sincronización activa de SnapMirror detectan automáticamente la presencia de una relación de replicación defectuosa y la devuelven a un estado RPO=0. Una vez que se restablece la replicación síncrona,

las rutas fallidas volverán a conectarse.

En muchos casos, las aplicaciones en clúster detectan automáticamente el retorno de las rutas fallidas, y dichas aplicaciones también volverán a estar online. En otros casos, puede ser necesario un análisis SAN a nivel de host o es posible que las aplicaciones deban volver a conectarse manualmente. Depende de la aplicación y cómo se configura, y en general tales tareas se pueden automatizar fácilmente. El propio ONTAP se repara automáticamente y no debería requerir la intervención del usuario para reanudar las operaciones de almacenamiento RPO=0.

Recuperación manual tras fallos

Cambiar el sitio preferido requiere una operación simple. I/O se detendrá durante un segundo o dos como autoridad sobre los cambios en el comportamiento de replicación entre los clústeres, pero I/O de otro modo no se verá afectado.

Configuración de almacenamiento en sistemas ASA R2

Descripción general

El sistema NetApp ASA R2 es una potente solución simplificada para clientes solo SAN que ejecutan cargas de trabajo esenciales. La combinación de la plataforma ASA R2 que ejecuta soluciones de almacenamiento de ONTAP y Microsoft SQL Server posibilita diseños de almacenamiento de bases de datos de nivel empresarial que satisfacen los requisitos de las aplicaciones más exigentes actuales.

Las siguientes plataformas ASA se clasifican como sistemas ASA R2 que admiten todos los protocolos SAN (iSCSI, FC, NVMe/FC y NVMe/TCP). Los protocolos iSCSI, FC, NVMe/FC y NVMe/TCP admiten una arquitectura activo-activo simétrica para multivía, de modo que todas las rutas entre los hosts y el almacenamiento estén activas/optimizadas:

- ASA A1K
- ASA A90
- ASA A70
- ASA A50
- ASA A30
- ASA A20

Para obtener más información, consulte "ASA de NetApp"

La optimización de una solución SQL Server en ONTAP requiere comprender el patrón y las características de E/S de SQL Server. Una buena distribución del almacenamiento para una base de datos de SQL Server debe soportar los requisitos de rendimiento de SQL Server y proporcionar la máxima capacidad de gestión de la infraestructura en su conjunto. Una buena distribución de almacenamiento también permite que la puesta en marcha inicial tenga éxito y que el entorno crezca sin problemas con el tiempo a medida que crece el negocio.

Diseño de almacenamiento de datos

Microsoft recomienda colocar los archivos de datos y de registro en unidades separadas. Para las aplicaciones que actualizan y solicitan datos simultáneamente, el archivo de registro tiene un gran consumo de escrituras y el archivo de datos (en función de la aplicación) tiene un gran volumen de lecturas y escrituras.

Para la recuperación de datos, el archivo de registro no es necesario. Por lo tanto, las solicitudes de datos pueden satisfacerse desde el archivo de datos ubicado en su propia unidad.

Cuando se crea una nueva base de datos, Microsoft recomienda especificar unidades independientes para los datos y los registros. Para mover archivos después de crear la base de datos, ésta debe desconectarse. Para obtener más recomendaciones de Microsoft, consulte "Coloque los archivos de datos y de registro en unidades separadas".

Consideraciones sobre la unidad de almacenamiento

La unidad de almacenamiento en ASA hace referencia a la LUN para hosts SCSI/FC o un espacio de nombres NVMe para hosts NVMe. Según el protocolo compatible, se le pedirá que cree LUN, espacio de nombres NVMe o ambos. Antes de crear una unidad de almacenamiento para la implementación de la base de datos, es importante comprender cómo varían las características y el patrón de I/O de SQL Server en función de la carga de trabajo y de los requisitos de backup y recuperación. Consulte las siguientes recomendaciones NetApp para la unidad de almacenamiento:

- Evite compartir la misma unidad de almacenamiento entre varias instancias de SQL Server que se ejecutan en el mismo host para evitar que la gestión resulte complicada. En el caso de ejecutar varias instancias de SQL Server en el mismo host, a menos que esté cerca del límite de unidades de almacenamiento en un nodo, evite el uso compartido y disponga en su lugar de una unidad de almacenamiento separada por instancia y cada host para facilitar la gestión de datos.
- Utilice puntos de montaje NTFS en lugar de letras de unidad para superar la limitación de 26 unidades en Windows.
- Deshabilite las programaciones de Snapshot y las políticas de retención. En su lugar, utilice SnapCenter para coordinar las copias Snapshot de la unidad de almacenamiento de datos de SQL Server.
- Coloque las bases de datos del sistema de SQL Server en una unidad de almacenamiento dedicada.
- Tempdb es una base de datos del sistema utilizada por SQL Server como espacio de trabajo temporal, especialmente para operaciones DBCC CHECKDB intensivas en E/S. Por lo tanto, coloque esta base de datos en una unidad de almacenamiento dedicada. En entornos de gran tamaño en los que el recuento de unidades de almacenamiento supone un reto, puede consolidar tempdb con bases de datos del sistema en la misma unidad de almacenamiento después de una planificación cuidadosa. La protección de datos para tempdb no es una prioridad alta porque esta base de datos se vuelve a crear cada vez que se reinicia SQL Server.
- Colocar archivos de datos de usuario (`.mdf`) en una unidad de almacenamiento separada porque son cargas de trabajo de lectura/escritura aleatorias. Es común crear backups de registros de transacciones con más frecuencia que los backups de bases de datos. Por este motivo, coloque los archivos de registro de transacciones (`.ldf`) en una unidad de almacenamiento o VMDK separados de los archivos de datos para que puedan crearse programaciones de backup independientes para cada uno. Esta separación también aísla la E/S de escritura secuencial de los archivos de registro de la E/S de lectura/escritura aleatoria de los archivos de datos y mejora significativamente el rendimiento de SQL Server.
- Asegúrese de que los archivos de la base de datos de usuario y el directorio de registro para almacenar la copia de seguridad de registros se encuentran en una unidad de almacenamiento independiente para evitar que la política de retención sobrescriba las instantáneas cuando se utilizan con la función SnapMirror con la política de almacén.
- No mezcle archivos de base de datos ni archivos que no sean de base de datos, como archivos relacionados con la búsqueda de texto completo, en la misma unidad de almacenamiento.
- La colocación de archivos secundarios de base de datos (como parte de un grupo de archivos) en una unidad de almacenamiento independiente mejora el rendimiento de la base de datos de SQL Server. Esta separación es válida sólo si el archivo de la base de datos `.mdf` no comparte su unidad de almacenamiento con ningún otro `.mdf` archivo.

- Al formatear el disco mediante el administrador de discos en el servidor Windows, asegúrese de que el tamaño de la unidad de asignación esté establecido en 64K para la partición.
- No coloque bases de datos de usuario ni bases de datos del sistema en una unidad de almacenamiento que aloje puntos de montaje.
- Consulte "Microsoft Windows e MPIO nativo bajo las prácticas recomendadas de ONTAP para SAN moderna" Para aplicar la compatibilidad con accesos múltiples en Windows a dispositivos iSCSI en las propiedades MPIO.
- Si utiliza una instancia de clúster de conmutación al nodo de respaldo Always On, las bases de datos de usuario deben colocarse en una unidad de almacenamiento compartida entre los nodos de clúster de conmutación al nodo de respaldo del servidor Windows y los recursos del clúster de discos físicos se asignan al grupo de clústeres asociado con la instancia de SQL Server.

Archivos de base de datos y grupos de archivos

La ubicación correcta del archivo de la base de datos de SQL Server en ONTAP es crítica durante la etapa de la implementación inicial. Esto garantiza un rendimiento óptimo, gestión del espacio, tiempos de backup y restauración que pueden configurarse para que se ajusten a sus necesidades empresariales.

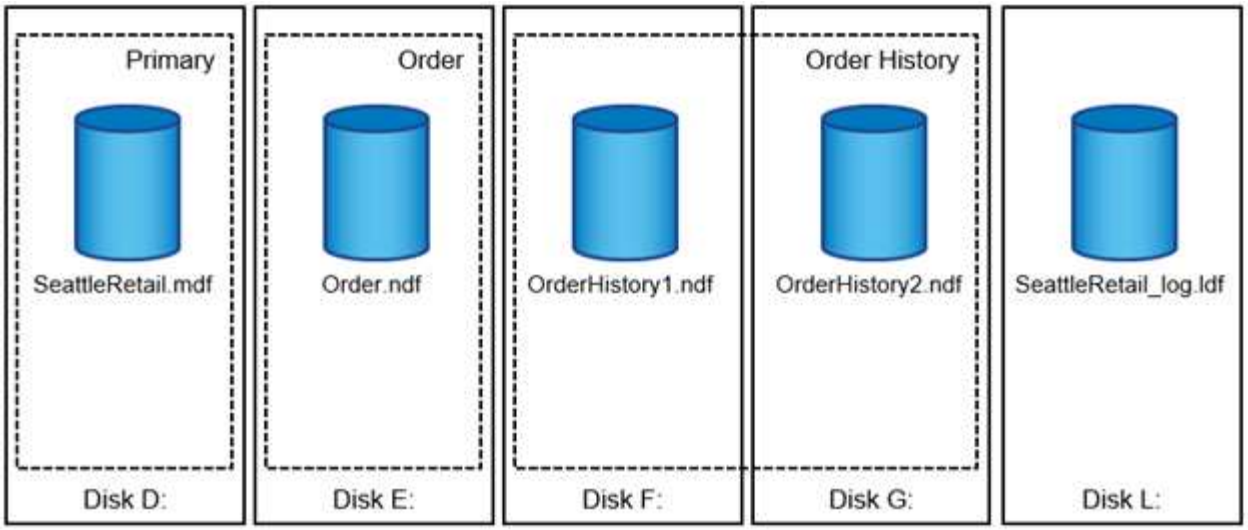
En teoría, SQL Server (64 bits) admite 32.767 bases de datos por instancia y 524.272TB GB de tamaño de base de datos, aunque la instalación típica suele tener varias bases de datos. Sin embargo, el número de bases de datos que SQL Server puede manejar depende de la carga y el hardware. No es raro ver instancias de SQL Server que alojan docenas, cientos o incluso miles de pequeñas bases de datos.

Archivos y grupo de archivos de bases de datos

Cada base de datos consta de uno o más archivos de datos y uno o varios archivos de registro de transacciones. El log de transacciones almacena la información sobre las transacciones de la base de datos y todas las modificaciones de datos realizadas por cada sesión. Cada vez que se modifican los datos, SQL Server almacena suficiente información en el log de transacciones para deshacer (realizar rollback) o rehacer (reproducir) la acción. Un registro de transacciones de SQL Server es una parte esencial de la reputación de SQL Server en cuanto a integridad y solidez de los datos. El registro de transacciones es vital para las capacidades de atomicidad, consistencia, aislamiento y durabilidad (ACID) de SQL Server. SQL Server escribe en el registro de transacciones tan pronto como se producen cambios en la página de datos. Cada sentencia de lenguaje de manipulación de datos (DML) (por ejemplo, SELECT, INSERT, UPDATE o DELETE) es una transacción completa, y el registro de transacciones se asegura de que se realice toda la operación basada en juegos, asegurándose de la atomicidad de la transacción.

Cada base de datos tiene un archivo de datos primario, que, por defecto, tiene la extensión .mdf. Además, cada base de datos puede tener archivos de base de datos secundarios. Esos archivos, por defecto, tienen extensiones .ndf.

Todos los archivos de base de datos se agrupan en grupos de archivos. Un grupo de archivos es la unidad lógica, que simplifica la administración de la base de datos. Permiten la separación entre la ubicación de objetos lógicos y los archivos físicos de la base de datos. Al crear las tablas de objetos de base de datos, especifique en qué grupo de archivos se deben colocar sin preocuparse por la configuración del archivo de datos subyacente.



La capacidad de colocar varios archivos de datos dentro del grupo de archivos permite distribuir la carga entre diferentes dispositivos de almacenamiento, lo que ayuda a mejorar el rendimiento de I/O del sistema. Por el contrario, el registro de transacciones no se beneficia de los varios archivos, ya que SQL Server escribe en el registro de transacciones de forma secuencial.

La separación entre la ubicación de objetos lógicos en los grupos de archivos y los archivos físicos de la base de datos le permite ajustar el diseño del archivo de la base de datos, aprovechando al máximo el subsistema de almacenamiento. La cantidad de archivos de datos que soportan una carga de trabajo maestra se puede modificar según sea necesario para admitir los requisitos de I/O y la capacidad esperada sin afectar a la aplicación. Esas variaciones en el diseño de la base de datos son transparentes para los desarrolladores de aplicaciones, que colocan los objetos de la base de datos en los grupos de archivos en lugar de en los archivos de la base de datos.

NetApp recomienda evitar el uso del grupo de archivos primario para cualquier cosa excepto objetos del sistema. La creación de un grupo de archivos independiente o un conjunto de grupos de archivos para los objetos de usuario simplifica la administración de la base de datos y la recuperación ante desastres, especialmente en el caso de bases de datos grandes.

Inicialización del archivo de instancia de base de datos

Puede especificar el tamaño inicial del archivo y los parámetros de crecimiento automático en el momento de crear la base de datos o agregar nuevos archivos a una base de datos existente. SQL Server utiliza un algoritmo de relleno proporcional al elegir en qué archivo de datos debe escribir los datos. Escribe una cantidad de datos proporcionalmente al espacio libre disponible en los archivos. Cuanto mayor sea el espacio libre del archivo, más escrituras gestionará.

NetApp recomienda que todos los archivos en un solo grupo de archivos tengan los mismos parámetros iniciales de tamaño y crecimiento automático, con el tamaño de crecimiento definido en megabytes en lugar de porcentajes. Esto ayuda al algoritmo de relleno proporcional a equilibrar de forma uniforme las actividades de escritura en los archivos de datos.

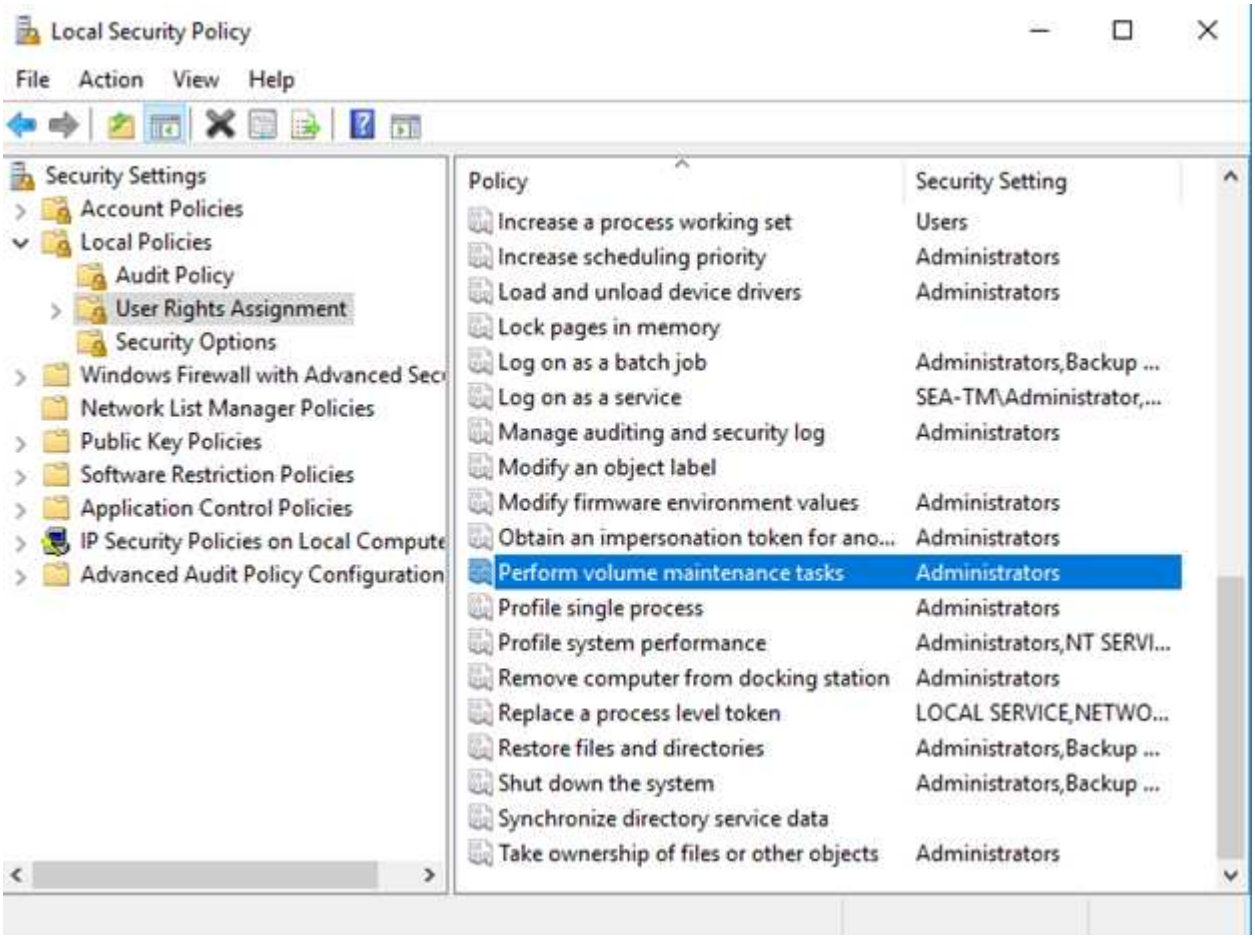
Cada vez que SQL Server crece archivos, llena el espacio recién asignado con ceros. Este proceso bloquea todas las sesiones que necesitan escribir en el archivo correspondiente o, en caso de crecimiento del log de transacciones, generar registros de log de transacciones.

SQL Server siempre pone a cero el registro de transacciones y ese comportamiento no se puede cambiar. Sin embargo, puede controlar si los archivos de datos están a cero habilitando o deshabilitando la inicialización

instantánea de archivos. La activación de la inicialización instantánea de archivos ayuda a acelerar el crecimiento de los archivos de datos y reduce el tiempo necesario para crear o restaurar la base de datos.

Un pequeño riesgo de seguridad está asociado con la inicialización instantánea de archivos. Cuando esta opción está activada, las partes no asignadas del archivo de datos pueden contener información de los archivos del sistema operativo eliminados anteriormente. Los administradores de bases de datos pueden examinar estos datos.

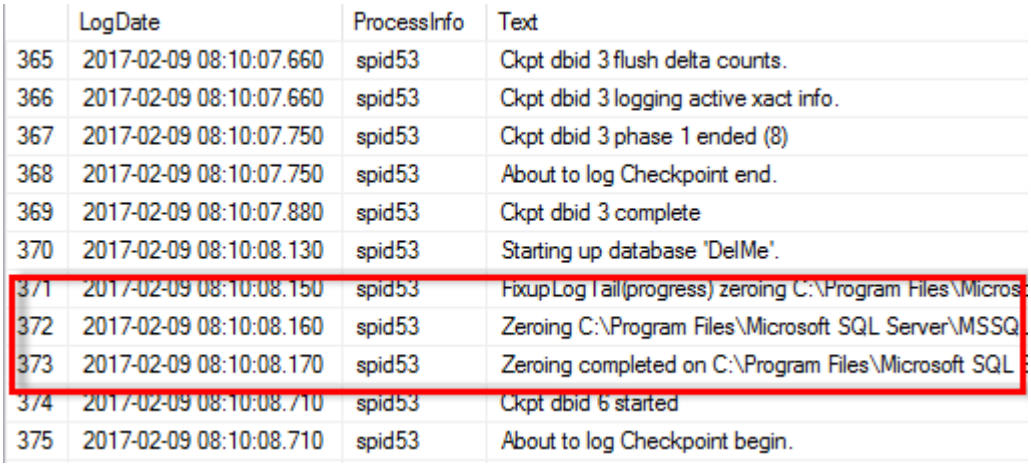
Puede activar la inicialización instantánea de archivos agregando el permiso SA_MANAGE_VOLUME_NAME, también conocido como “Realizar tarea de mantenimiento de volúmenes”, a la cuenta de inicio de SQL Server. Puede hacerlo en la aplicación de gestión de políticas de seguridad local (secpol.msc), como se muestra en la siguiente figura. Abra las propiedades del permiso “Realizar tarea de mantenimiento de volúmenes” y agregue la cuenta de inicio de SQL Server a la lista de usuarios allí.



Para comprobar si el permiso está habilitado, puede utilizar el código del siguiente ejemplo. Este código establece dos indicadores de rastreo que obligan a SQL Server a escribir información adicional en el log de errores, crear una base de datos pequeña y leer el contenido del log.

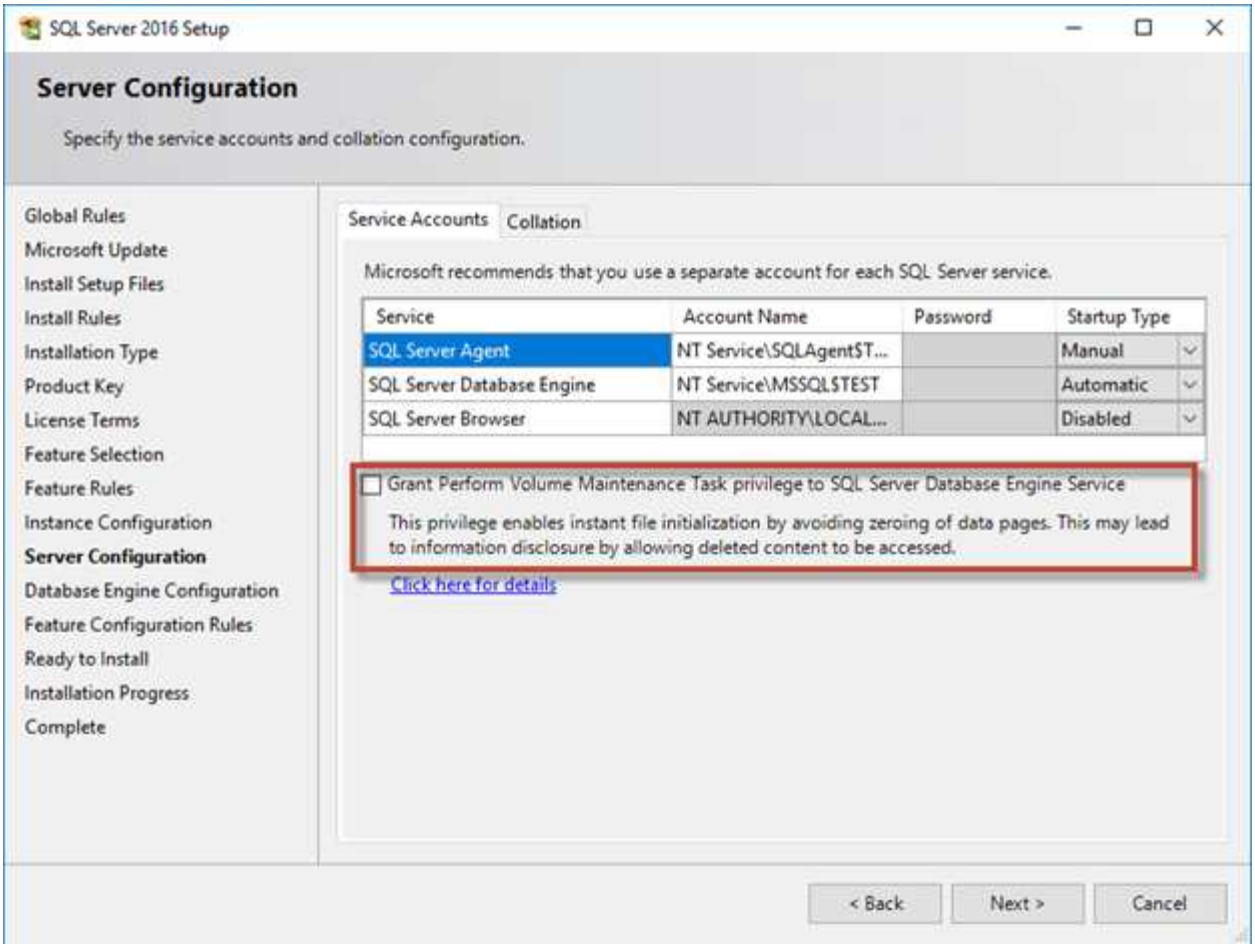
```
DBCC TRACEON(3004,3605,-1)
GO
CREATE DATABASE DelMe
GO
EXECUTE sp_readerrorlog
GO
DROP DATABASE DelMe
GO
DBCC TRACEOFF(3004,3605,-1)
GO
```

Cuando la inicialización instantánea de archivos no está activada, el registro de errores de SQL Server muestra que SQL Server pone a cero el archivo de datos de mdf además de poner a cero el archivo log ldf, como se muestra en el siguiente ejemplo. Cuando se activa la inicialización instantánea del archivo, sólo se muestra la puesta a cero del archivo log.



	LogDate	ProcessInfo	Text
365	2017-02-09 08:10:07.660	spid53	Ckpt dbid 3 flush delta counts.
366	2017-02-09 08:10:07.660	spid53	Ckpt dbid 3 logging active xact info.
367	2017-02-09 08:10:07.750	spid53	Ckpt dbid 3 phase 1 ended (8)
368	2017-02-09 08:10:07.750	spid53	About to log Checkpoint end.
369	2017-02-09 08:10:07.880	spid53	Ckpt dbid 3 complete
370	2017-02-09 08:10:08.130	spid53	Starting up database 'DelMe'.
371	2017-02-09 08:10:08.150	spid53	FixupLog Tail(progress) zeroing C:\Program Files\Micros
372	2017-02-09 08:10:08.160	spid53	Zeroing C:\Program Files\Microsoft SQL Server\MSSQ
373	2017-02-09 08:10:08.170	spid53	Zeroing completed on C:\Program Files\Microsoft SQL
374	2017-02-09 08:10:08.710	spid53	Ckpt dbid 6 started
375	2017-02-09 08:10:08.710	spid53	About to log Checkpoint begin.

La tarea Realizar mantenimiento de volumen se simplifica en SQL Server 2016 y, posteriormente, se proporciona como opción durante el proceso de instalación. Esta figura muestra la opción para otorgar al servicio del motor de base de datos SQL Server el privilegio para realizar la tarea de mantenimiento de volúmenes.



Otra opción importante de la base de datos que controla los tamaños de los archivos de la base de datos es la reducción automática. Cuando esta opción está habilitada, SQL Server reduce regularmente los archivos de la base de datos, reduce su tamaño y libera espacio al sistema operativo. Esta operación consume muchos recursos y rara vez es útil porque los archivos de la base de datos vuelven a crecer después de un tiempo cuando llegan nuevos datos al sistema. La reducción automática no debe estar activada en la base de datos.

Directorio de registro

El directorio de registro se especifica en SQL Server para almacenar datos de backup de registros de transacciones en el nivel de host. Si utiliza SnapCenter para realizar backup de archivos de registro, cada host SQL Server que utiliza SnapCenter debe tener un directorio de registro de host configurado para realizar backups de registros.

Coloque el directorio de registro en una unidad de almacenamiento dedicada. La cantidad de datos en el directorio de registro del host depende del tamaño de los backups y de la cantidad de días que se retienen los backups. SnapCenter solo permite un directorio de registro de host por cada host SQL Server. Puede configurar los directorios de registro de host en SnapCenter -⟶ Host -⟶ Configurar el plugin.

NetApp recomienda lo siguiente para un directorio de registro de host:

- Asegúrese de que el directorio de registro de host no esté compartido por ningún otro tipo de datos que pueda dañar los datos de la instantánea de backup.
- Cree el directorio de registro de host en una unidad de almacenamiento dedicada a la que SnapCenter copia los registros de transacciones.
- Si va a utilizar una instancia de clúster de conmutación al nodo de respaldo Always On, la unidad de almacenamiento utilizada para el directorio de registro de host debe ser un recurso de disco de clúster en el mismo grupo de clústeres que la instancia de SQL Server que se incluirá en un backup en SnapCenter.

Protección de datos

Las estrategias de backup de bases de datos se deben basar en requisitos del negocio identificados, no en capacidades teóricas. Al combinar la tecnología Snapshot de ONTAP y aprovechar las API de Microsoft SQL Server, puede realizar rápidamente backup consistente con las aplicaciones independientemente del tamaño de las bases de datos del usuario. Para obtener requisitos de gestión de datos más avanzados o de escalado horizontal, NetApp ofrece SnapCenter.

SnapCenter

SnapCenter es el software de protección de datos de NetApp para aplicaciones empresariales. Las bases de datos de SQL Server pueden protegerse de forma rápida y fácil con el complemento de SnapCenter para SQL Server y con operaciones de sistema operativo gestionadas por el plugin de SnapCenter para Microsoft Windows.

La instancia de SQL Server puede ser una configuración independiente, una instancia de clúster de conmutación por error o puede estar siempre en un grupo de disponibilidad. El resultado es que, a partir de un solo panel, las bases de datos pueden protegerse, clonarse y restaurarse a partir de copias principales o secundarias. SnapCenter puede gestionar bases de datos de SQL Server tanto en las instalaciones, en el cloud como en configuraciones híbridas.Las copias de bases de datos también se pueden crear en pocos minutos en el host original o alternativo para fines de desarrollo o generación de informes.

SQL Server también requiere coordinación entre el SO y el almacenamiento para garantizar que los datos correctos están presentes en las snapshots en el momento de la creación. En la mayoría de los casos, el único método seguro para hacerlo es con SnapCenter o T-SQL. Es posible que las instantáneas creadas sin esta coordinación adicional no se puedan recuperar de forma fiable.

Para obtener más detalles sobre el plugin de SQL Server para SnapCenter, consulte "TR-4714: Guía de mejores prácticas para SQL Server con NetApp SnapCenter".

Protección de la base de datos mediante instantáneas de T-SQL

En SQL Server 2022, Microsoft introdujo las copias Snapshot de T-SQL que ofrecen una ruta para el scripting y la automatización de las operaciones de backup. En lugar de realizar copias de tamaño completo, puede preparar la base de datos para instantáneas. Una vez que la base de datos está lista para el backup, se pueden aprovechar las API DE REST DE ONTAP para crear snapshots.

A continuación, se muestra un flujo de trabajo de backup de ejemplo:

1. Congelar una base de datos con el comando ALTER. Esto prepara la base de datos para una instantánea coherente en el almacenamiento subyacente. Después de congelar, puede descongelar la base de datos y registrar la instantánea con el comando BACKUP.
2. Realice copias Snapshot de varias bases de datos en las unidades de almacenamiento de forma simultánea con los nuevos comandos DEL GRUPO DE BACKUP y DEL SERVIDOR DE BACKUP.
3. Si la carga de trabajo de la base de datos se extiende en varias unidades de almacenamiento, cree grupos de coherencia para simplificar la tarea de gestión. El grupo de consistencia es una colección de unidades de almacenamiento que se administran como una sola unidad.
4. Realice copias de seguridad COMPLETAS o copias de seguridad COMPLETAS COPY_ONLY. Estas copias de seguridad también se registran en msdb.
5. Llevar a cabo una recuperación puntual mediante backups de registro realizados con el método de streaming normal después del backup COMPLETO de la instantánea. Las copias de seguridad diferenciales de transmisión también se admiten si se desea.

Para obtener más información, consulte "Documentación de Microsoft para conocer las instantáneas de T-SQL".

NetApp recomienda usar SnapCenter para crear copias snapshot. También funciona el método T-SQL descrito anteriormente, pero SnapCenter ofrece una automatización completa del proceso de backup, restauración y clonación. También realiza una detección para garantizar que se crean las snapshots correctas.

Utilice SnapCenter si las bases de datos de SQL Server están alojadas en un disco virtual que se ejecute en un entorno virtualizado de VMware. En caso de que las bases de datos se alojen en un servidor físico de configuración básica o en un SCSI de conexión para invitados, realice una copia de seguridad de la base de datos mediante el comando T-SQL snapshot.

Recuperación tras siniestros

Recuperación tras siniestros

Las bases de datos empresariales y las infraestructuras de aplicaciones a menudo requieren la replicación para protegerse de desastres naturales o de la interrupción inesperada del negocio con un tiempo de inactividad mínimo.

La función de replicación de grupos de disponibilidad siempre disponible de SQL Server puede ser una opción excelente, y NetApp ofrece opciones para integrar la protección de datos con disponibilidad permanente. Sin embargo, en algunos casos es posible que desee considerar la tecnología de replicación de ONTAP mediante las siguientes opciones.

SnapMirror

La tecnología SnapMirror ofrece una solución empresarial rápida y flexible para replicar datos en LAN y WAN. La tecnología SnapMirror solo transfiere los bloques de datos modificados al destino una vez que se creó el reflejo inicial, lo que reduce considerablemente los requisitos de ancho de banda de la red. Puede configurarse tanto en modo síncrono como asíncrono. La replicación síncrona de SnapMirror en NetApp ASA se configura mediante la sincronización activa de SnapMirror.

SnapMirror síncrono activo

Para muchos clientes, la continuidad empresarial requiere algo más que la mera posesión de una copia remota de los datos, requiere la capacidad de utilizar rápidamente los datos, lo que es posible en NetApp ONTAP mediante la sincronización activa de SnapMirror

Con la sincronización activa de SnapMirror, básicamente cuenta con dos sistemas ONTAP diferentes que mantienen copias independientes de los datos de su unidad lógica, pero que cooperan para presentar una única instancia de esa LUN. Desde el punto de vista del host, se trata de una única entidad de LUN. La sincronización activa de SnapMirror es compatible con LUN basado en iSCSI/FC.

La sincronización activa de SnapMirror puede proporcionar replicación RPO=0 y es fácil implementarla entre dos clústeres independientes.Una vez que las dos copias de datos están sincronizadas, los dos clústeres solamente deben reflejar escrituras. Cuando se produce una escritura en un clúster, se replica en otro clúster. La escritura solo se reconoce en el host cuando la escritura se ha completado en ambos sitios. Aparte de este comportamiento de división del protocolo, los dos clústeres son clústeres ONTAP normales.

Un caso de uso clave de SM-AS es la replicación granular. En ocasiones, no desea replicar todos los datos como una sola unidad, o debe poder conmutar al nodo de respaldo de forma selectiva ciertas cargas de trabajo.

Otro caso de uso clave de SM-AS es en las operaciones activo-activo, donde desea que existan copias de datos totalmente utilizables para estar disponibles en dos clústeres diferentes ubicados en dos ubicaciones diferentes con idénticas características de rendimiento y, si lo desea, no es necesario ampliar la SAN entre los sitios. Puede tener sus aplicaciones ya ejecutándose en ambos sitios, siempre que sea compatible con las aplicaciones, lo que reduce el RTO general durante las operaciones de conmutación al respaldo.

SnapMirror

Las siguientes son recomendaciones para SnapMirror para SQL Server:

- Utilice la replicación síncrona con SnapMirror Active Sync donde la demanda de una recuperación de datos rápida sea mayor y las soluciones asíncronas para obtener flexibilidad en un objetivo de punto de recuperación.
- Si utiliza SnapCenter para realizar backup de bases de datos y replicar snapshots en un clúster remoto, no programe actualizaciones de SnapMirror desde las controladoras con fines de consistencia. En lugar de eso, habilite las actualizaciones de SnapMirror desde SnapCenter para actualizar SnapMirror después de haber completado el backup completo o de registro.
- Equilibre las unidades de almacenamiento que contienen datos de SQL Server en diferentes nodos del clúster para permitir que todos los nodos del clúster compartan la actividad de replicación de SnapMirror. Esta distribución optimiza el uso de los recursos de los nodos.

Para obtener más información acerca de SnapMirror, consulte "TR-4015: Guía de configuración de SnapMirror y prácticas recomendadas para ONTAP 9".

SnapMirror síncrono activo

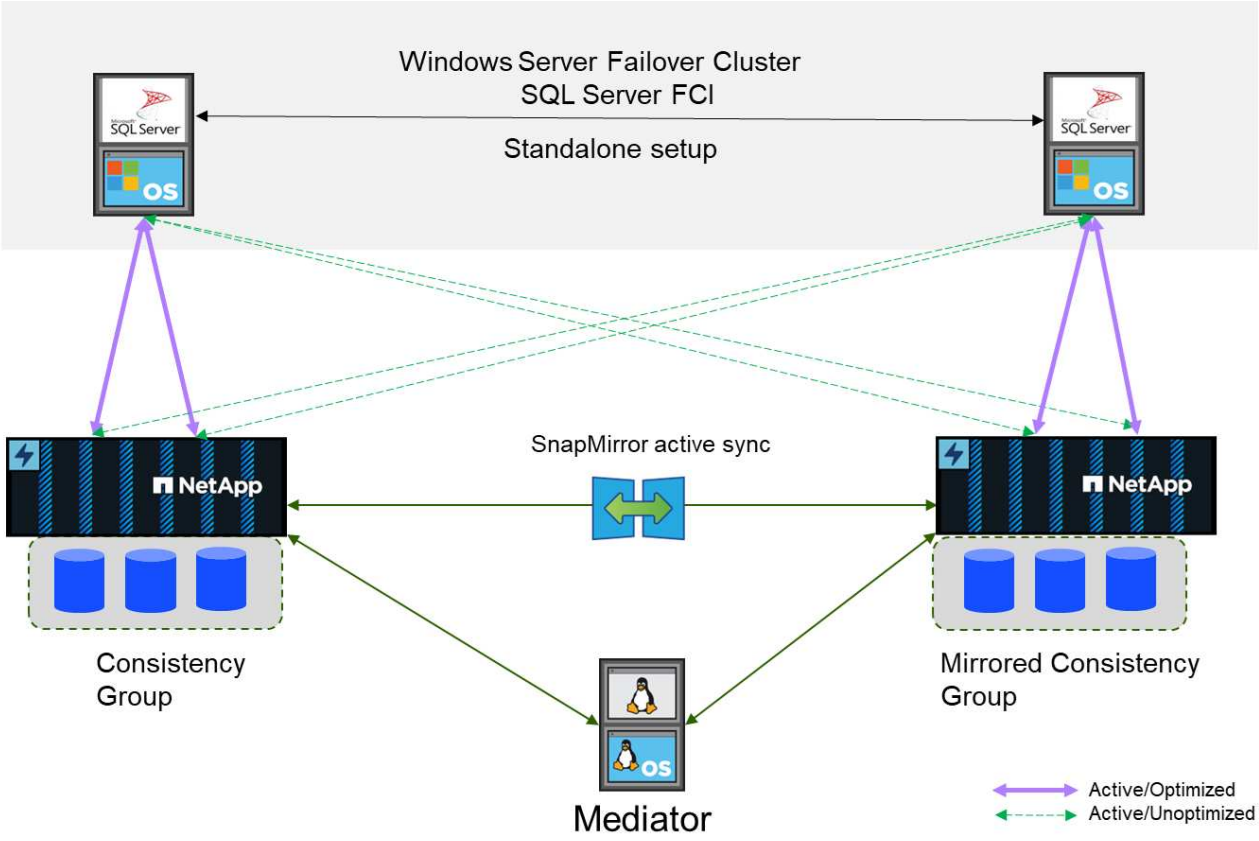
Descripción general

La sincronización activa de SnapMirror permite que las aplicaciones y bases de datos individuales de SQL Server continúen las operaciones durante interrupciones de las redes y el almacenamiento, con conmutación al respaldo transparente del almacenamiento sin intervención manual.

El modo Active Sync de SnapMirror admite arquitecturas activo-activo simétricas que proporciona replicación síncrona bidireccional para la continuidad del negocio y la recuperación ante desastres. Le ayuda a proteger el acceso a los datos para cargas de trabajo SAN críticas con acceso de lectura y escritura simultáneo a los datos en varios dominios de fallo, lo que garantiza operaciones ininterrumpidas y minimiza el tiempo de inactividad durante desastres o fallos del sistema.

Los hosts SQL Server acceden al almacenamiento a través de LUN de Fibre Channel (FC) o iSCSI. Replicación entre cada clúster que aloja una copia de los datos replicados. Dado que esta función es la replicación de nivel de almacenamiento, las instancias de SQL Server que se ejecutan en instancias de clúster de conmutación por error o host independiente pueden realizar operaciones de lectura/escritura en cualquier clúster. Para obtener información sobre los pasos de planificación y configuración, consulte "Documentación de ONTAP en sincronización activa de SnapMirror" .

Arquitectura de SnapMirror activo con activo-activo simétrico



Replicación síncrona

En condiciones de funcionamiento normal, cada copia es una réplica síncrona RPO=0 en todo momento, con una excepción. Si los datos no se pueden replicar, ONTAP liberará el requisito para replicar datos y reanudar el servicio de I/O en un sitio mientras las LUN del otro sitio se desconecten.

Hardware de almacenamiento

Al contrario que otras soluciones de recuperación ante desastres del almacenamiento, SnapMirror Active Sync ofrece una flexibilidad de plataforma asimétrica. No es necesario que el hardware de cada sitio sea idéntico. Esta funcionalidad permite ajustar el tamaño adecuado del hardware que se utiliza para dar soporte a SnapMirror de sincronización activa. El sistema de almacenamiento remoto puede ser idéntico al sitio principal si necesita soportar una carga de trabajo de producción completa, pero si un desastre provoca una reducción

de I/O, es posible que un sistema más pequeño en el sitio remoto sea más rentable.

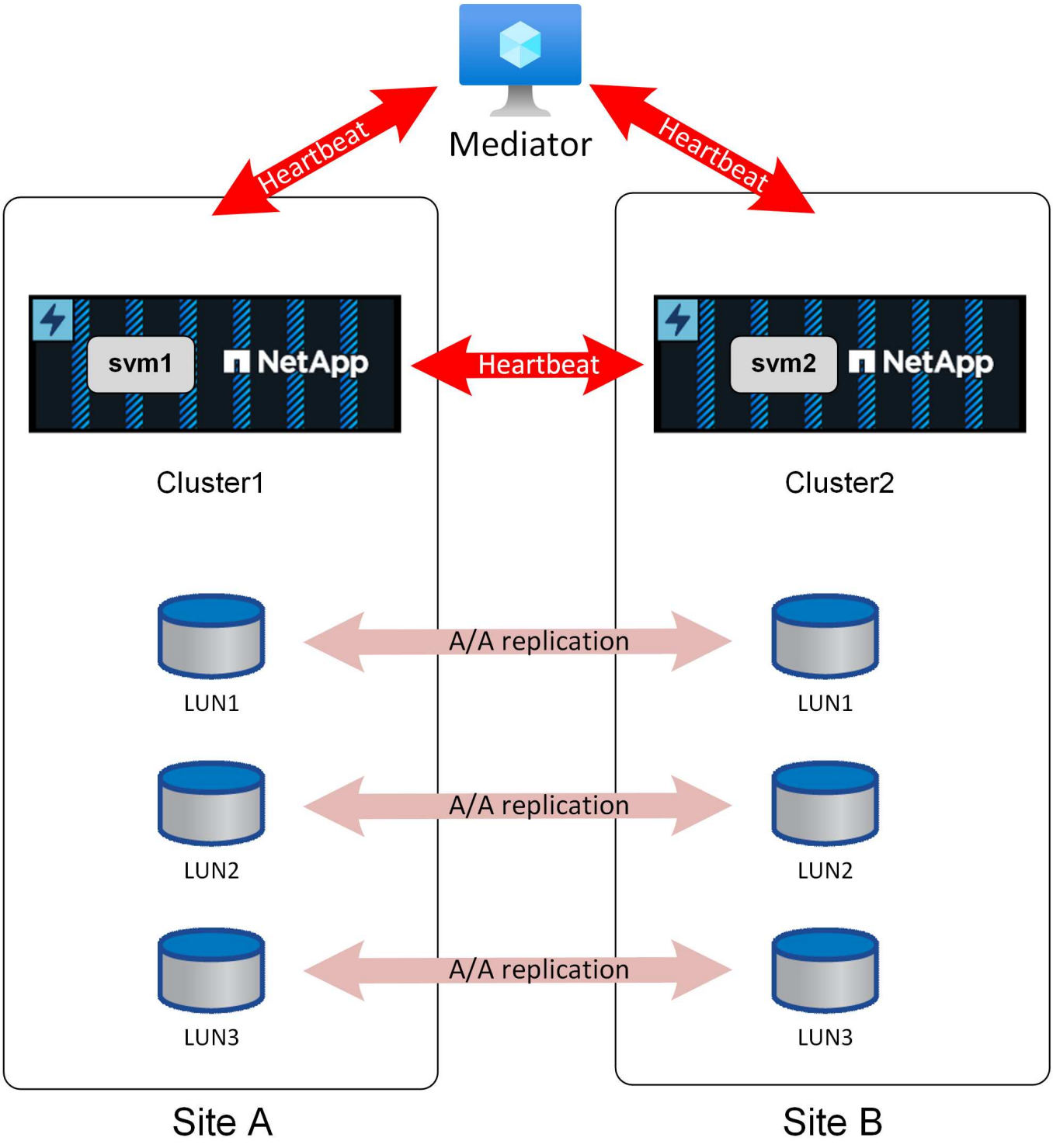
Mediador ONTAP

ONTAP Mediator es una aplicación de software que se descarga del soporte técnico de NetApp y que normalmente se implementa en una pequeña máquina virtual. El Mediador ONTAP no es un desempate. Es un canal de comunicación alternativo para los dos clústeres que participan en la replicación síncrona activa de SnapMirror. Las operaciones automatizadas son impulsadas por ONTAP en función de las respuestas recibidas del partner a través de conexiones directas y a través del mediador.

Mediador ONTAP

El mediador es necesario para automatizar la conmutación por error de forma segura. Lo ideal sería que se ubicara en un sitio 3rd independiente, pero todavía puede funcionar para la mayoría de las necesidades si se ubicara con uno de los clústeres que participan en la replicación.

El mediador no es realmente un desempate, aunque esa es efectivamente la función que proporciona. No realiza ninguna acción, sino que proporciona un canal de comunicación alternativo para la comunicación del clúster al clúster.



El desafío #1 con la conmutación automática por error es el problema de cerebro dividido, y ese problema surge si sus dos sitios pierden conectividad entre sí. ¿Qué debería pasar? No desea que dos sitios diferentes se designen a sí mismos como copias supervivientes de los datos, pero ¿cómo puede un solo sitio diferenciar entre la pérdida real del sitio opuesto y la incapacidad de comunicarse con el sitio opuesto?

Aquí es donde el mediador entra en la imagen. Si se coloca en un sitio 3rd y cada sitio tiene una conexión de red independiente con ese sitio, tiene una ruta adicional para que cada sitio valide el estado del otro. Mire la imagen de arriba otra vez y considere los siguientes escenarios.

- ¿Qué sucede si el mediador falla o es inaccesible desde uno o ambos sitios?
  - Los dos clústeres pueden comunicarse entre sí a través del mismo enlace utilizado para los servicios de replicación.
  - Los datos se siguen ofreciendo con la protección RPO=0
- ¿Qué sucede si falla el sitio A?
  - El sitio B verá que ambos canales de comunicación se caen.
  - El sitio B se hará cargo de los servicios de datos, pero sin el mirroring RPO=0
- ¿Qué sucede si falla el sitio B?
  - El sitio A verá que ambos canales de comunicación se caen.
  - El sitio A se hará cargo de los servicios de datos, pero sin el mirroring RPO=0

Hay otro escenario a considerar: Pérdida del enlace de replicación de datos. Si se pierde el enlace de replicación entre los sitios, obviamente el mirroring RPO=0 se convertirá en imposible. ¿Qué debería pasar entonces?

Esto se controla por el estado de sitio preferido. En una relación SM-AS, uno de los sitios es secundario al otro. Esto no afecta a las operaciones normales y todo el acceso a los datos es simétrico, pero si la replicación se interrumpe, el vínculo tendrá que romperse para reanudar las operaciones. Como resultado, el sitio preferido continuará con las operaciones sin mirroring y el sitio secundario detendrá el procesamiento de I/O hasta que se restaure la comunicación de la replicación.

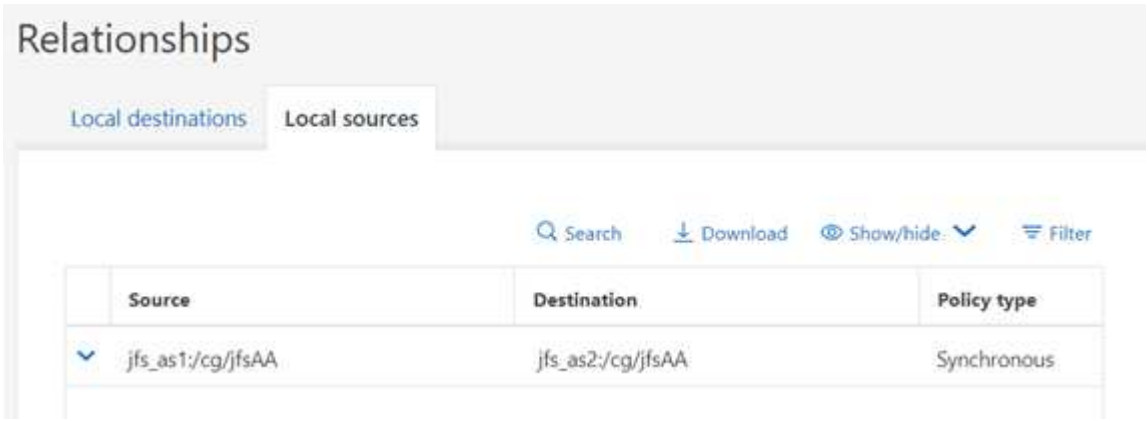
Sitio preferido

El comportamiento de sincronización activa de SnapMirror es simétrico, con una excepción importante: La configuración de sitio preferida.

La sincronización activa de SnapMirror considerará que un sitio es el «origen» y el otro el «destino». Esto implica una relación de replicación unidireccional, pero esto no se aplica al comportamiento de E/S. La replicación es bidireccional y simétrica, y los tiempos de respuesta de I/O son los mismos en cualquier lado del espejo.

La `source` designación controla el sitio preferido. Si se pierde el enlace de replicación, las rutas de LUN en la copia de origen seguirán sirviendo datos mientras las rutas de LUN en la copia de destino dejarán de estar disponibles hasta que se restablezca la replicación y SnapMirror vuelva a entrar en un estado síncrono. A continuación, las rutas reanudarán el servicio de datos.

La configuración de origen/destino se puede ver a través de SystemManager:



O en la CLI:

```
Cluster2::> snapmirror show -destination-path jfs_as2:/cg/jfsAA

                           Source Path: jfs_as1:/cg/jfsAA
                     Destination Path: jfs_as2:/cg/jfsAA
                    Relationship Type: XDP
                Relationship Group Type: consistencygroup
                    SnapMirror Schedule: -
                 SnapMirror Policy Type: automated-failover-duplex
                      SnapMirror Policy: AutomatedFailOverDuplex
                            Tries Limit: -
                      Throttle (KB/sec): -
                           Mirror State: Snapmirrored
                    Relationship Status: InSync
```

La clave es que la fuente es la máquina virtual de almacenamiento SVM en cluster1. Tal como se ha mencionado anteriormente, los términos «origen» y «destino» no describen el flujo de los datos replicados. Ambos sitios pueden procesar una escritura y replicarla en el sitio opuesto. De hecho, ambos clústeres son orígenes y destinos. El efecto de designar un clúster como origen simplemente controla qué clúster sobrevive como sistema de almacenamiento de lectura y escritura si se pierde el enlace de replicación.

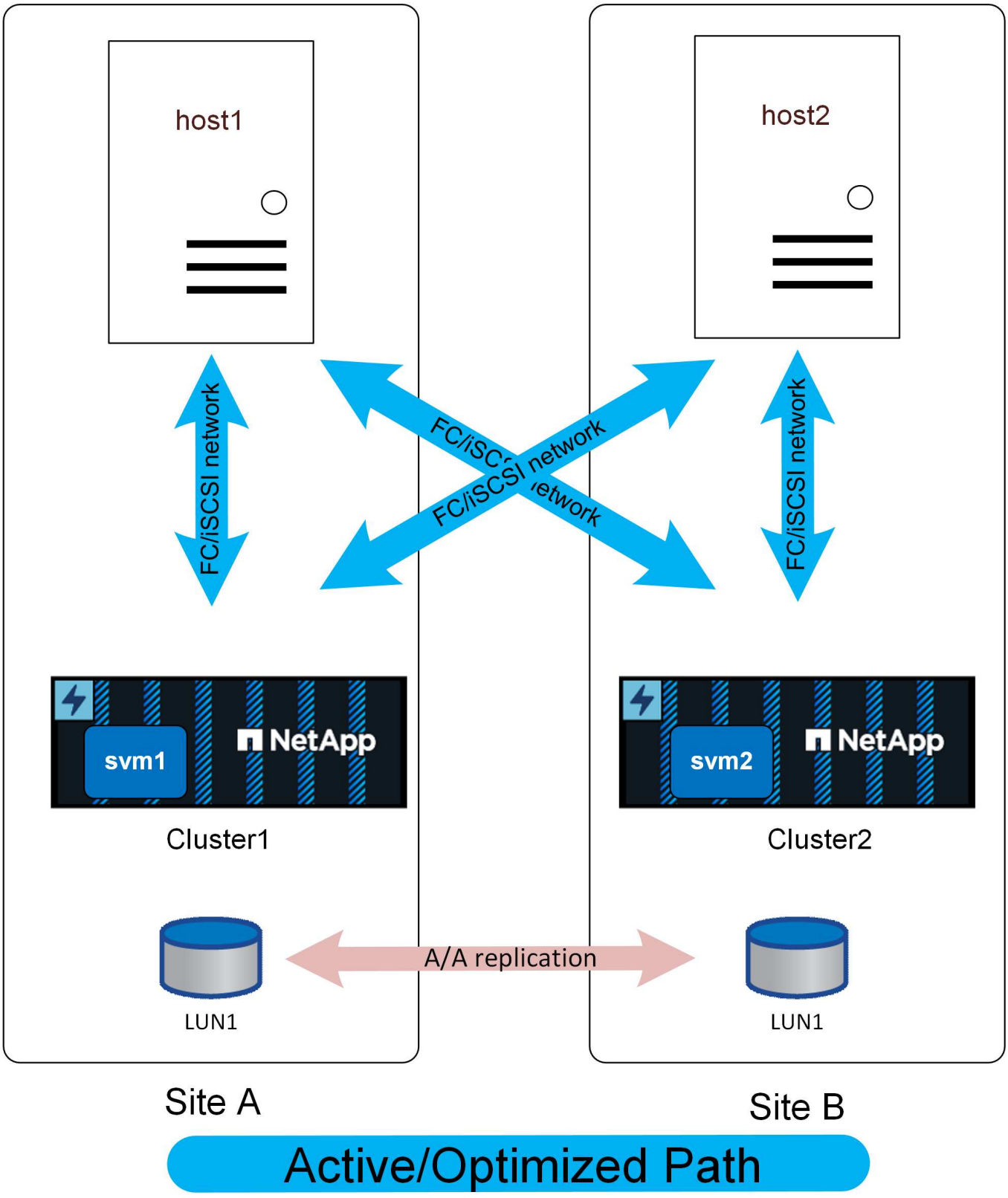
Topología de red

Acceso uniforme

La conexión de red de acceso uniforme significa que los hosts pueden acceder a las rutas en ambos sitios (o dominios de fallo dentro del mismo sitio).

Una característica importante de SM-AS es la capacidad de configurar los sistemas de almacenamiento para conocer dónde se encuentran los hosts. Cuando asigna las LUN a un host determinado, puede indicar si son proximales o no a un sistema de almacenamiento determinado.

Los sistemas NetApp ASA ofrecen accesos múltiples activo-activo en todas las rutas de un clúster. Esto también se aplica a las configuraciones SM-AS.



Con un acceso uniforme, IO estaría cruzando la WAN. Se trata de un clúster de red de malla completa y esto puede o no ser deseable para todos los casos de uso.

Si los dos sitios estuvieran separados por 100 metros con conectividad de fibra, no debería haber una latencia adicional detectable que cruce la WAN, pero si los sitios estuvieran separados por una distancia larga, el

rendimiento de lectura se vería afectado en ambos sitios. ASA con red de acceso no uniforme sería una opción para obtener las ventajas en coste y funciones de ASA sin incurrir en una penalización en el acceso a la latencia entre sitios ni utilizar la función de proximidad del host para permitir el acceso de lectura/escritura local del sitio para ambos sitios.

ASA con SM en una configuración de baja latencia ofrece dos ventajas interesantes. En primer lugar, esencialmente * duplica * el rendimiento para cualquier host individual porque IO puede ser atendido por el doble de controladores usando el doble de rutas. En segundo lugar, en un entorno de sitio único ofrece una disponibilidad extrema debido a que se puede perder un sistema de almacenamiento completo sin interrumpir el acceso al host.

Ajustes de proximidad

La proximidad se refiere a una configuración por clúster que indica que un ID de iniciador de iSCSI o WWN de host particular pertenece a un host local. Es un segundo paso opcional para configurar el acceso a LUN.

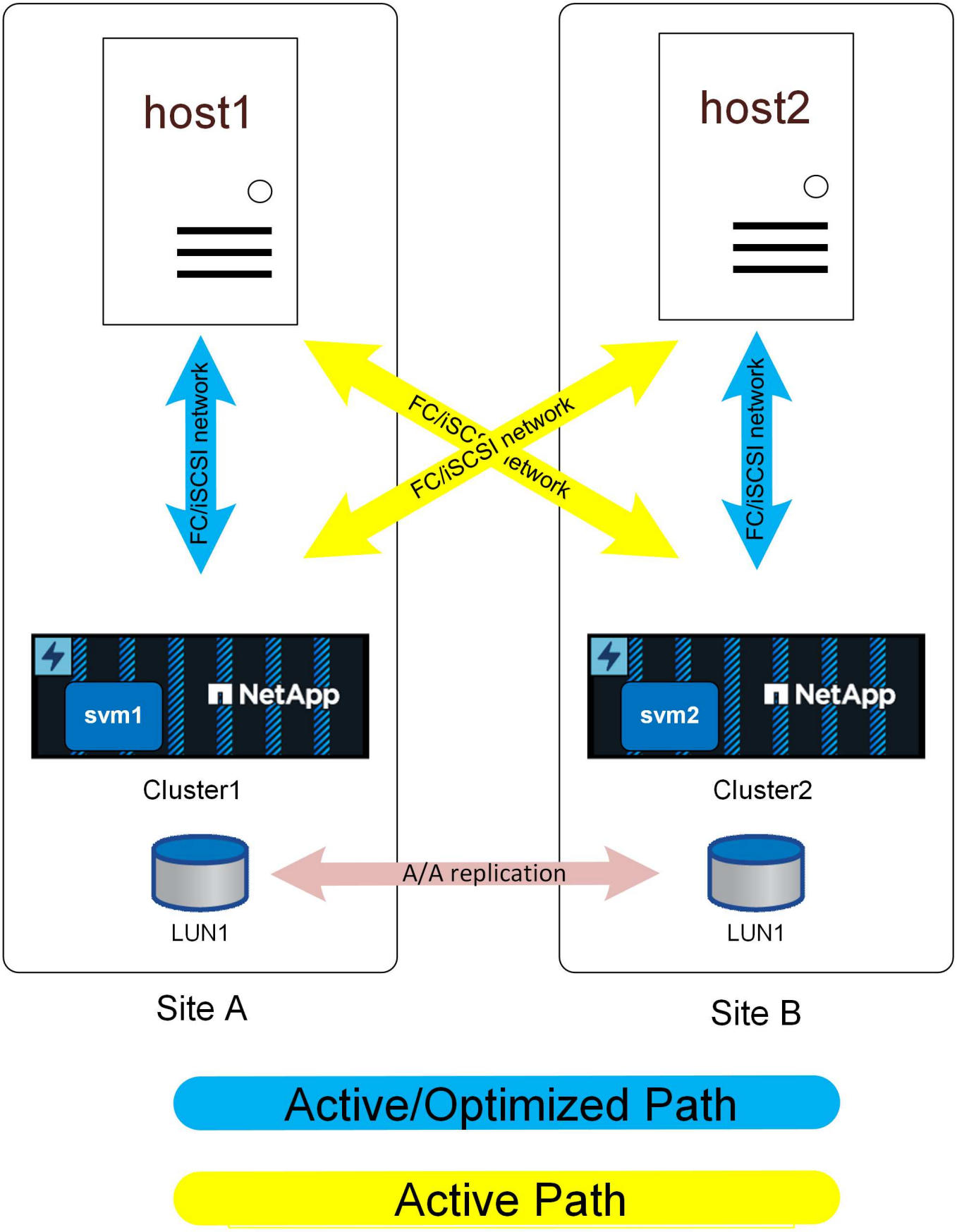
El primer paso es la configuración habitual del igroup. Cada LUN debe asignarse a un igroup que contiene los ID WWN/iSCSI de los hosts que necesitan acceder a ese LUN. Este controla el host que tiene *access* a una LUN.

El segundo paso opcional es configurar la proximidad del host. Esto no controla el acceso, controla *priority*.

Por ejemplo, se puede configurar un host del sitio A para acceder a una LUN protegida por sincronización activa de SnapMirror y, como la SAN se extiende a través de los sitios, las rutas están disponibles para ese LUN usando el almacenamiento en el sitio A o el almacenamiento del sitio B.

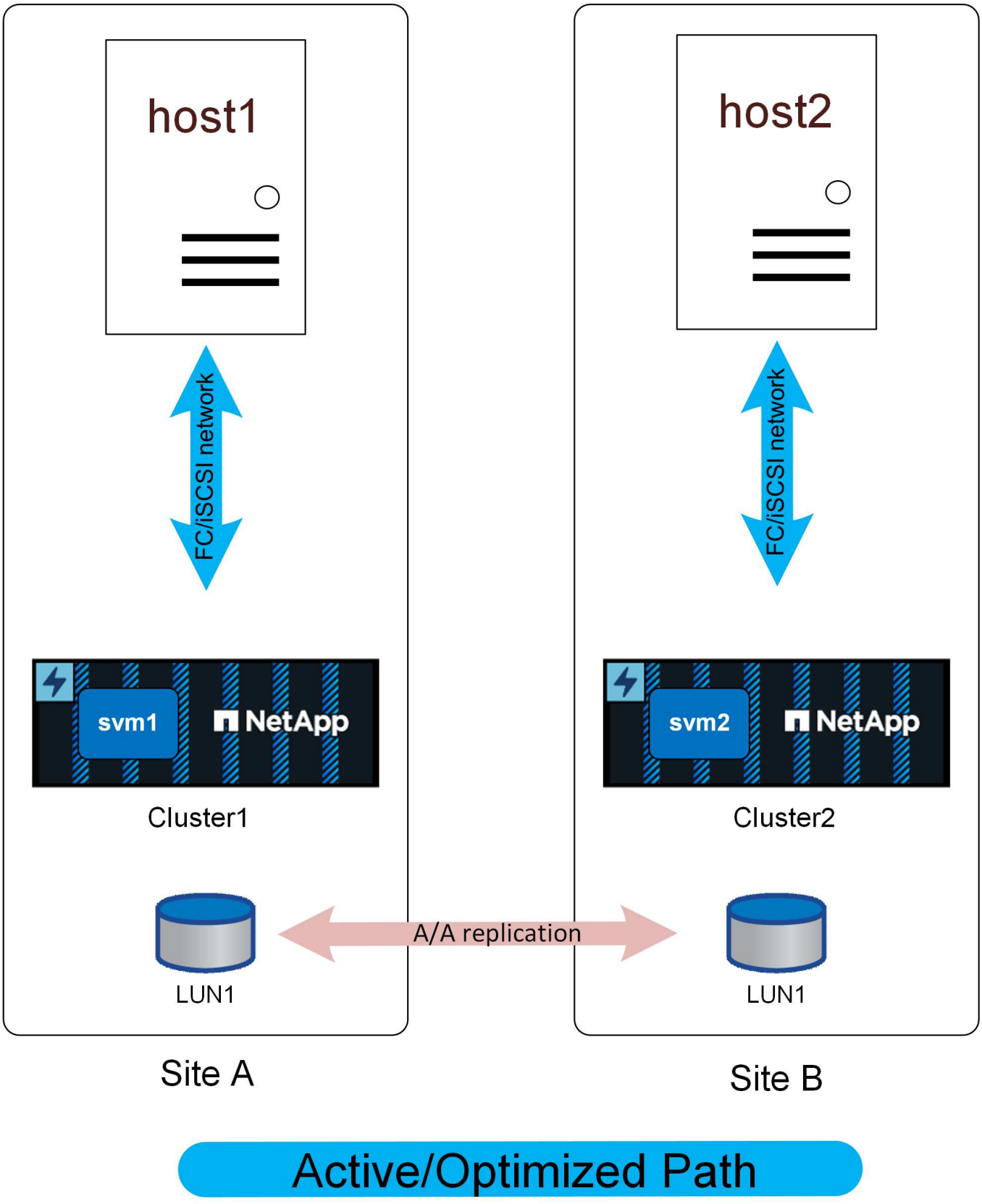
Sin configuración de proximidad, ese host usará ambos sistemas de almacenamiento por igual porque ambos sistemas de almacenamiento anunciarán rutas activas/optimizadas. Si la latencia SAN o el ancho de banda entre los sitios es limitada, es posible que no sea deseable y puede que desee asegurarse de que durante el funcionamiento normal cada host utilice preferentemente rutas hacia el sistema de almacenamiento local. Esto se configura añadiendo el ID de WWN/iSCSI de host al clúster local como un host proximal. Esto se puede hacer en la CLI o en SystemManager.

Las rutas de acceso aparecerán como se muestra a continuación cuando se haya configurado la proximidad del host.


host1
host2
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
svm1
NetApp
svm2
NetApp
Cluster1
Cluster2
A/A replication
LUN1
LUN1
Site A
Site B
Active/Optimized Path
Active Path

Acceso no uniforme

La red de acceso no uniforme significa que cada host solo tiene acceso a los puertos del sistema de almacenamiento local. La SAN no se extiende entre sitios (o dominios de fallos dentro del mismo sitio).



La principal ventaja de este método es la simplicidad en entornos SAN, eliminando la necesidad de extender una SAN por la red. Algunos clientes no tienen una conectividad de baja latencia suficiente entre los sitios o no disponen de la infraestructura para túnel el tráfico de SAN FC a través de una red intersitio.

La desventaja del acceso no uniforme es que ciertos escenarios de fallo, incluida la pérdida del enlace de replicación, provocarán que algunos hosts pierdan el acceso al almacenamiento. Las aplicaciones que se ejecutan como instancias únicas, como una base de datos sin cluster que inherentemente solo se ejecuta en un único host en cualquier montaje dado, fallarían si se perdiera la conectividad del almacenamiento local. Los datos seguirían estando protegidos, pero el servidor de la base de datos ya no tendría acceso. Deberá reiniciarse en un sitio remoto, preferiblemente mediante un proceso automatizado. Por ejemplo, VMware HA puede detectar una situación de todas las rutas inactivas en un servidor y reiniciar una máquina virtual en otro servidor donde haya rutas disponibles.

Por el contrario, una aplicación en cluster como Oracle RAC puede ofrecer un servicio que esté disponible al mismo tiempo en dos sitios diferentes. Perder un sitio no significa la pérdida del servicio de la aplicación en su conjunto. Las instancias siguen estando disponibles y en ejecución en el sitio superviviente.

En muchos casos, sería inaceptable que la sobrecarga de latencia adicional derivada de una aplicación que accede al almacenamiento a través de un enlace entre sitio y sitio. Esto significa que la disponibilidad mejorada de una red uniforme es mínima, ya que la pérdida de almacenamiento en un sitio llevaría a la necesidad de apagar los servicios en ese sitio que ha fallado de todos modos.

Existen rutas redundantes a través del clúster local que no se muestran en estos diagramas para simplificar el proceso. Los sistemas de almacenamiento de ONTAP son por sí mismos de alta disponibilidad, por lo que un fallo de una controladora no debe dar lugar a un fallo del sitio. Simplemente debe dar lugar a un cambio en el que se utilizan las rutas locales en el sitio afectado.

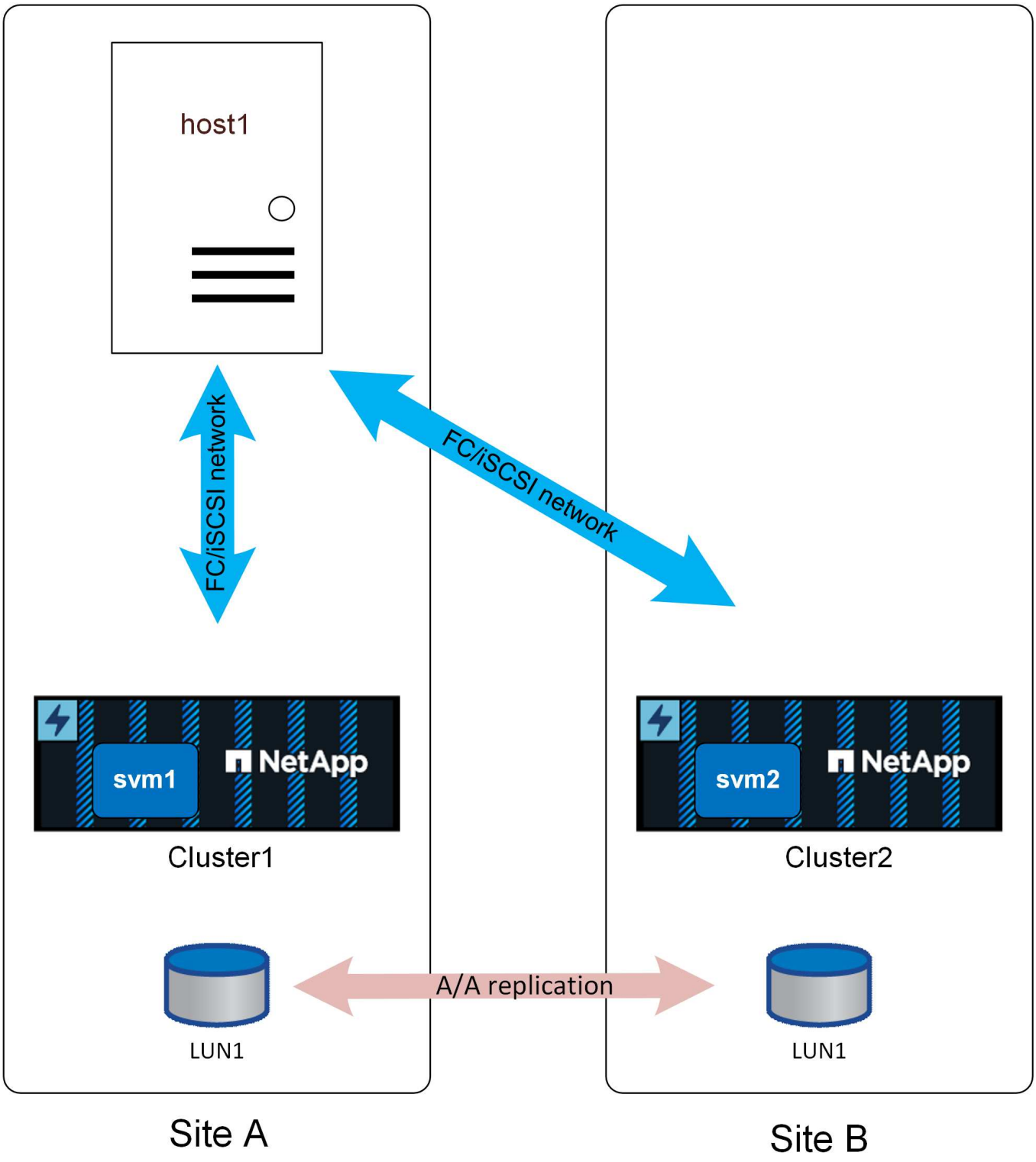
Descripción general

SQL Server se puede configurar para que funcione con la sincronización activa de SnapMirror de varias maneras. La respuesta correcta depende de la conectividad de red disponible, los requisitos de RPO y los requisitos de disponibilidad.

Instancia independiente de SQL Server

Las mejores prácticas para la distribución de archivos y la configuración del servidor son las mismas que se recomiendan en "SQL Server en ONTAP" la documentación.

Con una configuración independiente, SQL Server sólo podría ejecutarse en un sitio. Presumiblemente "uniforme"se utilizaría el acceso.



Gracias a un acceso uniforme, un fallo de almacenamiento en cualquiera de los sitios no interrumpía las operaciones de la base de datos. Un fallo completo del sitio en el sitio que incluyera el servidor de la base de datos, por supuesto, daría lugar a una interrupción del servicio.

Algunos clientes podrían configurar un sistema operativo que se ejecute en el sitio remoto con una configuración de SQL Server preconfigurada, actualizada con una versión de compilación equivalente a la de la instancia de producción. La conmutación por error requeriría activar esa instancia independiente de SQL Server en la ubicación alternativa, detectar LAS LUN e iniciar la base de datos. El proceso completo puede

automatizarse con el cmdlet de Windows PowerShell ya que no es necesario realizar operaciones en el almacenamiento.

"No uniforme" también se podía utilizar el acceso, pero el resultado sería una interrupción en la base de datos si se hubiera producido un error en el sistema de almacenamiento donde se encontraba el servidor de base de datos porque la base de datos no tendría rutas disponibles para el almacenamiento. Esto todavía puede ser aceptable en algunos casos. La sincronización activa de SnapMirror seguiría proporcionando protección de datos con objetivo de punto de recuperación = 0 y, en caso de fallo del sitio, la copia superviviente estaría activa y lista para reanudar las operaciones usando el mismo procedimiento usado con un acceso uniforme como se describió anteriormente.

Un proceso de conmutación por error simple y automatizado puede configurarse más fácilmente con el uso de un host virtualizado. Por ejemplo, si los archivos de datos de SQL Server se replican sincrónicamente en el almacenamiento secundario junto con un VMDK de arranque, entonces, en caso de desastre, el entorno completo podría activarse en el sitio alternativo. Un administrador puede activar manualmente el host en el sitio superviviente o automatizar el proceso mediante un servicio como la alta disponibilidad de VMware.

Instancia de cluster de failover de SQL Server

Las instancias de conmutación por error de SQL Server también se pueden alojar en un clúster de conmutación por error de Windows que se ejecute en un servidor físico o virtual como sistema operativo invitado. Esta arquitectura multihost proporciona flexibilidad de almacenamiento y instancia de SQL Server. Dicha puesta en marcha es útil en entornos con una gran demanda que buscan sólidos procesos de conmutación al respaldo y mantener un rendimiento mejorado. En una configuración de clúster de conmutación al nodo de respaldo, cuando un host o almacenamiento principal se ve afectado, SQL Services realizará una conmutación por error al host secundario; al mismo tiempo, el almacenamiento secundario estará disponible para prestar servicio de I/O. No se requiere ninguna secuencia de comandos de automatización ni intervención del administrador.

Escenarios de fallo

La planificación de una arquitectura completa de aplicaciones de sincronización activa de SnapMirror requiere comprender cómo SM-AS responderá en varias situaciones de conmutación por error planificadas e imprevistas.

Para los siguientes ejemplos, supongamos que el sitio A está configurado como el sitio preferido.

Pérdida de conectividad de replicación

Si se interrumpe la replicación de SM-AS, la E/S de escritura no se puede completar porque sería imposible que un clúster replique los cambios en el sitio opuesto.

Sitio A (Sitio preferido)

El resultado de un fallo del enlace de replicación en el sitio preferido será una pausa de aproximadamente 15 segundos en el procesamiento de I/O de escritura, ya que ONTAP reintenta las operaciones de escritura replicadas antes de que determine que el enlace de replicación es realmente inaccesible. Una vez transcurridos los 15 segundos, el sistema del sitio A reanuda el procesamiento de E/S de lectura y escritura. Las rutas de SAN no se modificarán y los LUN permanecerán en línea.

Centro B

Dado que el sitio B no es el sitio preferido de sincronización activa de SnapMirror, sus rutas de LUN dejarán de estar disponibles después de unos 15 segundos.

Fallo del sistema de almacenamiento

El resultado de un fallo del sistema de almacenamiento es casi idéntico al de perder el enlace de replicación. El sitio superviviente debería experimentar una pausa de IO de aproximadamente 15 segundos. Una vez transcurrido ese período de 15 segundos, IO se reanudará en ese sitio como de costumbre.

Pérdida del mediador

El servicio de mediador no controla directamente las operaciones de almacenamiento. Funciona como una ruta de control alternativa entre los clústeres. Existe principalmente para automatizar la conmutación al nodo de respaldo sin el riesgo de un escenario de cerebro dividido. En un funcionamiento normal, cada clúster está replicando los cambios en su compañero y, por lo tanto, cada clúster puede verificar que el clúster asociado esté en línea y sirviendo datos. Si el enlace de replicación falla, la replicación se detendría.

El motivo por el que se necesita un mediador para una conmutación por error automatizada segura es que, de otro modo, sería imposible que un clúster de almacenamiento pueda determinar si la pérdida de comunicación bidireccional se debió a una interrupción de la red o a un error real de almacenamiento.

El mediador proporciona una ruta alternativa para que cada clúster compruebe el estado de su compañero. Los escenarios son los siguientes:

- Si un clúster puede ponerse en contacto directamente con su socio, los servicios de replicación están operativos. No se requiere ninguna acción.
- Si un sitio preferido no puede ponerse en contacto con su partner directamente o a través del mediador, se asumirá que el partner no está disponible o que se ha aislado y ha desconectado las rutas de LUN. El sitio preferido procederá a liberar el estado RPO=0 y continuará procesando las I/O de lectura y escritura.
- Si un sitio no preferido no puede ponerse en contacto directamente con su socio, pero puede contactarlo a través del mediador, tomará sus rutas fuera de línea y esperará la devolución de la conexión de replicación.
- Si un sitio no preferido no puede contactar a su partner directamente o a través de un mediador operativo, asumirá que el partner no está disponible o que se ha aislado y ha desconectado las rutas de LUN. El sitio no preferido continuará liberando el estado RPO=0 y continuará procesando las I/O de lectura y escritura. Asumirá el rol del origen de replicación y se convertirá en el nuevo sitio preferido.

Si el mediador no está totalmente disponible:

- El fallo en los servicios de replicación por cualquier motivo, incluido el fallo del sitio o del sistema de almacenamiento no preferido, provocará que el sitio preferido libere el estado RPO=0 y reanude el procesamiento de I/O de lectura y escritura. El sitio no preferido desconectará sus rutas.
- Un fallo del sitio preferido provocará una interrupción porque el sitio no preferido no podrá verificar que el sitio opuesto esté realmente fuera de línea y, por lo tanto, no sería seguro para el sitio no preferido reanudar los servicios.

Restauración de servicios

Tras resolver un fallo, como restaurar la conectividad de sitio a sitio o encender un sistema fallido, los extremos de sincronización activa de SnapMirror detectan automáticamente la presencia de una relación de replicación defectuosa y la devuelven a un estado RPO=0. Una vez que se restablece la replicación síncrona, las rutas fallidas volverán a conectarse.

En muchos casos, las aplicaciones en clúster detectan automáticamente el retorno de las rutas fallidas, y dichas aplicaciones también volverán a estar online. En otros casos, puede ser necesario un análisis SAN a nivel de host o es posible que las aplicaciones deban volver a conectarse manualmente. Depende de la

aplicación y cómo se configura, y en general tales tareas se pueden automatizar fácilmente. El propio ONTAP se repara automáticamente y no debería requerir la intervención del usuario para reanudar las operaciones de almacenamiento RPO=0.

Recuperación manual tras fallos

Cambiar el sitio preferido requiere una operación simple. I/O se detendrá durante un segundo o dos como autoridad sobre los cambios en el comportamiento de replicación entre los clústeres, pero I/O de otro modo no se verá afectado.

Seguridad de datos

Proteger un entorno de base de datos de SQL Server es un esfuerzo multidimensional que va más allá de gestionar la propia base de datos. ONTAP ofrece varias funciones únicas diseñadas para proteger el aspecto de almacenamiento de la infraestructura de bases de datos.

Copias Snapshot

Las copias Snapshot de almacenamiento son réplicas puntuales de los datos objetivo. La implementación de ONTAP incluye la capacidad de establecer diversas políticas y almacenar hasta 1024 snapshots por volumen. Las copias Snapshot de ONTAP gestionan el espacio de manera eficiente. El espacio sólo se consume a medida que cambia el conjunto de datos original. También son de solo lectura. Una instantánea se puede eliminar, pero no se puede modificar.

En algunos casos, las copias Snapshot pueden programarse directamente en ONTAP. En otros casos, puede que se necesite software como SnapCenter para orquestar operaciones del sistema operativo o de la aplicación antes de crear snapshots. Sea cual sea el mejor método para su carga de trabajo, una estrategia de snapshot agresiva puede proporcionar seguridad de datos a través de acceso frecuente y fácilmente accesible a backups de todo tipo de elementos, desde LUN de arranque hasta bases de datos esenciales.

Un volumen de ONTAP flexible, o más sencillamente, un volumen no es sinónimo de una LUN. Los volúmenes son contenedores de gestión para datos, como archivos o LUN. Por ejemplo, se podría colocar una base de datos en un conjunto de franjas de 8 LUN, y todas las LUN estarían contenidas en un único volumen.

Para obtener más información sobre las snapshots, consulte "Documentación de ONTAP."

Snapshots a prueba de manipulación

A partir de ONTAP 9.12.1, las copias Snapshot no solo son de lectura, sino que también se pueden proteger de eliminaciones accidentales o intencionales. La función se denomina instantáneas a prueba de manipulaciones. Un período de retención puede establecerse y aplicarse mediante la política de Snapshot. Las instantáneas resultantes no se pueden eliminar hasta que hayan alcanzado su fecha de caducidad. No hay sustituciones administrativas o de centros de soporte.

Esto garantiza que un intruso, un intruso malintencionado o incluso un ataque de ransomware no puedan comprometer los backups, incluso si resultaran en acceso al propio sistema ONTAP. Al combinarlo con una programación de copias Snapshot frecuente, el resultado es una protección de datos extremadamente potente con un objetivo de punto de recuperación muy bajo.

Las instantáneas a prueba de manipulaciones no se pueden organizar en niveles mediante el pool de estructuras.

Para obtener más información sobre las instantáneas a prueba de manipulaciones, consulte "Documentación de ONTAP."

En la nueva plataforma ASA, replique las instantáneas en un clúster remoto mediante la directiva *vault* y, a continuación, bloquee el destino para hacer que las instantáneas sean a prueba de manipulaciones.

Replicación de SnapMirror

Las copias Snapshot también se pueden replicar en un sistema remoto. Esto incluye snapshots a prueba de manipulaciones, donde el período de retención se aplica y se aplica en el sistema remoto. El resultado son los mismos beneficios de la protección de datos que las copias Snapshot locales, pero los datos se encuentran en una segunda cabina de almacenamiento. Esto garantiza que la destrucción de la matriz original no comprometa los backups.

Un segundo sistema también abre nuevas opciones para la seguridad administrativa. Por ejemplo, algunos clientes de NetApp segregan las credenciales de autenticación para los sistemas de almacenamiento primario y secundario. Ningún usuario administrativo tiene acceso a ambos sistemas, lo que significa que un administrador malintencionado no puede eliminar todas las copias de datos.

Para obtener más información sobre SnapMirror, consulte "Documentación de ONTAP."

Máquinas virtuales de almacenamiento

Un sistema de almacenamiento ONTAP recientemente configurado es similar a un servidor VMware ESX aprovisionado recientemente, ya que ninguno de ellos admite ningún usuario hasta que se crea un equipo virtual. Con ONTAP, puede crear una máquina virtual de almacenamiento (SVM) que se convierte en la unidad más básica de gestión del almacenamiento. Cada SVM tiene sus propios recursos de almacenamiento, configuraciones de protocolos, direcciones IP y WWN de FCP. Esta es la base del multi-tenancy de ONTAP.

Por ejemplo, puede configurar una SVM para cargas de trabajo de producción cruciales y una segunda SVM en un segmento de red diferente para actividades de desarrollo. A continuación, podría restringir el acceso a la SVM de producción a ciertos administradores, a la vez que otorga a los desarrolladores un control más amplio sobre los recursos de almacenamiento en la SVM de desarrollo. Es posible que también necesite proporcionar una tercera SVM a sus equipos financieros y de RR. HH. Para almacenar datos especiales para la observación.

Para obtener más información sobre las SVM, consulte "Documentación de ONTAP."

RBAC administrativo

ONTAP ofrece un potente control de acceso basado en roles (RBAC) para inicios de sesión administrativos. Es posible que algunos administradores necesiten acceso completo al clúster, mientras que otros solo necesitarán acceso a ciertas SVM. Es posible que el personal de soporte avanzado necesite aumentar el tamaño de los volúmenes. El resultado es que puede otorgar a los usuarios administrativos el acceso necesario para realizar sus responsabilidades de trabajo, y nada más. Además, puede proteger estos inicios de sesión mediante PKI de varios proveedores, restringir el acceso sólo a las claves ssh y aplicar bloqueos de intentos de inicio de sesión fallidos.

Para obtener más información sobre el control de acceso administrativo, consulte "Documentación de

ONTAP."

Autenticación multifactor (MFA)

ONTAP y otros productos de NetApp ahora admiten la autenticación multifactor (MFA) mediante diversos métodos. El resultado es que un nombre de usuario / contraseña comprometido por sí solo no es un hilo de seguridad sin los datos del segundo factor, como un FOB o una aplicación para teléfonos inteligentes.

Si quiere más información sobre la autenticación multifactor (MFA), consulte "Documentación de ONTAP."

CONTROL DE ACCESO BASADO EN ROLES API

La automatización requiere llamadas a la API, pero no todas las herramientas requieren un acceso administrativo completo. Para ayudar a proteger los sistemas de automatización, el control de acceso basado en roles también está disponible a nivel de API. Puede limitar las cuentas de usuario de automatización a las llamadas API necesarias. Por ejemplo, el software de monitoreo no necesita acceso de cambio, solo requiere acceso de lectura. Los flujos de trabajo que aprovisionan almacenamiento no necesitan la capacidad de eliminar almacenamiento.

Para obtener más información acerca de la API RBAC, consulte "Documentación de ONTAP."

Verificación multi-admin (MAV)

La autenticación de múltiples factores puede ser llevada aún más lejos al requerir que dos administradores diferentes, cada uno con sus propias credenciales, aprueben ciertas actividades. Esto incluye cambiar los permisos de inicio de sesión, ejecutar comandos de diagnóstico y eliminar datos.

Para obtener más información sobre la verificación multi-admin (MAV), consulte "Documentación de ONTAP."

MySQL

Descripción general

MySQL y sus variantes, incluyendo MariaDB y Percona MySQL, es la base de datos más popular del mundo.

> Esta documentación sobre ONTAP y la base de datos MySQL sustituye a *TR-4722: Base de datos MySQL sobre las mejores prácticas de ONTAP que se había publicado anteriormente.*

ONTAP es una plataforma ideal para la base de datos MySQL porque ONTAP está literalmente diseñada para las bases de datos. Numerosas funciones, como las optimizaciones de latencia de I/O aleatorias, pasando por una calidad de servicio avanzada o una funcionalidad FlexClone básica, se crearon específicamente para cubrir las necesidades de cargas de trabajo de bases de datos.

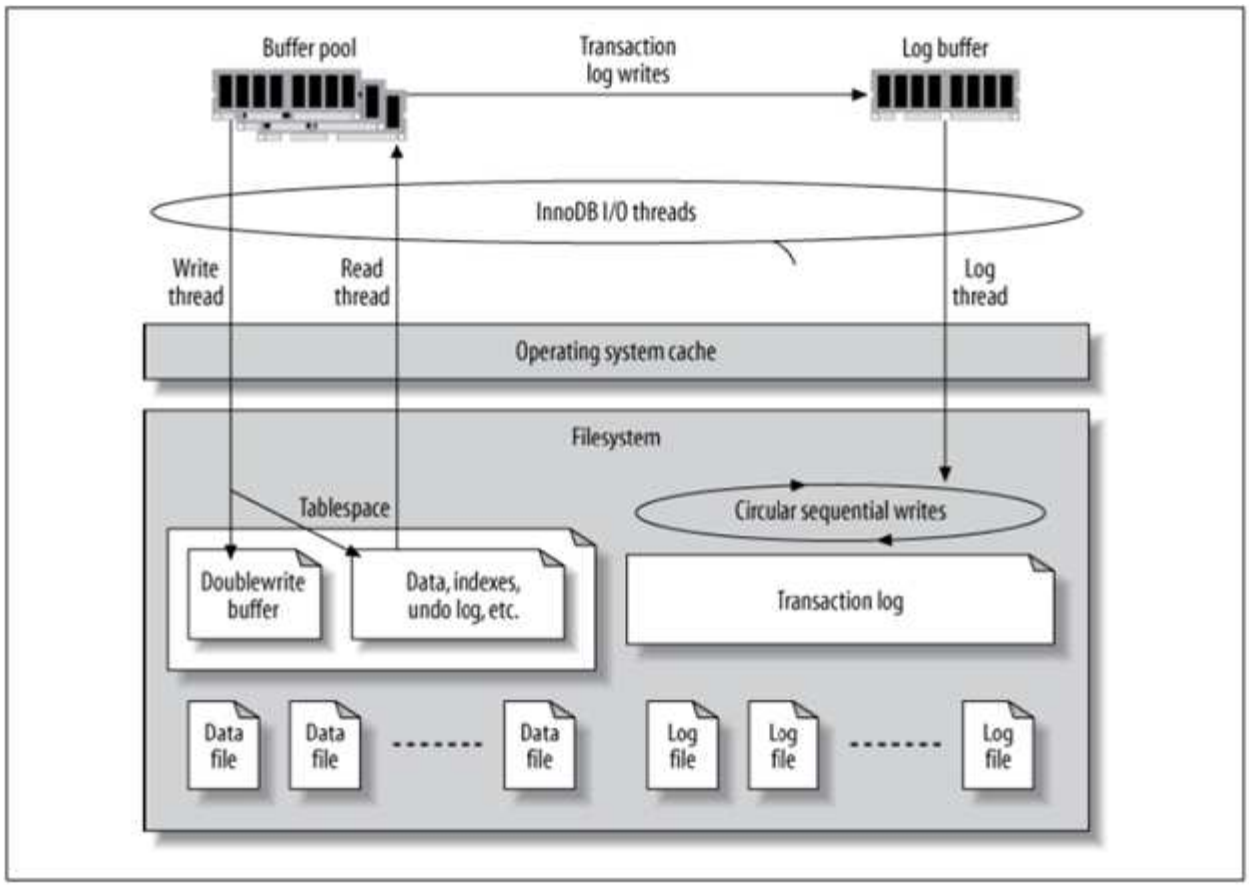
Otras funciones como las actualizaciones no disruptivas (entre ellas la sustitución de almacenamiento) garantizan que sus bases de datos cruciales seguirán estando disponibles. También se puede disponer de recuperación ante desastres instantánea para entornos grandes mediante MetroCluster o seleccionar bases de datos usando SnapMirror active sync.

Y lo que es más importante, ONTAP ofrece un rendimiento sin igual con la capacidad de dimensionar la solución en función de sus necesidades únicas. Nuestros sistemas de gama alta pueden ofrecer más de 1M 000 IOPS con latencias de microsegundos, pero si solo necesita 100K 000 IOPS, puede ajustar el tamaño de su solución de almacenamiento con una controladora más pequeña aún ejecutando exactamente el mismo sistema operativo de almacenamiento.

Configuración de la base de datos

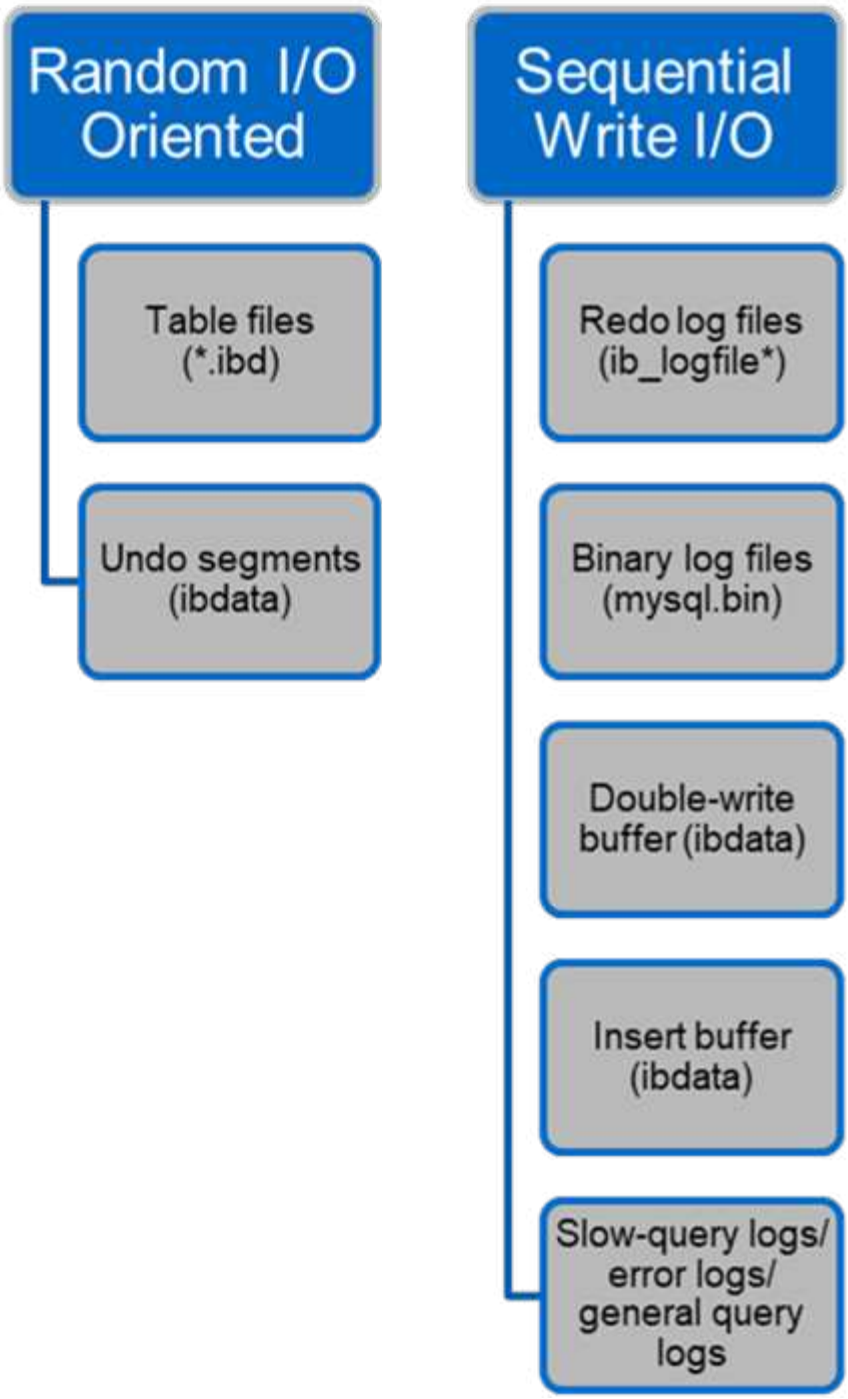
Estructura de archivos

InnoDB actúa como la capa media entre el almacenamiento y el servidor MySQL, almacena los datos en las unidades.



MySQL I/O se clasifica en dos tipos:

- I/O de archivo aleatoria
- E/S de archivo secuencial



Los archivos de datos se leen y se sobrescriben aleatoriamente, lo que da como resultado un elevado número de IOPS. Por lo tanto, se recomienda el almacenamiento SSD.

Los archivos de registro de recuperación y los archivos de registro binarios son registros transaccionales. Se escriben secuencialmente, por lo que puede obtener un buen rendimiento en HDD con la caché de escritura. Se produce una lectura secuencial en la recuperación, pero rara vez causa un problema de rendimiento, porque el tamaño de los archivos de registro suele ser menor que el de los archivos de datos y las lecturas secuenciales son más rápidas que las lecturas aleatorias (se producen en archivos de datos).

El buffer de doble escritura es una característica especial de InnoDB. En primer lugar, InnoDB escribe las páginas vaciadas en el buffer de doble escritura y, a continuación, escribe las páginas en sus posiciones

correctas en los archivos de datos. Este proceso evita la corrupción de páginas. Sin el búfer de doble escritura, la página puede dañarse si se produce un fallo de alimentación durante el proceso de escritura en unidades. Como la escritura en el búfer de doble escritura es secuencial, está muy optimizada para HDD. Las lecturas secuenciales se producen en la recuperación.

Como la NVRAM de ONTAP ya proporciona protección de escritura, no es necesario el almacenamiento en búfer de doble escritura. MySQL tiene un parámetro, `skip_innodb_doublewrite`, para desactivar el buffer de doble escritura. Esta característica puede mejorar sustancialmente el rendimiento.

El buffer INSERT también es una característica especial de InnoDB. Si los bloques de índice secundarios no únicos no están en la memoria, InnoDB inserta entradas en el buffer de inserción para evitar operaciones de E/S aleatorias. Periódicamente, el buffer de inserción se fusiona en los árboles de índice secundarios de la base de datos. El buffer de inserción reduce el número de operaciones de E/S fusionando las solicitudes de E/S en el mismo bloque; las operaciones de E/S aleatorias pueden ser secuenciales. El búfer de inserción también está altamente optimizado para HDD. Tanto las escrituras secuenciales como las lecturas se producen durante las operaciones normales.

Los segmentos de deshacer están orientados a E/S aleatorias. Para garantizar la concurrencia multiversión (MVCC), InnoDB debe registrar imágenes antiguas en los segmentos de deshacer. La lectura de imágenes anteriores de los segmentos de deshacer requiere lecturas aleatorias. Si ejecuta una transacción larga con lecturas repetibles (como mysqldump, transacción única) o ejecuta una consulta larga, pueden producirse lecturas aleatorias. Por lo tanto, almacenar segmentos de deshacer en SSD es mejor en esta instancia. Si ejecuta sólo transacciones o consultas cortas, las lecturas aleatorias no suponen un problema.

NetApp recomienda el siguiente diseño de almacenamiento debido a las características de E/S de InnoDB.

- Un volumen para almacenar archivos de MySQL orientados a I/O aleatorios y secuenciales
- Otro volumen para almacenar archivos de MySQL orientados a I/O puramente secuenciales

Este diseño también le ayuda a diseñar políticas y estrategias de protección de datos.

Parámetros de configuración

NetApp recomienda algunos parámetros de configuración MySQL importantes para obtener un rendimiento óptimo.

Parámetros	Valores
innodb_log_file_size	256M
innodb_flush_log_at_trx_commit	2
innodb_doublewrite	0
innodb_flush_method	fsync
innodb_buffer_pool_size	11G
innodb_io_capacity	8192
innodb_buffer_pool_instances	8
innodb_lru_scan_profund	8192
open_file_limit	65535

Para establecer los parámetros descritos en esta sección, debe cambiarlos en el archivo de configuración de MySQL (my.cnf). Las mejores prácticas de NetApp se deben a las pruebas que se realizan internamente.

innodb_log_file_size

Seleccionar el tamaño correcto para el tamaño del archivo de registro InnoDB es importante para las operaciones de escritura y para tener un tiempo de recuperación decente después de un fallo del servidor.

Dado que hay tantas transacciones registradas en el archivo, el tamaño del archivo de registro es importante para las operaciones de escritura. Cuando se modifican los registros, el cambio no se vuelve a escribir inmediatamente en el tablespace. En su lugar, el cambio se registra al final del archivo de registro y la página se marca como sucia. InnoDB utiliza su registro para convertir las operaciones de I/O aleatorias en operaciones de I/O secuenciales

Cuando el log está lleno, la página sucia se escribe en el tablespace en secuencia para liberar espacio en el archivo log. Por ejemplo, supongamos que un servidor se bloquea en medio de una transacción y que las operaciones de escritura solo se registran en el archivo de registro. Antes de que el servidor pueda volver a activarse, debe pasar por una fase de recuperación en la que se reproduzcan los cambios registrados en el archivo de registro. Cuantas más entradas haya en el archivo de registro, más tiempo tardará el servidor en recuperarse.

En este ejemplo, el tamaño del archivo log afecta tanto al tiempo de recuperación como al rendimiento de escritura. Al elegir el número correcto para el tamaño del archivo log, equilibre el tiempo de recuperación con respecto al rendimiento de escritura. Normalmente, cualquier cosa entre 128M y 512M es una buena relación calidad-precio.

innodb_flush_log_at_trx_commit

Cuando se produce un cambio en los datos, este no se escribe inmediatamente en el almacenamiento.

En su lugar, los datos se registran en un buffer de log, que es una parte de la memoria que InnoDB asigna a los cambios de buffer que se registran en el archivo log. InnoDB vacía el buffer en el archivo log cuando se confirma una transacción, cuando el buffer se llena, o una vez por segundo, lo que ocurra primero. La variable de configuración que controla este proceso es innodb_flush_log_at_trx_commit. Las opciones de valor incluyen:

- Cuando lo ajuste `innodb_flush_log_trx_at_commit=0`, InnoDB escribe los datos modificados (en el grupo de buffers de InnoDB) en el archivo log (ib_logfile) y vacía el archivo log (escribir en almacenamiento) cada segundo. Sin embargo, no hace nada cuando se confirma la transacción. Si hay un fallo de alimentación o un bloqueo del sistema, ninguno de los datos sin vaciar es recuperable, ya que no se escribe en el archivo de registro o en las unidades.
- Cuando lo ajuste `innodb_flush_log_trx_commit=1`, InnoDB escribe el buffer de log en el log de transacciones y se vacía en un almacenamiento duradero para cada transacción. Por ejemplo, para todas las confirmaciones de transacciones, InnoDB escribe en el log y, a continuación, escribe en el almacenamiento. Un almacenamiento más lento afecta negativamente al rendimiento; por ejemplo, se reduce el número de transacciones InnoDB por segundo.
- Cuando lo ajuste `innodb_flush_log_trx_commit=2`, InnoDB escribe el buffer de log en el archivo log en cada confirmación; sin embargo, no escribe datos en el almacenamiento. InnoDB vacía los datos una vez cada segundo. Incluso si hay un fallo de alimentación o un fallo del sistema, los datos de la opción 2 están disponibles en el archivo de registro y son recuperables.

Si el rendimiento es el objetivo principal, establezca el valor en 2. Como InnoDB escribe en las unidades una vez por segundo, no por cada confirmación de transacción, el rendimiento mejora drásticamente. Si se produce un fallo en el suministro eléctrico o un fallo, los datos se pueden recuperar del registro de transacciones.

Si la seguridad de los datos es el objetivo principal, establezca el valor en 1 para que, para cada confirmación de transacción, InnoDB se vacíe en las unidades. Sin embargo, el rendimiento puede verse afectado.

NetApp recomienda Establecer el valor innodb_flush_log_trx_commit en 2 para un mejor rendimiento.

innodb_doublewrite

Cuando `innodb_doublewrite` Está activado (por defecto), InnoDB almacena todos los datos dos veces: Primero en el buffer de doble escritura y luego en los archivos de datos reales.

Es posible desactivar este parámetro con `--skip-innodb_doublewrite` para pruebas de rendimiento o cuando le preocupa más el rendimiento superior que la integridad de los datos o posibles fallos. InnoDB utiliza una técnica de vaciado de archivos denominada doble escritura. Antes de escribir páginas en los archivos de datos, InnoDB las escribe en un área contigua denominada buffer de doble escritura. Una vez que se hayan completado las operaciones de escritura y vaciado en el buffer de doble escritura, InnoDB escribe las páginas en sus posiciones adecuadas en el archivo de datos. Si el sistema operativo o un proceso mysqld se bloquea durante la escritura de una página, InnoDB puede encontrar más tarde una buena copia de la página desde el buffer de doble escritura durante la recuperación de fallos.

NetApp recomienda deshabilitar el buffer de doble escritura. NVRAM de ONTAP sirve la misma función. El almacenamiento en búfer doble dañará innecesariamente el rendimiento.

innodb_buffer_pool_size

El pool de buffers de InnoDB es la parte más importante de cualquier actividad de ajuste.

InnoDB depende en gran medida del pool de buffers para almacenar en caché los índices y remar los datos, el índice hash adaptativo, el buffer INSERT y muchas otras estructuras de datos utilizadas internamente. El pool de búfer también almacena en búfer los cambios en los datos para que las operaciones de escritura no sean necesarias inmediatamente en el almacenamiento, lo que mejora el rendimiento. El pool de buffers es una parte integral de InnoDB y su tamaño debe ajustarse en consecuencia. Tenga en cuenta los siguientes factores al definir el tamaño del pool de buffers:

- Para una máquina exclusiva de InnoDB, establezca el tamaño del pool de buffers en 80% o más de RAM disponible.
- Si no es un servidor dedicado de MySQL, establezca el tamaño en 50% de RAM.

innodb_flush_method

El parámetro innodb_flush_method especifica cómo InnoDB abre y vacía los archivos log y de datos.

Optimizaciones

En la optimización de InnoDB, la configuración de este parámetro modifica el rendimiento de la base de datos cuando es aplicable.

Las siguientes opciones son para vaciar los archivos a través de InnoDB:

- `fsync`. InnoDB utiliza el `fsync()` llamada del sistema para vaciar los archivos de datos y de registro. Esta opción es el valor predeterminado.
- `O_DSYNC`. InnoDB utiliza el `O_DSYNC` opción para abrir y vaciar los archivos de registro y fsync() para vaciar los archivos de datos. InnoDB no utiliza `O_DSYNC` Directamente, porque ha habido problemas con él en muchas variedades de UNIX.
- `O_DIRECT`. InnoDB utiliza el `O_DIRECT` opción (o. `directio()` En Solaris) para abrir los archivos de datos y usos `fsync()` para vaciar los archivos de datos y de registro. Esta opción está disponible en algunas versiones de GNU/Linux, FreeBSD y Solaris.
- `O_DIRECT_NO_FSYNC`. InnoDB utiliza el `O_DIRECT` Durante el vaciado de I/O; sin embargo, omite el `fsync()` llamada del sistema posterior. Esta opción no es adecuada para algunos tipos de sistemas de archivos (por ejemplo, XFS). Si no está seguro de si su sistema de archivos requiere un `fsync()` llamada al sistema (por ejemplo, para conservar todos los metadatos del archivo), utilice el `O_DIRECT` en su lugar.

Observación

En las pruebas de laboratorio de NetApp, el `fsync` La opción predeterminada se utilizó en NFS y SAN, y fue un gran improvisador de rendimiento `O_DIRECT`. Mientras se utiliza el método de vaciado como `O_DIRECT` Con ONTAP, hemos observado que el cliente escribe muchas escrituras de un solo byte en el borde del bloque de 4096 KB de forma en serie. Estas escrituras aumentan la latencia en la red y el rendimiento disminuye.

innodb_io_capacity

En el plug-in InnoDB, se agregó un nuevo parámetro llamado innodb_io_capacity desde MySQL 5,7.

Controla el número máximo de IOPS que realiza InnoDB (lo que incluye la tasa de vaciado de páginas desfasadas y el tamaño de lote [ibuf] del buffer de inserción). El parámetro innodb_io_capacity define un límite superior de IOPS por tareas en segundo plano de InnoDB, como vaciar páginas del pool de buffers y fusionar datos del buffer de cambios.

Defina el parámetro innodb_io_capacity en el número aproximado de operaciones de E/S que el sistema puede realizar por segundo. Lo ideal es mantener la configuración lo más baja posible, pero no tan baja que las actividades en segundo plano se ralenticen. Si el valor es demasiado alto, los datos se eliminan del pool de buffers e insertan el buffer demasiado rápido para que el almacenamiento en caché proporcione una ventaja significativa.

NetApp recomienda que si utiliza esta configuración en NFS, analice el resultado de la prueba de IOPS (SysBench/fio) y establezca el parámetro en consecuencia. Utilice el valor más pequeño posible para vaciar y depurar para mantener el ritmo a menos que vea más páginas modificadas o sucias de las que desee en el pool de buffers de InnoDB.

No utilice valores extremos como 20.000 o más a menos que haya demostrado que los valores más bajos no son suficientes para su carga de trabajo.

El parámetro InnoDB_IO_CAPACITY regula las tasas de vaciado y la E/S relacionada

Puede dañar seriamente el rendimiento configurando este parámetro o el parámetro innodb_io_capacity_max demasiado alto y wastin

innodb_lru_scan_profund

La `innodb_lru_scan_depth` El parámetro influye en los algoritmos y la heurística de la operación de vaciado para el pool de buffers de InnoDB.

Este parámetro es principalmente interesante para los expertos en rendimiento que ajustan las cargas de trabajo con un gran volumen de I/O. Para cada instancia de pool de buffers, este parámetro especifica hasta qué punto en la lista de páginas de uso menos reciente (LRU) el thread del limpiador de páginas debe continuar escaneando, buscando páginas sucias para vaciar. Esta operación en segundo plano se realiza una vez por segundo.

Puede ajustar el valor hacia arriba o hacia abajo para minimizar el número de páginas libres. No establezca el valor mucho más alto de lo necesario, ya que los escaneos pueden tener un costo de rendimiento significativo. Además, considere ajustar este parámetro al cambiar el Núm. De instancias del pool de buffers, porque `innodb_lru_scan_depth * innodb_buffer_pool_instances` define la cantidad de trabajo que realiza el thread de limpieza de páginas cada segundo.

Una configuración inferior a la predeterminada es adecuada para la mayoría de las cargas de trabajo. Considere aumentar el valor solo si cuenta con capacidad de I/O de reserva con una carga de trabajo típica. Por el contrario, si una carga de trabajo con gran cantidad de escritura satura la capacidad de E/S, disminuya el valor, especialmente si tiene un pool de buffers grande.

open_file_limits

La `open_file_limits` el parámetro determina el número de archivos que el sistema operativo permite que mysqld abra.

El valor de este parámetro en tiempo de ejecución es el valor real permitido por el sistema y puede ser diferente del valor especificado al iniciar el servidor. El valor es 0 en sistemas donde MySQL no puede cambiar el número de archivos abiertos. Eficaz `open_files_limit` el valor se basa en el valor especificado en el inicio del sistema (si lo hay) y en los valores de `max_connections` y.. `table_open_cache` mediante el uso de estas fórmulas:

- 10 + `max_connections` + (`table_open_cache` 2)
- `max_connections` 5
- Límite del sistema operativo si es positivo
- Si el límite del sistema operativo es infinito: `open_files_limit` el valor se especifica en el inicio; 5.000 si no hay ninguno

El servidor intenta obtener el número de descriptores de archivo utilizando el máximo de estos cuatro valores. Si no se pueden obtener muchos descriptores, el servidor intenta obtener tantos como el sistema permita.

Configuración de hosts

Colocación de contenedores

La contenerización de bases de datos MySQL es cada vez más frecuente.

La gestión de contenedores de bajo nivel casi siempre se realiza a través de Docker. Las plataformas de gestión de contenedores, como OpenShift y Kubernetes, simplifican aún más la gestión de entornos de contenedores de gran tamaño. Los beneficios de la contenerización incluyen costos más bajos, porque no hay necesidad de licenciar un hipervisor. Además, los contenedores permiten que varias bases de datos se ejecuten aisladas entre sí mientras comparten el mismo kernel y sistema operativo subyacente. Los contenedores se pueden aprovisionar en microsegundos.

NetApp ofrece Astra Trident para proporcionar funcionalidades de gestión avanzadas del almacenamiento. Por ejemplo, Astra Trident permite que un contenedor creado en Kubernetes aprovisione automáticamente su almacenamiento en el nivel apropiado, aplique políticas de exportación, establezca políticas de Snapshot e incluso clone un contenedor a otro. Para obtener más información, consulte la "Documentación de Astra Trident".

Mesas de NFSv3 ranuras

El rendimiento de NFSv3 en Linux depende de un parámetro llamado `tcp_max_slot_table_entries`.

Las tablas de ranuras TCP son equivalentes a NFSv3 a la profundidad de la cola del adaptador de bus de host (HBA). En estas tablas se controla el número de operaciones de NFS que pueden extraordinarias a la vez. El valor predeterminado suele ser 16, que es demasiado bajo para un rendimiento óptimo. El problema opuesto ocurre en los kernels más nuevos de Linux, que pueden aumentar automáticamente el límite de la tabla de ranuras TCP a un nivel que sature el servidor NFS con solicitudes.

Para obtener un rendimiento óptimo y evitar problemas de rendimiento, ajuste los parámetros del núcleo que controlan las tablas de ranuras TCP.

Ejecute el `sysctl -a | grep tcp.*.slot_table` command, y observe los siguientes parámetros:

```
# sysctl -a | grep tcp.*.slot_table
sunrpc.tcp_max_slot_table_entries = 128
sunrpc.tcp_slot_table_entries = 128
```

Todos los sistemas Linux deben incluir `sunrpc.tcp_slot_table_entries`, pero solo algunos incluyen `sunrpc.tcp_max_slot_table_entries`. Ambos deben establecerse en 128.

Si no se establecen estos parámetros, puede tener efectos significativos en el rendimiento. En algunos casos, el rendimiento es limitado porque el sistema operativo linux no está emitiendo suficiente I/O. En otros casos, las latencias de I/O aumentan cuando el sistema operativo linux intenta emitir más operaciones de I/O de las que se pueden mantener.

Programadores de I/O.

El kernel de Linux permite un control de bajo nivel sobre la forma en que se programa la E/S para bloquear los dispositivos.

Los valores predeterminados en varias distribuciones de Linux varían considerablemente. MySQL recomienda que utilice `NOOP` o a `deadline` Planificador de I/O con I/O asíncrono nativo (AIO) en Linux. En general, los clientes de NetApp y las pruebas internas muestran mejores resultados con NoOps.

El motor de almacenamiento InnoDB de MySQL utiliza el subsistema de E/S asíncrono (AIO nativo) en Linux para realizar solicitudes de lectura anticipada y escritura para páginas de archivos de datos. Este comportamiento es controlado por el `innodb_use_native_aio` opción de configuración, que está activada de forma predeterminada. Con AIO nativo, el tipo de programador de E/S tiene mayor influencia en el rendimiento de E/S. Realice pruebas de rendimiento para determinar qué programador de I/O ofrece los mejores resultados para su carga de trabajo y su entorno.

Consulte la documentación relevante de Linux y MySQL para obtener instrucciones sobre la configuración del programador de I/O.

Descriptores de archivo

Para ejecutarse, el servidor MySQL necesita descriptores de archivo y los valores predeterminados no son suficientes.

Las utiliza para abrir nuevas conexiones, almacenar tablas en la caché, crear tablas temporales para resolver consultas complicadas y acceder a las persistentes. Si mysqld no puede abrir nuevos archivos cuando sea necesario, puede dejar de funcionar correctamente. Un síntoma común de este problema es el error 24, “Demasiados archivos abiertos”. El número de descriptores de archivo que mysqld puede abrir simultáneamente se define por el `open_files_limit` opción establecida en el archivo de configuración (`/etc/my.cnf`). Pero `open_files_limit` también depende de los límites del sistema operativo. Esta dependencia hace que la configuración de la variable sea más complicada.

MySQL no puede definir su `open_files_limit` opción superior a la especificada en `ulimit 'open files'`. Por lo tanto, debe establecer explícitamente estos límites en el nivel del sistema operativo para permitir que MySQL abra archivos según sea necesario. Hay dos formas de comprobar el límite de archivos en Linux:

- La `ulimit` command le proporciona rápidamente una descripción detallada de los parámetros que se permiten o bloquean. Los cambios realizados por la ejecución de este comando no son permanentes y se borrarán tras un reinicio del sistema.
- Cambios en la `/etc/security/limit.conf` el archivo es permanente y no se ve afectado por un reinicio del sistema.

Asegúrese de cambiar los límites duros y suaves para el usuario mysql. Los siguientes extractos son de la configuración:

```
mysql hard nofile 65535
mysql soft nofile 65353
```

En paralelo, actualice la misma configuración en `my.cnf` para utilizar completamente los límites de archivo abierto.

Configuración del almacenamiento

NFS

La documentación de MySQL recomienda el uso de NFSv4 para puestas en marcha de NAS.

Tamaños de transferencia NFS de ONTAP

De forma predeterminada, ONTAP limitará el tamaño de I/O de NFS a 64K. La E/S aleatoria con una base de datos MySQL utiliza un tamaño de bloque mucho más pequeño, que es muy inferior al máximo de 64K KB. Las E/S de bloques grandes suelen estar en paralelo, por lo que el máximo de 64K KB tampoco es una limitación.

Hay algunas cargas de trabajo en las que el máximo de 64K crea una limitación. En particular, las operaciones de un solo subproceso, como las operaciones de copia de seguridad de exploración de tabla completa, se ejecutarán de forma más rápida y eficiente si la base de datos puede realizar menos I/O pero más grandes. El tamaño óptimo de gestión de I/O para ONTAP con cargas de trabajo de base de datos es 256K. Las opciones de montaje de NFS indicadas para sistemas operativos específicos a continuación se han actualizado de la versión 64K a la 256K correspondiente.

El tamaño de transferencia máximo para una SVM de ONTAP determinada se puede cambiar de la siguiente manera:

```
Cluster01::> set advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.

Do you want to continue? {y|n}: y

Cluster01::*> nfs server modify -vserver vserver1 -tcp-max-xfer-size
262144
```

Nunca reduzca el tamaño máximo permitido de transferencia en ONTAP por debajo del valor de rsize/wsize de los sistemas de archivos NFS montados actualmente. Esto puede crear bloqueos o incluso corrupción de datos con algunos sistemas operativos. Por ejemplo, si los clientes NFS se establecen actualmente con un valor de rsize/wsize de 65536 000, el tamaño de transferencia máximo de ONTAP se podría ajustar entre 65536 000 y 1048576 000 sin que ello afecte a porque los propios clientes están limitados. Reducir el tamaño máximo de transferencia por debajo de 65536 puede dañar la disponibilidad o los datos.

NetApp recomienda

Ajuste de la siguiente configuración de NFSv4 fstab (/etc/fstab):

```
nfs4 rw,
hard,nointr,bg,vers=4,proto=tcp,noatime,rsize=262144,wsize=262144
```

Un problema común con NFSv3 era los archivos de registro InnoDB bloqueados después de una interrupción del suministro eléctrico. El uso de archivos de registro de hora o cambio solucionó este problema. Sin embargo, NFSv4 tiene operaciones de bloqueo y realiza un seguimiento de archivos abiertos y delegaciones.

SAN

Las bases de datos más pequeñas pueden colocarse en parejas de LUN estándar siempre que las demandas de I/O y capacidad estén dentro de los límites de un único sistema de archivos LUN. Por ejemplo, una base de datos que requiere aproximadamente 2K 000 IOPS aleatorias se puede alojar en un único sistema de archivos con una sola LUN. Del mismo modo, una base de datos con un tamaño de solo 100GB TB podría adaptarse en una única LUN sin crear un problema de gestión.

Las bases de datos de mayor tamaño requieren varios LUN. Por ejemplo, una base de datos que requiere 100K 000 IOPS probablemente necesitará al menos ocho LUN. Una única LUN se convertiría en un cuello de botella debido al número inadecuado de canales SCSI a las unidades. Igualmente, una base de datos de 10TB TB sería difícil gestionar una sola LUN de 10TB TB. Los administradores de volúmenes lógicos están diseñados para unir las funcionalidades de rendimiento y capacidad de varias LUN y así mejorar el rendimiento y la capacidad de gestión.

En ambos casos, debería ser suficiente una pareja de volúmenes de ONTAP. Con una configuración sencilla, la LUN de archivo de datos se colocaría en un volumen dedicado, al igual que las LUN de registro. Con una configuración de gestor de volúmenes lógico, todos los LUN del grupo de volúmenes de archivos de datos estarían en un volumen dedicado, y las LUN del grupo de volúmenes de registro estarían en un segundo volumen dedicado.

NetApp recomienda el uso de dos sistemas de archivos para implementaciones de MySQL en SAN:

- El primer sistema de archivos almacena todos los datos MySQL, incluidos los tablespaces, los datos y el índice.
- El segundo sistema de archivos almacena todos los registros (registros binarios, registros lentos y registros de transacciones).

Hay varias razones para separar los datos de esta manera, incluyendo:

- Los patrones de E/S de los archivos de datos y los archivos de registro son diferentes. Separarlos permitirá más opciones con controles de calidad de servicio.
- Para un uso óptimo de la tecnología Snapshot es necesario poder restaurar los archivos de datos de forma independiente. La combinación de archivos de datos con archivos de registro interfiere con la restauración de archivos de datos.
- La tecnología SnapMirror de NetApp se puede usar para proporcionar una funcionalidad de recuperación ante desastres simple y con bajo objetivo de punto de recuperación para una base de datos; no obstante, se requieren diferentes programaciones de replicación para los archivos y registros de datos.

Utilice esta distribución básica de dos volúmenes para preparar la solución para el futuro, de modo que todas las funciones de ONTAP se puedan utilizar si fuera necesario.

NetApp recomienda formatear su unidad con el sistema de archivos ext4 debido a las siguientes características:

- Enfoque ampliado de las funciones de gestión de bloques utilizadas en el sistema de archivos de registro en diario (JFS) y las funciones de asignación retrasada del sistema de archivos extendido (XFS).
- ext4 permite sistemas de archivos de hasta 1 exbibyte (2^60 bytes) y archivos de hasta 16 tebibytes (16 * 2^40 bytes). Por el contrario, el sistema de archivos ext3 solo admite un tamaño máximo del sistema de archivos de 16TB GB y un tamaño máximo de archivo de 2TB GB.
- En los sistemas de archivos ext4, la asignación de bloques múltiples (mballoc) asigna varios bloques para un archivo en una sola operación, en lugar de asignarlos uno por uno, como en ext3. Esta configuración reduce la sobrecarga de llamar al asignador de bloques varias veces y optimiza la asignación de memoria.
- Aunque XFS es el valor predeterminado para muchas distribuciones de Linux, administra los metadatos de manera diferente y no es adecuado para algunas configuraciones de MySQL.

NetApp recomienda usar opciones de tamaño de bloque 4K con la utilidad mkfs para alinearse con el tamaño de LUN de bloque existente.

```
mkfs.ext4 -b 4096
```

Las LUN de NetApp almacenan datos en bloques físicos de 4KB KB, lo que produce ocho bloques lógicos de 512 bytes.

Si no se configura el mismo tamaño de bloque, las operaciones de I/O no se alinearán con los bloques físicos correctamente y podrían escribir en dos unidades distintas de un grupo RAID, lo que dará como resultado latencia.

Es importante alinear las operaciones de I/O para que las operaciones de lectura/escritura sean fluidas. Sin embargo, cuando las operaciones de I/O se inician en un bloque lógico que no está al inicio de un bloque físico, la I/O se desalinea. Las operaciones de I/O se alinean solo cuando comienzan con un bloque lógico, es decir, el primer bloque lógico de un bloque físico.

Base de datos Oracle

Bases de datos de Oracle en ONTAP

ONTAP está diseñado para bases de datos de Oracle. Durante décadas, ONTAP se ha optimizado para las demandas específicas de las I/O de las bases de datos relacionales y se crearon varias funciones de ONTAP específicamente para satisfacer las necesidades de las bases de datos de Oracle e incluso a petición de la misma Oracle Inc.

> Esta documentación sustituye a los informes técnicos *TR-3633 publicados anteriormente: Bases de datos Oracle en ONTAP; TR-4591: Protección de datos de Oracle: Backup, recuperación, replicación; TR-4592: Oracle en MetroCluster; y TR-4534: Migración de bases de datos de Oracle a sistemas de almacenamiento de NetApp*

Además de las muchas formas posibles en que ONTAP aporta valor a su entorno de bases de datos, también presenta una amplia variedad de requisitos de usuario, como el tamaño de la base de datos, los requisitos de rendimiento y las necesidades de protección de datos. Las puestas en marcha conocidas del almacenamiento de NetApp incluyen todo, desde un entorno virtualizado de aproximadamente 6.000 bases de datos que se ejecutan con VMware ESX hasta un almacén de datos de instancia única con un tamaño actualmente de 996TB TB, que sigue creciendo. Como resultado, existen pocas mejores prácticas claras para configurar una base de datos Oracle en un almacenamiento de NetApp.

Los requisitos para operar una base de datos Oracle en el almacenamiento de NetApp se tratan de dos formas. En primer lugar, cuando existe una práctica recomendada clara, se llamará específicamente. En un nivel general, se explicarán muchas consideraciones de diseño que deben tratar los arquitectos de las soluciones de almacenamiento de Oracle basadas en sus requisitos empresariales específicos.

Configuración de ONTAP

RAID

RAID se refiere al uso de redundancia para proteger los datos contra la pérdida de una unidad.

De vez en cuando se plantean preguntas sobre los niveles de RAID en la configuración del almacenamiento NetApp utilizado para las bases de datos de Oracle y otras aplicaciones empresariales. Muchas de las mejores prácticas de Oracle heredadas sobre la configuración de la cabina de almacenamiento contienen advertencias sobre el uso de mirroring de RAID y/o la prevención de ciertos tipos de RAID. Aunque plantean puntos válidos, estas fuentes no se aplican a RAID 4 y a las tecnologías de NetApp RAID DP y RAID-TEC utilizadas en ONTAP.

RAID 4, RAID 5, RAID 6, RAID DP y RAID-TEC usan la paridad para garantizar que el fallo de una unidad no provoque la pérdida de datos. Estas opciones de RAID ofrecen un aprovechamiento del almacenamiento mucho mejor en comparación con mirroring, pero la mayoría de las implementaciones de RAID tienen un inconveniente que afecta a las operaciones de escritura. La finalización de una operación de escritura en otras implementaciones de RAID puede requerir varias lecturas de unidad para volver a generar los datos de paridad, un proceso comúnmente denominado penalización de RAID.

Sin embargo, ONTAP no implica este proceso de penalización por RAID. Esto se debe a la integración de

NetApp WAFL (Write Anywhere File Layout) con la capa RAID. Las operaciones de escritura se fusionan en la RAM y se preparan como una franja RAID completa, incluida la generación de paridad. ONTAP no necesita realizar una lectura para completar una escritura, lo que significa que ONTAP y WAFL evitan la penalización de RAID. El rendimiento de las operaciones cruciales para la latencia, como el registro de reconstrucción, no se ve afectado, y las escrituras de archivos de datos aleatorios no suponen ningún tipo de penalización de RAID por la necesidad de regenerar la paridad.

En cuanto a la fiabilidad estadística, incluso RAID DP ofrece una mejor protección que el mirroring RAID. El problema principal es la demanda que se realiza en las unidades durante una recompilación de RAID. Con un conjunto RAID reflejado, el riesgo de que se pierdan datos tras el fallo en una unidad durante la reconstrucción a su compañero en el conjunto RAID es mucho mayor que el riesgo de un fallo de triple unidad en un conjunto RAID DP.

Gestión de la capacidad

Gestionar una base de datos u otra aplicación empresarial con almacenamiento empresarial predecible, gestionable y de alto rendimiento requiere cierto espacio libre en las unidades para la gestión de datos y metadatos. La cantidad de espacio libre necesario depende del tipo de unidad utilizada y los procesos empresariales.

El espacio libre se define como el espacio que no se usa para datos reales e incluye espacio sin asignar en el propio agregado y el espacio no utilizado dentro de los volúmenes constituyentes. También se debe tener en cuenta el thin provisioning. Por ejemplo, un volumen puede contener 1TB 000 LUN de las cuales solo el 50% es utilizado por datos reales. En un entorno con thin provisioning, parece que esto consume 500GB TB de espacio de manera correcta. Sin embargo, en un entorno totalmente aprovisionado, parece que toda la capacidad de 1TB está en uso. Los 500GB GB de espacio no asignado están ocultos. Los datos reales no utilizan este espacio y, por lo tanto, debe incluirse en el cálculo del espacio libre total.

Las recomendaciones de NetApp para los sistemas de almacenamiento que se utilizan para aplicaciones empresariales son las siguientes:

Agregados SSD, incluidos los sistemas AFF

NetApp recomienda un mínimo de 10% de espacio libre. Esto incluye todo el espacio no utilizado, incluido el espacio libre dentro del agregado o un volumen y cualquier espacio libre que se asigne debido al uso de aprovisionamiento completo, pero que los datos reales no usan. El espacio lógico no es importante, la pregunta es cuánto espacio físico libre real está disponible para el almacenamiento de datos.

La recomendación de un 10% de espacio libre es muy conservadora. Los agregados SSD pueden admitir cargas de trabajo con niveles de utilización aún mayores sin afectar en absoluto al rendimiento. No obstante, a medida que aumenta el uso del agregado, también aumenta el riesgo de quedarse sin espacio si no se supervisa el uso de forma cuidadosa. Además, aunque ejecutar un sistema a un 99 % de capacidad puede que no afecte al rendimiento, probablemente se traduciría en un esfuerzo de gestión al intentar evitar que se llene completamente mientras se solicita hardware adicional. Además, la adquisición e instalación de unidades adicionales puede demorar algún tiempo.

Agregados de HDD, incluidos los agregados de Flash Pool

NetApp recomienda un mínimo de 15% de espacio libre cuando se utilizan unidades giratorias. Esto incluye todo el espacio no utilizado, incluido el espacio libre dentro del agregado o un volumen y cualquier espacio libre que se asigne debido al uso de aprovisionamiento completo, pero que los datos reales no usan. El rendimiento se verá afectado cuando el espacio libre se acerque al 10%.

Máquinas virtuales de almacenamiento

La gestión del almacenamiento de bases de datos de Oracle se centraliza en una máquina virtual de almacenamiento (SVM).

Una SVM, conocida como Vserver en la interfaz de línea de comandos de ONTAP, es una unidad funcional básica de almacenamiento, lo que resulta útil comparar una SVM con una máquina virtual «guest» en un servidor VMware ESX.

Cuando se instala por primera vez, ESX no tiene capacidades preconfiguradas, como alojar un sistema operativo invitado o admitir una aplicación de usuario final. Es un contenedor vacío hasta que se define una máquina virtual (VM). ONTAP es similar. Cuando ONTAP se instala por primera vez, no cuenta con funcionalidades de servicio de datos hasta que se crea una SVM. Es la personalidad de la SVM que define los servicios de datos.

Al igual que otros aspectos de la arquitectura de almacenamiento, las mejores opciones para el diseño de SVM y de la interfaz lógica (LIF) dependen en gran medida de los requisitos de escalado y las necesidades del negocio.

SVM

No existe ninguna práctica recomendada oficial para el aprovisionamiento de SVM para ONTAP. El método correcto depende de los requisitos de gestión y seguridad.

La mayoría de los clientes operan un SVM principal para la mayoría de sus requisitos diarios y después crean un número pequeño de SVM para necesidades especiales. Por ejemplo, es posible que desee crear:

- SVM para una base de datos empresarial crítica gestionada por un equipo especializado
- Una SVM para un grupo de desarrollo al que se le ha otorgado un control administrativo completo para que pueda gestionar su propio almacenamiento de forma independiente
- Una máquina virtual de almacenamiento SVM para datos empresariales confidenciales, como datos de recursos humanos o informes financieros, a los que debe limitarse el equipo administrativo

En un entorno multi-tenant, los datos de cada inquilino pueden recibir una SVM dedicada. El límite del número de SVM y LIF por clúster, pareja de alta disponibilidad y nodo dependen del protocolo que se utilice, del modelo de nodo y de la versión de ONTAP. Consulte la "Hardware Universe de NetApp" para estos límites.

Gestión del rendimiento con QoS de ONTAP

La gestión segura y eficaz de varias bases de datos Oracle requiere una estrategia de QoS eficaz. La razón es el aumento constante en las funcionalidades de rendimiento de un sistema de almacenamiento moderno.

En concreto, la creciente adopción del almacenamiento all-flash ha permitido consolidar las cargas de trabajo. Las cabinas de almacenamiento que se basan en medios giratorios tendían a admitir solo una cantidad limitada de cargas de trabajo con un gran volumen de I/O debido a las funcionalidades de IOPS limitadas de la

tecnología de unidades rotacionales más antigua. Una o dos bases de datos altamente activas saturarían las unidades subyacentes mucho antes de que las controladoras de almacenamiento alcanzaran sus límites. Esto ha cambiado. La funcionalidad de rendimiento de un número relativamente pequeño de unidades SSD puede saturar incluso las controladoras de almacenamiento más potentes. Esto significa que pueden aprovecharse todas las funcionalidades de las controladoras sin miedo al colapso repentino del rendimiento cuando se disparan los picos de latencia de los medios giratorios.

Como ejemplo de referencia, un sencillo sistema AFF A800 de alta disponibilidad de dos nodos es capaz de dar servicio a hasta un millón de IOPS aleatorias antes de que la latencia aumente por encima del milisegundo. Sería de esperar que muy pocas cargas de trabajo individuales alcancen estos niveles. El uso completo de esta cabina para el sistema A800 de AFF implicará alojar múltiples cargas de trabajo y hacerlo de forma segura y, al mismo tiempo, garantizar la previsibilidad, requiere controles de calidad de servicio.

Existen dos tipos de calidad de servicio en ONTAP: IOPS y ancho de banda. Los controles de calidad de servicio se pueden aplicar a SVM, volúmenes, LUN y archivos.

Calidad de servicio IOPS

Obviamente, un control de calidad de servicio de IOPS se basa en el número total de IOPS de un recurso determinado, pero hay una serie de aspectos de la calidad de servicio de IOPS que quizá no sean intuitivos. Al principio, algunos clientes se quedaron desconcertados por el aparente aumento de la latencia cuando se alcanza un umbral de IOPS. El aumento de la latencia es el resultado natural de la limitación de IOPS. Lógicamente, funciona de forma similar a un sistema de tokens. Por ejemplo, si un volumen determinado que contiene archivos de datos tiene un límite de 10K IOPS, cada I/O que llegue primero deberá recibir un token para continuar con el procesamiento. Mientras no se hayan consumido más de 10K tokens en un segundo determinado, no hay retrasos. Si las operaciones de I/O deben esperar para recibir el token, esta espera aparece como latencia adicional. Cuanto más fuerte sea una carga de trabajo que supere el límite de calidad de servicio, más tiempo debe esperar cada I/O en la cola para su procesamiento, lo cual parece que el usuario tiene una mayor latencia.

Tenga cuidado al aplicar controles QoS a los datos de transacción/redo log de la base de datos. Si bien las demandas de rendimiento del redo log suelen ser mucho más bajas que las de los archivos de datos, la actividad de redo log es rápida. El E/S se produce en pulsos breves y un límite de QoS que parece adecuado para los niveles medios de E/S de redo puede ser demasiado bajo para los requisitos reales. El resultado puede ser limitaciones de rendimiento graves ya que QoS se conecta con cada ráfaga de redo log. En general, el redo y el registro de archivos no deben estar limitados por QoS.

Calidad del ancho de banda

No todos los tamaños de I/O son iguales. Por ejemplo, una base de datos puede estar realizando un gran número de lecturas de bloque pequeño, lo que haría que se alcance el umbral de IOPS. pero las bases de datos también pueden estar realizando una operación de exploración de tabla completa que consistiría en un número muy pequeño de lecturas de bloque grandes, lo que consume una gran cantidad de ancho de banda pero relativamente pocas IOPS.

Del mismo modo, un entorno VMware podría generar un gran número de IOPS aleatorias durante el arranque, pero realizaría menos I/O, pero más grandes, durante un backup externo.

A veces, para gestionar el rendimiento de forma efectiva se requieren límites de IOPS o de calidad de servicio del ancho de banda o incluso ambos.

Calidad de servicio mínima/garantizada

Muchos clientes buscan una solución que incluya una calidad de servicio garantizada, una solución que se pueda conseguir más de lo que parece y que potencialmente supone un derroche. Por ejemplo, colocar 10 bases de datos con una garantía de 10K IOPS requiere configurar un sistema para un escenario en el que las 10 bases de datos se ejecuten simultáneamente a 10K 000 IOPS, para un total de 100K 000.

El mejor uso para los controles mínimos de calidad de servicio es proteger las cargas de trabajo cruciales. Por ejemplo, piense en una controladora ONTAP con un número máximo de IOPS de 500K KB posible y una combinación de cargas de trabajo de producción y desarrollo. Debe aplicar políticas de calidad de servicio máximas a las cargas de trabajo de desarrollo para evitar que una base de datos determinada monopolice la controladora. A continuación, aplicaría políticas mínimas de calidad de servicio a las cargas de trabajo de producción para asegurarse de que siempre tengan las IOPS necesarias disponibles cuando las necesite.

Calidad de servicio adaptativa

La calidad de servicio adaptativa se refiere a la función ONTAP, donde el límite de calidad de servicio se basa en la capacidad del objeto de almacenamiento. Rara vez se utiliza con bases de datos porque normalmente no hay ningún vínculo entre el tamaño de una base de datos y sus requisitos de rendimiento. Las bases de datos de gran tamaño pueden ser casi inertes, mientras que las bases de datos más pequeñas pueden ser las más intensivas en IOPS.

La calidad de servicio adaptativa puede resultar muy útil con los almacenes de datos de virtualización porque los requisitos de IOPS de dichos conjuntos de datos tienden a correlacionarse con el tamaño total de la base de datos. Es probable que los almacenes de datos más recientes que contienen 1TB TB de archivos VMDK requieran la mitad de rendimiento que un almacén de datos de 2TB GB. La calidad de servicio adaptativa le permite aumentar automáticamente los límites de calidad de servicio a medida que el almacén de datos se llena con datos.

Eficiencia

Las funciones de gestión eficiente del espacio de ONTAP se optimizan para las bases de datos de Oracle. En casi todos los casos, el mejor método es dejar los valores predeterminados con todas las funciones de eficiencia activadas.

Las funciones de eficiencia del espacio, como la compresión, la compactación y la deduplicación están diseñadas para aumentar la cantidad de datos lógicos que se adaptan a una determinada cantidad de almacenamiento físico. El resultado es una reducción de los costes y los gastos generales de gestión.

En un nivel superior, la compresión es un proceso matemático por el cual los patrones en los datos se detectan y codifican de manera que reducen los requisitos de espacio. Por el contrario, la deduplicación detecta bloques de datos repetidos y elimina las copias externas. La compactación permite que varios bloques lógicos de datos compartan el mismo bloque físico en medios.

Consulte las siguientes secciones sobre thin provisioning para obtener una explicación de la interacción entre la eficiencia del almacenamiento y la reserva fraccionaria.

Compresión

Antes de la disponibilidad de sistemas de almacenamiento all-flash, la compresión basada en cabinas era de un valor limitado debido a que la mayoría de las cargas de trabajo con un gran volumen de I/O requerían un gran número de discos para proporcionar un rendimiento aceptable. Los sistemas de almacenamiento contenían invariablemente mucha más capacidad de la necesaria como efecto secundario al gran número de

unidades. La situación ha cambiado con el aumento del almacenamiento de estado sólido. Ya no es necesario sobreaprovisionar enormemente las unidades solo para obtener un buen rendimiento. El espacio de las unidades de un sistema de almacenamiento puede coincidir con las necesidades de capacidad reales.

La mayor funcionalidad de IOPS de las unidades de estado sólido (SSD) casi siempre genera ahorro de costes en comparación con las unidades giratorias, pero la compresión puede conseguir un mayor ahorro al aumentar la capacidad efectiva de los medios de estado sólido.

Existen varias formas de comprimir datos. Muchas bases de datos incluyen sus propias funcionalidades de compresión, pero esto se observa muy rara vez en los entornos del cliente. La razón suele ser la penalización de rendimiento para un **cambio** a los datos comprimidos, además con algunas aplicaciones hay altos costos de licencia para la compresión a nivel de base de datos. Por último, existen las consecuencias de rendimiento generales para las operaciones de base de datos. Tiene poco sentido pagar un alto coste de licencia por CPU por una CPU que realiza compresión y descompresión de datos en lugar de trabajo real de base de datos. Una mejor opción es descargar el trabajo de compresión en el sistema de almacenamiento.

Compresión adaptativa

La compresión adaptativa se ha probado minuciosamente en cargas de trabajo empresariales sin que ello afecte al rendimiento, incluso en un entorno all-flash en el que la latencia se mide en microsegundos. Algunos clientes incluso han informado de un aumento del rendimiento con el uso de la compresión, ya que los datos siguen comprimidos en la caché, lo que aumenta efectivamente la cantidad de caché disponible en una controladora.

ONTAP gestiona bloques físicos en 4KB unidades. La compresión adaptativa usa un tamaño de bloque de compresión predeterminado de 8KB KB, lo que significa que los datos se comprimen en 8KB unidades. Esto coincide con el tamaño de bloque de 8KB KB que suelen utilizar las bases de datos relacionales. Los algoritmos de compresión son más eficientes a medida que se comprimen más datos como una sola unidad. Un tamaño de bloque de compresión de 32KB KB haría más eficiente el espacio que una unidad de bloques de compresión de 8KB KB. Esto significa que la compresión adaptativa con el tamaño de bloque de 8KB KB predeterminado conduce a tasas de eficiencia ligeramente más bajas, pero también ofrece una ventaja significativa si se usa un tamaño de bloque de compresión más pequeño. Las cargas de trabajo de bases de datos incluyen una gran cantidad de actividad de sobrescritura. Para sobrescribir un bloque de datos de 8KB GB de 32KB comprimido, es necesario volver a leer los 32KB TB completos de datos lógicos, descomprimirlos, actualizar la región de 8KB requerida, recomprimir y, a continuación, volver a escribir todo el 32KB en las unidades. Esta es una operación muy cara para un sistema de almacenamiento y es el motivo por el que algunas cabinas de almacenamiento de la competencia basadas en bloques de compresión más grandes también incurren en un impacto significativo en el rendimiento con las cargas de trabajo de base de datos.

> El tamaño de los bloques utilizado por la compresión adaptativa se puede aumentar hasta 32KB KB. Esto puede mejorar la eficiencia del almacenamiento y debe considerarse en el caso de archivos inactivos, como registros de transacciones y archivos de backup, cuando se almacena una cantidad sustancial de dichos datos en la cabina. En algunas situaciones, las bases de datos activas que usan un tamaño de bloque de 16KB KB o de 32KB KB también pueden beneficiarse de aumentar el tamaño de bloque de la compresión adaptativa para que coincida. Consulte a un representante de NetApp o de su partner para obtener orientación sobre si esto es adecuado para su carga de trabajo.

Los bloques de compresión superiores a los 8KB MB no se deben usar junto a la deduplicación en destinos de backup en streaming. El motivo es que los pequeños cambios en los datos de backup afectan a la ventana de compresión de 32KB:1. Si la ventana cambia, los datos comprimidos resultantes difieren en todo el archivo. La deduplicación ocurre después de la compresión, lo que significa que el motor de deduplicación ve cada backup comprimido de forma diferente. Si se requiere la deduplicación de backups en streaming, solo deberá usarse la compresión adaptativa de 8KB bloques. Es preferible recurrir a la compresión adaptativa, ya que funciona con un tamaño de bloque más pequeño y no interrumpe la eficiencia de la deduplicación. Por motivos similares, la compresión en el lado del host también interfiere con la eficiencia de la deduplicación.

Alineación de la compresión

La compresión adaptativa en un entorno de base de datos requiere tener en cuenta algún tipo de aspecto en la alineación de bloques de compresión. Hacerlo solo es una preocupación para los datos sujetos a sobrescrituras aleatorias de bloques muy específicos. Este enfoque es similar en concepto a la alineación general del sistema de archivos, donde el inicio de un sistema de archivos debe alinearse con un límite de dispositivo 4K y el tamaño de bloque de un sistema de archivos debe ser un múltiplo de 4K.

Por ejemplo, una escritura 8KB en un archivo se comprime solo si se alinea con un límite de 8KB KB en el propio sistema de archivos. Este punto significa que debe caer en los primeros 8KB del archivo, el segundo 8KB del archivo, y así sucesivamente. La forma más sencilla de garantizar una alineación correcta es utilizar el tipo de LUN correcto, cualquier partición creada debe tener un desplazamiento desde el inicio del dispositivo que sea un múltiplo de 8K y usar un tamaño de bloque del sistema de archivos que sea un múltiplo del tamaño del bloque de la base de datos.

Los datos como los backups o los registros de transacciones son operaciones escritas secuencialmente que abarcan varios bloques, todos ellos comprimidos. Por lo tanto, no hay necesidad de considerar la alineación. El único patrón de E/S preocupante es la sobrescritura aleatoria de archivos.

Compactación de datos

La compactación de datos es una tecnología que mejora la eficiencia de la compresión. Como se ha indicado anteriormente, la compresión adaptativa por sí sola puede proporcionar un ahorro de 2:1 KB, ya que se limita a almacenar una I/O de 8KB KB en un bloque de 4KB WAFL. Los métodos de compresión con tamaños de bloque más grandes ofrecen una mejor eficiencia. Sin embargo, no son adecuados para datos sujetos a sobrescrituras de bloques pequeños. La descompresión de 32KB unidades de datos, la actualización de una parte de 8KB, la recompresión y la escritura en las unidades genera una sobrecarga.

La compactación de datos permite almacenar varios bloques lógicos en bloques físicos. Por ejemplo, una base de datos con datos altamente comprimibles, como texto o bloques parcialmente completos, puede comprimirse de 8KB a 1KB. Sin compactación, esos 1KB TB de datos seguirían ocupando un bloque completo de 4KB KB. La compactación de datos inline permite almacenar 1KB TB de datos comprimidos en solo 1KB GB de espacio físico junto con otros datos comprimidos. No es una tecnología de compresión; simplemente es una forma más eficaz de asignar espacio en las unidades y, por tanto, no debe crear un efecto de rendimiento detectable.

El grado de ahorro obtenido varía. Por lo general, los datos que ya están comprimidos o cifrados no se pueden comprimir aún más y, por lo tanto, estos conjuntos de datos no se benefician de la compactación. Por el contrario, los archivos de datos recién inicializados que contienen poco más que metadatos de bloques y ceros se comprimen hasta 80:1.

Eficiencia de almacenamiento sensible a la temperatura

La eficiencia de almacenamiento sensible a la temperatura (TSSE) está disponible en ONTAP 9, e.8 y posteriores. Se basa en mapas de calor de acceso a bloques para identificar los bloques a los que se accede con poca frecuencia y comprimirlos con mayor eficiencia.

Deduplicación

La deduplicación es eliminar los tamaños de bloques duplicados de un conjunto de datos. Por ejemplo, si existiera el mismo bloque de 4KB KB en 10 archivos diferentes, la deduplicación redirigiría ese bloque de 4KB KB en los 10 archivos al mismo bloque físico de 4KB KB. El resultado sería una mejora de 10:1 veces en eficiencia en esos datos.

Los datos, como las LUN de arranque invitado de VMware, suelen deduplicar muy bien porque constan de varias copias de los mismos archivos del sistema operativo. Se ha observado una eficiencia de 100:1 y mayor.

Algunos datos no contienen datos duplicados. Por ejemplo, un bloque de Oracle contiene una cabecera que es única globalmente para la base de datos y un cola que es casi único. Como resultado, la deduplicación de una base de datos de Oracle rara vez produce un ahorro superior al 1%. La deduplicación con bases de datos de MS SQL es ligeramente mejor, pero los metadatos únicos a nivel de bloque siguen siendo una limitación.

En pocos casos, se ha observado un ahorro de espacio de hasta un 15 % en bases de datos con 16KB KB y tamaños de bloque grandes. El primer 4KB de cada bloque contiene el encabezado único a nivel mundial, y el último bloque de 4KB contiene el remolque casi único. Los bloques internos pueden optar a la deduplicación, aunque en la práctica esto se atribuye casi por completo a la deduplicación de datos puestos a cero.

Muchas cabinas de la competencia afirman la capacidad de deduplicar bases de datos basándose en la presunción de que una base de datos se copia varias veces. En este sentido, la deduplicación de NetApp también podría utilizarse, pero ONTAP ofrece una opción mejor: La tecnología FlexClone de NetApp. El resultado final es el mismo; se crean varias copias de una base de datos que comparten la mayoría de los bloques físicos subyacentes. El uso de FlexClone es mucho más eficiente que tomarse tiempo para copiar archivos de base de datos y después deduplicarlos. Es, de hecho, la no duplicación en lugar de la deduplicación, porque nunca se crea un duplicado.

Eficiencia y thin provisioning

Las funciones de eficiencia son formas de thin provisioning. Por ejemplo, una LUN de 100GB GB que ocupa un volumen de 100GB GB podría comprimirse hasta 50GB 000. Todavía no hay ahorros reales realizados porque el volumen sigue siendo de 100GB GB. Primero se debe reducir el volumen para que el espacio ahorrado se pueda usar en cualquier otro lugar del sistema. Si los cambios realizados en la LUN de 100GB TB más adelante hacen que los datos se puedan comprimir menos, el tamaño de la LUN aumentará y el volumen podría llenarse.

Se recomienda encarecidamente el aprovisionamiento ligero porque puede simplificar la gestión y, al mismo tiempo, proporcionar una mejora considerable en la capacidad utilizable con un ahorro de costes asociado. La razón es simple: Los entornos de bases de datos suelen incluir una gran cantidad de espacio vacío, un gran número de volúmenes y LUN, y datos comprimibles. El aprovisionamiento grueso provoca la reserva de espacio en el almacenamiento para volúmenes y LUN por si en algún momento llegan a estar llenos un 100 % y contienen un 100 % de datos que no se pueden comprimir. Es poco probable que esto ocurra. El thin provisioning permite reclamar y utilizar ese espacio en otra parte, y permite que la gestión de la capacidad se base en el propio sistema de almacenamiento en lugar de muchos volúmenes y LUN más pequeños.

Algunos clientes prefieren utilizar el aprovisionamiento pesado, ya sea para cargas de trabajo específicas o, por lo general, basándose en prácticas operativas y de adquisición establecidas.

Si un volumen se aprovisiona en exceso, debe tenerse cuidado desactivar por completo todas las funciones de eficiencia de ese volumen, incluida la descompresión y la eliminación de la deduplicación con `sis undo` el comando. El volumen no debe aparecer en `volume efficiency show` la salida. Si lo hace, el volumen sigue estando parcialmente configurado para las funciones de eficiencia. Como resultado, la sobrescritura garantiza un funcionamiento diferente, lo que aumenta la posibilidad de que las sobretensiones de la configuración hagan que el volumen se quede sin espacio inesperadamente, lo que producirá errores de I/O de la base de datos.

Mejores prácticas de eficiencia

NetApp recomienda lo siguiente:

Valores predeterminados de AFF

Los volúmenes creados en ONTAP en un sistema AFF all-flash son thin provisioning, con todas las funciones de eficiencia inline habilitadas. Aunque por lo general, las bases de datos no se benefician de la deduplicación y pueden incluir datos que no se pueden comprimir, la configuración predeterminada es adecuada para casi todas las cargas de trabajo. ONTAP está diseñado para procesar eficientemente todo tipo de datos y patrones de I/O, independientemente de que generen o no ahorros. Los valores predeterminados solo se deben cambiar si los motivos se entienden por completo y existe un beneficio para desviarse.

Recomendaciones generales

- Si los volúmenes o LUN no son con thin provisioning, debe deshabilitar todas las configuraciones de eficiencia, ya que el uso de estas funciones no proporciona ahorro y la combinación de aprovisionamiento grueso con la eficiencia de espacio habilitada puede provocar un comportamiento inesperado, incluidos errores de falta de espacio.
- Si los datos no están sujetos a sobrescrituras, como con backups o registros de transacciones de base de datos, puede lograr una mayor eficiencia habilitando TSSE con un bajo período de enfriamiento.
- Es posible que algunos archivos contengan una cantidad significativa de datos que no se puedan comprimir, por ejemplo, cuando la compresión ya está activada en el nivel de aplicación de los archivos está cifrada. Si se da alguna de estas situaciones, considere la posibilidad de deshabilitar la compresión para permitir un funcionamiento más eficiente en otros volúmenes que contengan datos comprimibles.
- No utilice la compresión 32KB ni la deduplicación con backups de bases de datos. Consulte la sección Compresión adaptativa para obtener más detalles.

Aprovisionamiento ligero

El thin provisioning para una base de datos de Oracle requiere una planificación cuidadosa porque el resultado es configurar más espacio en un sistema de almacenamiento del que necesariamente está disponible físicamente. Vale mucho la pena el esfuerzo porque, cuando se hace correctamente, el resultado es un ahorro significativo de costes y mejoras en la capacidad de gestión.

El thin provisioning se presenta de muchas formas y forma parte de muchas de las funciones que ofrece ONTAP para un entorno de aplicaciones empresariales. Además, thin provisioning está estrechamente relacionado con las tecnologías de eficiencia por el mismo motivo: Las funciones de eficiencia permiten almacenar más datos lógicos de lo que existen técnicamente en el sistema de almacenamiento.

Casi cualquier uso de las copias Snapshot implica thin provisioning. Por ejemplo, una base de datos de 10TB

TB típica en almacenamiento de NetApp incluye unos 30 días de copias Snapshot. Este arreglo da como resultado aproximadamente 10TB TB de datos visibles en el sistema de archivos activo y 300TB TB dedicados a las copias snapshot. El total de 310TB TB de almacenamiento suele residir en aproximadamente 12TB a 15TB GB de espacio. La base de datos activa consume 10TB GB y los 300TB TB restantes solo requieren de 2TB a 5TB GB de espacio, ya que solo se almacenan los cambios realizados en los datos originales.

La clonación es también un ejemplo de aprovisionamiento ligero. Un importante cliente de NetApp creó 40 clones de una base de datos de 80TB para que los utilizara el equipo de desarrollo. Si los 40 desarrolladores que utilizan estos clones sobrescribieran cada bloque en cada archivo de datos, se necesitarían más de 3,2PB GB de almacenamiento. En la práctica, la rotación es baja y el requisito de espacio colectivo se acerca a 40TB, ya que solo se almacenan cambios en las unidades.

Gestión del espacio

Se debe tener cierta precaución con el thin provisioning de un entorno de aplicaciones porque las tasas de cambios de los datos pueden aumentar de forma inesperada. Por ejemplo, el consumo de espacio debido a las instantáneas puede aumentar rápidamente si se reindexan las tablas de la base de datos o si se aplican parches a gran escala a los huéspedes de VMware. Una copia de seguridad fuera de lugar puede escribir una gran cantidad de datos en muy poco tiempo. Por último, puede ser difícil recuperar algunas aplicaciones si un sistema de archivos se queda sin espacio libre inesperadamente.

Afortunadamente, estos riesgos se pueden abordar con una cuidadosa configuración de `volume-autogrow` y.. `snapshot-autodelete` normativas. Como sus nombres implican, estas opciones permiten al usuario crear políticas que desactiven automáticamente el espacio consumido por las copias Snapshot o aumentar un volumen para alojar datos adicionales. Hay muchas opciones disponibles y las necesidades varían según el cliente.

Consulte "documentación de gestión de almacenamiento lógico" para obtener un análisis completo de estas funciones.

Reservas fraccionarias

La reserva fraccionaria es el comportamiento de una LUN en un volumen con respecto a la eficiencia del espacio. Cuando la opción `fractional-reserve` se establece en 100 %, todos los datos del volumen pueden experimentar una rotación del 100 % con cualquier patrón de datos sin agotar el espacio en el volumen.

Por ejemplo, piense en una base de datos en un único LUN de 250GB GB en un volumen de 1TB GB. La creación de una instantánea provocaría de inmediato la reserva de 250GB GB de espacio adicional en el volumen para garantizar que el volumen no se quede sin espacio por ningún motivo. El uso de reservas fraccionarias suele ser un desperdicio debido a que es extremadamente poco probable que cada byte del volumen de base de datos deba sobrescribirse. No hay razón para reservar espacio para un evento que nunca ocurre. Sin embargo, si un cliente no puede supervisar el consumo de espacio en un sistema de almacenamiento y debe tener la seguridad de que nunca se agota el espacio, se necesitarían reservas fraccionarias del 100% para utilizar copias Snapshot.

Compresión y deduplicación

La compresión y la deduplicación son ambas formas de thin provisioning. Por ejemplo, una huella de datos de 50TB MB puede comprimirse hasta 30TB MB, lo que supone un ahorro de 20TB MB. Para que la compresión proporcione beneficios, algunos de esos 20TB MB deben utilizarse para otros datos o el sistema de almacenamiento debe adquirirse con menos de 50TB TB. El resultado es almacenar más datos de los que están disponibles técnicamente en el sistema de almacenamiento. Desde el punto de vista de los datos, hay 50TB GB de datos, a pesar de que ocupa solo 30TB GB en las unidades.

Siempre existe la posibilidad de que cambie la capacidad de compresión de un conjunto de datos, lo que provocaría un aumento del consumo de espacio real. Este aumento del consumo significa que la compresión debe gestionarse como sucede con otras formas de thin provisioning en términos de supervisión y uso `volume-autogrow` y.. `snapshot-autodelete`.

La compresión y la deduplicación se tratan de forma más detallada en el enlace de sección:efficiency.html

Compresión y reservas fraccionarias

La compresión es una forma de thin provisioning. Las reservas fraccionarias afectan al uso de la compresión, con una nota importante; se reserva espacio con antelación para la creación de la instantánea. Normalmente, la reserva fraccionaria sólo es importante si existe una instantánea. Si no hay ninguna instantánea, la reserva fraccionaria no es importante. Este no es el caso con la compresión. Si se crea una LUN en un volumen con compresión, ONTAP conserva el espacio para acomodar una copia de Snapshot. Este comportamiento puede ser confuso durante la configuración, pero es esperado.

Como ejemplo, piense en un volumen de 10GB GB con una LUN de 5GB TB que se ha comprimido en 2,5GB sin copias Snapshot. Considere estos dos escenarios:

- La reserva fraccionaria = 100 da como resultado el uso de 7,5GB
- La reserva fraccionaria = 0 da como resultado el uso de 2,5GB

El primer escenario incluye 2,5GB GB de consumo de espacio para los datos actuales y 5GB GB de espacio para representar una rotación del 100% de la fuente antes del uso de la tecnología Snapshot. El segundo escenario no reserva espacio extra.

Aunque esta situación pueda parecer confusa, es poco probable que se encuentre en la práctica. La compresión implica thin provisioning y thin provisioning de un entorno de LUN requiere reservas fraccionarias. Siempre es posible que los datos comprimidos se sobrescriban en algo que no se pueda comprimir, lo que significa que un volumen debe estar aplicado mediante thin provisioning para que la compresión produzca ahorro.

NetApp recomienda las siguientes configuraciones de reserva:

- Configurado `fractional-reserve` a 0 cuando se implementa la supervisión de la capacidad básica junto con `volume-autogrow` y.. `snapshot-autodelete`.
- Configurado `fractional-reserve` a 100 si no hay capacidad de monitoreo o si es imposible agotar el espacio bajo cualquier circunstancia.

Espacio libre y asignación de espacio LVM

La eficiencia del thin provisioning de las LUN activas en un entorno de sistema de archivos se puede perder con el tiempo a medida que se eliminan los datos. A menos que los datos eliminados se sobrescriban con ceros (consulte también "ASMRU" O bien, el espacio se libera con la recuperación de espacio TRIM/UNMAP, los datos «borrados» ocupan cada vez más espacio en blanco sin asignar en el sistema de archivos. Además, el thin provisioning de LUN activos es de uso limitado en muchos entornos de bases de datos, ya que los archivos de datos se inicializan en su tamaño completo en el momento de la creación.

Una planificación cuidadosa de la configuración de LVM puede mejorar la eficiencia y minimizar la necesidad de aprovisionar el almacenamiento y redimensionar las LUN. Cuando se utiliza un LVM como Veritas VxVM u Oracle ASM, los LUN subyacentes se dividen en extensiones que solo se utilizan cuando es necesario. Por ejemplo, si un conjunto de datos empieza con un tamaño de 2TB GB, pero podría crecer hasta 10TB TB con el tiempo, este conjunto de datos podría colocarse en 10TB LUN con thin provisioning organizados en un

grupo de discos de LVM. Ocuparía solo 2TB GB de espacio en el momento de la creación y solo reclamaría espacio adicional a medida que se asignan extensiones para acomodar el crecimiento de los datos. Este proceso es seguro siempre y cuando se supervise el espacio.

Recuperación tras fallos y cambio de ONTAP

Se requiere comprender las funciones de toma de control y conmutación de sitios de almacenamiento para garantizar que estas operaciones no interrumpan las operaciones de la base de datos de Oracle. Además, los argumentos utilizados por las operaciones de toma de control y conmutación de sitios pueden afectar a la integridad de los datos si se usan incorrectamente.

- En condiciones normales, las escrituras entrantes en una controladora determinada se reflejan de forma síncrona en su compañero. En un entorno NetApp MetroCluster, las escrituras también se reflejan en una controladora remota. No se reconoce en la aplicación host hasta que se almacena una escritura en medios no volátiles en todas las ubicaciones.
- El medio que almacena los datos de escritura se denomina memoria no volátil o NVMEM. También se conoce a veces como memoria de acceso aleatorio no volátil (NVRAM), y se puede considerar como una caché de escritura aunque funciona como un diario. En un funcionamiento normal, los datos de NVMEM no se leen; solo se utilizan para proteger los datos en caso de un fallo de software o hardware. Cuando se escriben datos en las unidades, los datos se transfieren desde la RAM del sistema, no desde NVMEM.
- Durante una operación de toma de control, un nodo de una pareja de alta disponibilidad toma el control de las operaciones de su compañero. Una conmutación de sitios es básicamente la misma, pero se aplica a las configuraciones de MetroCluster en las que un nodo remoto toma las funciones de un nodo local.

Durante las operaciones de mantenimiento rutinarias, una operación de toma de control o de conmutación de sitios debería ser transparente, excepto en una breve pausa potencial de las operaciones cuando cambian las rutas de red. Sin embargo, las redes pueden ser complicadas y es fácil cometer errores, por lo que NetApp recomienda encarecidamente probar exhaustivamente las operaciones de toma de control y conmutación antes de poner un sistema de almacenamiento en producción. Hacerlo es la única forma de asegurarse de que todas las rutas de red están configuradas correctamente. En un entorno SAN, compruebe cuidadosamente la salida del comando `sanlun lun show -p` para asegurarse de que todas las rutas primarias y secundarias esperadas estén disponibles.

Se debe tener cuidado al emitir una toma de control forzada o cambio. Al forzar un cambio en la configuración de almacenamiento con estas opciones, se ignorará el estado de la controladora propietaria de las unidades y el nodo alternativo tomará el control de las unidades de manera forzada. El forzado incorrecto de una toma de control puede provocar la pérdida de datos o la corrupción. Esto se debe a que una toma de control o una conmutación por error forzada pueden descartar el contenido de NVMEM. Una vez completada la toma de control o la conmutación por error, la pérdida de esos datos implica que los datos almacenados en las unidades pueden revertir a un estado ligeramente más antiguo desde el punto de vista de la base de datos.

En raras ocasiones se debería necesitar una toma de control forzada con un par de alta disponibilidad normal. En prácticamente todas las situaciones de fallo, un nodo se apaga e informa al partner para que se produzca una conmutación automática al respaldo. Hay algunos casos periféricos, como un fallo gradual en el que se pierde la interconexión entre nodos y después se pierde una controladora, en el que se requiere una toma de control forzada. En esta situación, el mirroring entre nodos se pierde antes del fallo de la controladora, lo que significa que la controladora superviviente ya no tendría una copia de las escrituras en curso. Entonces, se debe forzar la toma de control, lo que significa que potencialmente se pueden perder los datos.

La misma lógica se aplica a un switchover de MetroCluster. En condiciones normales, una conmutación es prácticamente transparente. Sin embargo, un desastre puede resultar en una pérdida de conectividad entre el sitio sobreviviente y el sitio del desastre. Desde el punto de vista del sitio sobreviviente, el problema podría ser

nada más que una interrupción en la conectividad entre sitios, y el sitio original podría aún estar procesando datos. Si un nodo no puede comprobar el estado de la controladora principal, solo es posible realizar una conmutación de sitios forzada.

NetApp recomienda tomar las siguientes precauciones:

- Tenga mucho cuidado de no forzar accidentalmente una toma de control o una conmutación de sitios. Normalmente, no se debe forzar, y forzar el cambio puede provocar la pérdida de datos.
- Si se requiere una toma de control forzada o una conmutación por error, asegúrese de que las aplicaciones estén cerradas, todos los sistemas de archivos estén desmontados y los grupos de volúmenes del gestor de volúmenes lógicos (LVM) se varyoffs. Los grupos de discos de ASM deben estar desmontados.
- En caso de una conmutación de MetroCluster forzada, elimine el nodo fallido de todos los recursos de almacenamiento que sobrevivan. Para obtener más información, consulte la Guía de gestión de MetroCluster y recuperación ante desastres para la versión relevante de ONTAP.

MetroCluster y varios agregados

MetroCluster es una tecnología de replicación síncrona que cambia al modo asíncrono en caso de interrupción de la conectividad. Esta es la solicitud más común de los clientes, porque la replicación síncrona garantizada implica que la interrupción de la conectividad del sitio provoca una parada completa de las operaciones de I/O de la base de datos, lo que impide que la base de datos funcione.

Con MetroCluster, los agregados se resincronizan rápidamente después de restaurar la conectividad. A diferencia de otras tecnologías de almacenamiento, MetroCluster nunca debería requerir un nuevo mirroring completo tras un fallo del sitio. Sólo se deben enviar los cambios delta.

En conjuntos de datos que abarcan agregados, existe el pequeño riesgo de que se requieran pasos adicionales de recuperación de datos en un escenario de desastre continuo. Específicamente, si (a) se interrumpe la conectividad entre sitios, (b) se restaura la conectividad, (c) los agregados alcanzan un estado en el que algunos están sincronizados y otros no, y luego (d) se pierde el sitio principal, el resultado es un sitio superviviente en el que los agregados no están sincronizados entre sí. Si esto sucede, algunas partes del conjunto de datos se sincronizan entre sí y no es posible activar aplicaciones, bases de datos o almacenes de datos sin recuperación. Si un conjunto de datos abarca agregados, NetApp recomienda aprovechar los backups basados en instantáneas con una de las muchas herramientas disponibles para verificar la capacidad de recuperación rápida en este escenario inusual.

Configuración de la base de datos

Tamaños de bloque

ONTAP utiliza internamente un tamaño de bloque variable, lo que significa que las bases de datos Oracle se pueden configurar con el tamaño de bloque deseado. Sin embargo, los tamaños de bloque del sistema de archivos pueden afectar al rendimiento y, en algunos casos, un tamaño de bloque de redo más grande puede mejorar el rendimiento.

Tamaños de bloque de archivos de datos

Algunos sistemas operativos ofrecen diferentes tamaños de bloque del sistema de archivos. En el caso de los

sistemas de archivos que admiten archivos de datos de Oracle, el tamaño de bloque debe ser 8KB cuando se utiliza la compresión. Cuando no se necesita compresión, se puede utilizar un tamaño de bloque de 8KB KB o 4KB KB.

Si se coloca un archivo de datos en un sistema de archivos con un bloque de 512 bytes, es posible que los archivos estén mal alineados. El LUN y el sistema de archivos podrían alinearse correctamente de acuerdo con las recomendaciones de NetApp, pero la I/O de archivo estaría mal alineada. Tal desalineación podría causar graves problemas de rendimiento.

Los sistemas de archivos compatibles con redo logs deben utilizar un tamaño de bloque que sea múltiplo del tamaño del bloque de redo. Esto generalmente requiere que tanto el sistema de archivos redo log como el propio redo log utilicen un tamaño de bloque de 512 bytes.

Rehacer tamaños de bloques

Con tasas de redo muy elevadas, es posible que los bloques de 4KB KB rindan mejor porque las tasas de rehacer elevadas permiten realizar I/O en operaciones cada vez más eficientes. Si las tasas de redo son mayores que 50Mbps, considere la posibilidad de probar un tamaño de bloque de 4KB KB.

Se han identificado algunos problemas de los clientes con bases de datos que utilizan redo logs con un tamaño de bloque de 512 bytes en un sistema de archivos con un tamaño de bloque de 4KB KB y muchas transacciones muy pequeñas. La sobrecarga involucrada en la aplicación de varios cambios de 512 bytes a un único bloque del sistema de archivos de 4KB se tradujo en problemas de rendimiento que se resolvieron mediante el cambio del sistema de archivos para que utilizara un tamaño de bloque de 512 bytes.

NetApp recomienda que no cambie el tamaño del bloque de redo a menos que se lo indique un servicio de atención al cliente relevante o una organización de servicios profesionales o que el cambio se base en la documentación oficial del producto.

db_file_multibloque_read_count

La `db_file_multiblock_read_count` El parámetro controla el Núm. Máximo de bloques de bases de datos Oracle que Oracle lee como una sola operación durante la E/S secuencial

Sin embargo, este parámetro no afecta a la cantidad de bloques que Oracle lee durante cualquier operación de lectura ni afecta a las operaciones de lectura aleatorias Solo se ve afectado el tamaño de bloque de I/O secuencial.

Oracle recomienda que el usuario deje este parámetro sin definir. Al hacerlo, el software de la base de datos puede definir automáticamente el valor óptimo. Por lo general, este parámetro se establece en un valor que proporciona un tamaño de I/O de 1MB. Por ejemplo, una lectura de 1MB de bloques de 8KB requeriría la lectura de 128 bloques y el valor predeterminado de este parámetro sería, por lo tanto, de 128.

La mayoría de los problemas de rendimiento de la base de datos observados por NetApp en los sitios de los clientes implican una configuración incorrecta para este parámetro. Hay motivos válidos para cambiar este valor con las versiones 8 y 9 de Oracle. Como resultado, el parámetro puede estar presente sin saberlo en `init.ora` Archivos porque la base de datos se actualizó in situ a Oracle 10 y versiones posteriores. Una configuración heredada de 8 o 16, en comparación con el valor predeterminado de 128, daña significativamente el rendimiento de I/O secuencial.

NetApp recomienda configurar el `db_file_multiblock_read_count` el parámetro no debe estar presente en el `init.ora` archivo. NetApp nunca se ha encontrado con una situación en la que cambiar este parámetro mejoró el rendimiento, pero hay muchos casos en los que causó daños claros en el rendimiento de I/O secuencial.

filesystemio_options

Parámetro de inicialización de Oracle `filesystemio_options` Controla el uso de la E/S asíncrona y directa

Contrariamente a la creencia común, las E/S asincrónicas y directas no son mutuamente excluyentes. NetApp ha observado que este parámetro suele estar mal configurado en los entornos del cliente, y esta mala configuración es el responsable directo de muchos problemas de rendimiento.

La E/S asíncrona significa que las operaciones de I/O de Oracle se pueden paralelizar. Antes de la disponibilidad de E/S asíncrona en varios sistemas operativos, los usuarios configuraron numerosos procesos de escritura de base de datos y cambiaron la configuración del proceso del servidor. Con la E/S asíncrona, el propio sistema operativo realiza E/S en nombre del software de base de datos de forma paralela y altamente eficiente. Este proceso no pone los datos en riesgo y las operaciones críticas, como el redo registro de Oracle, se siguen realizando de forma síncrona.

La E/S directa omite la caché de buffers del SO. Las E/S en un sistema UNIX normalmente fluyen a través de la caché de buffers del sistema operativo. Esto es útil para aplicaciones que no mantienen una caché interna, pero Oracle tiene su propia caché de buffers en SGA. En casi todos los casos, es mejor habilitar la E/S directa y asignar la RAM del servidor a la SGA en lugar de confiar en la caché de buffers del SO. Oracle SGA utiliza la memoria de forma más eficaz. Además, cuando la I/O fluye por el búfer del SO, se somete a un procesamiento adicional, lo que aumenta las latencias. El aumento de las latencias es especialmente notable en operaciones pesadas de I/O de escritura cuando un requisito crucial es la baja latencia.

Las opciones para `filesystemio_options` son:

- **Async.** Oracle envía solicitudes de E/S al sistema operativo para su procesamiento. Este proceso permite a Oracle realizar otro trabajo en lugar de esperar la finalización de E/S y, por lo tanto, aumenta la paralelización de E/S.
- **Directio.** Oracle realiza E/S directamente contra archivos físicos en lugar de enrutar E/S a través de la caché del SO host.
- **None.** Oracle utiliza E/S síncronas y en buffer En esta configuración, la elección entre los procesos de servidor compartido y dedicado y el número de dbwriters son más importantes.
- **Setall.** Oracle utiliza E/S tanto asíncrona como directa En casi todos los casos, el uso de `setall` es óptimo.

La `filesystemio_options` El parámetro no tiene ningún efecto en los entornos DNFS y ASM. El uso de DNFS o ASM da como resultado el uso de E/S tanto asíncrona como directa

Algunos clientes se han encontrado con problemas de E/S asíncronos en el pasado, especialmente con versiones anteriores de Red Hat Enterprise Linux 4 (RHEL4). Algunos consejos anticuados en Internet todavía sugieren evitar la IO asíncrona debido a la información obsoleta. La E/S asíncrona es estable en todos los sistemas operativos actuales. No hay motivo para desactivarlo, sin un error conocido en el sistema operativo.

Si una base de datos ha estado utilizando E/S en búfer, un cambio a E/S directa también puede justificar un cambio en el tamaño de SGA. Al desactivar las E/S en buffer, se elimina la ventaja de rendimiento que

proporciona la caché del SO del host para la base de datos. Al volver a agregar RAM a SGA se soluciona este problema. El resultado neto debe ser una mejora en el rendimiento de E/S.

Aunque casi siempre es mejor utilizar RAM para Oracle SGA que para el almacenamiento en caché de buffers del sistema operativo, puede ser imposible determinar el mejor valor. Por ejemplo, puede ser preferible utilizar E/S en buffer con tamaños SGA muy pequeños en un servidor de bases de datos con muchas instancias de Oracle activas de forma intermitente. Esta disposición permite el uso flexible de la RAM libre restante en el SO por todas las instancias de base de datos en ejecución. Se trata de una situación muy inusual, pero se ha observado en algunos sitios de clientes.

NetApp recomienda ajuste `filesystemio_options` para `setall`, Pero tenga en cuenta que, en algunas circunstancias, la pérdida de la caché de buffers del host puede requerir un aumento en Oracle SGA.

Tiempo de espera de RAC

Oracle RAC es un producto de clusterware con varios tipos de procesos internos de latido que controlan el estado del cluster.

La información de la "recuento de errores" La sección incluye información crítica para entornos Oracle RAC que utilizan almacenamiento en red y, en muchos casos, la configuración predeterminada de Oracle RAC deberá cambiarse para garantizar que el cluster RAC sobrevive los cambios de ruta de red y las operaciones de failover/switchover de almacenamiento.

tiempo de espera del disco

El parámetro de RAC relacionado con el almacenamiento primario es `disktimeout`. Este parámetro controla el umbral en el que debe completarse la E/S del archivo de quorum. Si la `disktimeout` Se supera el parámetro y el nodo RAC se expulsa del clúster. El valor predeterminado de este parámetro es 200. Este valor debería ser suficiente para los procedimientos estándar de toma de control y devolución del almacenamiento.

NetApp recomienda probar exhaustivamente las configuraciones de RAC antes de colocarlas en producción, ya que existen muchos factores que afectan a una toma de control o al retorno primario. Además del tiempo necesario para que se complete la conmutación por error del almacenamiento, también se requiere más tiempo para que se propaguen los cambios del protocolo de control de agregación de enlaces (LACP). Además, el software multivía SAN debe detectar un tiempo de espera de I/O y volver a intentarlo en una ruta alternativa. Si una base de datos está extremadamente activa, se debe poner en cola una gran cantidad de E/S y volver a intentarlo antes de procesar la E/S del disco de quorum.

Si no se puede realizar una toma de control o una devolución del almacenamiento real, el efecto se puede simular mediante pruebas de extracción de cables en el servidor de bases de datos.

NetApp recomienda lo siguiente:

- Dejando el `disktimeout` parámetro con el valor predeterminado de 200.
- Pruebe siempre a fondo una configuración de RAC.

recuento de errores

La `misscount` Normalmente, el parámetro sólo afecta al latido de red entre los nodos de RAC. El valor predeterminado es 30 segundos. Si los binarios de grid se encuentran en una cabina de almacenamiento o si la unidad de arranque del sistema operativo no es local, este parámetro puede volverse importante. Esto

incluye hosts con unidades de arranque ubicadas en una SAN FC, sistemas operativos arrancados NFS y unidades de arranque ubicadas en almacenes de datos de virtualización, como un archivo VMDK.

Si el acceso a una unidad de arranque se interrumpe por una toma de control o una restauración del almacenamiento, es posible que la ubicación binaria del grid o todo el sistema operativo se bloquee temporalmente. El tiempo necesario para que ONTAP complete la operación de almacenamiento y que el sistema operativo cambie de rutas y reanude las I/O puede superar el `misscount` umbral. Como resultado, un nodo se expulsa inmediatamente después de restaurar la conectividad con el LUN de arranque o los binarios de grid. En la mayoría de los casos, la expulsión y el reinicio posterior se producen sin mensajes de registro que indiquen el motivo del reinicio. No todas las configuraciones se ven afectadas, por lo que debe realizar pruebas de cualquier host basado en almacenes de datos, arranque en NFS o arranque en SAN en un entorno RAC para que RAC se mantenga estable si se interrumpe la comunicación con la unidad de arranque.

En el caso de unidades de arranque no locales o de un sistema de archivos no local `grid` binarios, el `misscount` será necesario cambiar para que coincida `disktimeout`. Si se cambia este parámetro, realice otras pruebas para identificar también cualquier efecto sobre el comportamiento de RAC, como el tiempo de conmutación por error del nodo.

NetApp recomienda lo siguiente:

- Abandone el `misscount` parámetro con el valor por defecto de 30 a menos que se aplique una de las siguientes condiciones:
  - `grid` Los binarios se encuentran en una unidad conectada a la red, como las unidades basadas en almacén de datos, NFS, iSCSI y FC.
  - El sistema operativo se inicia mediante SAN.
- En tales casos, evalúe el efecto de las interrupciones de la red que afectan el acceso al sistema operativo o. `GRID_HOME` sistemas de ficheros: En algunos casos, estas interrupciones provocan que los daemons de Oracle RAC se atasquen, lo que puede provocar un `misscount`-basado en tiempo de espera y desalojo. El tiempo de espera predeterminado es 27 segundos, que es el valor de `misscount` menos `reboottime`. En tales casos, aumentar `misscount` a 200 para coincidir `disktimeout`.

Configuración de hosts

AIX

Temas de configuración para bases de datos de Oracle en IBM AIX con ONTAP.

I/O concurrente

Lograr un rendimiento óptimo en IBM AIX requiere el uso de E/S concurrentes Sin operaciones de I/O simultáneas, es probable que las limitaciones de rendimiento se deban a que AIX realiza I/O atómicas serializadas, lo que conlleva una sobrecarga significativa.

En un principio, NetApp recomendó utilizar el `cio` Opción de montaje para forzar el uso de E/S concurrentes en el sistema de archivos, pero este proceso tenía inconvenientes y ya no es necesario. Desde la introducción de AIX 5,2 y Oracle 10gR1, Oracle en AIX puede abrir archivos individuales para I/O simultánea, en lugar de forzar las operaciones de I/O simultáneas en todo el sistema de archivos.

El mejor método para habilitar E/S concurrente es establecer el `init.ora` parámetro `filesystemio_options` para `setall`. Al hacerlo, Oracle puede abrir archivos específicos para utilizarlos

con E/S simultáneas

Uso `cio` Como opción de montaje fuerza el uso de I/O concurrente, lo cual puede tener consecuencias negativas. Por ejemplo, al forzar la E/S simultánea se desactiva la lectura anticipada en los sistemas de archivos, lo que puede dañar el rendimiento de las E/S que se producen fuera del software de la base de datos Oracle, como copiar archivos y realizar copias de seguridad en cinta. Además, productos como Oracle GoldenGate y SAP BR*Tools no son compatibles con el uso del `cio` Opción de montaje con determinadas versiones de Oracle.

NetApp recomienda lo siguiente:

- No utilice la `cio` opción de montaje en el nivel de sistema de archivos. En su lugar, habilite la I/O simultánea mediante el uso de `filesystemio_options=setall`.
- Utilice sólo el `cio` la opción de montaje debería si no es posible configurarla `filesystemio_options=setall`.

Opciones de montaje de AIX NFS

En la siguiente tabla, se enumeran las opciones de montaje de AIX NFS para bases de datos de instancia única de Oracle.

Tipo de archivo	Opciones de montaje
Directorio Raíz de ADR	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144`
Archivos de control Archivos de datos Rehacer registros	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144`
`ORACLE_HOME`	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144, intr`

En la siguiente tabla, se enumeran las opciones de montaje de AIX NFS para RAC.

Tipo de archivo	Opciones de montaje
Directorio Raíz de ADR	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144`
Archivos de control Archivos de datos Rehacer registros	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144, nointr,noac`
`CRS/Voting`	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144, nointr,noac`
Específico `ORACLE_HOME`	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144`
Compartido `ORACLE_HOME`	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144, nointr`

La diferencia principal entre las opciones de montaje de instancia única y RAC es la adición de `noac` a las opciones de montaje. Esta adición tiene el efecto de deshabilitar el almacenamiento en caché del SO del host que permite que todas las instancias del clúster RAC tengan una vista uniforme del estado de los datos.

Aunque utilice el `cio` monte la opción y la `init.ora` parámetro `filesystemio_options=setall` tiene el mismo efecto de deshabilitar el almacenamiento en caché de host, sigue siendo necesario utilizarlo `noac`. `noac` es necesario para el uso compartido `ORACLE_HOME` Despliegues para facilitar la coherencia de archivos como archivos de contraseñas de Oracle y. `spfile` archivos de parámetros. Si cada instancia de un clúster de RAC tiene un dedicado `ORACLE_HOME`, entonces este parámetro no es necesario.

Opciones de montaje jfs/JFS2 de AIX

En la siguiente tabla se enumeran las opciones de montaje jfs/JFS2 de AIX.

Tipo de archivo	Opciones de montaje
Directorio Raíz de ADR	Valores predeterminados
Archivos de control Archivos de datos Rehacer registros	Valores predeterminados
ORACLE_HOME	Valores predeterminados

Antes de utilizar AIX `hdisk` los dispositivos de cualquier entorno, incluidas las bases de datos, comprueban el parámetro `queue_depth`. Este parámetro no es la profundidad de la cola del HBA, más bien se relaciona con la profundidad de la cola SCSI de una persona `hdisk device. Depending on how the LUNs are configured, the value for `queue_depth` puede ser demasiado bajo para un buen rendimiento. Las pruebas han demostrado que el valor óptimo es 64.

HP-UX

Temas de configuración para bases de datos de Oracle en HP-UX con ONTAP.

Opciones de montaje NFS de HP-UX

En la siguiente tabla se enumeran las opciones de montaje de HP-UX NFS para una única instancia.

Tipo de archivo	Opciones de montaje
Directorio Raíz de ADR	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144, suid`
Archivos de control Archivos de datos Rehacer registros	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144,forc edirectio, nointr,suid`
`ORACLE_HOME`	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144, suid`

En la siguiente tabla se enumeran las opciones de montaje de HP-UX NFS para RAC.

Tipo de archivo	Opciones de montaje
Directorio Raíz de ADR	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144, noac,suid`
Archivos de control Archivos de datos Rehacer registros	`rw, bg,hard, [vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144, nointr,noac,forcedirectio,suid`
CRS/votación	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144, nointr,noac, forcedirectio,suid`
Específico `ORACLE_HOME`	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144, suid`
Compartido `ORACLE_HOME`	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144, nointr,noac,suid`

La diferencia principal entre las opciones de montaje de instancia única y RAC es la adición de `noac` y.. `forcedirectio` a las opciones de montaje. Esta adición tiene el efecto de deshabilitar el almacenamiento en caché del sistema operativo del host, lo que permite que todas las instancias del clúster RAC tengan una vista coherente del estado de los datos. Aunque utilice el `init.ora` parámetro `filesystemio_options=setall` tiene el mismo efecto de deshabilitar el almacenamiento en caché de host, sigue siendo necesario utilizarlo `noac` y.. `forcedirectio`.

La razón `noac` es necesario para el uso compartido `ORACLE_HOME` Despliegues es para facilitar la coherencia de archivos como archivos de contraseñas de Oracle y archivos spfiles. Si cada instancia de un clúster de RAC tiene un dedicado `ORACLE_HOME`, este parámetro no es necesario.

Opciones de montaje HP-UX VxFS

Utilice las siguientes opciones de montaje para sistemas de archivos que alojan binarios de Oracle:

```
delaylog,nodatainlog
```

Utilice las siguientes opciones de montaje para sistemas de archivos que contienen archivos de datos, redo logs, archive logs y archivos de control en los que la versión de HP-UX no admite E/S simultáneas:

```
nodatainlog,mincache=direct,convosync=direct
```

Cuando se admiten E/S simultáneas (VxFS 5.0.1 y posteriores, o con ServiceGuard Storage Management Suite), utilice estas opciones de montaje para sistemas de archivos que contengan archivos de datos, redo logs, archive logs y archivos de control:

```
delaylog,cio
```

El parámetro `db_file_multiblock_read_count` Es especialmente crítico en entornos VxFS. Oracle recomienda que este parámetro permanezca sin definir en Oracle 10g R1 y posteriores a menos que se indique lo contrario específicamente. El valor por defecto con un tamaño de bloque de Oracle 8KB es 128. Si el valor de este parámetro se fuerza a 16 o menos, quite el `convosync=direct` Opción de montaje porque puede dañar el rendimiento de I/O secuencial. Este paso daña otros aspectos del rendimiento y solo debe tomarse si el valor de `db_file_multiblock_read_count` debe cambiarse a partir del valor predeterminado.

Linux

Temas de configuración específicos del sistema operativo Linux.

Tablas de ranuras TCP Linux NFSv3

Las tablas de ranuras TCP son equivalentes a NFSv3 a la profundidad de la cola del adaptador de bus de host (HBA). En estas tablas se controla el número de operaciones de NFS que pueden extraordinarias a la vez. El valor predeterminado suele ser 16, que es demasiado bajo para un rendimiento óptimo. El problema opuesto ocurre en los kernels más nuevos de Linux, que pueden aumentar automáticamente el límite de la tabla de ranuras TCP a un nivel que sature el servidor NFS con solicitudes.

Para obtener un rendimiento óptimo y evitar problemas de rendimiento, ajuste los parámetros del núcleo que controlan las tablas de ranuras TCP.

Ejecute el `sysctl -a | grep tcp.*.slot_table` command, y observe los siguientes parámetros:

```
# sysctl -a | grep tcp.*.slot_table
sunrpc.tcp_max_slot_table_entries = 128
sunrpc.tcp_slot_table_entries = 128
```

Todos los sistemas Linux deben incluir `sunrpc.tcp_slot_table_entries`, pero solo algunos incluyen `sunrpc.tcp_max_slot_table_entries`. Ambos deben establecerse en 128.

Si no se establecen estos parámetros, puede tener efectos significativos en el rendimiento. En algunos casos, el rendimiento es limitado porque el sistema operativo linux no está emitiendo suficiente I/O. En otros casos, las latencias de I/O aumentan cuando el sistema operativo linux intenta emitir más operaciones de I/O de las que se pueden mantener.

Opciones de montaje de Linux NFS

En la siguiente tabla, se enumeran las opciones de montaje de NFS de Linux para una instancia única.

Tipo de archivo	Opciones de montaje
Directorio Raíz de ADR	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144`

Tipo de archivo	Opciones de montaje
Archivos de control Archivos de datos Rehacer registros	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144,nointr`
ORACLE_HOME	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144,nointr`

La siguiente tabla enumera las opciones de montaje de NFS de Linux para RAC.

Tipo de archivo	Opciones de montaje
Directorio Raíz de ADR	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144,actimeo=0`
Archivos de control Archivos de datos Rehacer registros	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144,nointr,actimeo=0`
CRS/votación	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144,nointr,noac,actimeo=0`
Específico `ORACLE_HOME`	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144`
Compartido `ORACLE_HOME`	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144,nointr,actimeo=0`

La diferencia principal entre las opciones de montaje de instancia única y RAC es la adición de `actimeo=0` a las opciones de montaje. Esta adición tiene el efecto de deshabilitar el almacenamiento en caché del sistema operativo del host, lo que permite que todas las instancias del clúster RAC tengan una vista coherente del estado de los datos. Aunque utilice el `init.ora` parámetro `filesystemio_options=setall` tiene el mismo efecto de deshabilitar el almacenamiento en caché de host, sigue siendo necesario utilizarlo `actimeo=0`.

La razón `actimeo=0` es necesario para el uso compartido `ORACLE_HOME` Despliegues es para facilitar la consistencia de archivos como los archivos de contraseñas de Oracle y spfiles. Si cada instancia de un clúster de RAC tiene un dedicado `ORACLE_HOME`, entonces este parámetro no es necesario.

Por lo general, los archivos que no son de base de datos se deben montar con las mismas opciones utilizadas para los archivos de datos de instancia única, aunque las aplicaciones específicas pueden tener requisitos diferentes. Evite las opciones de montaje `noac` y.. `actimeo=0` si es posible, ya que estas opciones desactivan la lectura anticipada y el almacenamiento en búfer de nivel de sistema de archivos. Esto puede causar graves problemas de rendimiento en procesos como extracción, traducción y carga.

ACCESO y GETATTR

Algunos clientes han observado que un nivel extremadamente alto de otros IOPS, como EL ACCESO y GETATTR, puede dominar sus cargas de trabajo. En casos extremos, las operaciones como las de lectura y escritura pueden ser tan bajas como el 10 % del total. Este es un comportamiento normal con cualquier base

de datos que incluya el uso `actimeo=0` y/o. `noac` En Linux, porque estas opciones provocan que el sistema operativo Linux vuelva a cargar constantemente los metadatos de los archivos del sistema de almacenamiento. Las operaciones como EL ACCESO y GETATTR son operaciones de bajo impacto que se proporcionan desde la caché de ONTAP en un entorno de base de datos. No se deben considerar IOPS auténticos, como lecturas y escrituras, que crean una demanda real de sistemas de almacenamiento. Sin embargo, estas otras IOPS crean una cierta carga, sobre todo en entornos RAC. Para solucionar esta situación, habilite DNFS, que omite la caché de buffers del sistema operativo y evita estas operaciones de metadatos innecesarias.

NFS directo de Linux

Una opción de montaje adicional denominada `nosharecache`, Es necesario cuando (a) DNFS está activado y (b) un volumen de origen se monta más de una vez en un único servidor (c) con un montaje NFS anidado. Esta configuración se ve principalmente en entornos que admiten aplicaciones SAP. Por ejemplo, un único volumen de un sistema NetApp podría tener un directorio ubicado en `/vol/oracle/base` y un segundo en `/vol/oracle/home`. Si `/vol/oracle/base` está montado en `/oracle` y.. `/vol/oracle/home` está montado en `/oracle/home`, El resultado son montajes NFS anidados que se originan en la misma fuente.

El sistema operativo puede detectar el hecho de que `/oracle` y `/oracle/home` residen en el mismo volumen, que es el mismo sistema de archivos de origen. A continuación, el sistema operativo utiliza el mismo identificador de dispositivo para acceder a los datos. Al hacerlo, se mejora el uso del almacenamiento en caché del sistema operativo y algunas otras operaciones, pero interfiere con DNFS. Si DNFS debe acceder a un archivo, como `spfile` , activado `/oracle/home`, puede intentar utilizar erróneamente la ruta de acceso incorrecta a los datos. El resultado es una operación de I/O con errores. En estas configuraciones, agregue `nosharecache` la opción de montaje a cualquier sistema de archivos NFS que comparta un volumen de origen con otro sistema de archivos NFS en ese host. Al hacerlo, se fuerza al sistema operativo Linux a asignar un identificador de dispositivo independiente para ese sistema de archivos.

Linux Direct NFS y Oracle RAC

El uso de DNFS ofrece ventajas especiales de rendimiento para Oracle RAC en el sistema operativo Linux, ya que Linux no dispone de un método para forzar la entrada/salida directa, que se necesita con RAC para lograr coherencia entre los nodos. Como solución alternativa, Linux requiere el uso de `actimeo=0` Opción de montaje, que hace que los datos de archivo caduquen inmediatamente desde la caché del sistema operativo. Esta opción, a su vez, fuerza al cliente NFS de Linux a volver a leer constantemente los datos de atributos, lo que daña la latencia y aumenta la carga en la controladora de almacenamiento.

Al habilitar DNFS se omite el cliente NFS del host y se evita este daño. Varios clientes han informado de mejoras significativas en el rendimiento en clústeres RAC y reducciones considerables en la carga de ONTAP (especialmente con respecto a otras IOPS) al habilitar DNFS.

Linux Direct NFS y archivo oranfstab

Al utilizar DNFS en Linux con la opción multipathing, se deben utilizar varias subredes. En otros sistemas operativos, se pueden establecer varios canales DNFS mediante el `LOCAL` y.. `DONTROUTE` Opciones para configurar varios canales DNFS en una sola subred. Sin embargo, esto no funciona correctamente en Linux y puede resultar en problemas de rendimiento inesperados. Con Linux, cada NIC utilizada para el tráfico DNFS debe estar en una subred diferente.

Programador de I/O.

El kernel de Linux permite un control de bajo nivel sobre la forma en que se programa la E/S para bloquear los dispositivos. Los valores por defecto en varias distribuciones de Linux varían considerablemente. Las pruebas demuestran que la fecha límite suele ofrecer los mejores resultados, pero en ocasiones NOOP ha sido ligeramente mejor. La diferencia de rendimiento es mínima, pero pruebe ambas opciones si es necesario

extraer el máximo rendimiento posible de una configuración de base de datos. CFQ es el valor predeterminado en muchas configuraciones y ha demostrado tener problemas de rendimiento significativos con cargas de trabajo de bases de datos.

Consulte la documentación relevante del proveedor de Linux para obtener instrucciones sobre la configuración del programador de E/S.

Accesos múltiples

Algunos clientes se han encontrado con fallos durante la interrupción de la red porque el daemon multivía no se estaba ejecutando en su sistema. En versiones recientes de Linux, el proceso de instalación del sistema operativo y el daemon de rutas múltiples pueden dejar estos sistemas operativos vulnerables a este problema. Los paquetes están instalados correctamente, pero no están configurados para el inicio automático después de un reinicio.

Por ejemplo, el valor predeterminado para el daemon multipath en RHEL5,5 puede aparecer del siguiente modo:

```
[root@host1 iscsi]# chkconfig --list | grep multipath
multipathd      0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

Esto se puede corregir con los siguientes comandos:

```
[root@host1 iscsi]# chkconfig multipathd on
[root@host1 iscsi]# chkconfig --list | grep multipath
multipathd      0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Duplicación de ASM

La duplicación de ASM puede requerir cambios en la configuración multivía de Linux para permitir que ASM reconozca un problema y cambie a un grupo de fallos alternativo. La mayoría de las configuraciones de ASM en ONTAP utilizan redundancia externa, lo que significa que la cabina externa ofrece protección de datos y ASM no refleja datos. Algunos sitios utilizan ASM con redundancia normal para proporcionar duplicación bidireccional, normalmente en diferentes sitios.

La configuración de Linux que se muestra en la "Documentación de utilidades de host de NetApp" Incluya parámetros multivía que generen la cola indefinida de I/O. Esto significa que una I/O en un dispositivo LUN sin rutas activas espera tanto tiempo como sea necesario para que finalice la I/O. Esto suele ser deseable ya que los hosts Linux esperan todo el tiempo necesario para que se completen los cambios de ruta SAN, para que se reinicien los switches FC o para que un sistema de almacenamiento complete una conmutación al respaldo.

Este comportamiento de puesta en cola ilimitada provoca un problema con el mirroring de ASM debido a que ASM debe recibir un error de I/O para que vuelva a intentar I/O en un LUN alternativo.

Defina los siguientes parámetros en Linux `multipath.conf` Archivo para LUN de ASM utilizados con la duplicación de ASM:

```
polling_interval 5
no_path_retry 24
```

Estos valores crean un timeout de 120 segundos para los dispositivos ASM. El tiempo de espera se calcula como el `polling_interval` * `no_path_retry` como segundos. Puede que sea necesario ajustar el valor exacto en algunas circunstancias, pero un tiempo de espera de 120 segundos debería ser suficiente para la mayoría de los usos. Concretamente, 120 segundos deberían permitir que se produzca una toma de control o una devolución de la controladora sin que se produzca un error de I/O, lo que provocaría que el grupo de errores se desconectara.

A inferior `no_path_retry` Value puede reducir el tiempo necesario para que ASM cambie a un grupo de fallos alternativo, pero esto también aumenta el riesgo de una conmutación por error no deseada durante actividades de mantenimiento como la toma de control de un controlador. El riesgo se puede mitigar mediante una supervisión cuidadosa del estado de duplicación de ASM. Si se produce una conmutación al respaldo no deseada, los duplicados pueden volver a sincronizarse rápidamente si la resincronización se realiza con relativa rapidez. Para obtener información adicional, consulte la documentación de Oracle on ASM Fast Mirror Resync para ver la versión del software de Oracle en uso.

Opciones de montaje de Linux xfs, ext3 y ext4

NetApp recomienda usar las opciones de montaje predeterminadas.

ASMLib/AFD (Controlador de Filtro de ASM)

Temas de configuración específicos del sistema operativo Linux mediante AFD y ASMLib

Tamaños de bloque ASMLib

ASMLib es una biblioteca de gestión de ASM opcional y utilidades asociadas. Su valor principal es la capacidad para estampar un LUN o un archivo basado en NFS como un recurso ASM con una etiqueta legible para el ser humano.

Las versiones recientes de ASMLib detectan un parámetro de LUN llamado Logical Blocks per Physical Block Exponent (LBPPBE). El destino SCSI de ONTAP no notificó este valor hasta hace poco. Ahora devuelve un valor que indica que se prefiere un tamaño de bloque de 4KB KB. Esta no es una definición de tamaño de bloque, pero es una indicación para cualquier aplicación que utilice LBPPBE de que las E/S de un determinado tamaño podrían manejarse de manera más eficiente. Sin embargo, ASMLib interpreta LBPPBE como un tamaño de bloque y marca de forma persistente la cabecera ASM cuando se crea el dispositivo ASM.

Este proceso puede causar problemas con actualizaciones y migraciones de varias maneras, todo ello en función de la incapacidad de mezclar dispositivos ASMLib con diferentes tamaños de bloque en el mismo grupo de discos ASM.

Por ejemplo, las matrices más antiguas generalmente reportaron un valor LBPPBE de 0 o no reportaron este valor en absoluto. ASMLib lo interpreta como un tamaño de bloque de 512 bytes. Las cabinas más recientes se interpretarán con un tamaño de bloque de 4KB KB. No es posible mezclar dispositivos de 512 bytes y 4KB en el mismo grupo de discos ASM. Al hacerlo, se bloquearía a un usuario para que no aumente el tamaño del grupo de discos de ASM utilizando LUN de dos matrices o aprovechando ASM como herramienta de migración. En otros casos, es posible que RMAN no permita la copia de archivos entre un grupo de discos de ASM con un tamaño de bloque de 512 bytes y un grupo de discos de ASM con un tamaño de bloque de 4KB KB.

La solución preferida es parchear ASMLib. El identificador de error de Oracle es 13999609 y el parche está presente en oracleasm-support-2,1.8-1 y superior. Este parche permite al usuario definir el parámetro `ORACLEASM_USE_LOGICAL_BLOCK_SIZE` para `true` en la `/etc/sysconfig/oracleasm` archivo de configuración. Al hacerlo, se bloquea ASMLib para que no utilice el parámetro LBPPBE, lo que significa que los LUN de la nueva matriz ahora se reconocen como dispositivos de bloque de 512 bytes.

> La opción no cambia el tamaño de bloque en LUN que ASMLib estampó anteriormente. Por ejemplo, si un grupo de discos ASM con bloques de 512 bytes debe migrarse a un nuevo sistema de almacenamiento que notifique un bloque de 4KB KB, la opción `ORACLEASM_USE_LOGICAL_BLOCK_SIZE` Debe establecerse antes de que las nuevas LUN se estampen con ASMLib. Si los dispositivos ya han sido estampados por oracleasm, deben ser reformateados antes de ser reincorporados con un nuevo tamaño de bloque. En primer lugar, desconfigure el dispositivo con `oracleasm deletedisk`, Y, a continuación, borre los primeros 1GB del dispositivo con `dd if=/dev/zero of=/dev/mapper/device bs=1048576 count=1024`. Por último, si el dispositivo se ha particionado previamente, utilice `kpartx` Comando para eliminar particiones obsoletas o simplemente reiniciar el sistema operativo.

Si no se puede aplicar un parche a ASMLib, se puede eliminar ASMLib de la configuración. Este cambio es disruptivo y requiere el desestampado de discos de ASM y asegurarse de que el `asm_diskstring` el parámetro se ha definido correctamente. Sin embargo, este cambio no requiere la migración de datos.

Tamaños de bloque de unidad de filtro de ASM (AFD)

AFD es una biblioteca de gestión de ASM opcional que se está convirtiendo en el reemplazo de ASMLib. Desde el punto de vista del almacenamiento, es muy similar a ASMLib, pero incluye características adicionales como la capacidad de bloquear E/S no Oracle para reducir las posibilidades de errores de usuario o aplicación que podrían dañar los datos.

Tamaños de bloques de dispositivos

Al igual que ASMLib, AFD también lee el parámetro LUN Bloques lógicos por Exponente de bloque físico (LBPPBE) y utiliza de forma predeterminada el tamaño del bloque físico, no el tamaño del bloque lógico.

Esto podría crear un problema si se agrega AFD a una configuración existente donde los dispositivos ASM ya están formateados como dispositivos de bloque de 512 bytes. El controlador AFD reconocería el LUN como un dispositivo 4K y la discrepancia entre la etiqueta ASM y el dispositivo físico impediría el acceso. Del mismo modo, las migraciones se verían afectadas porque no es posible mezclar dispositivos de 512 bytes y 4KB en el mismo grupo de discos de ASM. Al hacerlo, se bloquearía a un usuario para que no aumente el tamaño del grupo de discos de ASM utilizando LUN de dos matrices o aprovechando ASM como herramienta de migración. En otros casos, es posible que RMAN no permita la copia de archivos entre un grupo de discos de ASM con un tamaño de bloque de 512 bytes y un grupo de discos de ASM con un tamaño de bloque de 4KB KB.

La solución es simple: AFD incluye un parámetro para controlar si utiliza los tamaños de bloque lógicos o físicos. Este es un parámetro global que afecta a todos los dispositivos del sistema. Para forzar a AFD a utilizar el tamaño de bloque lógico, establezca `options oracleafd oracleafd_use_logical_block_size=1` en la `/etc/modprobe.d/oracleafd.conf` archivo.

Tamaños de transferencia multivía

Los cambios recientes del kernel de linux aplican las restricciones de tamaño de I/O enviadas a dispositivos multivía y el AFD no cumple con estas restricciones. A continuación, se rechazan las I/O, lo que hace que la ruta de LUN se desconecte. El resultado es una incapacidad para instalar Oracle Grid, configurar ASM o crear una base de datos.

La solución es especificar manualmente la longitud máxima de transferencia del archivo multipath.conf para las LUN de ONTAP:

```
devices {
            device {
                vendor "NETAPP"
                product "LUN.*"
                max_sectors_kb 4096
        }
    }
```

Incluso si no existe ningún problema en la actualidad, este parámetro debe configurarse si se utiliza AFD para garantizar que una actualización de linux futura no cause problemas de forma inesperada.

Microsoft Windows

Temas de configuración de bases de datos de Oracle en Microsoft Windows con ONTAP.

NFS

Oracle admite el uso de Microsoft Windows con el cliente NFS directo. Esta funcionalidad ofrece un acceso a las ventajas de gestión de NFS, incluida la capacidad de ver archivos de distintos entornos, cambiar el tamaño de volúmenes de forma dinámica y utilizar un protocolo IP menos costoso. Consulte la documentación oficial de Oracle para obtener información sobre la instalación y configuración de una base de datos en Microsoft Windows mediante DNFS. No existen mejores prácticas especiales.

SAN

Para una eficiencia de compresión óptima, asegúrese de que el sistema de archivos NTFS utilice una unidad de asignación de 8K o más. El uso de una unidad de asignación de 4K, que suele ser la predeterminada, afecta negativamente a la eficiencia de la compresión.

Solaris

Temas de configuración específicos del sistema operativo Solaris.

Opciones de montaje NFS de Solaris

En la siguiente tabla se enumeran las opciones de montaje NFS de Solaris para una única instancia.

Tipo de archivo	Opciones de montaje
Directorio Raíz de ADR	`rw,bg,hard,[vers=3,vers=4.1], roto=tcp, timeo=600,rsize=262144,wsize=262144`
Archivos de control Archivos de datos Rehacer registros	`rw,bg,hard,[vers=3,vers=4.1],proto=tcp, timeo=600,rsize=262144,wsize=262144, nointr,llock,suid`

Tipo de archivo	Opciones de montaje
ORACLE_HOME	rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144,suid

Uso de `llock` se ha demostrado que mejora drásticamente el rendimiento en entornos de cliente al eliminar la latencia asociada con la adquisición y la liberación de bloqueos en el sistema de almacenamiento. Utilice esta opción con cuidado en entornos en los que se han configurado varios servidores para montar los mismos sistemas de archivos y Oracle está configurado para montar estas bases de datos. Aunque esta es una configuración muy inusual, es utilizada por un pequeño número de clientes. Si una instancia se inicia accidentalmente por segunda vez, se pueden producir daños en los datos porque Oracle no puede detectar los archivos de bloqueo en el servidor externo. Los bloqueos NFS no ofrecen protección de otro modo; al igual que en la versión 3 de NFS, solo son orientativos.

Debido a que el `llock` y.. `forcedirectio` los parámetros se excluyen entre sí, es importante hacerlo `filesystemio_options=setall` está presente en la `init.ora` archiva así `directio` se utiliza. Sin este parámetro, se utiliza el almacenamiento en caché del búfer del sistema operativo del host y el rendimiento se puede ver afectado negativamente.

En la siguiente tabla se muestran las opciones de montaje de Solaris NFS RAC.

Tipo de archivo	Opciones de montaje
Directorio Raíz de ADR	rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144,noac
Archivos de control Archivos de datos Rehacer registros	rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144,nointr,noac,forcedirectio
CRS/votación	rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144,nointr,noac,forcedirectio
Específico ORACLE_HOME	rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144,suid
Compartido ORACLE_HOME	rw,bg,hard,[vers=3,vers=4.1],proto=tcp,timeo=600,rsize=262144,wsize=262144,nointr,noac,suid

La diferencia principal entre las opciones de montaje de instancia única y RAC es la adición de `noac` y.. `forcedirectio` a las opciones de montaje. Esta adición tiene el efecto de deshabilitar el almacenamiento en caché del sistema operativo del host, lo que permite que todas las instancias del clúster RAC tengan una vista coherente del estado de los datos. Aunque utilice el `init.ora` parámetro `filesystemio_options=setall` tiene el mismo efecto de deshabilitar el almacenamiento en caché de host, sigue siendo necesario utilizarlo `noac` y.. `forcedirectio`.

La razón `actimeo=0` es necesario para el uso compartido `ORACLE_HOME` Despliegues es para facilitar la coherencia de archivos como archivos de contraseñas de Oracle y archivos spfiles. Si cada instancia de un clúster de RAC tiene un dedicado `ORACLE_HOME`, este parámetro no es necesario.

Opciones de montaje UFS de Solaris

NetApp recomienda usar la opción de montaje de registro para conservar la integridad de los datos en caso de bloqueo del host Solaris o interrupción de la conectividad de FC. La opción de montaje logging también conserva la facilidad de uso de los backups de Snapshot.

ZFS de Solaris

Solaris ZFS debe instalarse y configurarse cuidadosamente para ofrecer un rendimiento óptimo.

mvector

Solaris 11 incluyó un cambio en la forma en que procesa grandes operaciones de E/S, lo que puede dar lugar a graves problemas de rendimiento en las matrices de almacenamiento SAN. El problema está documentado en el informe de errores de seguimiento de NetApp 630173, que indica que Solaris 11 ZFS Performance Regression.

Esto no es un bug de ONTAP. Se trata de un defecto de Solaris cuyo seguimiento se realiza bajo los defectos de Solaris 7199305 y 7082975.

Puede consultar a los Servicios de Soporte Oracle para averiguar si la versión de Solaris 11 está afectada o puede probar la solución provisional cambiando `zfs_mvector_max_size` a un valor menor.

Para ello, ejecute el siguiente comando como root:

```
[root@host1 ~]# echo "zfs_mvector_max_size/W 0t131072" |mdb -kw
```

Si surge algún problema inesperado de este cambio, se puede revertir fácilmente ejecutando el siguiente comando como root:

```
[root@host1 ~]# echo "zfs_mvector_max_size/W 0t1048576" |mdb -kw
```

Kernel

El rendimiento fiable de ZFS requiere un kernel de Solaris parcheado contra problemas de alineación de LUN. La corrección se introdujo con el parche 147440-19 en Solaris 10 y con SRU 10,5 para Solaris 11. Utilice sólo Solaris 10 y versiones posteriores con ZFS.

Configuración de LUN

Para configurar una LUN, complete los siguientes pasos:

1. Cree una LUN del tipo `solaris`.
2. Instale el kit de utilidades de host (HUK) adecuado especificado por el "Herramienta de matriz de interoperabilidad de NetApp (IMT)".
3. Siga las instrucciones del HUK exactamente como se describe. Los pasos básicos se describen a continuación, pero consulte la "documentación más reciente" para el procedimiento adecuado.
   a. Ejecute el `host_config` utilidad para actualizar el `sd.conf/sdd.conf` archivo. Al hacerlo, las unidades SCSI pueden detectar correctamente LUN de ONTAP.

b. Siga las instrucciones proporcionadas por el `host_config` Utilidad para habilitar la entrada/salida multivía (MPIO).

c. Reiniciar. Este paso es necesario para que cualquier cambio se reconozca en el sistema.

4. Cree particiones en las LUN y compruebe que están correctamente alineadas. Consulte el Apéndice B: Verificación de alineación de WAFL para obtener instrucciones sobre cómo probar y confirmar la alineación directamente.

zpools

Sólo se debe crear un zpool después de los pasos del "Configuración de LUN" se realizan. Si el procedimiento no se realiza correctamente, puede provocar una degradación grave del rendimiento debido a la alineación de E/S. Para un rendimiento óptimo en ONTAP es necesario alinear el I/O con un límite de 4K GbE en una unidad. Los sistemas de archivos creados en un zpool utilizan un tamaño de bloque efectivo que se controla mediante un parámetro denominado `ashift`, que se puede ver ejecutando el comando `zdb -C`.

Valor de `ashift` el valor por defecto es 9, que significa 2^9, o 512 bytes. Para un rendimiento óptimo, el `ashift` El valor debe ser 12 (2^12=4K). Este valor se define en el momento en que se crea zpool y no se puede cambiar, lo que significa que los datos en zpools con `ashift` los datos que no sean 12 se deben migrar copiando a un zpool recién creado.

Después de crear un zpool, verifique el valor de `ashift` antes de continuar. Si el valor no es 12, las LUN no se detectaron correctamente. Destruya zpool, verifique que todos los pasos mostrados en la documentación de utilidades de host relevantes se hayan realizado correctamente y vuelva a crear zpool.

Zpools y LDOMs de Solaris

Los LDOMs de Solaris crean un requisito adicional para asegurarse de que la alineación de E/S es correcta. Aunque un LUN se puede detectar correctamente como dispositivo 4K, un dispositivo virtual vdsk en un LDOM no hereda la configuración del dominio de E/S. El vdsk basado en esa LUN vuelve a tener de forma predeterminada un bloque de 512 bytes.

Se necesita un archivo de configuración adicional. En primer lugar, se deben aplicar parches a los LDOM individuales para el bug de Oracle 15824910 para activar las opciones de configuración adicionales. Este parche se ha portado a todas las versiones utilizadas actualmente de Solaris. Una vez que se aplica el parche a LDOM, está listo para la configuración de las nuevas LUN correctamente alineadas de la siguiente manera:

1. Identifique los LUN o LUN que se van a utilizar en el nuevo zpool. En este ejemplo, es el dispositivo c2d1.

```
[root@LDOM1 ~]# echo | format
Searching for disks...done
AVAILABLE DISK SELECTIONS:
  0. c2d0 <Unknown-Unknown-0001-100.00GB>
     /virtual-devices@100/channel-devices@200/disk@0
  1. c2d1 <SUN-ZFS Storage 7330-1.0 cyl 1623 alt 2 hd 254 sec 254>
     /virtual-devices@100/channel-devices@200/disk@1
```

2. Recuperar la instancia vdc de los dispositivos que se van a utilizar para una agrupación ZFS:

```
[root@LDOM1 ~]#  cat /etc/path_to_inst
#
# Caution! This file contains critical kernel state
#
"/fcoe" 0 "fcoe"
"/iscsi" 0 "iscsi"
"/pseudo" 0 "pseudo"
"/scsi_vhci" 0 "scsi_vhci"
"/options" 0 "options"
"/virtual-devices@100" 0 "vnex"
"/virtual-devices@100/channel-devices@200" 0 "cnex"
"/virtual-devices@100/channel-devices@200/disk@0" 0 "vdc"
"/virtual-devices@100/channel-devices@200/pciv-communication@0" 0 "vpci"
"/virtual-devices@100/channel-devices@200/network@0" 0 "vnet"
"/virtual-devices@100/channel-devices@200/network@1" 1 "vnet"
"/virtual-devices@100/channel-devices@200/network@2" 2 "vnet"
"/virtual-devices@100/channel-devices@200/network@3" 3 "vnet"
"/virtual-devices@100/channel-devices@200/disk@1" 1 "vdc" << We want
this one
```

3. Editar `/platform/sun4v/kernel/drv/vdc.conf`:

```
block-size-list="1:4096";
```

Esto significa que a la instancia de dispositivo 1 se le asigna un tamaño de bloque de 4096.

Como ejemplo adicional, supongamos que las instancias de vdsk 1 a 6 deben configurarse para un tamaño de bloque de 4K KB y. `/etc/path_to_inst` se lee de la siguiente manera:

```
"/virtual-devices@100/channel-devices@200/disk@1" 1 "vdc"
"/virtual-devices@100/channel-devices@200/disk@2" 2 "vdc"
"/virtual-devices@100/channel-devices@200/disk@3" 3 "vdc"
"/virtual-devices@100/channel-devices@200/disk@4" 4 "vdc"
"/virtual-devices@100/channel-devices@200/disk@5" 5 "vdc"
"/virtual-devices@100/channel-devices@200/disk@6" 6 "vdc"
```

4. La final `vdc.conf` el archivo debe contener lo siguiente:

```
block-size-list="1:8192","2:8192","3:8192","4:8192","5:8192","6:8192";
```

Precaución
El LDOM debe reiniciarse después de configurar vdc.conf y crear vdsk. Este paso no se puede evitar. El cambio de tamaño del bloque solo se aplica después de un reinicio. Continúe con la configuración de zpool y asegúrese de que el ashift está correctamente ajustado en 12 como se ha descrito anteriormente.

Registro de Intención de ZFS (ZIL)

Por lo general, no hay razón para localizar el registro de intención ZFS (ZIL) en un dispositivo diferente. El registro puede compartir espacio con el pool principal. El uso principal de un ZIL separado es cuando se utilizan unidades físicas que carecen de las funciones de almacenamiento en caché de escritura en cabinas de almacenamiento modernas.

sesgo logarítmico

Ajuste la `logbias` Parámetro en sistemas de archivos ZFS que alojan datos de Oracle.

```
zfs set logbias=throughput <filesystem>
```

Usar este parámetro reduce los niveles generales de escritura. En los valores predeterminados, los datos escritos se confirman primero en el ZIL y, a continuación, en el pool de almacenamiento principal. Este enfoque es adecuado para una configuración que utiliza una configuración de unidad simple, que incluye un dispositivo ZIL basado en SSD y medios giratorios para el pool de almacenamiento principal. Esto se debe a que permite un commit en una sola transacción de I/O en el medio de menor latencia disponible.

Cuando se utiliza una cabina de almacenamiento moderna que incluye su propia funcionalidad de almacenamiento en caché, este método no suele ser necesario. En raras ocasiones, es posible que sea conveniente comprometer una escritura con una sola transacción en el registro, como una carga de trabajo que consta de escrituras aleatorias altamente concentradas y sensibles a la latencia. Existen consecuencias en la amplificación de escritura, ya que los datos registrados se escriben finalmente en el pool de almacenamiento principal, lo que provoca el doble de la actividad de escritura.

E/S directa

Muchas aplicaciones, incluidos los productos de Oracle, pueden omitir la caché de buffers del host activando la E/S directa Esta estrategia no funciona como se esperaba con los sistemas de archivos ZFS. Aunque se omite la caché de buffers del host, ZFS continúa almacenando los datos en caché. Esta acción puede provocar resultados engañosos cuando se usan herramientas como fio o sio para realizar pruebas de rendimiento, ya que es difícil predecir si I/O está llegando al sistema de almacenamiento o si se está almacenando en caché localmente dentro del sistema operativo. Esta acción también hace que sea muy difícil utilizar estas pruebas sintéticas para comparar el rendimiento de ZFS con otros sistemas de archivos. Como cuestión práctica, hay poca o ninguna diferencia en el rendimiento del sistema de archivos con las cargas de trabajo de los usuarios reales.

Varios zpools

Las copias de seguridad basadas en instantáneas, las restauraciones, los clones y el archivado de datos basados en ZFS se deben realizar en el nivel de zpool y, por lo general, requieren varios zpools. Un zpool es análogo a un grupo de discos LVM y debe configurarse usando las mismas reglas. Por ejemplo, es probable que una base de datos se disponga mejor con los archivos de datos en los que reside `zpool1` y los registros de archivo, los archivos de control y los registros de recuperación en los que residen `zpool2`. Este enfoque permite realizar un backup dinámico estándar en el que la base de datos se coloca en modo de backup

dinámico, seguido de una copia Snapshot de `zpool1`. A continuación, la base de datos se elimina del modo de backup dinámico, se fuerza el archivo de registro y una copia de Snapshot de `zpool2` se ha creado. Una operación de restauración requiere el desmontaje de los sistemas de archivos zfs y desconectar zpool íntegramente, a continuación de una operación de restauración de SnapRestore. El zpool se puede poner en línea de nuevo y la base de datos se recupera.

filesystemio_options

Parámetro de Oracle `filesystemio_options` Funciona de forma diferente con ZFS. Si `setall` o. `directio` Se utiliza, las operaciones de escritura son síncronas y omiten la caché de buffers del sistema operativo, pero ZFS almacena en búfer las lecturas. Esta acción causa dificultades en el análisis de rendimiento porque a veces la caché ZFS intercepta y suministra servicio a las E/S, lo que hace que la latencia de almacenamiento y el total de E/S sean menores de lo que podría parecer.

Configuración de red

Interfaces lógicas

Las bases de datos de Oracle necesitan acceder al almacenamiento. Las interfaces lógicas (LIF) son las tuberías de red que conecta una máquina virtual de almacenamiento (SVM) a la red y, por tanto, a la base de datos. Es necesario diseñar un LIF adecuado para garantizar que exista un ancho de banda suficiente para cada carga de trabajo de la base de datos. La conmutación por error no conlleva la pérdida de los servicios de almacenamiento.

En esta sección se ofrece una descripción general de los principios clave del diseño de LIF. Para obtener documentación más completa, consulte "Documentación de gestión de red de ONTAP". Al igual que otros aspectos de la arquitectura de bases de datos, las mejores opciones para las máquinas virtuales de almacenamiento (SVM, conocidas como Vserver en la CLI) y el diseño de la interfaz lógica (LIF) dependen en gran medida de los requisitos de escalado y las necesidades empresariales.

Tenga en cuenta los siguientes temas principales al crear una estrategia de LIF:

- **Rendimiento.** ¿Es suficiente el ancho de banda de la red?
- **Resiliencia.** ¿Hay algún punto de falla en el diseño?
- **Capacidad de gestión.** ¿Se puede escalar la red de forma no disruptiva?

Estos temas se aplican a la solución completa, desde el host, los switches y el sistema de almacenamiento.

Tipos de LIF

Hay varios tipos de LIF. "Documentación de ONTAP sobre tipos de LIF" Puede proporcionar información más completa sobre este tema, pero desde una perspectiva funcional, los LIF se pueden dividir en los siguientes grupos:

- **LIF de administración de clúster y nodos.** LIF utilizadas para administrar el clúster de almacenamiento.
- **LIF de administración de SVM.** Interfaces que permiten el acceso a una SVM a través de la API REST o ONTAPI (también conocida como ZAPI) para funciones como la creación de instantáneas o el redimensionamiento de volúmenes. Productos como SnapManager para Oracle (SMO) deben tener acceso a una LIF de gestión de SVM.

- **LIF de datos.** Interfaces para FC, iSCSI, NVMe/FC, NVMe/TCP, NFS, o datos SMB/CIFS.

> También puede utilizarse una LIF de datos que se utiliza para el tráfico NFS al cambiar la política de firewall de `data` para `mgmt` O cualquier otra política que permita HTTP, HTTPS o SSH. Este cambio puede simplificar la configuración de red ya que evita la configuración de cada host para obtener acceso a tanto a la LIF de datos de NFS como a una LIF de gestión separada. No se puede configurar una interfaz para iSCSI y para el tráfico de gestión, a pesar de que ambos usen un protocolo IP. En los entornos iSCSI, se requiere una LIF de gestión separada.

Diseño de LIF SAN

El diseño de LIF en un entorno SAN es relativamente sencillo por una de las razones: La multivía. Todas las implementaciones de SAN modernas permiten a un cliente acceder a los datos a través de múltiples rutas de red independientes y seleccionar la mejor ruta o las mejores rutas para acceder. Como resultado, el rendimiento con respecto al diseño de las LIF es más sencillo de abordar porque los clientes SAN equilibran automáticamente la carga de I/O en las mejores rutas disponibles.

Si una ruta deja de estar disponible, el cliente selecciona automáticamente una ruta diferente. La simplicidad resultante del diseño hace que los LIF SAN sean generalmente más gestionables. Esto no significa que un entorno SAN siempre se gestione con mayor facilidad, ya que existen otros muchos aspectos del almacenamiento SAN que son mucho más complicados que NFS. Simplemente significa que el diseño de LIF SAN es más sencillo.

Rendimiento

El aspecto más importante con respecto al rendimiento de LIF en un entorno SAN es el ancho de banda. Por ejemplo, un clúster ONTAP AFF de dos nodos con dos puertos FC de 16GB Gb por nodo permite hasta 32GB Gbps de ancho de banda hacia/desde cada nodo.

Resiliencia

Los LIF DE SAN no conmutan al nodo de respaldo en un sistema de almacenamiento AFF. Si falla un LIF de SAN debido a la recuperación tras fallos de la controladora, el software multivía del cliente detecta la pérdida de una ruta y redirige las I/O a otro LIF. Con los sistemas de almacenamiento de ASA, los LIF conmutarán por error tras un breve retraso, pero esto no interrumpe las I/O porque ya hay rutas activas en la otra controladora. El proceso de conmutación por error tiene lugar para restaurar el acceso de host en todos los puertos definidos.

Gran capacidad de administración

La migración de LIF es una tarea mucho más común en un entorno NFS porque la migración de LIF suele asociarse con la reubicación de volúmenes en el clúster. No es necesario migrar un LIF en un entorno SAN cuando se reubican volúmenes en el par de alta disponibilidad. Esto se debe a que, una vez finalizado el movimiento de volúmenes, ONTAP envía una notificación a la SAN sobre un cambio en las rutas y los clientes SAN vuelven a optimizarse automáticamente. La migración de LIF con SAN está asociada principalmente a los grandes cambios de hardware físico. Por ejemplo, si es necesaria una actualización sin interrupciones de las controladoras, se migra un LIF SAN al nuevo hardware. Si se encuentra que un puerto FC está defectuoso, puede migrarse un LIF a un puerto no utilizado.

Recomendaciones de diseño

NetApp hace las siguientes recomendaciones:

- No cree más rutas de las necesarias. Un número excesivo de rutas complica la gestión general y puede provocar problemas en la conmutación al nodo de respaldo de rutas en algunos hosts. Además, algunos hosts tienen limitaciones inesperadas de la ruta para configuraciones como el arranque SAN.
- Muy pocas configuraciones deberían requerir más de cuatro rutas a una LUN. El valor de tener más de dos nodos de rutas de publicidad para los LUN es limitado porque no se puede acceder al agregado que aloja una LUN si se produce un error en el nodo propietario de la LUN y su partner de alta disponibilidad. La creación de rutas en nodos que no sean el par de alta disponibilidad primario no es útil en esta situación.
- Aunque puede gestionar el número de rutas visibles de LUN si selecciona qué puertos se incluyen en las zonas FC, suele ser más fácil incluir todos los puntos de destino potenciales en la zona FC y controlar la visibilidad de la LUN a nivel de ONTAP.
- En ONTAP 8,3 y versiones posteriores, la función de asignación selectiva de LUN (SLM) es la opción predeterminada. Con SLM, cualquier nuevo LUN se anuncia automáticamente desde el nodo propietario del agregado subyacente y el partner de alta disponibilidad del nodo. Esta disposición evita la necesidad de crear conjuntos de puertos o configurar la división en zonas para limitar la accesibilidad del puerto. Cada LUN está disponible en el número mínimo de nodos necesarios, tanto para un rendimiento óptimo como para una resiliencia.
  *En el caso de que una LUN deba migrarse fuera de los dos controladores, los nodos adicionales se pueden agregar con el `lun mapping add-reporting-nodes` Comando para que las LUN se anuncien en los nodos nuevos. Al hacerlo, se crean rutas de SAN adicionales a las LUN para la migración de la LUN. Sin embargo, el host debe realizar una operación de detección para utilizar las rutas nuevas.
- No se preocupe demasiado por el tráfico indirecto. Es mejor evitar el tráfico indirecto en un entorno con un gran volumen de I/O para el que cada microsegundo de latencia es crucial, pero el efecto de rendimiento visible es insignificante para las cargas de trabajo típicas.

Diseño de LIF NFS

A diferencia de los protocolos SAN, NFS tiene una capacidad limitada de definir varias rutas para los datos. Las extensiones paralelas de NFS (pNFS) instaladas en NFSv4 solucionan esta limitación, pero, como las velocidades de ethernet han alcanzado los 100GB GbE y más allá, rara vez hay valor en añadir rutas adicionales.

Rendimiento y resiliencia

Aunque medir el rendimiento de LIF de SAN se trata, principalmente, de calcular el ancho de banda total de todas las rutas principales, determinar el rendimiento de LIF NFS requiere observar con más detenimiento la configuración de red exacta. Por ejemplo, se pueden configurar dos puertos 10Gb GbE como puertos físicos sin configurar o como grupo de interfaces del protocolo de control de agregación de enlaces (LACP). Si se configuran como un grupo de interfaces, hay varias políticas de equilibrio de carga disponibles que funcionan de forma diferente en función de si el tráfico se conmuta o se enruta. Por último, Oracle Direct NFS (dNFS) ofrece configuraciones de equilibrio de carga que no existen en ningún cliente NFS del sistema operativo en este momento.

A diferencia de los protocolos SAN, los sistemas de archivos NFS requieren resiliencia en la capa de protocolo. Por ejemplo, un LUN siempre está configurado con multivía habilitado, lo que significa que hay varios canales redundantes disponibles para el sistema de almacenamiento, cada uno de los cuales utiliza el protocolo FC. Un sistema de archivos NFS, por otro lado, depende de la disponibilidad de un único canal TCP/IP que solo se puede proteger en la capa física. Esta disposición es el motivo por el cual existen opciones como la conmutación por error de puerto y la agregación de puertos LACP.

En un entorno NFS, se proporciona rendimiento y flexibilidad en la capa de protocolo de red. Como resultado, ambos temas están entrelazados y deben discutirse juntos.

Enlace las LIF a grupos de puertos

Para enlazar una LIF a un grupo de puertos, asocie la dirección IP de LIF con un grupo de puertos físicos. El principal método para añadir puertos físicos juntos es LACP. La funcionalidad de tolerancia a fallos de LACP es bastante sencilla; cada puerto de un grupo de LACP se supervisa y se elimina del grupo de puertos en caso de que se produzca un funcionamiento incorrecto. No obstante, existen muchos conceptos erróneos sobre cómo funciona LACP con respecto al rendimiento:

- LACP no requiere que la configuración del switch coincida con el extremo. Por ejemplo, ONTAP puede configurarse con balanceo de carga basado en IP, mientras que un switch puede utilizar balanceo de carga basado en MAC.
- Cada punto final que utiliza una conexión LACP puede elegir de forma independiente el puerto de transmisión de paquetes, pero no puede elegir el puerto utilizado para la recepción. Esto significa que el tráfico de ONTAP a un destino en particular está vinculado a un puerto en particular, y el tráfico de retorno podría llegar a una interfaz diferente. Sin embargo, esto no causa problemas.
- LACP no distribuye el tráfico de manera uniforme en todo momento. En un entorno de gran tamaño con muchos clientes NFS, el resultado suele utilizarse incluso en todos los puertos de una agregación de LACP. Sin embargo, cualquier sistema de archivos NFS en el entorno está limitado al ancho de banda de un solo puerto, no a toda la agregación.
- Si bien las políticas LACP de robin-robin están disponibles en ONTAP, estas políticas no abordan la conexión desde un switch a un host. Por ejemplo, una configuración con un tronco LACP de cuatro puertos en un host y un tronco LACP de cuatro puertos en ONTAP solo puede leer un sistema de archivos utilizando un único puerto. Aunque ONTAP puede transmitir datos a través de los cuatro puertos, actualmente no hay tecnologías de switches disponibles que se envíen del switch al host a través de los cuatro puertos. Solo se utiliza uno.

El enfoque más común en entornos de mayor tamaño que consisten en muchos hosts de base de datos es crear un agregado LACP de un número adecuado de interfaces 10Gb (o más rápidas) mediante el equilibrio de carga de IP. Este enfoque permite a ONTAP ofrecer un uso uniforme de todos los puertos, siempre y cuando existan suficientes clientes. El equilibrio de carga se desglosa cuando hay menos clientes en la configuración porque la conexión troncal LACP no redistribuye la carga de forma dinámica.

Cuando se establece una conexión, el tráfico en una dirección determinada se coloca en un solo puerto. Por ejemplo, una base de datos que realiza una exploración de tabla completa en un sistema de archivos NFS conectado a través de un tronco LACP de cuatro puertos lee los datos aunque solo una tarjeta de interfaz de red (NIC). Si sólo hay tres servidores de base de datos en un entorno de este tipo, es posible que los tres estén leyendo desde el mismo puerto, mientras que los otros tres puertos estén inactivos.

Enlazar LIF a puertos físicos

La vinculación de una LIF a un puerto físico provoca un control más granular sobre la configuración de red, ya que una dirección IP determinada en un sistema ONTAP solo está asociada con un puerto de red a la vez. A continuación, la resiliencia se lleva a cabo mediante la configuración de grupos de conmutación al respaldo y las políticas de conmutación por error.

Políticas de conmutación por error y grupos de conmutación por error

El comportamiento de las LIF durante la interrupción de la red está controlado por las políticas de conmutación por error y los grupos de recuperación tras fallos. Las opciones de configuración han cambiado con las distintas versiones de ONTAP. Consulte la "Documentación de gestión de redes de ONTAP para políticas y grupos de conmutación por error" Para obtener detalles específicos de la versión de ONTAP que se va a poner en marcha.

ONTAP 8,3 y superiores permiten la gestión de recuperación tras fallos de LIF en función de dominios de retransmisión. Por lo tanto, un administrador puede definir todos los puertos que tienen acceso a una subred determinada y permitir que ONTAP seleccione una LIF de conmutación al nodo de respaldo adecuada. Algunos clientes pueden utilizar este enfoque, pero tiene limitaciones en un entorno de red de almacenamiento de alta velocidad debido a la falta de previsibilidad. Por ejemplo, un entorno puede incluir ambos puertos 1GB para acceso rutinario al sistema de archivos y puertos 10Gb para las operaciones de I/O del archivo de datos Si ambos tipos de puertos existen en el mismo dominio de retransmisión, la conmutación por error de LIF puede provocar que se muevan las operaciones de I/O del archivo de datos de un puerto 10Gb a un puerto 1GB.

En resumen, tenga en cuenta las siguientes prácticas:

1. Configure un grupo de failover como definido por el usuario.
2. Rellenar el grupo de recuperación tras fallos con puertos en el controlador asociado de recuperación tras fallos de almacenamiento (SFO) de modo que los LIF sigan a los agregados durante una conmutación al nodo de respaldo de almacenamiento. Esto evita la creación de tráfico indirecto.
3. Utilice puertos de conmutación por error con las características de rendimiento correspondientes a la LIF original. Por ejemplo, un LIF en un único puerto físico 10Gb debería incluir un grupo de conmutación por error con un único puerto 10Gb. Un LIF LACP de cuatro puertos debe conmutar por error a otro LIF LACP de cuatro puertos. Estos puertos serían un subconjunto de los puertos definidos en el dominio de retransmisión.
4. Establezca la política de recuperación tras fallos únicamente en SFO-partner. Al hacerlo, se asegura de que el LIF siga al agregado durante la recuperación tras fallos.

Reversión automática

Ajuste la `auto-revert` parámetro como desee. La mayoría de los clientes prefieren establecer este parámetro en `true` Para que la LIF vuelva a su puerto de inicio. Sin embargo, en algunos casos, los clientes han establecido esto en 'false' para que se pueda investigar una conmutación por error inesperada antes de devolver una LIF a su puerto de origen.

Proporción de LIF a volumen

Un concepto erróneo común es que debe haber una relación de 1:1 GbE entre los volúmenes y los LIF de NFS. Aunque esta configuración es necesaria para mover un volumen a cualquier punto de un clúster mientras no se crea tráfico de interconexión adicional, no es categóricamente un requisito. Hay que tener en cuenta el tráfico entre clústeres, pero la mera presencia del tráfico entre clústeres no crea problemas. Muchas de las pruebas de rendimiento publicadas creadas para ONTAP incluyen I/O predominantemente indirectas

Por ejemplo, un proyecto de base de datos que contiene una cantidad relativamente pequeña de bases de datos críticas para el rendimiento que solo requerían un total de 40 volúmenes podría justificar un volumen de 1:1 GB para la estrategia LIF, una disposición que requeriría 40 direcciones IP. Posteriormente, cualquier volumen se podría mover a cualquier parte del clúster junto con la LIF asociada; el tráfico siempre sería directo, minimizando todas las fuentes de latencia incluso a niveles de microsegundos.

Como ejemplo por contador, un entorno alojado de gran tamaño se podría gestionar más fácilmente con una relación de 1:1:1 entre clientes y las LIF. Con el tiempo, es posible que se deba migrar un volumen a un nodo diferente, lo cual provocaría cierto tráfico indirecto. Sin embargo, el efecto de rendimiento debe ser indetectable a menos que los puertos de red en el conmutador de interconexión estén saturados. Si hay algún problema, se puede establecer un nuevo LIF en nodos adicionales y el host puede actualizarse en la siguiente ventana de mantenimiento para eliminar el tráfico indirecto de la configuración.

Configuración TCP/IP y ethernet

Muchos clientes de Oracle en ONTAP utilizan ethernet, el protocolo de red de NFS, iSCSI, NVMe/TCP y, especialmente, el cloud.

Configuración del sistema operativo host

La mayoría de la documentación del proveedor de aplicaciones incluye configuraciones TCP y ethernet específicas para garantizar que la aplicación funcione de manera óptima. Estas mismas configuraciones suelen ser suficientes para ofrecer también un rendimiento óptimo del almacenamiento basado en IP.

Control de flujo Ethernet

Esta tecnología permite a un cliente solicitar que un remitente detenga temporalmente la transmisión de datos. Esto suele hacerse porque el receptor no puede procesar los datos entrantes con la suficiente rapidez. Al mismo tiempo, solicitar que un remitente cesara la transmisión era menos perjudicial que tener un receptor descarte de paquetes porque los buffers estaban llenos. Este ya no es el caso con las pilas TCP utilizadas en los sistemas operativos actualmente. De hecho, el control de flujo causa más problemas de los que resuelve.

Los problemas de rendimiento causados por el control de flujo de Ethernet han aumentado en los últimos años. Esto se debe a que el control de flujo Ethernet funciona en la capa Physical. Si una configuración de red permite que un sistema operativo del host envíe una solicitud de control de flujo de Ethernet a un sistema de almacenamiento, el resultado es una pausa en las operaciones de I/O de todos los clientes conectados. Debido a que una única controladora de almacenamiento atiende cada vez más a un número de clientes, la probabilidad de que uno o varios de estos clientes envíen solicitudes de control de flujo aumenta. El problema se ha observado con frecuencia en las instalaciones de los clientes con una amplia virtualización del SO.

Una NIC de un sistema NetApp no debe recibir solicitudes de control de flujo. El método utilizado para lograr este resultado varía según el fabricante del conmutador de red. En la mayoría de los casos, el control de flujo en un conmutador Ethernet se puede establecer en `receive desired` o. `receive on`, lo que significa que una solicitud de control de flujo no se reenvía al controlador de almacenamiento. En otros casos, la conexión de red en la controladora de almacenamiento puede no permitir la deshabilitación de control de flujo. En estos casos, los clientes deben configurarse para que nunca envíen solicitudes de control de flujo, ya sea cambiando a la configuración de NIC en el propio servidor host o a los puertos de switch a los que está conectado el servidor host.

NetApp recomienda asegurarse de que los controladores de almacenamiento NetApp no reciban paquetes de control de flujo Ethernet. Por lo general, esto puede realizarse mediante la configuración de los puertos del switch a los que está conectada la controladora, pero algunas limitaciones en el hardware del switch pueden requerir cambios en el lado del cliente.

Tamaños de MTU

Se ha demostrado que el uso de tramas gigantes ofrece alguna mejora del rendimiento en las redes 1GB al reducir la sobrecarga de la CPU y de la red, pero el beneficio no suele ser significativo.

NetApp recomienda implementar marcos jumbo cuando sea posible, tanto para obtener beneficios potenciales de rendimiento como para preparar la solución para el futuro.

El uso de tramas gigantes en una red 10Gb es casi obligatorio. Esto se debe a que la mayoría de las implementaciones de 10Gb alcanzan un límite de paquetes por segundo sin tramas gigantes antes de alcanzar la marca de 10Gb. El uso de tramas gigantes mejora la eficiencia del procesamiento TCP/IP porque permite que el sistema operativo, el servidor, las NIC y el sistema de almacenamiento procesen menos

paquetes, pero más grandes. La mejora del rendimiento varía de NIC a NIC, pero es significativa.

En las implementaciones de tramas gigantes, existe la creencia común, aunque incorrecta, de que todos los dispositivos conectados deben admitir tramas gigantes y que el tamaño de MTU debe coincidir de extremo a extremo En su lugar, los dos extremos de red negocian el tamaño de trama más alto mutuamente aceptable al establecer una conexión. En un entorno típico, un switch de red se establece con un tamaño de MTU de 9216, la controladora NetApp se establece en 9000 y los clientes se configuran con una combinación de 9000 y 1514. Los clientes que admiten un MTU de 9000 pueden utilizar tramas gigantes, y los clientes que solo puedan admitir 1514 pueden negociar un valor inferior.

Los problemas con esta disposición son raros en un entorno completamente conmutado. Sin embargo, tenga cuidado en un entorno enrutado que ningún enrutador intermedio se vea forzado a fragmentar tramas gigantes.

NetApp recomienda configurar lo siguiente:

- Las tramas gigantes son deseables, pero no se requieren con Ethernet de 1GB Gb (GbE).
- Se requieren tramas gigantes para lograr el máximo rendimiento, con 10GbE y más rápido.

Parámetros de TCP

A menudo hay tres ajustes mal configurados: Marcas de tiempo TCP, reconocimiento selectivo (SACK) y escalado de ventana TCP. Muchos documentos desactualizados en Internet recomiendan deshabilitar uno o varios de estos parámetros para mejorar el rendimiento. Había algo de mérito en esta recomendación hace muchos años, cuando las capacidades de la CPU eran mucho menores y había un beneficio en reducir la sobrecarga en el procesamiento TCP siempre que fuera posible.

Sin embargo, con los sistemas operativos modernos, deshabilitar cualquiera de estas características de TCP generalmente no resulta en ningún beneficio detectable, a la vez que también puede dañar el rendimiento. Los daños en el rendimiento son especialmente probables en entornos de red virtualizados, ya que estas características son necesarias para gestionar eficazmente la pérdida de paquetes y los cambios en la calidad de la red.

NetApp recomienda habilitar las marcas de tiempo TCP, EL SACK y el escalado de la ventana TCP en el host, y los tres parámetros deben estar activados por defecto en cualquier sistema operativo actual.

Configuración de SAN FC

La configuración de SAN FC para bases de datos de Oracle consiste principalmente en seguir prácticas recomendadas diarias de SAN.

Esto incluye medidas de planificación típicas, como asegurar que exista suficiente ancho de banda en la SAN entre el host y el sistema de almacenamiento, comprobar que existan todas las rutas de SAN entre todos los dispositivos requeridos, mediante la configuración de puertos FC requerida por el proveedor de switches FC, para evitar la contención de ISL, y con una supervisión adecuada del tejido SAN.

División en zonas

Una zona de FC nunca debe contener más de un iniciador. Tal arreglo puede parecer funcionar inicialmente, pero la comunicación entre iniciadores finalmente interfiere con el rendimiento y la estabilidad.

Las zonas multidestino se consideran generalmente seguras, aunque en raras ocasiones el comportamiento

de los puertos de destino FC de diferentes proveedores ha causado problemas. Por ejemplo, evite incluir los puertos de destino de una cabina de almacenamiento NetApp y otra que no sea de NetApp en la misma zona. Además, es aún más probable que la ubicación de un sistema de almacenamiento NetApp y un dispositivo de cinta en la misma zona cause problemas.

Red de conexión directa

A veces, los administradores de almacenamiento prefieren simplificar sus infraestructuras eliminando los switches de red de la configuración. Esto puede ser soportado en algunos escenarios.

ISCSI y NVMe/TCP

Un host que utilice iSCSI o NVMe/TCP se puede conectar directamente a un sistema de almacenamiento y funcionar normalmente. El motivo son las rutas. Las conexiones directas a dos controladoras de almacenamiento diferentes dan como resultado dos rutas independientes para el flujo de datos. La pérdida de una ruta, un puerto o una controladora no impide que se utilice la otra ruta.

NFS

Se puede utilizar el almacenamiento NFS conectado directamente, pero con una limitación considerable: El fallo no funcionará si no se realiza una ejecución significativa de secuencias de comandos, que sería responsabilidad del cliente.

El motivo por el que la recuperación tras fallos sin interrupciones se complica gracias al almacenamiento NFS de conexión directa es el enrutamiento que se produce en el sistema operativo local. Por ejemplo, supongamos que un host tiene una dirección IP de 192.168.1.1/24 y está directamente conectado a una controladora ONTAP con la dirección IP 192.168.1.50/24. Durante la conmutación al nodo de respaldo, esa dirección 192.168.1.50 puede conmutar al nodo de respaldo a la otra controladora y estará disponible para el host, pero ¿cómo detecta el host su presencia? La dirección 192.168.1.1 original todavía existe en la NIC host que ya no se conecta a un sistema operativo. El tráfico destinado a 192.168.1.50 seguiría enviándose a un puerto de red inoperable.

La segunda NIC del SO podría configurarse como 19 2.168.1.2 y sería capaz de comunicarse con la dirección fallida en 192.168.1.50, pero las tablas de enrutamiento locales tendrían un valor predeterminado de usar una dirección **y solo una** para comunicarse con la subred 192.168.1.0/24. Un administrador de sistema podría crear un marco de scripting que detectara una conexión de red fallida y alterara las tablas de enrutamiento locales o activara o desactivara las interfaces. El procedimiento exacto dependerá del sistema operativo en uso.

En la práctica, los clientes de NetApp disponen de NFS conectado directamente, pero normalmente solo para cargas de trabajo en las que se pueden pausar I/O durante las recuperaciones tras fallos. Cuando se utilizan montajes duros, no debe haber ningún error de E/S durante dichas pausas. El I/O se debe bloquear hasta que los servicios se restauren, ya sea mediante una conmutación de retorno tras recuperación o intervención manual para mover las direcciones IP entre las NIC del host.

Conexión directa FC

No es posible conectar directamente un host a un sistema de almacenamiento ONTAP mediante el protocolo FC. La razón es el uso de NPIV. El WWN que identifica un puerto ONTAP FC con la red de FC utiliza un tipo de virtualización denominado NPIV. Cualquier dispositivo conectado a un sistema ONTAP debe poder reconocer un WWN de NPIV. No hay proveedores de HBA actuales que ofrezcan un HBA que se pueda instalar en un host que admita un destino NPIV.

Configuración del almacenamiento

FC SAN

Alineación de LUN

La alineación de LUN hace referencia a optimizar las I/O con respecto al diseño del sistema de archivos subyacente.

Directiva no resuelta en <stdin> - Incluir::lun-alignment.adoc[]

Consulte también la discusión sobre la alineación de los bloques de compresión en la sección "Eficiencia". Cualquier diseño alineado con los límites de bloques de compresión de 8KB KB también se alineará con los límites de 4KB KB.

Advertencias de desalineación

Directiva no resuelta en <stdin> - Include::database-misalignment-warnings.adoc[]

La alineación en entornos Solaris es más complicada. Consulte "Configuración de host SAN ONTAP" si quiere más información.

Precaución
En entornos Solaris x86, tenga cuidado adicional con la alineación correcta, ya que la mayoría de las configuraciones tienen varias capas de particiones. Los segmentos de partición de Solaris x86 normalmente existen en la parte superior de una tabla de particiones de registro de inicio maestro estándar.

Ajuste de tamaño de LUN y número de LUN

Seleccionar el tamaño óptimo de LUN y el número de LUN que se utilizarán es fundamental para lograr un rendimiento y una capacidad de gestión óptimos en las bases de datos de Oracle.

Una LUN es un objeto virtualizado en ONTAP que existe en todas las unidades del agregado host. Como resultado, el rendimiento de la LUN no se ve afectado por su tamaño porque la LUN aprovecha todo el potencial de rendimiento del agregado sin importar el tamaño que se haya elegido.

Para comodidad, es posible que los clientes deseen usar una LUN de un tamaño determinado. Por ejemplo, si una base de datos se crea en un LVM u un grupo de discos de ASM de Oracle compuesto por dos LUN de 1TB GB cada uno, dicho grupo de discos debe aumentar en incrementos de 1TB TB. Es preferible crear el grupo de discos a partir de ocho LUN de 500GB cada uno para que el grupo de discos se pueda aumentar en incrementos menores.

Se desaconseja la práctica de establecer un tamaño de LUN estándar universal porque, al hacerlo, se puede complicar la capacidad de gestión. Por ejemplo, un tamaño de LUN estándar de 100GB TB puede funcionar bien cuando una base de datos o un almacén de datos está entre 1TB y 2TB TB, pero el tamaño de una base de datos o un almacén de datos de 20TB TB requeriría 200 LUN. Esto significa que los tiempos de reinicio del servidor son más largos, hay más objetos que gestionar en las distintas interfaces de usuario y productos como SnapCenter deben realizar la detección de muchos objetos. Si se usa menos LUN, de mayor tamaño se evitan estos problemas.

- El número de LUN es más importante que el tamaño de la LUN.

- El tamaño de LUN está controlado principalmente por requisitos del número de LUN.
- Evite crear más LUN de las necesarias.

Número de LUN

A diferencia del tamaño de LUN, el número de LUN afecta al rendimiento. El rendimiento de la aplicación depende a menudo de la capacidad para realizar I/O paralelas mediante la capa SCSI. Como resultado, dos LUN ofrecen mejor rendimiento que una única LUN. El uso de LVM como Veritas VxVM, Linux LVM2 u Oracle ASM es el método más sencillo para aumentar el paralelismo.

Los clientes de NetApp suelen experimentar un beneficio mínimo gracias al aumento del número de LUN por encima de dieciséis, aunque, en pruebas de entornos 100% con unidades de estado sólido con I/O aleatorias muy pesadas, se ha demostrado una mejora adicional de hasta 64 000 LUN.

NetApp recomienda lo siguiente:

En general, entre cuatro y dieciséis LUN son suficientes para admitir las necesidades de I/O de cualquier carga de trabajo de bases de datos en concreto. Menos de cuatro LUN puede crear limitaciones de rendimiento debido a las limitaciones de las implementaciones SCSI del host.

Ubicación de LUN

La colocación óptima de los LUN de bases de datos en volúmenes de ONTAP depende principalmente de cómo se utilicen varias funciones de ONTAP.

Volúmenes

Un punto común de confusión con los clientes que empiezan a utilizar ONTAP es el uso de FlexVols, conocido normalmente como «volúmenes».

Un volumen no es una LUN. Estos términos se usan sinónimos con muchos otros productos de proveedores, incluidos los proveedores de cloud. Los volúmenes de ONTAP son simplemente contenedores de gestión. No sirven datos por sí mismas, ni ocupan el espacio. Son contenedores para archivos o LUN y existen para mejorar y simplificar la capacidad de gestión, especialmente a escala.

Volúmenes y LUN

Normalmente, los LUN relacionados se ubican en un único volumen. Por ejemplo, una base de datos que requiere 10 LUN suele tener 10 LUN colocadas en el mismo volumen.

- Usar una proporción 1:1 de LUN y volúmenes, lo que significa una LUN por volumen, no es * una práctica recomendada formal.
- En su lugar, los volúmenes deben verse como contenedores para las cargas de trabajo o conjuntos de datos. Puede que haya una única LUN por volumen, o que haya muchos. La respuesta correcta depende de los requisitos de capacidad de gestión.
- La dispersión de LUN por un número innecesario de volúmenes puede provocar problemas de sobrecarga adicionales y programación para operaciones como las operaciones de snapshot, el número excesivo de objetos que se muestran en la interfaz de usuario y que pueda alcanzar los límites de volúmenes de plataforma antes de alcanzar el límite de LUN.

Volúmenes, LUN y snapshots

Las políticas y las programaciones de Snapshot se colocan en el volumen, no en la LUN. Un conjunto de datos formado por 10 LUN solo requeriría una única política de Snapshot cuando esas LUN se ubiquen en el mismo volumen.

Además, la coubicación de todas las LUN relacionadas para un conjunto de datos determinado en un único volumen proporciona operaciones de instantánea atómica. Por ejemplo, una base de datos que residía en 10 LUN o un entorno de aplicación basado en VMware formado por 10 sistemas operativos diferentes podría protegerse como un único objeto consistente si las LUN subyacentes se colocan en un único volumen. Si se colocan en diferentes volúmenes, las instantáneas pueden o no estar sincronizadas al 100%, incluso si se programan al mismo tiempo.

En algunos casos, podría haber que dividir un conjunto relacionado de LUN en dos volúmenes distintos debido a los requisitos de recuperación. Por ejemplo, una base de datos podría tener cuatro LUN para archivos de datos y dos LUN para registros. En este caso, un volumen de archivo de datos con 4 LUN y un volumen de registro con 2 LUN podrían ser la mejor opción. La razón es la capacidad de recuperación independiente. Por ejemplo, el volumen de archivos de datos se podría restaurar de forma selectiva a un estado anterior, lo que significa que las cuatro LUN se revertirían al estado de la snapshot, mientras que el volumen de registro con sus datos cruciales no se vería afectado.

Volúmenes, LUN y SnapMirror

Las políticas y las operaciones de SnapMirror son, como las operaciones de Snapshot, realizadas en el volumen, no en la LUN.

Ubicar conjuntamente LUN relacionadas en un único volumen le permite crear una única relación de SnapMirror y actualizar todos los datos contenidos con una única actualización. Al igual que con las instantáneas, la actualización también será una operación atómica. Se garantizaría que el destino de SnapMirror tendrá una única réplica puntual de los LUN de origen. Si las LUN se distribuyeron entre varios volúmenes, las réplicas pueden o no ser coherentes entre sí.

Volúmenes, LUN y calidad de servicio

Aunque la calidad de servicio se puede aplicar de forma selectiva a LUN individuales, normalmente es más fácil configurarla en el nivel de volumen. Por ejemplo, todas las LUN utilizadas por los invitados de un servidor ESX determinado podrían colocarse en un solo volumen y, a continuación, podría aplicarse una política de calidad de servicio adaptable de ONTAP. El resultado es un límite IOPS por TB con escala automática que se aplica a todas las LUN.

Del mismo modo, si una base de datos necesitara 100K 000 IOPS y ocupase 10 LUN, sería más fácil establecer un único límite de 100K IOPS en un único volumen que establecer 10 límites individuales de 10K IOPS, uno en cada LUN.

Diseños de varios volúmenes

Hay algunos casos en los que distribuir las LUN en varios volúmenes puede ser beneficioso. El motivo primario es la segmentación de la controladora. Por ejemplo, un sistema de almacenamiento de alta disponibilidad podría estar alojando una única base de datos donde se requiera todo el potencial de procesamiento y almacenamiento en caché de cada controladora. En este caso, un diseño típico sería colocar la mitad de las LUN de un único volumen de la controladora 1 y la otra mitad de los LUN de un único volumen en la controladora 2.

Del mismo modo, la segmentación de la controladora puede utilizarse para equilibrar la carga. Un sistema de alta disponibilidad que alojara 100 bases de datos de 10 LUN cada una se podría diseñar donde cada base de

datos reciba un volumen de 5 LUN en cada una de las dos controladoras. El resultado es una carga simétrica garantizada de cada controladora a medida que se aprovisionan las bases de datos adicionales.

Sin embargo, ninguno de estos ejemplos implica una relación de volumen/LUN de 1:1 GB. El objetivo sigue siendo optimizar la gestión mediante la colocalización de LUN relacionadas en volúmenes.

Un ejemplo donde tiene sentido la relación de 1:1 LUN con volumen es la colocación en contenedores, donde cada LUN podría representar realmente una única carga de trabajo y cada una de ellas debería gestionarse de forma individual. En tales casos, una relación 1:1 puede ser óptima.

Cambio de tamaño de LUN y cambio de tamaño de LVM

Cuando un sistema de archivos basado en SAN ha alcanzado su límite de capacidad, hay dos opciones para aumentar el espacio disponible:

- Aumente el tamaño de las LUN
- Agregue una LUN a un grupo de volúmenes existente y aumente el volumen lógico contenido

Aunque el redimensionamiento de LUN es una opción para aumentar la capacidad, generalmente es mejor usar un LVM, incluido Oracle ASM. Uno de los principales motivos por los que existen LVM es evitar la necesidad de cambiar el tamaño de las LUN. Con un LVM, se unen varias LUN en un pool virtual de almacenamiento. Los volúmenes lógicos tallados en este pool son administrados por el LVM y pueden ser fácilmente redimensionados. Otra ventaja es la eliminación de los puntos de sobrecarga en una unidad concreta al distribuir un volumen lógico determinado entre todas las LUN disponibles. Normalmente, la migración transparente puede realizarse utilizando el administrador de volúmenes para reubicar las extensiones subyacentes de un volumen lógico a nuevas LUN.

Segmentación de LVM

La segmentación de LVM hace referencia a distribuir datos entre varias LUN. El resultado es una mejora espectacular del rendimiento en muchas bases de datos.

Antes de la era de las unidades flash, se utilizaba la segmentación para ayudar a superar las limitaciones de rendimiento de las unidades giratorias. Por ejemplo, si un sistema operativo necesita realizar una operación de lectura de 1MB KB, para leer que 1MB TB de datos de una sola unidad se requeriría buscar y leer muchos cabezales de unidad ya que 1MB se transfiere lentamente. Si esos 1MB TB de datos se segmentaron en 8 LUN, el sistema operativo podría emitir ocho operaciones de lectura de 128K KB en paralelo y reducir el tiempo necesario para realizar la transferencia de 1MB GB.

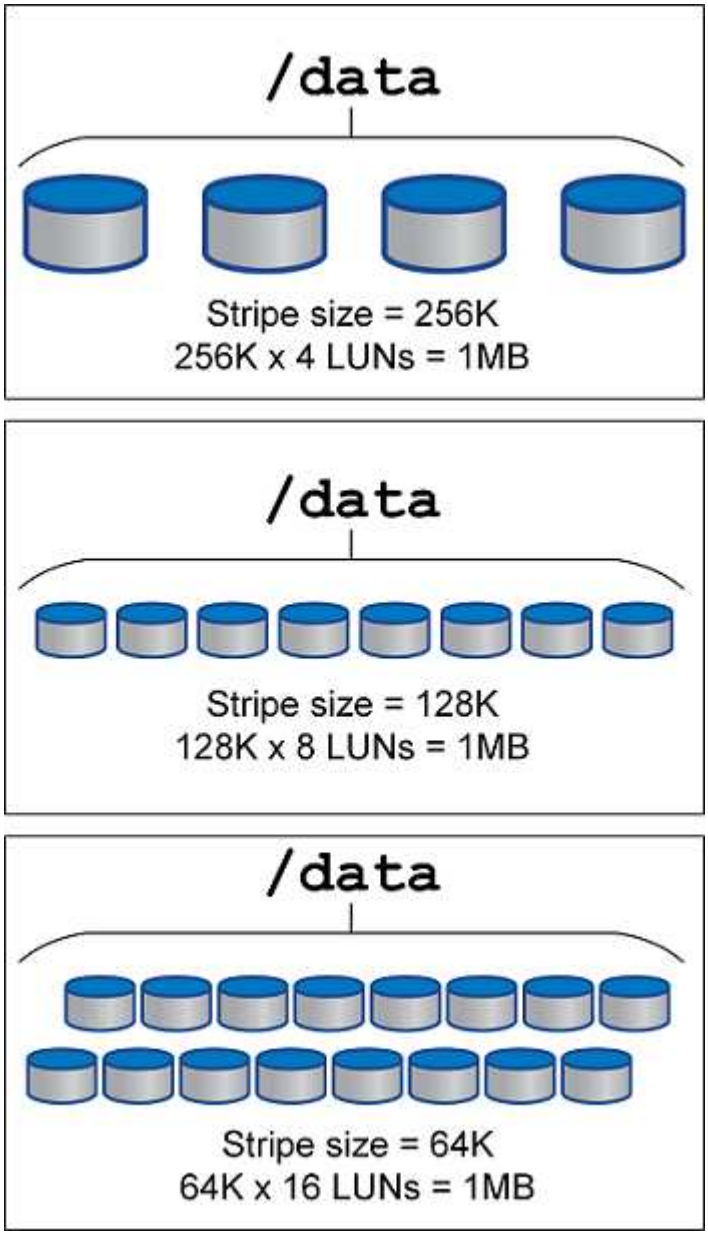
La segmentación con unidades giratorias era más difícil porque se tenía que conocer el patrón de I/O con anterioridad. Si la segmentación no se ajustó correctamente para los patrones de I/O reales, las configuraciones seccionadas podrían dañar el rendimiento. Con las bases de datos de Oracle y, especialmente con las configuraciones all-flash, la segmentación es mucho más fácil de configurar y se ha demostrado que mejora drásticamente el rendimiento.

Los gestores de volúmenes lógicos como Oracle ASM segmentan por defecto, pero el LVM del sistema operativo nativo no lo hacen. Algunos de ellos unen varias LUN como un dispositivo concatenado, lo que da como resultado archivos de datos que existen en un único dispositivo LUN. Esto provoca puntos calientes. Otras implementaciones de LVM toman por defecto extensiones distribuidas. Esto es similar a la segmentación, pero es más grueso. Las LUN del grupo de volúmenes se dividen en partes grandes, denominadas extensiones y normalmente se miden en muchos megabytes, y los volúmenes lógicos se distribuyen por esas extensiones. El resultado es que las operaciones de I/O aleatorias en un archivo se deben distribuir bien entre las LUN, pero las operaciones de I/O secuenciales no son tan eficientes como podrían.

La I/O de aplicaciones con rendimiento intensivo casi siempre es una (a) en unidades del tamaño de bloque básico o (b) un megabyte.

El principal objetivo de una configuración seccionada es garantizar que la I/O de archivo único se pueda realizar como una unidad única y que las I/O de varios bloques, que deben tener un tamaño de 1MB TB, se puedan paralelizar de manera uniforme entre todas las LUN del volumen seccionado. Esto significa que el tamaño de franja no debe ser menor que el tamaño del bloque de la base de datos y el tamaño de franja multiplicado por el número de LUN debe ser 1MB.

En la siguiente figura, se muestran tres opciones posibles para el ajuste del tamaño de la franja y el ancho. Se selecciona el número de LUN para satisfacer los requisitos de rendimiento tal como se han descrito anteriormente, pero en todos los casos los datos totales de una sola franja es 1MB.



NFS

Descripción general

NetApp lleva más de 30 años proporcionando almacenamiento NFS de clase empresarial y su uso está creciendo con la tendencia hacia las infraestructuras basadas en cloud debido a la sencillez de la tecnología.

El protocolo NFS incluye varias versiones con diferentes requisitos. Para obtener una descripción completa de la configuración de NFS con ONTAP, consulte "TR-4067 NFS en prácticas recomendadas de ONTAP". Las siguientes secciones cubren algunos de los requisitos más críticos y los errores comunes del usuario.

Versiones de NFS

El cliente NFS del sistema operativo debe ser compatible con NetApp.

- NFSv3 es compatible con sistemas operativos que siguen el estándar NFSv3.
- NFSv3 es compatible con el cliente Oracle dNFS.
- NFSv4 es compatible con todos los sistemas operativos que siguen el estándar NFSv4.
- NFSv4,1 y NFSv4,2 requieren soporte de SO específico. Consulte la "NetApp IMT" Para sistemas operativos compatibles.
- La compatibilidad de Oracle dNFS para NFSv4,1 requiere Oracle 12.2.0.2 o superior.

> La "Matriz de compatibilidad de NetApp" Para NFSv3 y NFSv4 no incluye sistemas operativos específicos. Todos los sistemas operativos que obedecen a RFC son generalmente compatibles. Al buscar en IMT en línea compatibilidad con NFSv3 o NFSv4, no seleccione un sistema operativo concreto porque no se mostrarán coincidencias. Todos los sistemas operativos están soportados implícitamente por la política general.

Tablas de ranuras TCP Linux NFSv3

Las tablas de ranuras TCP son equivalentes a NFSv3 a la profundidad de la cola del adaptador de bus de host (HBA). En estas tablas se controla el número de operaciones de NFS que pueden extraordinarias a la vez. El valor predeterminado suele ser 16, que es demasiado bajo para un rendimiento óptimo. El problema opuesto ocurre en los kernels más nuevos de Linux, que pueden aumentar automáticamente el límite de la tabla de ranuras TCP a un nivel que sature el servidor NFS con solicitudes.

Para obtener un rendimiento óptimo y evitar problemas de rendimiento, ajuste los parámetros del núcleo que controlan las tablas de ranuras TCP.

Ejecute el `sysctl -a | grep tcp.*.slot_table` command, y observe los siguientes parámetros:

```
# sysctl -a | grep tcp.*.slot_table
sunrpc.tcp_max_slot_table_entries = 128
sunrpc.tcp_slot_table_entries = 128
```

Todos los sistemas Linux deben incluir `sunrpc.tcp_slot_table_entries`, pero solo algunos incluyen `sunrpc.tcp_max_slot_table_entries`. Ambos deben establecerse en 128.

Si no se establecen estos parámetros, puede tener efectos significativos en el rendimiento. En algunos casos, el rendimiento es limitado porque el sistema operativo linux no está emitiendo suficiente I/O. En otros casos, las latencias de I/O aumentan cuando el sistema operativo linux intenta emitir más operaciones de I/O de las que se pueden mantener.

ADR y NFS

Algunos clientes han informado de problemas de rendimiento derivados de una cantidad excesiva de I/O en los datos de `ADR` ubicación. Por lo general, el problema no ocurre hasta que se acumulan muchos datos de rendimiento. Se desconoce el motivo del exceso de E/S, pero este problema parece ser el resultado de que los procesos de Oracle exploran repetidamente el directorio de destino en busca de cambios.

Extracción del `noac` y/o. `actimeo=0` Las opciones de montaje permiten almacenar en caché el sistema operativo del host y reducen los niveles de I/O de almacenamiento.

NetApp recomienda no colocar `ADR` datos en un sistema de archivos con `noac` o. `actimeo=0` ya que son probables problemas de rendimiento. Separar `ADR` los datos en un punto de montaje diferente si es necesario.

nfs-rootonly y mount-rootonly

ONTAP incluye una opción de NFS denominada `nfs-rootonly` Esto controla si el servidor acepta conexiones de tráfico NFS desde puertos altos. Como medida de seguridad, solo el usuario root puede abrir conexiones TCP/IP utilizando un puerto de origen inferior a 1024 porque dichos puertos normalmente están reservados para el uso del sistema operativo, no para los procesos del usuario. Esta restricción ayuda a garantizar que el tráfico NFS provenga de un cliente NFS del sistema operativo real y no de un proceso malicioso que emula un cliente NFS. El cliente dNFS de Oracle es un controlador de espacio de usuario, pero el proceso se ejecuta como raíz, por lo que generalmente no es necesario cambiar el valor de `nfs-rootonly`. Las conexiones se realizan a partir de puertos bajos.

La `mount-rootonly` La opción solo se aplica a NFSv3. Controla si la llamada DE MONTAJE RPC se acepta desde puertos superiores a 1024. Cuando se utiliza dNFS, el cliente vuelve a ejecutarse como raíz, por lo que puede abrir puertos por debajo de 1024. Este parámetro no tiene efecto.

Los procesos que abren conexiones con dNFS a través de NFS versiones 4,0 y superiores no se ejecutan como raíz y, por lo tanto, requieren puertos a través de 1024. La `nfs-rootonly` El parámetro debe estar establecido en disabled para que dNFS complete la conexión.

Si `nfs-rootonly` Está habilitada, el resultado es un bloqueo durante la fase de montaje al abrir las conexiones dNFS. La salida sqlplus tiene un aspecto similar al siguiente:

```
SQL>startup
ORACLE instance started.
Total System Global Area 4294963272 bytes
Fixed Size                  8904776 bytes
Variable Size             822083584 bytes
Database Buffers         3456106496 bytes
Redo Buffers                7868416 bytes
```

El parámetro se puede cambiar de la siguiente manera:

```
Cluster01::> nfs server modify -nfs-rootonly disabled
```

En raras ocasiones, es posible que necesite cambiar nfs-rootonly y mount-rootonly a disabled. Si un servidor administra un número extremadamente grande de conexiones TCP, es posible que no haya puertos por debajo de 1024 GbE disponibles y que el sistema operativo se vea forzado a utilizar puertos más altos. Estos dos parámetros de ONTAP necesitarían ser cambiados para permitir que la conexión se complete.

Políticas de exportación NFS: Superusuario y setuid

Si los binarios de Oracle se encuentran en un recurso compartido NFS, la política de exportación debe incluir permisos de superusuario y setuid.

Las exportaciones NFS compartidas que se utilizan para servicios de archivos genéricos, como los directorios iniciales de usuario, suelen aplastar al usuario raíz. Esto significa que una solicitud del usuario root en un host que ha montado un sistema de archivos se vuelve a asignar como un usuario diferente con privilegios inferiores. Esto ayuda a proteger los datos al impedir que un usuario root de un servidor determinado acceda a los datos del servidor compartido. El bit setuid también puede ser un riesgo de seguridad en un entorno compartido. El bit setuid permite que un proceso se ejecute como un usuario diferente al usuario que llama al comando. Por ejemplo, un script de shell que era propiedad de root con el bit setuid se ejecuta como root. Si ese script de shell pudiera ser cambiado por otros usuarios, cualquier usuario que no sea root podría emitir un comando como root actualizando el script.

Los binarios de Oracle incluyen archivos propiedad de root y utilizan el bit setuid. Si los binarios de Oracle se instalan en un recurso compartido NFS, la política de exportación debe incluir los permisos de superusuario y setuid adecuados. En el ejemplo siguiente, la regla incluye ambos `allow-suid` y permisos `superuser` Acceso (root) para clientes NFS mediante la autenticación del sistema.

```
Cluster01::> export-policy rule show -vserver vserver1 -policyname orabin
-fields allow-suid,superuser
vserver   policyname ruleindex superuser allow-suid
--------- ---------- --------- --------- ----------
vserver1  orabin     1         sys       true
```

Configuración de NFSv4/4,1

Para la mayoría de las aplicaciones, hay muy poca diferencia entre NFSv3 y NFSv4. Las operaciones de I/O de aplicaciones suelen ser muy sencillas y no se benefician de forma significativa de algunas de las funciones avanzadas disponibles en NFSv4. Las versiones superiores de NFS no deberían considerarse como una «actualización» desde el punto de vista del almacenamiento de base de datos, sino como versiones de NFS que incluyen funciones adicionales. Por ejemplo, si se requiere la seguridad de extremo a extremo del modo de privacidad de kerberos (krb5p), se necesita NFSv4.

NetApp recomienda usar NFSv4,1 si se requieren capacidades de NFSv4. Existen algunas mejoras funcionales en el protocolo NFSv4 en NFSv4,1 que mejoran la resiliencia en ciertos casos perimetrales.

Cambiar a NFSv4 es más complicado que simplemente cambiar las opciones de montaje de vers=3 a vers=4,1. Para obtener una explicación más completa de la configuración de NFSv4 con ONTAP, que incluye

instrucciones para configurar el sistema operativo, consulte "Prácticas recomendadas de TR-4067 NFS en ONTAP". En las siguientes secciones de este documento técnico se explican algunos de los requisitos básicos para el uso de NFSv4.

NFSv4 dominio

Una explicación completa de la configuración de NFSv4/4,1 está fuera del alcance de este documento, pero un problema que se encuentra comúnmente es una discrepancia en la asignación de dominio. Desde un punto de vista sysadmin, los sistemas de archivos NFS parecen comportarse normalmente, pero las aplicaciones informan de errores sobre permisos y/o setuid en determinados archivos. En algunos casos, los administradores han concluido incorrectamente que los permisos de los binarios de la aplicación se han dañado y han ejecutado comandos chown o chmod cuando el problema real era el nombre de dominio.

El nombre de dominio NFSv4 se establece en la SVM de ONTAP:

```
Cluster01::> nfs server show -fields v4-id-domain
vserver   v4-id-domain
--------- ------------
vserver1  my.lab
```

El nombre de dominio NFSv4 del host se establece en `/etc/idmap.cfg`

```
[root@host1 etc]# head /etc/idmapd.conf
[General]
#Verbosity = 0
# The following should be set to the local NFSv4 domain name
# The default is the host's DNS domain name.
Domain = my.lab
```

Los nombres de dominio deben coincidir. Si no lo hacen, aparecerán errores de asignación similares a los siguientes en la `/var/log/messages`:

```
Apr 12 11:43:08 host1 nfsidmap[16298]: nss_getpwnam: name 'root@my.lab'
does not map into domain 'default.com'
```

Los binarios de aplicaciones, como los binarios de Oracle Database, incluyen archivos propiedad de root con el bit setuid, lo que significa que una discrepancia en los nombres de dominio NFSv4 provoca fallos en el inicio de Oracle y una advertencia sobre la propiedad o los permisos de un archivo llamado `oradism`, que se encuentra en la `$ORACLE_HOME/bin` directorio. Debería aparecer de la siguiente manera:

```
[root@host1 etc]# ls -l /orabin/product/19.3.0.0/dbhome_1/bin/oradism
-rwsr-x--- 1 root oinstall 147848 Apr 17  2019
/orabin/product/19.3.0.0/dbhome_1/bin/oradism
```

Si este archivo aparece con la propiedad de Nadie, puede haber un problema de asignación de dominio

NFSv4.

```
[root@host1 bin]# ls -l oradism
-rwsr-x--- 1 nobody oinstall 147848 Apr 17  2019 oradism
```

Para solucionarlo, compruebe la `/etc/idmap.cfg` Haga un archivo con la configuración de v4-id-domain en ONTAP y asegúrese de que son consistentes. Si no lo son, realice los cambios necesarios, ejecute `nfsidmap -c`, y esperar un momento para que los cambios se propaguen. La propiedad del archivo debe reconocerse correctamente como root. Si un usuario había intentado ejecutar `chown root` En este archivo antes de que se corrigiera la configuración de los dominios NFS, es posible que sea necesario ejecutarlo `chown root` de nuevo.

NFS directo de Oracle (dNFS)

Las bases de datos de Oracle pueden utilizar NFS de dos maneras.

En primer lugar, puede utilizar un sistema de archivos montado utilizando el cliente NFS nativo que forma parte del sistema operativo. A veces, esto se denomina nfs del núcleo o knfs. El sistema de archivos NFS es montado y utilizado por la base de datos Oracle exactamente igual que cualquier otra aplicación utilizaría un sistema de archivos NFS.

El segundo método es Oracle Direct NFS (dNFS). Se trata de una implementación del estándar NFS dentro del software de base de datos Oracle. No cambia la forma en que el DBA configura o gestiona las bases de datos Oracle. Siempre que el sistema de almacenamiento disponga de la configuración correcta, el uso de dNFS debe ser transparente para el equipo de administradores de bases de datos y los usuarios finales.

Una base de datos con la función dNFS activada todavía tiene montados los sistemas de archivos NFS habituales. Una vez abierta la base de datos, Oracle Database abre un conjunto de sesiones TCP/IP y ejecuta las operaciones NFS directamente.

NFS directo

El valor principal de Direct NFS de Oracle es omitir el cliente NFS host y realizar operaciones de archivos NFS directamente en un servidor NFS. Para activarlo sólo es necesario cambiar la biblioteca de Oracle Disk Manager (ODM). Las instrucciones para este proceso se proporcionan en la documentación de Oracle.

El uso de dNFS permite mejorar considerablemente el rendimiento de I/O y disminuye la carga en el host y el sistema de almacenamiento, ya que el proceso de I/O se realiza de la forma más eficiente posible.

Además, Oracle dNFS incluye una **opción** para el acceso múltiple de la interfaz de red y la tolerancia a fallos. Por ejemplo, se pueden enlazar dos interfaces de 10Gb GbE para ofrecer un ancho de banda de 20Gb Gb/s. El fallo de una interfaz provoca que se vuelvan a intentar I/O en la otra interfaz. El funcionamiento general es muy similar al multivía FC. La tecnología MultiPath era común hace años, cuando ethernet de 1GB Gb era el estándar más común. Una NIC de 10Gb es suficiente para la mayoría de las cargas de trabajo de Oracle, pero si se necesitan más, se pueden vincular 10Gb NIC.

Cuando se utiliza dNFS, es crítico que se instalen todos los parches descritos en Oracle Doc 1495104,1. Si no se puede instalar un parche, se debe evaluar el entorno para asegurarse de que los errores descritos en ese documento no causen problemas. En algunos casos, la imposibilidad de instalar los parches necesarios impide el uso de dNFS.

No utilice dNFS con ningún tipo de resolución de nombres por turnos, incluidos DNS, DDNS, NIS o cualquier otro método. Esto incluye la función de equilibrio de carga DNS disponible en ONTAP. Cuando una base de

datos Oracle que utiliza dNFS resuelve un nombre de host en una dirección IP, no debe cambiar en las consultas posteriores. Esto puede provocar fallos en la base de datos de Oracle y daños en los datos.

Habilitando dNFS

Oracle dNFS puede trabajar con NFSv3 sin necesidad de configuración más allá de habilitar la biblioteca dNFS (consulte la documentación de Oracle para ver el comando específico necesario), pero si dNFS no puede establecer la conectividad, puede volver silenciosamente al cliente NFS del núcleo. Si esto sucede, el rendimiento puede verse seriamente afectado.

Si desea utilizar la multiplexación dNFS a través de múltiples interfaces, con NFSv4.X, o utilizar el cifrado, debe configurar un archivo oranfstab. La sintaxis es extremadamente estricta. Pequeños errores en el archivo pueden provocar el bloqueo del inicio o el paso por alto del archivo oranfstab.

En el momento de la redacción de este documento, la función multivía de dNFS no funciona con NFSv4,1 con las versiones recientes de Oracle Database. Un archivo oranfstab que especifica NFSv4,1 como protocolo sólo puede utilizar una sentencia PATH única para una exportación determinada. El motivo es que ONTAP no admite el trunking ClientID. Los parches de Oracle Database para resolver esta limitación pueden estar disponibles en el futuro.

La única forma de estar seguro de que dNFS funciona como se espera es consultar las tablas v$dnfs.

A continuación se muestra un archivo oranfstab de ejemplo ubicado en /etc. Esta es una de las múltiples ubicaciones en las que se puede colocar un archivo oranfstab.

```
[root@jfs11 trace]# cat /etc/oranfstab
server: NFSv3test
path: jfs_svmdr-nfs1
path: jfs_svmdr-nfs2
export: /dbf mount: /oradata
export: /logs mount: /logs
nfs_version: NFSv3
```

El primer paso es comprobar que dNFS está operativo para los sistemas de archivos especificados:

```
SQL> select dirname,nfsversion from v$dnfs_servers;

DIRNAME
-----------------------------------
NFSVERSION
----------------
/logs
NFSv3.0

/dbf
NFSv3.0
```

Esta salida indica que dNFS está en uso con estos dos sistemas de archivos, pero **no** significa que oranfstab está operativo. Si se presentara un error, dNFS habría detectado automáticamente los sistemas de archivos

NFS del host y es posible que todavía vea la misma salida de este comando.

La multivía se puede comprobar de la siguiente manera:

```
SQL> select svrname,path,ch_id from v$dnfs_channels;

SVRNAME
------------------------------------
PATH
------------------------------------
     CH_ID
----------
NFSv3test
jfs_svmdr-nfs1
         0

NFSv3test
jfs_svmdr-nfs2
         1

SVRNAME
------------------------------------
PATH
------------------------------------
     CH_ID
----------

NFSv3test
jfs_svmdr-nfs1
         0

NFSv3test
jfs_svmdr-nfs2

[output truncated]

SVRNAME
------------------------------------
PATH
------------------------------------
     CH_ID
----------
NFSv3test
jfs_svmdr-nfs2
         1

NFSv3test
```

```
jfs_svmdr-nfs1
         0

SVRNAME
------------------------------------
PATH
------------------------------------
     CH_ID
----------

NFSv3test
jfs_svmdr-nfs2
         1


66 rows selected.
```

Estas son las conexiones que utiliza dNFS. Hay dos rutas y canales visibles para cada entrada SVRNAME. Esto significa que la multivía está funcionando, lo que significa que se reconoció y procesó el archivo oranfstab.

Acceso directo a sistemas de archivos del host y NFS

En ocasiones, el uso de dNFS puede ocasionar problemas en las aplicaciones o actividades del usuario que se basan en los sistemas de archivos visibles montados en el host, ya que el cliente dNFS accede al sistema de archivos fuera de banda desde el sistema operativo host. El cliente dNFS puede crear, eliminar y modificar archivos sin el conocimiento del sistema operativo.

Cuando se utilizan las opciones de montaje para bases de datos de instancia única, se activa el almacenamiento en caché de atributos de archivo y directorio, lo que también significa que el contenido de un directorio está en caché. Por lo tanto, dNFS puede crear un archivo, y hay un breve retraso antes de que el sistema operativo vuelva a leer el contenido del directorio y el archivo se haga visible para el usuario. Esto no es generalmente un problema, pero, en raras ocasiones, utilidades como SAP BR*Tools pueden tener problemas. Si esto sucede, solucione el problema cambiando las opciones de montaje para utilizar las recomendaciones para Oracle RAC. Este cambio provoca la deshabilitación de todo el almacenamiento en caché del host.

Cambie las opciones de montaje solo cuando (a) se utiliza dNFS y (b) se produce un problema debido a un desfase en la visibilidad de los archivos. Si no se utiliza dNFS, el rendimiento se reduce al utilizar las opciones de montaje de Oracle RAC en una base de datos de instancia única.

> Consulte la nota `nosharecache` sobre en "Opciones de montaje de Linux NFS" para ver un problema de dNFS específico de Linux que puede producir resultados inusuales.

Arrendamientos y bloqueos de NFS

NFSv3 está sin estado. Esto implica efectivamente que el servidor NFS (ONTAP) no realiza un seguimiento de qué sistemas de archivos están montados, quién o qué bloqueos están realmente instalados.

ONTAP dispone de algunas funciones que registrarán los intentos de montaje, por lo que tiene una idea de qué clientes pueden acceder a los datos y puede que haya bloqueos asesores, pero no se garantiza que esa información esté al 100% completa. No se puede completar, ya que el seguimiento del estado del cliente NFS no forma parte del estándar NFSv3.1.

NFSv4 Estado

Por el contrario, NFSv4 tiene estado. El servidor NFSv4 rastrea qué clientes están utilizando qué sistemas de archivos, qué archivos existen, qué archivos y/o regiones de archivos están bloqueados, etc. Esto significa que debe haber una comunicación regular entre un servidor NFSv4 para mantener los datos de estado actualizados.

Los estados más importantes que gestiona el servidor NFS son NFSv4 bloqueos y NFSv4 arrendamientos y están muy entrelazados. Necesitas entender cómo cada uno trabaja por sí mismo, y cómo se relacionan entre sí.

NFSv4 bloqueos

Con NFSv3, las cerraduras son un aviso. Un cliente NFS aún puede modificar o eliminar un archivo «bloqueado». Un bloqueo NFSv3 no caduca por sí mismo, debe ser eliminado. Esto crea problemas. Por ejemplo, si tiene una aplicación en cluster que crea NFSv3 bloqueos y uno de los nodos falla, ¿qué debe hacer? Puede codificar la aplicación en los nodos supervivientes para eliminar los bloqueos, pero ¿cómo sabe que es seguro? ¿Puede que el nodo «fallido» esté operativo, pero no se comunica con el resto del clúster?

Con NFSv4, las cerraduras tienen una duración limitada. Mientras el cliente que mantiene los bloqueos continúe registrando en el servidor NFSv4, no se permitirá a ningún otro cliente adquirir estos bloqueos. Si un cliente no se registra en NFSv4, el servidor eventualmente revoca los bloqueos y otros clientes podrán solicitar y obtener bloqueos.

NFSv4 arrendamientos

NFSv4 bloqueos están asociados a un arrendamiento NFSv4. Cuando un cliente NFSv4 establece una conexión con un servidor NFSv4, obtiene un permiso. Si el cliente obtiene un bloqueo (hay muchos tipos de bloqueos), el bloqueo se asocia con la concesión.

Esta concesión tiene un timeout definido. De forma predeterminada, ONTAP establecerá el valor de tiempo de espera en 30 segundos:

```
Cluster01::*> nfs server show -vserver vserver1 -fields v4-lease-seconds

vserver   v4-lease-seconds
--------- ----------------
vserver1  30
```

Esto significa que un cliente NFSv4 necesita registrarse con el servidor NFSv4 cada 30 segundos para renovar sus arrendamientos.

El arrendamiento se renueva automáticamente por cualquier actividad, por lo que si el cliente está haciendo trabajo no hay necesidad de realizar operaciones de adición. Si una aplicación se vuelve silenciosa y no está haciendo un trabajo real, tendrá que realizar una especie de operación de mantenimiento de la vida (llamada SECUENCIA) en su lugar. En esencia, es solo decir «sigo aquí, actualice mis contratos de arrendamiento».

```
 *Question:* What happens if you lose network connectivity for 31 seconds?
NFSv3 está sin estado. No se espera la comunicación de los clientes. NFSv4
aparece con estado y, una vez que transcurre el período de concesión, la
concesión caduca, se revocan los bloqueos, y los archivos bloqueados se
ponen a disposición de otros clientes.
```

Con NFSv3, puede mover los cables de red, reiniciar los switches de red, realizar cambios de configuración y estar bastante seguro de que no sucedería nada malo. Las aplicaciones normalmente solo esperarían pacientemente a que la conexión de red vuelva a funcionar.

Con NFSv4, tienes 30 segundos (a menos que hayas aumentado el valor de ese parámetro dentro de ONTAP) para completar tu trabajo. Si sobrepasa eso, se agota el tiempo de arrendamiento. Normalmente, esto provoca fallos de aplicación.

Por ejemplo, si tiene una base de datos Oracle y experimenta una pérdida de conectividad de red (a veces denominada «partición de red») que supera el tiempo de espera de concesión, bloqueará la base de datos.

A continuación, se muestra un ejemplo de lo que ocurre en el log de alertas de Oracle si esto sucede:

```
2022-10-11T15:52:55.206231-04:00
Errors in file /orabin/diag/rdbms/ntap/NTAP/trace/NTAP_ckpt_25444.trc:
ORA-00202: control file: '/redo0/NTAP/ctrl/control01.ctl'
ORA-27072: File I/O error
Linux-x86_64 Error: 5: Input/output error
Additional information: 4
Additional information: 1
Additional information: 4294967295
2022-10-11T15:52:59.842508-04:00
Errors in file /orabin/diag/rdbms/ntap/NTAP/trace/NTAP_ckpt_25444.trc:
ORA-00206: error in writing (block 3, # blocks 1) of control file
ORA-00202: control file: '/redo1/NTAP/ctrl/control02.ctl'
ORA-27061: waiting for async I/Os failed
```

Si observa los syslogs, debería ver varios de estos errores:

```
Oct 11 15:52:55 host1 kernel: NFS: nfs4_reclaim_open_state: Lock reclaim
failed!
Oct 11 15:52:55 host1 kernel: NFS: nfs4_reclaim_open_state: Lock reclaim
failed!
Oct 11 15:52:55 host1 kernel: NFS: nfs4_reclaim_open_state: Lock reclaim
failed!
```

Los mensajes de registro suelen ser el primer signo de un problema, aparte de la congelación de la aplicación. Normalmente, no verá nada durante la interrupción de la red, porque los procesos y el propio SO están bloqueados al intentar acceder al sistema de archivos NFS.

Los errores aparecen después de que la red vuelva a funcionar. En el ejemplo anterior, una vez que se restablece la conectividad, el sistema operativo intentó volver a adquirir los bloqueos, pero era demasiado tarde. El arrendamiento había caducado y se eliminaron los bloqueos. Esto produce un error que se propaga hasta la capa de Oracle y provoca el mensaje en el log de alertas. Es posible que vea variaciones en estos patrones en función de la versión y la configuración de la base de datos.

En resumen, NFSv3 tolera la interrupción de la red, pero NFSv4 es más sensible e impone un período de arrendamiento definido.

¿Qué pasa si un tiempo de espera de 30 segundos no es aceptable? ¿Qué pasa si administra una red que cambia dinámicamente en la que se reinician los switches o se reubican los cables y el resultado es la interrupción ocasional de la red? Puede optar por ampliar el período de arrendamiento, pero si lo desea, requiere una explicación de NFSv4 períodos de gracia.

NFSv4 periodos de gracia

Si se reinicia un servidor NFSv3, está listo para servir IO casi al instante. No estaba manteniendo ningún tipo de estado sobre los clientes. El resultado es que la operación de toma de control de ONTAP parece estar casi al instante. En el momento en que un controlador está listo para comenzar a servir datos, enviará un ARP a la red que indica el cambio en la topología. En general, los clientes lo detectan de forma casi instantánea y se reanuda el flujo de los datos.

NFSv4, sin embargo, producirá una breve pausa. Es solo parte de cómo funciona NFSv4.

> Las siguientes secciones están actualizadas a partir de ONTAP 9.15,1, pero el comportamiento de arrendamiento y bloqueo, así como las opciones de ajuste pueden cambiar de versión a versión. Si necesita ajustar los tiempos de espera de arrendamiento/bloqueo NFSv4, consulte al soporte de NetApp para obtener la información más reciente.

Los servidores NFSv4 necesitan realizar un seguimiento de los arrendamientos, los bloqueos y quién utiliza qué datos. Si un servidor NFS produce una alarma y se reinicia, pierde energía durante un momento, o se reinicia durante la actividad de mantenimiento, el resultado es la concesión/bloqueo y se pierde otra información del cliente. El servidor necesita averiguar qué cliente está utilizando qué datos antes de reanudar las operaciones. Aquí es donde entra el período de gracia.

Si de repente apaga el servidor NFSv4. Cuando vuelva a estar activo, los clientes que intenten reanudar I/O obtendrán una respuesta que diga «He perdido información de arrendamiento/bloqueo. ¿Desea volver a registrar sus bloqueos? Ese es el comienzo del período de gracia. El valor predeterminado es 45 segundos en ONTAP:

```
Cluster01::> nfs server show -vserver vserver1 -fields v4-grace-seconds

vserver   v4-grace-seconds
--------- ----------------
vserver1  45
```

El resultado es que, después de un reinicio, una controladora pausará el I/O mientras todos los clientes recuperan sus concesiones y bloqueos. Una vez que finaliza el período de gracia, el servidor reanudará las operaciones de E/S.

Este período de gracia controla la reclamación de concesión durante los cambios de la interfaz de red, pero hay un segundo período de gracia que controla la recuperación durante la conmutación por error del

almacenamiento, `locking.grace_lease_seconds`. Esta es una opción de nivel de nodo.

```
cluster01::> node run [node names or *] options
locking.grace_lease_seconds
```

Por ejemplo, si necesitaba realizar recuperaciones tras fallos de LIF y necesitaba reducir el período de gracia, cambiaría `v4-grace-seconds`. Si desea mejorar el tiempo de reanudación de I/O durante la recuperación tras fallos de la controladora, debería cambiar `locking.grace_lease_seconds`.

Solo altere estos valores con precaución y después de comprender completamente los riesgos y las consecuencias. Las pausas de I/O implicadas en las operaciones de recuperación tras fallos y migración con NFSv4.X no se pueden evitar completamente. Los períodos de bloqueo, arrendamiento y gracia forman parte de NFS RFC. Para muchos clientes, NFSv3 es preferible porque los tiempos de recuperación tras fallos son más rápidos.

Tiempos de espera de leasing frente a períodos de gracia

El período de gracia y el período de arrendamiento están conectados. Como se ha mencionado anteriormente, el tiempo de espera predeterminado de la concesión es de 30 segundos, lo que significa que NFSv4 clientes deben realizar el check in con el servidor al menos cada 30 segundos o pierden sus arrendamientos y, a su vez, sus bloqueos. El período de gracia existe para permitir que un servidor NFS vuelva a generar los datos de concesión/bloqueo y, de forma predeterminada, es de 45 segundos. El período de gracia debe ser superior al período de arrendamiento. Esto garantiza que un entorno de cliente NFS diseñado para renovar arrendamientos al menos cada 30 segundos pueda conectarse con el servidor después de un reinicio. Un período de gracia de 45 segundos asegura que todos aquellos clientes que esperan renovar sus arrendamientos al menos cada 30 segundos definitivamente tienen la oportunidad de hacerlo.

Si un tiempo de espera de 30 segundos no es aceptable, puede optar por ampliar el período de arrendamiento.

Si desea aumentar el tiempo de espera de concesión a 60 segundos para soportar una interrupción de la red de 60 segundos, también tendrá que aumentar el período de gracia. Esto significa que experimentará pausas más largas de I/O durante la recuperación tras fallos de la controladora.

Esto no debería ser normalmente un problema. Los usuarios habituales solo actualizan las controladoras de ONTAP una o dos veces al año, y las recuperaciones tras fallos no planificadas debido a fallos de hardware son extremadamente raras. Además, si tenía una red en la que una interrupción de la red de 60 segundos era preocupante y necesitaba un tiempo de espera de concesión de 60 segundos, es probable que no se oponga a una conmutación por error rara del sistema de almacenamiento, lo que provoca una pausa de 61 segundos. Ya ha reconocido que tiene una red que se detiene durante más de 60 segundos con bastante frecuencia.

Almacenamiento en caché NFS

La presencia de cualquiera de las siguientes opciones de montaje provoca la deshabilitación del almacenamiento en caché del host:

```
cio, actimeo=0, noac, forcedirectio
```

Estos ajustes pueden tener un efecto negativo grave en la velocidad de la instalación del software, la aplicación de parches y las operaciones de copia de seguridad/restauración. En algunos casos, especialmente

con aplicaciones en cluster, estas opciones son necesarias como consecuencia inevitable de la necesidad de proporcionar coherencia de la caché en todos los nodos del cluster. En otros casos, los clientes utilizan estos parámetros por error y el resultado es un daño innecesario en el rendimiento.

Muchos clientes eliminan temporalmente estas opciones de montaje durante la instalación o aplicación de parches de los archivos binarios de la aplicación. Esta eliminación se puede realizar de forma segura si el usuario comprueba que ningún otro proceso está utilizando activamente el directorio de destino durante el proceso de instalación o aplicación de parches.

Los tamaños de transferencia de NFS

De forma predeterminada, ONTAP limita el tamaño de I/O de NFS a 64K.

La I/O aleatoria con la mayoría de aplicaciones y bases de datos utiliza un tamaño de bloque mucho más pequeño, que es muy inferior al máximo de 64K KB. Las operaciones de I/O de grandes bloques suelen estar en paralelo, por lo que el máximo de 64K KB tampoco se limita a obtener el ancho de banda máximo.

Hay algunas cargas de trabajo en las que el máximo de 64K crea una limitación. En particular, las operaciones de subproceso único como la operación de copia de seguridad o recuperación o una exploración de tabla completa de la base de datos se ejecutan de forma más rápida y eficiente si la base de datos puede realizar menos E/S pero más grandes. El tamaño óptimo de gestión de I/O para ONTAP es de 256K KB.

El tamaño de transferencia máximo para una SVM de ONTAP determinada se puede cambiar de la siguiente manera:

```
Cluster01::> set advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
Cluster01::*> nfs server modify -vserver vserver1 -tcp-max-xfer-size
262144
Cluster01::*>
```

> No reduzca nunca el tamaño máximo permitido de transferencia en ONTAP por debajo del valor de rsize/wsize de los sistemas de archivos NFS montados actualmente. Esto puede crear bloqueos o incluso corrupción de datos con algunos sistemas operativos. Por ejemplo, si los clientes NFS se establecen actualmente con un valor de rsize/wsize de 65536 000, el tamaño de transferencia máximo de ONTAP se podría ajustar entre 65536 000 y 1048576 000 sin que ello afecte a porque los propios clientes están limitados. Reducir el tamaño máximo de transferencia por debajo de 65536 puede dañar la disponibilidad o los datos.

NVFAIL

NVFAIL es una función de ONTAP que garantiza la integridad en situaciones catastróficas de conmutación por error.

Las bases de datos son vulnerables a daños durante eventos de conmutación por error de almacenamiento debido a que mantienen cachés internos de gran tamaño. Si un evento catastrófico requiere forzar una conmutación por error de ONTAP o forzar la conmutación por error de MetroCluster, independientemente del estado de la configuración general, el resultado es que los cambios confirmados previamente se pueden

descartar de forma efectiva. El contenido de la cabina de almacenamiento se retrocede en el tiempo y el estado de la caché de base de datos ya no refleja el estado de los datos del disco. Esta inconsistencia provoca daños en los datos.

El almacenamiento en caché puede tener lugar en la capa de aplicaciones o del servidor. Por ejemplo, una configuración de Oracle Real Application Cluster (RAC) con servidores activos tanto en un sitio primario como en un sitio remoto almacena datos en caché en Oracle SGA. Una operación de conmutación de sitios forzada que provocara una pérdida de datos pondría la base de datos en riesgo de dañarse, ya que los bloques almacenados en el SGA podrían no coincidir con los bloques del disco.

Un uso menos obvio del almacenamiento en caché se da en la capa del sistema de archivos del sistema de sistemas operativos. Los bloques de un sistema de archivos NFS montado se pueden almacenar en caché en el sistema operativo. Como alternativa, un sistema de archivos en clúster basado en las LUN ubicadas en el sitio primario podría montarse en servidores en el sitio remoto y una vez más podrían almacenarse los datos en caché. Un fallo de NVRAM o una toma de control forzada o una conmutación de sitios forzada en estas situaciones podría provocar daños en el sistema de archivos.

ONTAP protege las bases de datos y los sistemas operativos de este escenario con NVFAIL y su configuración asociada.

Utilidad de Reclamación de ASM (ASMRU)

ONTAP elimina de manera eficiente los bloques puestos a cero que se escriben en un archivo o LUN cuando se habilita la compresión en línea. Las utilidades como Oracle ASM Reclamation Utility (ASRU) funcionan escribiendo ceros en extensiones de ASM no utilizadas.

Esto permite a los administradores de bases de datos reclamar espacio en la cabina de almacenamiento después de la eliminación de los datos. ONTAP intercepta los ceros y desasigna el espacio de la LUN. El proceso de recuperación es extremadamente rápido porque no se escriben datos en el sistema de almacenamiento.

Desde el punto de vista de la base de datos, el grupo de discos de ASM contiene ceros, y leer esas regiones de las LUN daría como resultado un flujo de ceros, pero ONTAP no almacena los ceros en las unidades. En su lugar, se realizan cambios sencillos en los metadatos que marcan internamente las regiones en cero de la LUN como vacías de datos.

Por motivos similares, las pruebas de rendimiento que involucran datos puestos a cero no son válidas porque en realidad los bloques de ceros no se procesan como escrituras en la cabina de almacenamiento.

> Al utilizar ASRU, asegúrese de que todos los parches recomendados por Oracle están instalados.

Virtualización

La virtualización de bases de datos con VMware, Oracle OLVM o KVM es una opción cada vez más común para los clientes de NetApp que eligieron la virtualización incluso para las bases de datos más importantes.

Compatibilidad

Existen muchos malentendidos acerca de las normativas de soporte de Oracle para la virtualización, especialmente para los productos VMware. No es raro escuchar que Oracle no admite la virtualización. Esta noción es incorrecta y conduce a la pérdida de oportunidades para beneficiarse de la virtualización. El ID de documento de Oracle 249212,1 analiza los requisitos reales y los clientes rara vez consideran que son una preocupación.

Si se produce un problema en un servidor virtualizado y dicho problema es desconocido previamente para los Servicios de Soporte Oracle, es posible que se solicite al cliente que reproduzca el problema en el hardware físico. Es posible que un cliente de Oracle que ejecuta una versión de borde de sangrado de un producto no desee utilizar la virtualización debido a la posibilidad de problemas de compatibilidad, pero esta situación no ha sido un mundo real para los clientes de virtualización que utilizan versiones de productos de Oracle generalmente disponibles.

Presentación de almacenamiento

Los clientes que están considerando la virtualización de sus bases de datos deben basar sus decisiones sobre almacenamiento en sus necesidades empresariales. Aunque esta es una afirmación generalmente verdadera para todas las decisiones DE TI, es especialmente importante para los proyectos de bases de datos, porque el tamaño y el alcance de los requisitos varían considerablemente.

Existen tres opciones básicas para la presentación del almacenamiento:

- LUN virtualizados en almacenes de datos de hipervisores
- LUN iSCSI gestionadas por el iniciador iSCSI en la máquina virtual, no el hipervisor
- Sistemas de archivos NFS montados por la máquina virtual (no desde un almacén de datos basado en NFS)
- Asignaciones directas de dispositivos. Los clientes no se ven favorecidos por los RDM de VMware, pero los dispositivos físicos siguen siendo a menudo asignados de forma similar directamente con la virtualización de KVM y OLVM.

Rendimiento

El método de presentar almacenamiento a un invitado virtualizado no suele afectar al rendimiento. Todos los SO host, los controladores de red virtualizados y las implementaciones de almacenes de datos de hipervisor están muy optimizados y, por lo general, pueden consumir todo el ancho de banda de red FC o IP disponible entre el hipervisor y el sistema de almacenamiento, siempre que se sigan las prácticas recomendadas básicas. En algunos casos, obtener un rendimiento óptimo puede ser ligeramente más sencillo usando un método de presentación de almacenamiento en comparación con otro, pero el resultado final debería ser comparable.

Gran capacidad de administración

El factor clave para decidir cómo presentar el almacenamiento a un invitado virtualizado es la capacidad de gestión. No hay un método correcto o incorrecto. El mejor enfoque depende de las necesidades operativas, las habilidades y las preferencias de TI.

Los factores a considerar incluyen:

- **Transparencia.** Cuando una VM administra sus sistemas de archivos, es más fácil para un administrador de bases de datos o un administrador del sistema identificar el origen de los sistemas de archivos para sus datos. No se accede a los sistemas de archivos y LUN de manera diferente a con un servidor físico.

- **Consistencia.** Cuando una VM es propietaria de sus sistemas de archivos, el uso o no uso de una capa de hipervisor afecta a la capacidad de gestión. Los mismos procedimientos para aprovisionamiento, supervisión, protección de datos, etc. se pueden utilizar en todo el conjunto, incluidos los entornos virtualizados y no virtualizados.

  Por otro lado, en un centro de datos virtualizado al 100% de lo contrario, puede que sea preferible también utilizar el almacenamiento basado en almacenes de datos en toda la huella en la misma razón mencionada anteriormente: Consistencia: La capacidad de usar los mismos procedimientos para aprovisionamiento, protección, montorización y protección de datos.

- **Estabilidad y resolución de problemas.** Cuando una VM es propietaria de sus sistemas de archivos, ofrecer un rendimiento bueno y estable y solucionar problemas son más simples porque toda la pila de almacenamiento está presente en la VM. El único rol del hipervisor es transportar tramas FC o IP. Cuando se incluye un almacén de datos en una configuración, esto complica la configuración introduciendo otro conjunto de tiempos de espera, parámetros, archivos de registro y posibles errores.
- **Portabilidad.** Cuando una VM posee sus sistemas de archivos, el proceso de mover un entorno de Oracle se vuelve mucho más sencillo. Los sistemas de archivos se pueden mover fácilmente entre huéspedes virtualizados y no virtualizados.
- * Bloqueo del proveedor.* Después de colocar los datos en un almacén de datos, usar un hipervisor diferente o extraer los datos del entorno virtualizado se vuelve completamente difícil.
- **Activación de instantáneas.** Los procedimientos de respaldo tradicionales en un entorno virtualizado pueden convertirse en un problema debido al ancho de banda relativamente limitado. Por ejemplo, un tronco 10GbE de cuatro puertos podría ser suficiente para soportar las necesidades de rendimiento diarias de muchas bases de datos virtualizadas, pero tal tronco sería insuficiente para realizar copias de seguridad con RMAN u otros productos de copia de seguridad que requieran transmitir una copia de tamaño completo de los datos. El resultado es que un entorno virtualizado cada vez más consolidado debe realizar backups a través de snapshots de almacenamiento. Esto evita la necesidad de sobrecargar la configuración del hipervisor únicamente para admitir los requisitos de ancho de banda y CPU de la ventana de backup.

  El uso de sistemas de archivos propiedad de invitados a veces facilita el uso de backups y restauraciones basados en copias Snapshot, ya que los objetos de almacenamiento que necesitan protección pueden dirigirse con mayor facilidad. Sin embargo, cada vez es más grande la cantidad de productos de protección de datos de virtualización que se integran bien con los almacenes de datos y las copias Snapshot. La estrategia de backup debe consistir completamente antes de tomar una decisión sobre cómo presentar el almacenamiento a un host virtualizado.

Controladores paravirtualizados

Para un rendimiento óptimo, el uso de controladores de red paravirtualizados es fundamental. Cuando se utiliza un almacén de datos, se requiere un controlador SCSI paravirtualizado. Un controlador de dispositivo paravirtualizado permite a un invitado integrarse más profundamente en el hipervisor, en lugar de un controlador emulado en el que el hipervisor pasa más tiempo de CPU imitando el comportamiento del hardware físico.

RAM de sobrecompromiso

Sobrecomprometer RAM significa configurar más RAM virtualizada en varios hosts de la que existe en el hardware físico. Si lo hace, se pueden producir problemas de rendimiento inesperados. Al virtualizar una base de datos, el hipervisor no debe intercambiar los bloques subyacentes del SGA de Oracle en el almacenamiento. Si lo hace, los resultados de rendimiento son muy inestables.

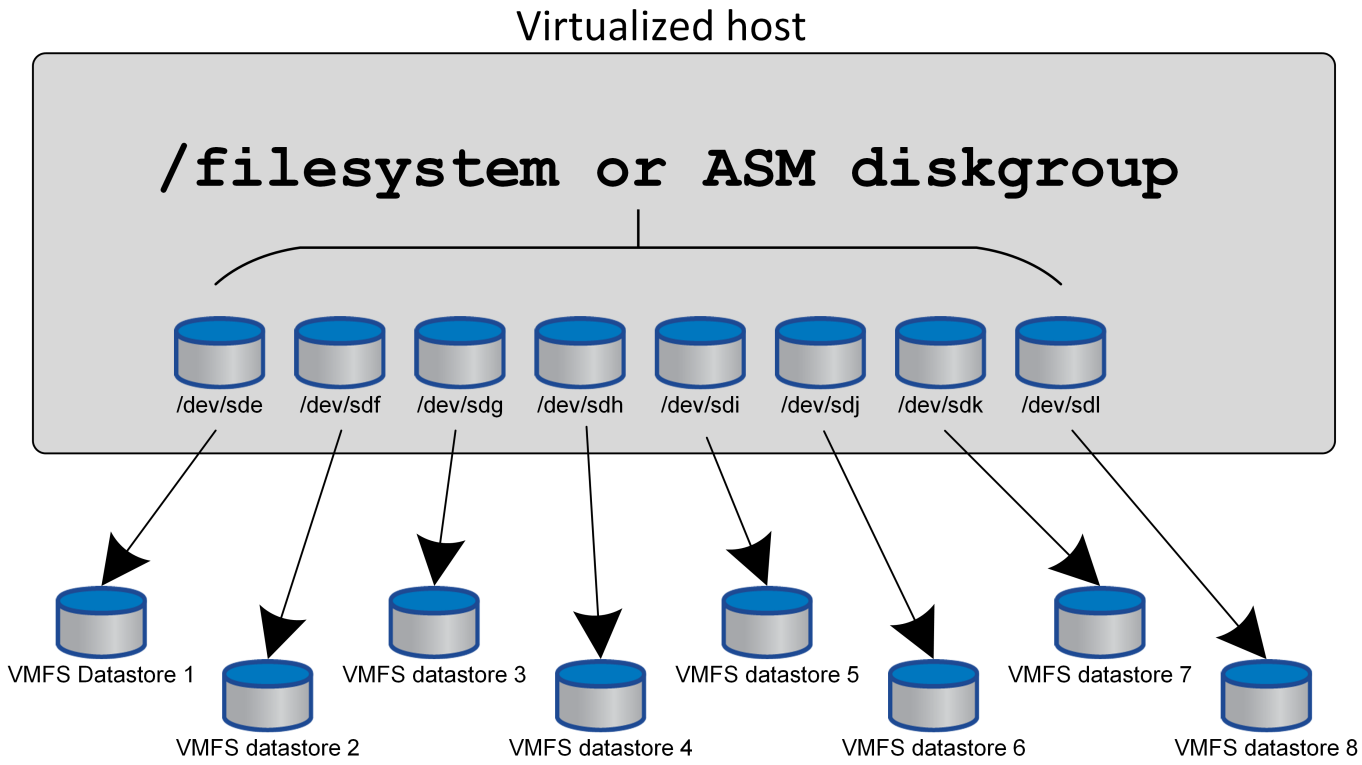
Segmentación de almacenes de datos

Cuando se usan bases de datos con almacenes de datos, hay un factor crucial que debe tenerse en cuenta con respecto al rendimiento: La segmentación.

Las tecnologías de almacenes de datos como VMFS pueden abarcar varios LUN, pero no son dispositivos segmentados. Las LUN se concatenan. El resultado final pueden ser puntos de sobrecarga de la LUN. Por ejemplo, una base de datos de Oracle típica puede tener un grupo de discos ASM de 8 LUN. Se pueden aprovisionar los 8 LUN virtualizados en un almacén de datos VMFS de 8 LUN, pero no hay garantía de cuáles LUN residirán los datos. La configuración resultante podría ser todos los 8 LUN virtualizados que ocupen una única LUN dentro del almacén de datos VMFS. Esto se convierte en un cuello de botella en el rendimiento.

La segmentación suele ser necesaria. Con algunos hipervisores, incluido KVM, es posible crear un almacén de datos con la segmentación de LVM, como se describe "aquí". Con VMware, la arquitectura parece un poco diferente. Cada LUN virtualizado debe colocarse en un almacén de datos VMFS diferente.

Por ejemplo:



El impulsor principal de este enfoque no es ONTAP, sino que se debe a una limitación inherente al número de operaciones que una sola máquina virtual o LUN de hipervisor puede prestar servicio en paralelo. Por lo general, una sola LUN de ONTAP puede admitir muchas más IOPS de las que puede solicitar un host. El límite de rendimiento de una LUN es casi universal debido al SO del host. Como resultado, la mayoría de las bases de datos necesitan entre 4 y 8 LUN para satisfacer sus necesidades de rendimiento.

Las arquitecturas de VMware deben planificar sus arquitecturas con cuidado para asegurarse de que no se encuentren los máximos de almacén de datos o ruta de LUN con este enfoque. Además, no es necesario disponer de un conjunto único de almacenes de datos VMFS para cada base de datos. La principal necesidad es asegurarse de que cada host tenga un conjunto limpio de 4-8 rutas de I/O desde las LUN virtualizadas hasta las LUN de back-end del sistema de almacenamiento propiamente dicho. En raras ocasiones, incluso más almacenes de datos pueden ser útiles para las demandas de rendimiento realmente extremas, pero 4-8 LUN suelen ser suficientes para el 95% de todas las bases de datos. Un solo volumen ONTAP que contiene 8

LUN puede admitir hasta 250.000 IOPS de bloques de Oracle aleatorias con una configuración típica de SO/ONTAP/red.

Organización en niveles

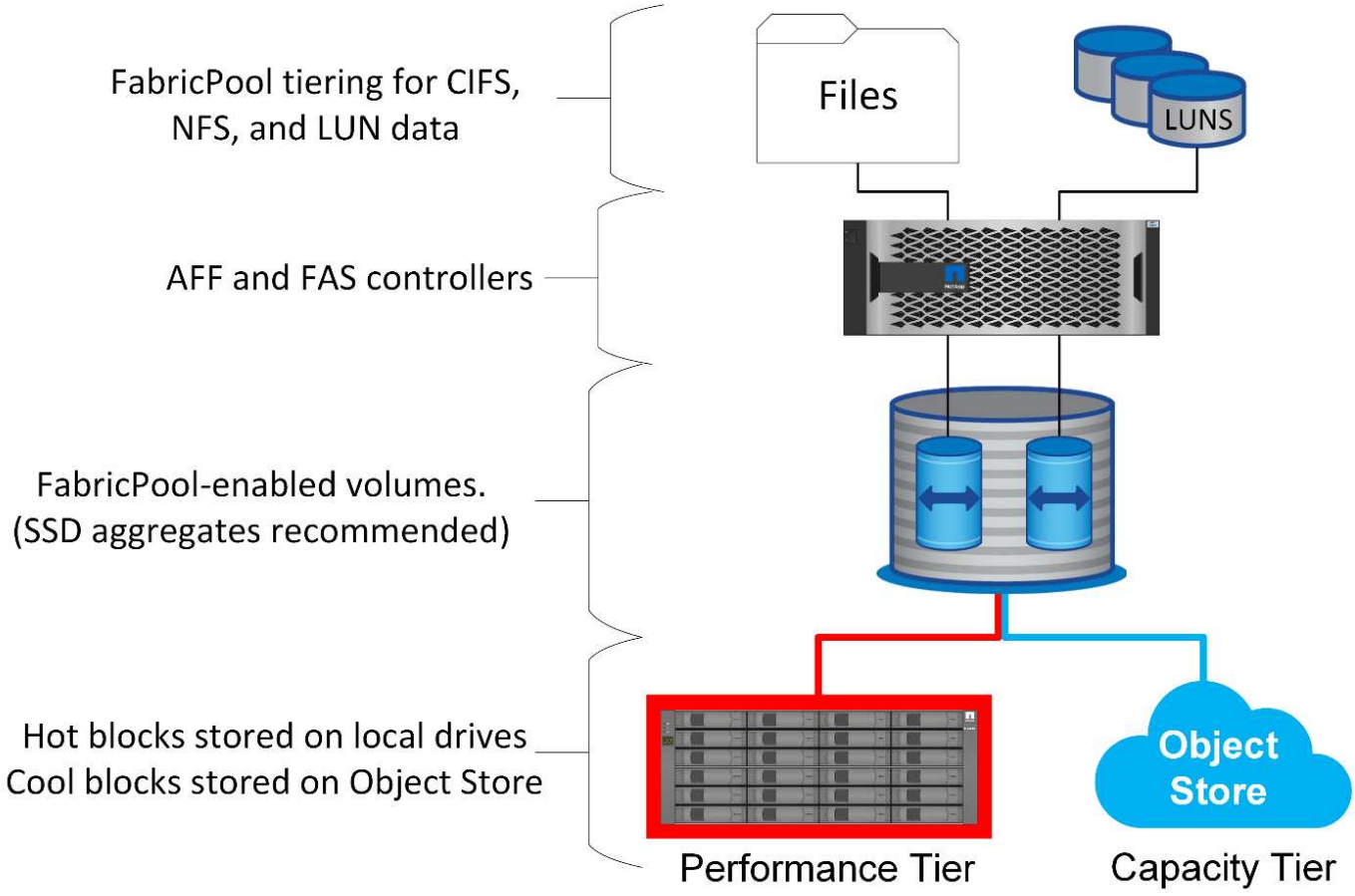
Descripción general

Comprender cómo afecta el almacenamiento por niveles FabricPool a Oracle y otras bases de datos requiere comprender la arquitectura de FabricPool de bajo nivel.

Arquitectura

FabricPool es una tecnología de organización en niveles que clasifica los bloques como activos o inactivos y los coloca en el nivel de almacenamiento más adecuado. El nivel de rendimiento con mayor frecuencia se encuentra en el almacenamiento SSD y aloja los bloques de datos activos. El nivel de capacidad está ubicado en un almacén de objetos y aloja los bloques de datos inactivos. La compatibilidad de almacenamiento de objetos incluye NetApp StorageGRID, ONTAP S3, almacenamiento Microsoft Azure Blob, servicio de almacenamiento de objetos en el cloud de Alibaba, almacenamiento de objetos de IBM Cloud, almacenamiento de Google Cloud y Amazon AWS S3.

Existen varias políticas de organización en niveles disponibles que controlan la clasificación de los bloques como activos o inactivos, y las políticas se pueden establecer por volumen y modificar según sea necesario. Solo se mueven los bloques de datos entre los niveles de rendimiento y capacidad. Los metadatos que definen la LUN y la estructura del sistema de archivos siempre permanecen en el nivel de rendimiento. Como resultado, la gestión se centraliza en ONTAP. Los archivos y los LUN no aparecen diferentes de los datos almacenados en cualquier otra configuración de ONTAP. La controladora NetApp AFF o FAS aplica las políticas definidas para mover datos al nivel adecuado.



Proveedores de almacenes de objetos

Los protocolos de almacenamiento de objetos utilizan solicitudes HTTP o HTTPS sencillas para almacenar grandes cantidades de objetos de datos. El acceso al almacenamiento de objetos debe ser fiable, porque el acceso a los datos desde ONTAP depende de atender solicitudes rápidamente. Entre las opciones se incluyen las opciones de acceso estándar y poco frecuente de Amazon S3, y Microsoft Azure Hot and Cool Blob Storage, IBM Cloud y Google Cloud. No se admiten opciones de archivado como Amazon Glacier y Amazon Archive porque el tiempo necesario para recuperar los datos puede superar las tolerancias de las aplicaciones y los sistemas operativos del host.

También se ofrece compatibilidad con NetApp StorageGRID y es una solución empresarial óptima. Es un sistema de almacenamiento de objetos de alto rendimiento, escalable y altamente seguro que puede proporcionar redundancia geográfica para los datos de FabricPool, así como otras aplicaciones de almacenamiento de objetos que tienen cada vez más probabilidades de formar parte de entornos de aplicaciones empresariales.

StorageGRID también puede reducir los costes al evitar los cargos por salida que imponen muchos proveedores de cloud público por leer los datos de sus servicios.

Los datos y metadatos

Tenga en cuenta que el término «datos» aquí se aplica a los bloques de datos reales, no a los metadatos. Solo los bloques de datos se organizan en niveles, mientras que los metadatos permanecen en el nivel de rendimiento. Además, el estado de un bloque como activo o inactivo solo se ve afectado por la lectura del bloque de datos real. La simple lectura del nombre, la marca de tiempo o los metadatos de propiedad de un archivo no afecta a la ubicación de los bloques de datos subyacentes.

Completos

Aunque FabricPool puede reducir significativamente el espacio físico de almacenamiento, no es por sí misma una solución de backup. Los metadatos de NetApp WAFL siempre permanecen en el nivel de rendimiento. Si un desastre catastrófico destruye el nivel de rendimiento, no se puede crear un nuevo entorno con los datos del nivel de capacidad porque no contiene metadatos de WAFL.

Sin embargo, FabricPool puede formar parte de una estrategia de backup. Por ejemplo, FabricPool se puede configurar con la tecnología de replicación SnapMirror de NetApp. Cada mitad del reflejo puede tener su propia conexión con un destino de almacenamiento de objetos. El resultado es dos copias independientes de los datos. La copia primaria consiste en los bloques del nivel de rendimiento y los bloques asociados del nivel de capacidad, y la réplica es un segundo conjunto de bloques de rendimiento y capacidad.

Políticas de organización en niveles

Políticas de organización en niveles

ONTAP tiene disponibles cuatro políticas que controlan cómo los datos de Oracle en el nivel de rendimiento se convierten en candidatos para reubicar al nivel de capacidad.

Solo Snapshot

La `snapshot-only` `tiering-policy` se aplica sólo a los bloques que no se comparten con el sistema de archivos activo. Básicamente, provoca la organización en niveles de los backups de las bases de datos. Los bloques se convierten en candidatos para organizar por niveles después de que se crea una copia Snapshot y se sobrescribe el bloque, lo que genera un bloque que solo existe dentro de la copia Snapshot. El retraso antes de a. `snapshot-only` el bloque se considera frío y está controlado por el `tiering-minimum-cooling-days` configuración para el volumen. El intervalo a partir de ONTAP 9,8 es de 2 a 183 días.

Muchos conjuntos de datos tienen tasas de cambio bajas, lo que resulta en un ahorro mínimo de esta política. Por ejemplo, una base de datos típica observada en ONTAP tiene una tasa de cambio inferior al 5% a la semana. Los archive logs de la base de datos pueden ocupar mucho espacio, pero normalmente continúan existiendo en el sistema de archivos activo y, por lo tanto, no serían candidatos para la organización en niveles bajo esta política.

Automático

La `auto` la política de organización en niveles amplía la clasificación por niveles tanto a bloques específicos de snapshots como a bloques del sistema de archivos activo. El retardo antes de que un bloque se considere frío es controlado por el `tiering-minimum-cooling-days` configuración para el volumen. El intervalo a partir de ONTAP 9,8 es de 2 a 183 días.

Este método permite opciones de organización en niveles que no están disponibles con el `snapshot-only` política. Por ejemplo, una política de protección de datos puede requerir 90 días de ciertos archivos de registro para ser retenidos. Si se establece un período de enfriamiento de 3 días, los archivos de registro anteriores a 3 días se almacenarán en niveles desde la capa de rendimiento. Esta acción libera espacio considerable en el nivel de rendimiento a la vez que le permite ver y gestionar los 90 días completos de datos.

Ninguno

La `none` la política de organización en niveles evita que cualquier bloque adicional se organice en niveles desde la capa de almacenamiento, pero todos los datos que permanezcan en el nivel de capacidad permanecen en el nivel de capacidad hasta que se leen. Si a continuación se lee el bloque, se retira y se coloca en el nivel de rendimiento.

El motivo principal para utilizar el `none` la política de organización en niveles es para evitar que los bloques se organicen en niveles, pero podría resultar útil cambiar las políticas con el tiempo. Por ejemplo, pongamos por caso que un conjunto de datos concreto se organiza ampliamente en niveles en la capa de capacidad, pero surge una necesidad inesperada de funcionalidades de rendimiento completas. La política se puede cambiar para evitar cualquier organización en niveles adicional y para confirmar que los bloques que se lean a medida que los aumentos de I/O permanecen en el nivel de rendimiento.

Todo

La `all` la política de organización en niveles reemplaza el `backup` Normativa a partir de ONTAP 9,6. La `backup` Política aplicada solo a los volúmenes de protección de datos, lo que significa un destino de SnapMirror o NetApp SnapVault. La `all` la política funciona de la misma manera, pero no se limita a los volúmenes de protección de datos.

Con esta política, los bloques se consideran inmediatamente inactivos y elegibles para organizarse en niveles en la capa de capacidad de inmediato.

Esta política resulta especialmente adecuada para backups a largo plazo. También se puede utilizar como una forma de gestión de almacenamiento jerárquico (HSM). Anteriormente, se utilizaba HSM para organizar en niveles los bloques de datos de un archivo en cinta y, al mismo tiempo, mantener el propio archivo visible en el sistema de archivos. Un volumen FabricPool con el `all` la política le permite almacenar archivos en un nivel visible y gestionable pero consume prácticamente ningún espacio en el nivel de almacenamiento local.

Políticas de recuperación

Las políticas de organización en niveles controlan qué bloques de la base de datos de Oracle se organizan en niveles desde el nivel de rendimiento al nivel de capacidad. Las políticas de recuperación controlan lo que sucede cuando se lee un bloque que se ha organizado en niveles.

Predeterminado

Inicialmente, todos los volúmenes FabricPool se establecen en `default`, que significa que el comportamiento está controlado por la `política de recuperación de nubes. `El comportamiento exacto depende de la política de organización en niveles utilizada.

- `auto`- solo recuperar datos de lectura aleatoria
- `snapshot-only`- recuperar todos los datos de lectura secuencial o aleatoria
- `none`- recuperar todos los datos de lectura secuencial o aleatoria
- `all`- no recuperar datos del nivel de capacidad

En lectura

Ajuste `cloud-retrieval-policy` en la lectura sobrescribe el comportamiento predeterminado, de modo que la lectura de cualquier dato por niveles provoca que esos datos se devuelvan al nivel de rendimiento.

Por ejemplo, es posible que un volumen se haya usado ligeramente durante mucho tiempo en `auto` la política de organización en niveles y la mayoría de los bloques están ahora organizados en niveles.

Si un cambio inesperado en las necesidades empresariales requirió que algunos de los datos se escanearan repetidamente para preparar un determinado informe, puede ser conveniente cambiar el `cloud-retrieval-`

`policy` para `on-read` para garantizar que todos los datos que se leen se devuelven al nivel de rendimiento, incluidos datos de lectura secuencial y aleatoria. Esto mejoraría el rendimiento de I/O secuenciales en el volumen.

Promocione

El comportamiento de la política de promoción depende de la política de organización en niveles. Si la política de organización en niveles es `auto`, y, a continuación, ajuste el `cloud-retrieval-policy `to `promote` devuelve todos los bloques del nivel de capacidad en el siguiente análisis de organización en niveles.

Si la política de organización en niveles es `snapshot-only`, entonces, los únicos bloques que se devuelven son los bloques asociados al sistema de archivos activo. Normalmente, esto no tendría ningún efecto porque los únicos bloques organizados en niveles en `snapshot-only` la política sería bloques asociados exclusivamente a las instantáneas. No habría bloques por niveles en el sistema de archivos activo.

Sin embargo, si un SnapRestore de volumen o una operación de clonado de archivos se restauraron los datos de un volumen desde una copia Snapshot, es posible que algunos de los bloques organizados en niveles debido a que solo estaban asociados a snapshots ahora sean requeridos por el sistema de archivos activo. Puede ser conveniente cambiar temporalmente el `cloud-retrieval-policy` política a. `promote` para recuperar rápidamente todos los bloques necesarios localmente.

Nunca

No recupere bloques del nivel de capacidad.

Estrategias de organización en niveles

Organización en niveles de archivos completa

Aunque la organización en niveles de FabricPool opera a nivel de bloques, en algunos casos se puede utilizar para la organización en niveles de archivos.

Muchas aplicaciones están organizadas por fecha, y por lo general es menos probable que se acceda a estos datos a medida que envejecen. Por ejemplo, un banco puede tener un repositorio de archivos PDF que contenga cinco años de extractos de clientes, pero sólo están activos los últimos meses. FabricPool se puede usar para reubicar archivos de datos más antiguos en el nivel de capacidad. Un período de enfriamiento de 14 días garantizaría que los 14 días más recientes de archivos PDF permanezcan en el nivel de rendimiento. Además, los archivos que se leen al menos cada 14 días permanecerán activos y, por consiguiente, permanecerán en el nivel de rendimiento.

Normativas

Para implementar un método de organización en niveles basado en archivos, debe tener archivos que se escriban y no se modifiquen posteriormente. La `tiering-minimum-cooling-days` la política debe establecerse lo suficientemente alta para que los archivos que pueda necesitar permanezcan en el nivel de rendimiento. Por ejemplo, un conjunto de datos para los que se requieren los 60 días de datos más recientes y un rendimiento óptimo garantiza configurar el `tiering-minimum-cooling-days` hasta 60. También se pueden obtener resultados similares en función de los patrones de acceso a archivos. Por ejemplo, si se requieren los últimos 90 días de datos y la aplicación accede a ese intervalo de 90 días, los datos permanecerán en el nivel de rendimiento. Mediante la configuración de `tiering-minimum-cooling-days` en el periodo 2, se obtiene una organización en niveles inmediata después de que los datos se vuelven menos activos.

La `auto` se requiere una política para impulsar la organización en niveles de estos bloques porque solo el `auto` la política afecta a los bloques que están en el sistema de archivos activo.

> Cualquier tipo de acceso a los datos restablece los datos del mapa de calor. La detección de virus, la indexación e incluso la actividad de backup que lee los archivos de origen evita la segmentación, ya que es necesario `tiering-minimum-cooling-days` nunca se ha alcanzado el umbral.

Organización parcial en niveles de archivos

Dado que FabricPool funciona a nivel de bloque, los archivos que están sujetos a cambios se pueden organizar parcialmente en niveles en el almacenamiento de objetos y, al mismo tiempo, permanecen parcialmente en el nivel de rendimiento.

Esto es común con las bases de datos. Las bases de datos que se sabe que contienen bloques inactivos también son candidatas para la organización en niveles de FabricPool. Por ejemplo, una base de datos de gestión de cadena de suministro puede contener información histórica que debe estar disponible si es necesario, pero que no se puede acceder durante las operaciones normales. FabricPool se puede utilizar para reubicar selectivamente los bloques inactivos.

Por ejemplo, los archivos de datos que se ejecutan en un volumen FabricPool con a. `tiering-minimum-cooling-days` periodo de 90 días: conserva los bloques a los que se ha accedido en los 90 días anteriores en el nivel de rendimiento. Sin embargo, todo lo que no se acceda durante 90 días se reubica al nivel de capacidad. En otros casos, la actividad normal de la aplicación conserva los bloques correctos en el nivel correcto. Por ejemplo, si una base de datos se utiliza normalmente para procesar los 60 días anteriores de datos de forma regular, es mucho menor `tiering-minimum-cooling-days` el período se puede establecer porque la actividad natural de la aplicación garantiza que los bloques no se reubiquen antes de tiempo.

> La `auto` la política debe utilizarse con cuidado con las bases de datos. Muchas bases de datos tienen actividades periódicas como el proceso de final del trimestre o las operaciones de reindexación. Si el período de estas operaciones es mayor que el `tiering-minimum-cooling-days` se pueden producir problemas de rendimiento. Por ejemplo, si el procesamiento a final de trimestre requiere 1TB TB de datos que de otro modo no se han modificado, esos datos podrían estar presentes ahora en el nivel de capacidad. Las lecturas del nivel de capacidad a menudo son extremadamente rápidas y pueden no causar problemas de rendimiento, pero los resultados exactos dependerán de la configuración del almacén de objetos.

Normativas

La `tiering-minimum-cooling-days` la política debe establecerse lo suficientemente alta para conservar los archivos que pueden ser necesarios en el nivel de rendimiento. Por ejemplo, una base de datos en la que los 60 días de datos más recientes podrían ser necesarios con un rendimiento óptimo justificaría establecer el `tiering-minimum-cooling-days` periodo hasta 60 días. También se podrían lograr resultados similares en función de los patrones de acceso de los archivos. Por ejemplo, si se requieren los 90 días de datos más recientes y la aplicación accede a ese intervalo de 90 días de datos, los datos permanecerán en el nivel de rendimiento. Ajuste de `tiering-minimum-cooling-days` un periodo de hasta 2 días clasificaría los datos en niveles inmediatamente después de que los datos se vuelvan menos activos.

La `auto` se requiere una política para impulsar la organización en niveles de estos bloques porque solo el `auto` la política afecta a los bloques que están en el sistema de archivos activo.

Cualquier tipo de acceso a los datos restablece los datos del mapa de calor. Por lo tanto, las exploraciones de tablas completas de la base de datos e incluso la actividad de copia de seguridad que lee los archivos de origen impiden la organización en niveles porque es necesario `tiering-minimum-cooling-days` nunca se ha alcanzado el umbral.

Organización en niveles de archive log

Quizás el uso más importante de FabricPool sea mejorar la eficiencia de los datos fríos conocidos, como los registros de transacciones de base de datos.

La mayoría de las bases de datos relacionales funcionan en modo de archivado de registros de transacciones para ofrecer una recuperación puntual. Los cambios en las bases de datos se confirman registrando los cambios en los registros de transacciones y el registro de transacciones se conserva sin sobrescribirse. El resultado, puede ser un requisito para conservar un enorme volumen de registros de transacciones archivados. Existen ejemplos similares con muchos otros flujos de trabajo de aplicaciones que generan datos que deben conservarse, pero es muy poco probable que se acceda jamás.

FabricPool resuelve estos problemas al ofrecer una única solución con organización en niveles integrada. Los archivos se almacenan y siguen siendo accesibles en su ubicación habitual, pero prácticamente no ocupan espacio en la matriz primaria.

Normativas

Utilice un `tiering-minimum-cooling-days` la política de unos días provoca una retención de bloques en los archivos creados recientemente (que son los archivos con mayor probabilidad de que sean necesarios a corto plazo) en el nivel de rendimiento. Los bloques de datos de los archivos antiguos se mueven al nivel de capacidad.

La `auto` aplica la clasificación por niveles de avisos cuando se alcanza el umbral de enfriamiento independientemente de si los registros se han suprimido o siguen existiendo en el sistema de archivos primario. También se simplifica la gestión, almacenar todos los registros potencialmente necesarios en una sola ubicación del sistema de archivos activo. No hay razón para buscar a través de instantáneas para localizar un archivo que necesita ser restaurado.

Algunas aplicaciones, como Microsoft SQL Server, truncan los archivos de registro de transacciones durante las operaciones de backup de modo que los registros ya no estén en el sistema de archivos activo. Se puede ahorrar capacidad mediante el uso del `snapshot-only` la política de organización en niveles, solo el `auto` la política no es útil para los datos de registro porque rara vez deben enfriarse los datos de registro en el sistema de archivos activo.

Organización en niveles de Snapshot

La versión inicial de FabricPool se dirigía al caso de uso de backup. El único tipo de bloques que se podía organizar en niveles eran bloques que ya no estaban asociados a los datos del sistema de archivos activo. Por lo tanto, solo se pueden mover los bloques de datos de Snapshot al nivel de capacidad. Esta sigue siendo una de las opciones de organización en niveles más seguras cuando hay que garantizar que el rendimiento nunca se vea afectado.

Políticas: Snapshots locales

Existen dos opciones para organizar en niveles los bloques Snapshot inactivos en el nivel de capacidad. En

primer lugar, el `snapshot-only` la política solo apunta a los bloques de instantáneas. Aunque la `auto` la política incluye el `snapshot-only` bloques, también organiza en niveles bloques del sistema de archivos activo. Esto podría no ser deseable.

La `tiering-minimum-cooling-days` el valor se debe establecer en un período de tiempo que permita que los datos que pueden necesitarse durante una restauración estén disponibles en el nivel de rendimiento. Por ejemplo, la mayoría de los escenarios de restauración de una base de datos de producción crucial incluyen un punto de restauración en algún momento en los pocos días anteriores. Ajuste A `tiering-minimum-cooling-days` el valor de 3 garantizaría que cualquier restauración del archivo da como resultado un archivo que proporciona un rendimiento máximo inmediatamente. Todos los bloques de los archivos activos se encuentran presentes en un almacenamiento rápido sin necesidad de recuperarlos del nivel de capacidad.

Políticas: Snapshots replicadas

Un snapshot que se replica con SnapMirror o SnapVault solo se usa para la recuperación deberá utilizar FabricPool `all` política. Con esta política, los metadatos se replican, pero todos los bloques de datos se envían inmediatamente al nivel de capacidad, lo que genera un rendimiento máximo. La mayoría de los procesos de recuperación implican una I/O secuencial, que es inherentemente eficiente. El tiempo de recuperación del almacén de objetos se debe evaluar, pero en una arquitectura bien diseñada, no es necesario que este proceso de recuperación sea significativamente más lento que la recuperación de datos locales.

Si también se van a usar los datos replicados para la clonación, el `auto` la política es más apropiada, con un `tiering-minimum-cooling-days` valor que abarca los datos que se espera que se utilicen regularmente en un entorno de clonación. Por ejemplo, el conjunto de trabajo activo de una base de datos puede incluir datos leídos o escritos en los tres días anteriores, pero también podría incluir otros 6 meses de datos históricos. Si es así, entonces el `auto` En el destino de SnapMirror, el conjunto de trabajo está disponible en el nivel de rendimiento.

Organización en niveles de backup

Las copias de seguridad de aplicaciones tradicionales incluyen productos como Oracle Recovery Manager, que crea copias de seguridad basadas en archivos fuera de la ubicación de la base de datos original.

```
 `tiering-minimum-cooling-days` policy of a few days preserves the most
recent backups, and therefore the backups most likely to be required for
an urgent recovery situation, on the performance tier. The data blocks of
the older files are then moved to the capacity tier.
La `auto` la política más adecuada para los datos de backup. Esto
garantiza la clasificación por niveles de avisos cuando se ha alcanzado el
umbral de enfriamiento independientemente de si los archivos se han
suprimido o siguen existiendo en el sistema de archivos primario. También
simplifica la gestión almacenar todos los archivos potencialmente
necesarios en una sola ubicación del sistema de archivos activo. No hay
razón para buscar a través de instantáneas para localizar un archivo que
necesita ser restaurado.
```

La `snapshot-only` la política podría funcionar, pero esa política solo se aplica a los bloques que ya no están en el sistema de archivos activo. Por lo tanto, los archivos en un recurso compartido NFS o SMB deben

eliminarse primero para poder organizar los datos en niveles.

Esta política sería aún menos eficiente con una configuración de LUN porque la eliminación de un archivo de una LUN solo elimina las referencias de archivos de los metadatos del sistema de archivos. Los bloques reales de las LUN permanecen en su lugar hasta que se sobrescriben. Esta situación puede crear un retraso prolongado entre el momento en que se elimina un archivo y el tiempo que se sobrescriben los bloques y se convierten en candidatos para la organización en niveles. El traslado de la `snapshot-only` Bloques en el nivel de capacidad pero, en general, la gestión de datos de backup de FabricPool funciona mejor con el `auto` política.

Este enfoque ayuda a los usuarios a gestionar el espacio necesario para los backups de una forma más eficiente, pero el propio FabricPool no es una tecnología de backup. La organización en niveles de los archivos de backup en el almacén de objetos simplifica la gestión, ya que los archivos siguen visibles en el sistema de almacenamiento original, pero los bloques de datos del destino del almacén de objetos dependen del sistema de almacenamiento original. Si se pierde el volumen de origen, los datos del almacén de objetos ya no se pueden usar.

Interrupciones de acceso al almacén de objetos

La organización en niveles de un conjunto de datos con FabricPool provoca una dependencia entre la cabina de almacenamiento principal y el nivel de almacén de objetos. Hay muchas opciones de almacenamiento de objetos que ofrecen distintos niveles de disponibilidad. Es importante comprender el impacto de una posible pérdida de conectividad entre la cabina de almacenamiento primaria y el nivel de almacenamiento de objetos.

Si una I/O emitida a ONTAP requiere datos del nivel de capacidad y ONTAP no puede alcanzar el nivel de capacidad para recuperar los bloques, se agotará el tiempo de espera de las I/O finalmente. El efecto de este tiempo de espera depende del protocolo utilizado. En un entorno NFS, ONTAP responde con una respuesta EJUKEBOX o EDELAY, dependiendo del protocolo. Algunos sistemas operativos anteriores pueden interpretarlo como un error, pero los sistemas operativos actuales y los niveles de parches actuales del cliente Oracle Direct NFS lo tratan como un error recuperable y siguen esperando a que se complete la E/S.

Un tiempo de espera menor se aplica a los entornos SAN. Si se requiere un bloque en el entorno de almacén de objetos y permanece inaccesible durante dos minutos, se devuelve un error de lectura al host. El volumen ONTAP y los LUN permanecen en línea, pero el SO del host puede marcar el sistema de archivos como está en estado de error.

Problemas de conectividad del almacenamiento de objetos `snapshot-only` la política es menos problemática, ya que únicamente los datos de backup están organizados en niveles. Los problemas de comunicación ralentizarían la recuperación de datos, pero de otro modo no afectarían a los datos que se están utilizando activamente. La `auto` y.. `all` Las políticas permiten la clasificación por niveles de los datos inactivos de la LUN activa, lo que significa que un error durante la recuperación de datos del almacén de objetos puede afectar a la disponibilidad de la base de datos. Una implementación de SAN con estas políticas solo debe utilizarse con almacenamiento de objetos de clase empresarial y conexiones de red diseñadas para obtener una alta disponibilidad. NetApp StorageGRID es la opción superior.

Protección de datos de Oracle

Protección de datos con ONTAP

NetApp sabe que los datos más críticos se encuentran en las bases de datos.

Una empresa no puede operar sin acceso a sus datos y, a veces, los datos definen el negocio. Estos datos deben protegerse; sin embargo, la protección de datos no solo garantiza un backup utilizable; se trata de realizar backups de forma rápida y fiable, además de almacenarlos de forma segura.

El otro lado de la protección de datos es la recuperación de datos. Cuando no se puede acceder a los datos, la empresa se ve afectada y puede dejar de funcionar hasta que se restauren los datos. Este proceso debe ser rápido y fiable. Por último, la mayoría de las bases de datos deben protegerse frente a desastres, lo que significa mantener una réplica de la base de datos. La réplica debe estar lo suficientemente actualizada. También debe ser rápido y sencillo hacer de la réplica una base de datos completamente operativa.

Esta documentación sustituye al informe técnico *TR-4591 publicado anteriormente: Protección de datos de Oracle: Backup, recuperación y replicación.*

Planificación

La arquitectura de protección de datos empresariales adecuada depende de los requisitos empresariales relacionados con la retención de datos, la capacidad de recuperación y la tolerancia a interrupciones durante diversos eventos.

Por ejemplo, piense en el número de aplicaciones, bases de datos y conjuntos de datos importantes. Crear una estrategia de backup para un único conjunto de datos que garantice el cumplimiento de los acuerdos de nivel de servicio típicos es bastante sencillo, ya que no hay muchos objetos que gestionar. A medida que aumenta el número de conjuntos de datos, la supervisión se hace más complicada y los administradores pueden verse forzados a invertir cada vez más tiempo en solucionar los fallos de backup. A medida que un entorno llega al cloud y escala el proveedor de servicios, se necesita un enfoque totalmente diferente.

El tamaño del conjunto de datos también afecta a la estrategia. Por ejemplo, existen muchas opciones para backup y recuperación con una base de datos 100GB porque el conjunto de datos es tan pequeño. La simple copia de los datos de los medios de backup con herramientas tradicionales suele proporcionar un objetivo de tiempo de recuperación suficiente para la recuperación. Una base de datos de 100TB suele necesitar una estrategia completamente diferente a menos que el objetivo de tiempo de recuperación permita una interrupción de varios días, en cuyo caso puede ser aceptable un procedimiento tradicional de backup y recuperación basado en copia.

Por último, existen factores fuera del propio proceso de backup y recuperación. Por ejemplo, ¿existen bases de datos que respalden actividades de producción críticas, lo que convierte la recuperación en un evento raro que solo realizan los administradores de bases de datos cualificados? Alternativamente, ¿las bases de datos forman parte de un entorno de desarrollo de gran tamaño en el que la recuperación es una ocurrencia frecuente y gestionada por un EQUIPO de TECNOLOGÍA generalista?

Planificación de objetivos de tiempo, objetivos de punto de recuperación y acuerdos de nivel de servicio

ONTAP le permite adaptar con facilidad una estrategia de protección de datos de base de datos de Oracle a sus requisitos empresariales.

Entre estos requisitos se incluyen factores como la velocidad de recuperación, la pérdida de datos máxima permitida y las necesidades de retención de backup. El plan de protección de datos también debe tener en cuenta varios requisitos normativos para la retención y restauración de datos. Por último, deben tenerse en

cuenta diferentes escenarios de recuperación de datos, que van desde la recuperación típica y previsible que se produce por errores de usuarios o aplicaciones hasta escenarios de recuperación de desastres que incluyen la pérdida completa de un sitio.

Los cambios pequeños en las políticas de protección y recuperación de datos pueden tener un efecto significativo en la arquitectura general de almacenamiento, respaldo y recuperación. Es crucial definir y documentar los estándares antes de comenzar a trabajar de diseño, para evitar complicar la arquitectura de protección de datos. Las funciones o niveles de protección innecesarios generan costes innecesarios y gastos generales de gestión, y un requisito que al principio se pasa por alto puede dirigir un proyecto en la dirección equivocada o requerir cambios de diseño de última hora.

Objetivo de tiempo de recuperación

El objetivo de tiempo de recuperación (RTO) define el tiempo máximo permitido para la recuperación de un servicio. Por ejemplo, una base de datos de recursos humanos podría tener un objetivo de tiempo de recuperación de 24 horas porque, si bien sería un inconveniente perder el acceso a estos datos durante la jornada laboral, la empresa aún puede seguir funcionando. Por el contrario, una base de datos que respalde el libro mayor general de un banco tendría un RTO medido en minutos o incluso segundos. Un RTO de cero no es posible, porque debe haber una manera de diferenciar entre una interrupción real del servicio y un evento rutinario, como un paquete de red perdido. Sin embargo, un objetivo de tiempo de recuperación de casi cero es un requisito típico.

Objetivo de punto de recuperación

El objetivo de punto de recuperación (RPO) define la pérdida de datos máxima tolerable. En muchos casos, el objetivo de punto de recuperación solo viene determinado por la frecuencia de las copias Snapshot o las actualizaciones de snapmirror.

En algunos casos, el objetivo de punto de recuperación puede hacerse más agresivo ya que protege de forma selectiva ciertos datos con mayor frecuencia. En un contexto de base de datos, el RPO suele ser una cuestión de cuántos datos de registro se pueden perder en una situación específica. En un escenario típico de recuperación en el que una base de datos está dañada debido a un error de producto o de usuario, el RPO debe ser cero, lo que significa que no debe haber pérdida de datos. El procedimiento de recuperación implica restaurar una copia anterior de los archivos de base de datos y, a continuación, volver a reproducir los archivos de registro para que el estado de la base de datos alcance el momento deseado. Los archivos de registro necesarios para esta operación ya deben estar en su lugar en la ubicación original.

En escenarios inusuales, los datos de registro pueden perderse. Por ejemplo, un ataque accidental o malintencionado `rm -rf *` de archivos de base de datos podría resultar en la eliminación de todos los datos. La única opción sería restaurar desde la copia de seguridad, incluidos los archivos de registro, y algunos datos inevitablemente se perderían. La única opción para mejorar el RPO en un entorno de backup tradicional sería realizar backups repetidos de los datos de registro. Sin embargo, esto tiene limitaciones debido al movimiento constante de datos y la dificultad de mantener un sistema de backup como un servicio en constante ejecución. Una de las ventajas de los sistemas de almacenamiento avanzados es la capacidad de proteger los datos frente a daños accidentales o malintencionados en los archivos para proporcionar, de este modo, un mejor objetivo de punto de recuperación sin transferir datos.

Recuperación tras siniestros

La recuperación tras desastres incluye la arquitectura de TI, las políticas y los procedimientos necesarios para recuperar un servicio en caso de desastre físico. Esto puede incluir inundaciones, incendios o personas que actúen con intención maliciosa o negligente.

La recuperación ante desastres va más allá de un conjunto de procedimientos de recuperación. Se trata del proceso completo de identificar los diversos riesgos, de definir los requisitos de recuperación de datos y

continuidad del servicio, y de proporcionar la arquitectura correcta con los procedimientos asociados.

Cuando se establecen requisitos de protección de datos, es fundamental diferenciar entre los requisitos típicos de RPO y RTO, así como los requisitos de RPO y RTO necesarios para la recuperación ante desastres. Algunos entornos de aplicaciones requieren un objetivo de punto de recuperación de cero y un objetivo de tiempo de recuperación de casi cero para situaciones de pérdida de datos, que van desde un error relativamente normal del usuario hasta un incendio que destruya un centro de datos. Sin embargo, estos altos niveles de protección tienen consecuencias administrativas y de costes.

En general, los requisitos de recuperación de datos sin desastre deben ser estrictos por dos motivos. En primer lugar, los errores en las aplicaciones y los errores de los usuarios que dañan los datos son previsibles hasta el punto de que son casi inevitables. En segundo lugar, no es difícil diseñar una estrategia de backup que proporcione un RPO de cero y un RTO bajo, siempre que el sistema de almacenamiento no esté destruido. No hay motivo para no abordar un riesgo significativo que sea fácil de solucionar, por lo que los objetivos de RPO y RTO para la recuperación local deben ser agresivos.

Los requisitos del objetivo de tiempo de recuperación ante desastres y del objetivo de punto de recuperación varían mucho más según la probabilidad de que se produzca un desastre y las consecuencias de la pérdida de datos o las interrupciones de un negocio. Los requisitos del objetivo de punto de recuperación y del objetivo de tiempo de recuperación deben basarse en las necesidades reales de la empresa, no en los principios generales. Deben explicar múltiples escenarios de desastre lógicos y físicos.

Desastres lógicos

Entre los desastres lógicos se encuentra la corrupción de datos causada por los usuarios, errores de la aplicación o del SO y mal funcionamiento del software. Los desastres lógicos también pueden incluir ataques maliciosos de terceros con virus o gusanos, o mediante la explotación de las vulnerabilidades de las aplicaciones. En estos casos, la infraestructura física permanece intacta, pero los datos subyacentes ya no son válidos.

Un tipo cada vez más común de desastre lógico se conoce como ransomware, en el que se utiliza un vector de ataque para cifrar los datos. El cifrado no daña los datos, pero no los hace disponibles hasta que se realiza el pago a un tercero. Un número cada vez mayor de empresas se dirigen específicamente a ataques de ransomware. Para esta amenaza, NetApp ofrece copias Snapshot a prueba de manipulaciones donde ni siquiera el administrador de almacenamiento puede cambiar los datos protegidos antes de la fecha de caducidad configurada.

Desastres físicos

Los desastres físicos incluyen la falla de los componentes de una infraestructura que supera sus capacidades de redundancia y dan lugar a una pérdida de datos o una prolongada pérdida de servicio. Por ejemplo, la protección RAID proporciona redundancia de unidades de disco y el uso de HBA proporciona redundancia de puertos FC y cables FC. Los errores de hardware de dichos componentes son previsibles y no afectan a la disponibilidad.

En un entorno empresarial, generalmente es posible proteger la infraestructura de todo un sitio con componentes redundantes hasta el punto en que el único escenario de desastre físico previsible es la pérdida completa del sitio. En ese caso, el plan de la recuperación ante desastres depende de la replicación entre sitios.

Protección de datos síncrona y asíncrona

En un mundo ideal, todos los datos se replicarían de forma sincrónica en sitios dispersos geográficamente. Dicha replicación no siempre es factible o incluso posible por varias razones:

- La replicación síncrona aumenta inevitablemente la latencia de escritura porque todos los cambios deben replicarse en ambas ubicaciones antes de que la aplicación o base de datos pueda continuar con el procesamiento. El efecto sobre el rendimiento resultante es a veces inaceptable, lo que descarta el uso del mirroring síncrono.
- Al aumentar la adopción del almacenamiento SSD del 100 %, es más probable que se note latencia de escritura adicional, ya que las expectativas de rendimiento incluyen cientos de miles de IOPS y latencia inferior al milisegundo. Para obtener todas las ventajas del uso del 100 % de las unidades SSD es necesario volver a analizar la estrategia de recuperación ante desastres.
- Los conjuntos de datos siguen creciendo en términos de bytes, generando retos que exigen un ancho de banda suficiente para sostener la replicación síncrona.
- Los conjuntos de datos también crecen en términos de complejidad, lo que genera retos con la gestión de la replicación síncrona a gran escala.
- Las estrategias basadas en cloud a menudo implican mayores distancias de replicación y latencia, lo que excluye aún más el uso del mirroring síncrono.

NetApp ofrece soluciones que incluyen replicación sincrónica para las exigencias de recuperación de datos más exigentes y soluciones asincrónicas que permiten un mejor rendimiento y flexibilidad. Además, la tecnología de NetApp se integra sin problemas con muchas soluciones de replicación de terceros, como Oracle DataGuard

Tiempo de retención

El aspecto final de una estrategia de protección de datos es el tiempo de retención, que puede variar drásticamente.

- Normalmente, se requieren 14 días de backups nocturnos en el sitio principal y 90 días de backups almacenados en un sitio secundario.
- Muchos clientes crean archivos trimestrales independientes almacenados en diferentes medios.
- Es posible que una base de datos constantemente actualizada no necesite datos históricos y que las copias de seguridad solo se conserven durante unos pocos días.
- Los requisitos normativos pueden requerir la capacidad de recuperación hasta el punto de cualquier transacción arbitraria en un periodo de 365 días.

Disponibilidad de bases de datos

ONTAP se ha diseñado para ofrecer la máxima disponibilidad de las bases de datos de Oracle. Este documento no incluye una descripción completa de las funciones de alta disponibilidad de ONTAP. Sin embargo, al igual que sucede con la protección de datos, un conocimiento básico de esta funcionalidad es importante cuando se diseña una infraestructura de base de datos.

Parejas de HA

La unidad básica de alta disponibilidad es el par de alta disponibilidad. Cada pareja contiene enlaces redundantes para admitir la replicación de datos hacia NVRAM. NVRAM no es una caché de escritura. La RAM dentro de la controladora funciona como caché de escritura. El objetivo de la NVRAM es registrar temporalmente los datos como protección frente a un fallo inesperado del sistema. En este sentido, es similar a un redo log de base de datos.

Tanto la NVRAM como un redo log de base de datos se utilizan para almacenar datos rápidamente, lo que

permite que los cambios en los datos se confirmen lo más rápidamente posible. La actualización de los datos persistentes en las unidades (o archivos de datos) no se realiza hasta más adelante durante un proceso denominado punto de control en las plataformas ONTAP y en la mayoría de las bases de datos. Ni los datos de NVRAM ni los registros de recuperación de bases de datos se leen durante las operaciones normales.

Si una controladora falla abruptamente, es posible que existan cambios pendientes almacenados en la NVRAM que aún no se hayan escrito en las unidades. La controladora asociada detecta el fallo, toma el control de las unidades y aplica los cambios requeridos que se han almacenado en NVRAM.

Toma de control y retorno al nodo primario

La toma de control y la devolución hace referencia al proceso de transferencia de la responsabilidad de los recursos de almacenamiento entre los nodos de un par de alta disponibilidad. La toma de control y el retorno al nodo primario tienen dos aspectos:

- Gestión de la conectividad de red que permite el acceso a las unidades
- Gestión de las unidades en sí

Las interfaces de red que admiten el tráfico CIFS y NFS están configuradas tanto con un directorio raíz como con una ubicación de recuperación tras fallos. Una toma de control incluye mover las interfaces de red a su directorio raíz temporal en una interfaz física ubicada en las mismas subredes que la ubicación original. Un retorno primario incluye mover las interfaces de red de vuelta a sus ubicaciones originales. El comportamiento exacto se puede ajustar según sea necesario.

Las interfaces de red que admiten protocolos de bloques SAN como iSCSI y FC no se reubican durante la toma de control y el retorno al nodo primario. En su lugar, los LUN se deben aprovisionar con rutas que incluyan un par de HA completo, lo que da como resultado una ruta primaria y una secundaria.

> También se pueden configurar rutas adicionales a controladoras adicionales para admitir la reubicación de datos entre nodos de un clúster más grande, pero esto no forma parte del proceso de alta disponibilidad.

El segundo aspecto de la toma de control y la restauración es la transferencia de la propiedad del disco. El proceso exacto depende de múltiples factores, incluyendo la razón de la toma de control/devolución y las opciones de la línea de comandos emitidas. El objetivo es realizar la operación de la manera más eficiente posible. Aunque parezca que el proceso general requiera varios minutos, el momento en el que la propiedad de la unidad se realiza la transición de nodo a nodo generalmente se puede medir en segundos.

Tiempo de toma de control

El host de I/O experimenta una breve pausa en I/O durante operaciones de toma de control y devolución; pero no debe producirse una interrupción en las aplicaciones en un entorno configurado correctamente. El proceso de transición real en el que se demora I/O suele medirse en segundos, pero el host puede requerir más tiempo para reconocer el cambio en las rutas de datos y volver a enviar las operaciones de I/O.

La naturaleza de la interrupción depende del protocolo:

- Una interfaz de red que admite problemas de tráfico NFS y CIFS una solicitud de Protocolo de resolución de direcciones (ARP) a la red después de la transición hacia una nueva ubicación física. Esto hace que los conmutadores de red actualicen sus tablas de direcciones de control de acceso a medios (MAC) y reanuden el procesamiento de E/S. Las interrupciones en el caso de toma de control y devolución planificadas suelen medirse en segundos y, en muchos casos, no se pueden detectar. Puede que algunas redes sean más lentas para reconocer completamente el cambio en la ruta de red y algunos sistemas operativos pueden poner en cola muchas E/S en muy poco tiempo que deben reintentarse. Esto puede

ampliar el tiempo necesario para reanudar la actividad de I/O.

- Una interfaz de red que admite protocolos SAN no realiza la transición a una nueva ubicación. Un SO host debe cambiar la ruta o las rutas en uso. La pausa en I/O observada por el host depende de varios factores. Desde el punto de vista de un sistema de almacenamiento, el período en el que no se puede ofrecer I/O es solo unos segundos. Sin embargo, los sistemas operativos de host diferentes pueden requerir más tiempo para permitir que se agote el tiempo de espera de una E/S antes de volver a intentarlo. Los sistemas operativos más nuevos son más capaces de reconocer un cambio de ruta mucho más rápido, pero los sistemas operativos más antiguos normalmente requieren hasta 30 segundos para reconocer un cambio.

En la siguiente tabla, se muestran los tiempos de toma de control esperados durante el que el sistema de almacenamiento no puede ofrecer datos a un entorno de aplicación. No debe haber ningún error en ningún entorno de aplicación, la toma de control debería aparecer como una breve pausa en el procesamiento de E/S.

	NFS	AFF	ASA
Toma de control planificada	15 seg	6-10 seg	2-3 seg
Respaldo no planificado	30 seg	6-10 seg	2-3 seg

Sumas de comprobación e integridad de los datos

ONTAP y sus protocolos admitidos incluyen varias funciones que protegen la integridad de las bases de datos de Oracle, incluidos los datos en reposo y la transmisión de datos a través de la red.

La protección de datos lógicos en ONTAP consta de tres requisitos clave:

- Los datos deben protegerse contra la corrupción de datos.
- Los datos deben protegerse contra un fallo de unidad.
- Los cambios en los datos deben protegerse contra la pérdida.

Estas tres necesidades se tratan en las siguientes secciones.

Corrupción de la red: Sumas de comprobación

El nivel más básico de protección de datos es la suma de comprobación, que es un código especial de detección de errores almacenado junto con los datos. La corrupción de datos durante la transmisión de red se detecta con el uso de una suma de comprobación y, en algunos casos, varias sumas de comprobación.

Por ejemplo, una trama de FC incluye una forma de suma de comprobación denominada comprobación de redundancia cíclica (CRC) para asegurarse de que la carga útil no está dañada en tránsito. El transmisor envía tanto los datos como el CRC de los datos. El receptor de una trama FC vuelve a calcular el CRC de los datos recibidos para asegurarse de que coincida con el CRC transmitido. Si el CRC recién calculado no coincide con el CRC conectado a la trama, los datos están dañados y se descarta o rechaza la trama de FC. Las operaciones de I/O iSCSI incluyen sumas de comprobación en las capas TCP/IP y Ethernet y, para una protección adicional, también se puede incluir protección CRC opcional en la capa SCSI. Cualquier daño de bit en el cable se detecta mediante la capa TCP o la capa IP, lo que provoca la retransmisión del paquete. Al igual que con FC, los errores en el CRC de SCSI provocan un descarte o el rechazo de la operación.

Daños en unidades: Sumas de comprobación

También se utilizan sumas de comprobación para verificar la integridad de los datos almacenados en las unidades. Los bloques de datos escritos en las unidades se almacenan con una función de suma de comprobación que genera un número impredecible ligado a los datos originales. Cuando se leen datos de la unidad, la suma de comprobación se vuelve a calcular y se compara con la suma de comprobación almacenada. Si no coincide, los datos se han dañado y deben ser recuperados por la capa RAID.

Datos dañados: Escrituras perdidas

Uno de los tipos de daños más difíciles de detectar es una escritura perdida o ubicada incorrectamente. Cuando se reconoce una escritura, se debe escribir en el soporte en la ubicación correcta. Los datos dañados in situ son relativamente fáciles de detectar usando una sencilla suma de comprobación almacenada con los datos. Sin embargo, si la escritura simplemente se pierde, es posible que aún exista la versión anterior de los datos y la suma de comprobación sea correcta. Si la escritura se realiza en una ubicación física incorrecta, la suma de comprobación asociada sería una vez más válida para los datos almacenados, aunque la escritura haya destruido otros datos.

La solución a este reto es la siguiente:

- Una operación de escritura debe incluir metadatos que indiquen la ubicación donde se espera que se encuentre la escritura.
- Una operación de escritura debe incluir algún tipo de identificador de versión.

Cuando ONTAP escribe un bloque, incluye los datos donde pertenece el bloque. Si una lectura posterior identifica un bloque, pero los metadatos indican que pertenece a la ubicación 123 cuando se encontró en la ubicación 456, la escritura se ha colocado de forma incorrecta.

Detectar una escritura totalmente perdida es más difícil. La explicación es muy complicada, pero básicamente ONTAP almacena los metadatos de manera que una operación de escritura da como resultado actualizaciones en dos ubicaciones distintas en las unidades. Si se pierde una escritura, una lectura posterior de los datos y los metadatos asociados muestra dos identidades de versión diferentes. Esto indica que la unidad no completó la escritura.

Los daños en la escritura perdidos o mal ubicados son extremadamente raros, pero, a medida que las unidades siguen creciendo y los conjuntos de datos pasan a la escala de exabytes, el riesgo aumenta. La detección de escritura perdida debe incluirse en cualquier sistema de almacenamiento que admita cargas de trabajo de base de datos.

Fallos de unidad: RAID, RAID DP y RAID-TEC

Si se detecta que un bloque de datos en una unidad está dañado, o que toda la unidad falla y no está totalmente disponible, los datos deben reconstituirse. Esto se realiza en ONTAP utilizando unidades de paridad. Los datos se dividen entre varias unidades de datos y, a continuación, se generan datos de paridad. Se almacena por separado de los datos originales.

ONTAP utilizó originalmente RAID 4, que utiliza una sola unidad de paridad para cada grupo de unidades de datos. El resultado fue que cualquier unidad del grupo podría fallar sin producir una pérdida de datos. Si se produjo un error en la unidad de paridad, no se dañaron los datos y se pudo construir una nueva unidad de paridad. Si falla una unidad de datos única, las unidades restantes podrían usarse con la unidad de paridad para volver a generar los datos ausentes.

Cuando las unidades eran pequeñas, la posibilidad estadística de que fallaran en dos unidades a la vez era insignificante. A medida que aumenta la capacidad de las unidades, también aumenta el tiempo necesario para reconstruir los datos tras un fallo de unidad. Esto ha aumentado el intervalo en el que un segundo fallo

de unidad provocaría la pérdida de datos. Además, el proceso de recompilación crea una gran cantidad de I/O adicionales en las unidades supervivientes. A medida que las unidades envejecen, también aumenta el riesgo de la carga adicional que produce un segundo fallo de unidad. Por último, incluso si el riesgo de pérdida de datos no aumentara con el uso continuado de RAID 4, las consecuencias de la pérdida de datos serían más graves. Cuantos más datos se pierdan en caso de un fallo de un grupo RAID, más tiempo se necesitaría para recuperar los datos, lo que prolonga la interrupción del negocio.

Estos problemas llevaron a NetApp a desarrollar la tecnología NetApp RAID DP, una variante de RAID 6. Esta solución incluye dos unidades de paridad, lo que significa que dos unidades cualesquiera de un grupo RAID pueden fallar sin crear pérdida de datos. El tamaño de las unidades ha continuado creciendo, lo que finalmente llevó a NetApp a desarrollar la tecnología NetApp RAID-TEC, que introduce una tercera unidad de paridad.

Algunas mejores prácticas históricas de bases de datos recomiendan el uso de RAID-10, también conocido como mirroring segmentado. Esto ofrece menos protección de datos que RAID DP, ya que existen varias situaciones de fallo de dos discos, mientras que en RAID DP no hay ninguna.

También hay algunas mejores prácticas históricas de bases de datos que indican que se prefiere RAID-10 a las opciones de RAID-4/5/6 debido a cuestiones de rendimiento. En ocasiones, estas recomendaciones se refieren a una penalización de RAID. Aunque estas recomendaciones son generalmente correctas, no son aplicables a las implementaciones de RAID en ONTAP. El problema de rendimiento está relacionado con la regeneración de paridad. Con las implementaciones de RAID tradicionales, procesar las escrituras aleatorias rutinarias realizadas por una base de datos requiere varias lecturas de disco para regenerar los datos de paridad y completar la escritura. La penalización se define como las IOPS de lectura adicional necesarias para ejecutar operaciones de escritura.

ONTAP no incurre en una penalización de RAID, ya que las escrituras se almacenan en memoria donde se genera la paridad y se escriben en el disco como una única franja de RAID. No se requieren lecturas para completar la operación de escritura.

En resumen, en comparación con RAID 10, RAID DP y RAID-TEC ofrecen mucha más capacidad utilizable, una mejor protección ante fallos de unidad y sin sacrificios de rendimiento.

Protección contra fallos del hardware: NVRAM

Cualquier cabina de almacenamiento que sirva a una carga de trabajo de base de datos debe procesar operaciones de escritura lo más rápido posible. Además, una operación de escritura debe protegerse contra pérdidas provocadas por eventos inesperados, como un fallo de alimentación. Esto significa que cualquier operación de escritura debe almacenarse de forma segura en al menos dos ubicaciones.

Los sistemas AFF y FAS confían en NVRAM para cumplir estos requisitos. El proceso de escritura funciona de la siguiente manera:

1. Los datos de escritura entrantes se almacenan en la RAM.
2. Los cambios que se deben realizar en los datos del disco se registran en NVRAM en el nodo local y el asociado. NVRAM no es una caché de escritura, sino un diario similar a un redo log de base de datos. En condiciones normales, no se lee. Solo se utiliza para recuperación, como después de un fallo de alimentación durante el procesamiento de I/O.
3. A continuación, la escritura se reconoce en el host.

El proceso de escritura en esta fase se completa desde el punto de vista de la aplicación y los datos están protegidos contra pérdidas debido a que están almacenados en dos ubicaciones diferentes. Eventualmente, los cambios se escriben en el disco, pero este proceso es fuera de banda desde el punto de vista de la aplicación, porque se produce una vez que se reconoce la escritura y, por lo tanto, no afecta a la latencia. Este

proceso es una vez más similar al registro de la base de datos. Un cambio en la base de datos se registra en los redo logs lo antes posible y el cambio se confirma como confirmado. Las actualizaciones de los archivos de datos se producen mucho más tarde y no afectan directamente a la velocidad de procesamiento.

En caso de que se produzca un fallo en la controladora, la controladora asociada toma la propiedad de los discos necesarios y reproduce los datos registrados en la NVRAM para recuperar las operaciones de I/O que estuvieran en curso al producirse el fallo.

Protección contra fallos de hardware: NVFAIL

Como hemos visto anteriormente, la escritura no se reconoce hasta que se haya iniciado sesión en la NVRAM local y NVRAM en al menos otra controladora. Este método garantiza que un fallo de hardware o una interrupción del suministro eléctrico no provoquen la pérdida de operaciones de I/O en tránsito Si la NVRAM local falla o la conectividad con el partner de alta disponibilidad falla, estos datos en curso ya no se duplicarán.

Si la NVRAM local informa de un error, el nodo se apaga. Este apagado hace que se produzca una conmutación al nodo de respaldo con una controladora asociada de alta disponibilidad. No se pierden datos porque la controladora que experimenta el fallo no reconoció la operación de escritura.

ONTAP no permite una conmutación por error cuando los datos no están sincronizados a menos que se vean obligados a recurrir a la conmutación por error. Al forzar un cambio en las condiciones de esta manera, se reconoce que los datos podrían dejarse atrás en la controladora original y que la pérdida de datos es aceptable.

Las bases de datos son especialmente vulnerables a los daños si se fuerza una conmutación por error porque las bases de datos mantienen grandes cachés internos de datos en el disco. Si se produce una conmutación por error forzada, los cambios previamente aceptados se descartan efectivamente. El contenido de la cabina de almacenamiento retrocede efectivamente en el tiempo y el estado de la caché de base de datos ya no refleja el estado de los datos del disco.

Para proteger datos contra esta situación, ONTAP permite configurar volúmenes para una protección especial contra un fallo NVRAM. Cuando se activa, este mecanismo de protección hace que un volumen entre en un estado denominado NVFAIL. Este estado provoca errores de I/O que provocan el cierre de una aplicación para que no utilicen datos obsoletos. No se deben perder los datos porque debe haber alguna escritura reconocida en la cabina de almacenamiento.

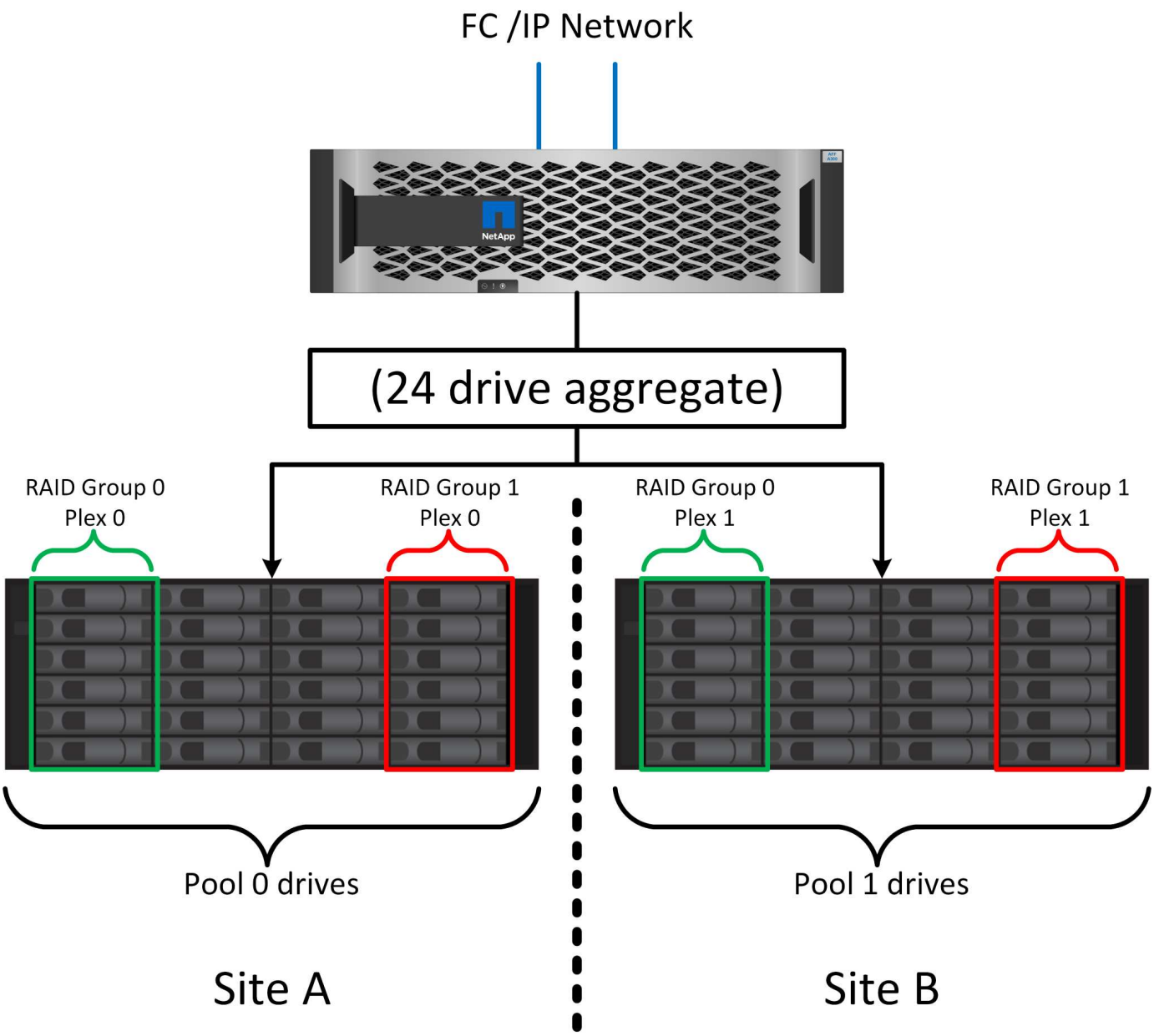
Los siguientes pasos habituales son para que un administrador apague completamente los hosts antes de volver a poner manualmente los LUN y los volúmenes de nuevo en línea. Aunque estos pasos pueden implicar cierto trabajo, este enfoque es la manera más segura de garantizar la integridad de los datos. No todos los datos requieren esta protección, por lo que el comportamiento NVFAIL se puede configurar volumen por volumen.

Protección frente a fallos de sitios y bandejas: SyncMirror y complejos

SyncMirror es una tecnología de mirroring que mejora, pero no sustituye, RAID DP ni RAID-TEC. Refleja el contenido de dos grupos RAID independientes. La configuración lógica es la siguiente:

- Las unidades se configuran en dos pools según la ubicación. Un pool se compone de todas las unidades en el sitio A, y el segundo pool se compone de todas las unidades en el sitio B.
- A continuación, se crea un pool de almacenamiento común, conocido como agregado, basado en conjuntos reflejados de grupos RAID. Se extrae un número igual de unidades en cada sitio. Por ejemplo, un agregado SyncMirror de 20 unidades estaría compuesto por 10 unidades del sitio A y 10 unidades del sitio B.
- Cada conjunto de unidades en un sitio determinado se configura automáticamente como uno o varios

grupos RAID-DP o RAID-TEC completamente redundantes, independientemente del uso del mirroring. Esto proporciona una protección de datos continua, incluso después de la pérdida de un sitio.



La figura anterior muestra una configuración de SyncMirror de ejemplo. Se creó un agregado de 24 unidades en la controladora con 12 unidades de una bandeja asignada en el sitio A y 12 unidades de una bandeja asignada en el sitio B. Las unidades se agruparon en dos grupos RAID reflejados. RAID Group 0 incluye un plex de 6 unidades en el sitio A duplicado en un plex de 6 unidades en el sitio B. Del mismo modo, RAID Group 1 incluye un plex de 6 unidades en el sitio A duplicado en un plex de 6 unidades en el sitio B.

Normalmente, SyncMirror se utiliza para proporcionar mirroring remoto con sistemas MetroCluster, con una copia de los datos de cada sitio. En ocasiones, se ha utilizado para proporcionar un nivel adicional de redundancia en un único sistema. En particular, proporciona redundancia a nivel de bandeja. Una bandeja de unidades ya contiene fuentes de alimentación y controladoras duales y en general es poco más que chapa metálica, pero en algunos casos, la protección adicional puede estar garantizada. Por ejemplo, un cliente de NetApp ha puesto en marcha SyncMirror para una plataforma móvil de análisis en tiempo real que se usa durante las pruebas de automoción. El sistema se separó en dos racks físicos alimentados por fuentes de alimentación independientes de sistemas UPS independientes.

Sumas de comprobación

El tema de las sumas de comprobación es de particular interés para los administradores de bases de datos que están acostumbrados a usar backups en streaming de Oracle RMAN, que migran a backups basados en instantáneas. Una función de RMAN es que realiza comprobaciones de integridad durante las operaciones de copia de seguridad. Aunque esta función posee cierto valor, su principal ventaja es en una base de datos que no se utiliza en una cabina de almacenamiento moderna. Cuando se utilizan unidades físicas en una base de datos de Oracle, resulta casi seguro que los daños eventualmente se producen cuando las unidades envejecen, un problema que resuelven las sumas de comprobación basadas en cabinas de almacenamiento reales.

Con una cabina de almacenamiento real, la integridad de los datos se protege utilizando sumas de comprobación en varios niveles. Si los datos están dañados en una red basada en IP, la capa Protocolo de control de transmisión (TCP) rechaza los datos del paquete y solicita la retransmisión. El protocolo FC incluye sumas de comprobación, al igual que los datos SCSI encapsulados. Después de que se encuentra en la cabina, ONTAP tiene protección RAID y suma de comprobación. La corrupción puede ocurrir, pero, como en la mayoría de las matrices empresariales, se detecta y corrige. Normalmente, falla una unidad completa, solicita una reconstrucción de RAID y la integridad de la base de datos no se ve afectada. Todavía es posible que los bytes individuales en una unidad sean dañados por la radiación cósmica o las células flash que fallan. Si esto sucede, se producirá un error en la comprobación de paridad, se producirá un error en la unidad y se iniciará la recompilación de RAID. Una vez más, la integridad de los datos no se ve afectada. La última línea de defensa es el uso de sumas de control. Si, por ejemplo, un error catastrófico de firmware en una unidad daña datos que de algún modo no se detectó mediante una comprobación de paridad de RAID, la suma de comprobación no coincidiría y ONTAP evitaría la transferencia de un bloque dañado antes de que la base de datos de Oracle pudiera recibirlo.

La arquitectura de archivo de datos y redo log de Oracle también está diseñada para ofrecer el nivel más alto posible de integridad de datos, incluso en circunstancias extremas. En el nivel más básico, los bloques de Oracle incluyen suma de comprobación y comprobaciones lógicas básicas con casi todas las E/S. Si Oracle no se ha bloqueado o ha puesto un tablespace fuera de línea, los datos estarán intactos. El grado de comprobación de la integridad de los datos es ajustable y Oracle también puede configurarse para confirmar las escrituras. Como resultado, casi todos los escenarios de accidente y fallo se pueden recuperar, y en el caso extremadamente raro de una situación irrecuperable, la corrupción se detecta rápidamente.

La mayoría de los clientes de NetApp que utilizan bases de datos Oracle interrumpen el uso de RMAN y otros productos de backup después de la migración a backups basados en snapshots. Todavía hay opciones en las que se puede utilizar RMAN para realizar la recuperación a nivel de bloque con SnapCenter. Sin embargo, en el día a día, RMAN, NetBackup y otros productos sólo se utilizan ocasionalmente para crear copias de archivado mensuales o trimestrales.

Algunos clientes eligen correr `dbv` periódicamente para realizar comprobaciones de integridad de sus bases de datos existentes. NetApp desaconseja esta práctica porque crea una carga de I/O innecesaria. Como se mencionó anteriormente, si la base de datos no estaba experimentando problemas anteriormente, la posibilidad de `dbv` La detección de un problema es cercana a cero, y esta utilidad crea una carga secuencial de I/O muy elevada en la red y el sistema de almacenamiento. A menos que exista un motivo para creer que existe corrupción, como la exposición a un bug de Oracle conocido, no hay motivo para ejecutarse `dbv`.

Conceptos básicos de backup y recuperación

Backups basados en Snapshot

La base de la protección de datos de bases de datos de Oracle en ONTAP es la tecnología Snapshot de NetApp.

Los valores clave son los siguientes:

- **Simplicidad.** Una instantánea es una copia de solo lectura del contenido de un contenedor de datos en un momento específico.
- **Eficiencia.** Las instantáneas no requieren espacio en el momento de la creación. El espacio solo se consume cuando se modifican los datos.
- **Capacidad de gestión.** Una estrategia de copia de seguridad basada en instantáneas es fácil de configurar y administrar porque las instantáneas son una parte nativa del sistema operativo de almacenamiento. Si el sistema de almacenamiento está encendido, está listo para crear backups.
- **Escalabilidad.** Se pueden conservar hasta 1024 copias de seguridad de un único contenedor de archivos y LUN. En el caso de conjuntos de datos complejos, es posible proteger varios contenedores de datos con un único conjunto coherente de copias Snapshot.
- El rendimiento no se ve afectado, independientemente de que un volumen contenga 1024 snapshots o ninguna.

Aunque muchos proveedores de almacenamiento ofrecen tecnología Snapshot, la tecnología Snapshot dentro de ONTAP es única y ofrece beneficios importantes para los entornos de aplicaciones y bases de datos empresariales:

- Las copias Snapshot forman parte del sistema de archivos WAFL (Write-Anywhere File Layout) subyacente. No son una tecnología complementaria ni externa. Esto simplifica la gestión, ya que el sistema de almacenamiento es el sistema de backup.
- Las copias Snapshot no afectan al rendimiento, a excepción de algunos casos periféricos como cuando se almacenan tantos datos en copias snapshot que el sistema de almacenamiento subyacente llena.
- El término «grupo de coherencia» se utiliza a menudo para referirse a una agrupación de objetos de almacenamiento que se gestionan como una colección consistente de datos. Una Snapshot de un volumen ONTAP determinado constituye un backup de grupo de coherencia.

Las copias Snapshot de ONTAP también ofrecen una escalabilidad mejor que la tecnología de la competencia. Los clientes pueden almacenar 5, 50 o 500 copias Snapshot sin que esto afecte al rendimiento. El número máximo de snapshots que se permite actualmente en un volumen es 1024. Si se requiere más retención de instantáneas, existen opciones para configurar las instantáneas en cascada a volúmenes adicionales.

Como resultado, proteger un conjunto de datos alojado en ONTAP es sencillo y altamente escalable. Los backups no requieren el traslado de datos, por lo que puede adaptarse a las necesidades del negocio en lugar de a las limitaciones de las tasas de transferencia de red, un gran número de unidades de cinta o áreas de almacenamiento provisional de discos.

¿Una snapshot es un backup?

Una pregunta frecuente acerca del uso de las copias Snapshot como estrategia de protección de datos es el hecho de que los datos «reales» y los datos de copias Snapshot se encuentran en las mismas unidades. La pérdida de esas unidades provocaría la pérdida de los datos primarios y el backup.

Este es un problema válido. Los snapshots locales se usan para necesidades de backup y recuperación diarias y, en ese sentido, la snapshot es un backup. Cerca del 99 % de todos los escenarios de recuperación en entornos NetApp utilizan copias Snapshot para satisfacer incluso los requisitos de objetivo de tiempo de recuperación más agresivos.

Sin embargo, las copias Snapshot locales nunca deberían ser la única estrategia de backup, por lo que NetApp ofrece tecnología como la replicación de SnapMirror y SnapVault para replicar de forma rápida y eficiente copias Snapshot en un conjunto de unidades independiente. En una solución correctamente

diseñada con copias Snapshot y replicación Snapshot, el uso de la cinta puede minimizarse tal vez a un archivo trimestral o eliminarse totalmente.

Backups basados en Snapshot

Existen muchas opciones para usar las copias Snapshot de ONTAP para proteger los datos, y las copias Snapshot son la base de muchas otras funciones de ONTAP, como replicación, recuperación ante desastres y clonación. Una descripción completa de la tecnología de instantáneas está fuera del alcance de este documento, pero en las siguientes secciones se proporciona una descripción general.

Existen dos métodos principales para crear una copia Snapshot de un conjunto de datos:

- Backups coherentes con los fallos
- Backups para aplicaciones

Un backup coherente con los fallos de un conjunto de datos hace referencia a la captura de toda la estructura del conjunto de datos en un único punto de tiempo. Si el conjunto de datos se almacena en un único volumen, el proceso es sencillo; se puede crear una copia Snapshot en cualquier momento. Si un conjunto de datos abarca volúmenes, es necesario crear una snapshot de grupo de coherencia (CG). Existen varias opciones para crear snapshots de CG, como el software NetApp SnapCenter, funciones nativas del grupo de coherencia ONTAP y scripts que se mantienen por el usuario.

Los backups coherentes con los fallos se utilizan principalmente cuando la recuperación punto del backup es suficiente. Cuando se necesita una recuperación más granular, por lo general se necesitan backups coherentes con las aplicaciones.

A menudo, la palabra «consistente» en «coherente con las aplicaciones» resulta una denominación errónea. Por ejemplo, colocar una base de datos de Oracle en modo de backup se denomina backup coherente con las aplicaciones, pero los datos no se hacen coherentes ni se ponen en modo inactivo de ninguna forma. Los datos siguen cambiando durante el backup. Por el contrario, la mayoría de los backups de MySQL y Microsoft SQL Server realmente ralentizan los datos antes de ejecutar el backup. VMware puede o no hacer que ciertos archivos sean consistentes.

Grupos de consistencia

El término «grupo de coherencia» hace referencia a la capacidad de una cabina de almacenamiento para gestionar varios recursos de almacenamiento como una sola imagen. Por ejemplo, una base de datos puede consistir en 10 LUN. La cabina debe ser capaz de realizar backup, restaurar y replicar esos 10 LUN de forma coherente. La restauración no es posible si las imágenes de las LUN no eran consistentes en el punto de backup. Para replicar estos 10 LUN es necesario que todas las réplicas estén perfectamente sincronizadas entre sí.

El término «grupo de coherencia» no se utiliza con frecuencia cuando se habla de ONTAP, porque la coherencia siempre ha sido una función básica del volumen y de la arquitectura de agregado en ONTAP. Muchas otras cabinas de almacenamiento gestionan LUN o sistemas de archivos como unidades individuales. Podrían configurarse opcionalmente como «grupo de consistencia» para fines de protección de datos, pero este es un paso adicional en la configuración.

ONTAP siempre ha podido capturar imágenes de datos replicadas y locales coherentes. Aunque los distintos volúmenes de un sistema ONTAP no suelen describirse formalmente como un grupo de coherencia, eso es lo que son. Una copia Snapshot de ese volumen es una imagen de grupo de coherencia, la restauración de esa copia Snapshot es una restauración de grupo de coherencia, y tanto SnapMirror como SnapVault ofrecen replicación de grupo de coherencia.

Snapshots de grupo de coherencia

Las snapshots de grupo de consistencia (cg-snapshots) son una extensión de la tecnología Snapshot básica de ONTAP. Una operación Snapshot estándar crea una imagen coherente de todos los datos dentro de un único volumen, pero a veces es necesario crear un conjunto coherente de instantáneas en varios volúmenes e incluso entre varios sistemas de almacenamiento. El resultado es un conjunto de instantáneas que se pueden utilizar de la misma manera que una instantánea de un solo volumen individual. Se pueden utilizar para la recuperación de datos locales, replicar para la recuperación ante desastres o clonar como una única unidad coherente.

El mayor uso conocido de cg-snapshots es para un entorno de base de datos de aproximadamente 1PB GB de tamaño que abarca 12 controladoras. Las cg-snapshots creadas en este sistema se han utilizado para backup, recuperación y clonado.

La mayoría de las veces, cuando un conjunto de datos abarca volúmenes y se debe conservar el orden de escritura, el software de gestión elegido utiliza automáticamente una instantánea de cg. No es necesario comprender los detalles técnicos de cg-snapshots en estos casos. No obstante, hay situaciones en las que los complejos requisitos de protección de datos requieran un control detallado del proceso de protección y replicación de datos. Los flujos de trabajo de automatización o el uso de scripts personalizados para llamar a las API de cg-snapshot son algunas de las opciones. Para comprender la mejor opción y el rol de cg-snapshot se requiere una explicación más detallada de la tecnología.

La creación de un conjunto de cg-snapshots es un proceso de dos pasos:

1. Establezca el aislamiento de escritura en todos los volúmenes de destino.
2. Crear snapshots de dichos volúmenes mientras se encuentra en estado protegido.

El cercado de escritura se establece en serie. Esto significa que, a medida que se configura el proceso de barrera en varios volúmenes, las operaciones de I/O de escritura se congelan en el primer volumen de la secuencia, a medida que sigue confirmándose con los volúmenes que aparecen más adelante. Esto puede parecer que, en un principio, no cumple el requisito de conservación de la orden de escritura, pero eso solo se aplica a I/O que se emite de forma asíncrona en el host y no depende de ninguna otra escritura.

Por ejemplo, una base de datos puede emitir muchas actualizaciones de archivos de datos asíncronos y permitir que el sistema operativo vuelva a ordenar la I/O y completarlas de acuerdo con su propia configuración del programador. El orden de este tipo de I/O no se puede garantizar porque la aplicación y el sistema operativo ya han liberado el requisito de conservar el orden de escritura.

Como ejemplo de contador, la mayor parte de la actividad de registro de la base de datos es síncrona. La base de datos no continúa con más escrituras de registro hasta que se reconozca la E/S y se mantenga el orden de esas escrituras. Si un registro de I/O llega a un volumen cercado, no se reconoce y la aplicación se bloquea en otras escrituras. Del mismo modo, la I/O de metadatos del sistema de archivos suele ser síncrona. Por ejemplo, no se debe perder una operación de eliminación de archivos. Si un sistema operativo con un sistema de archivos xfs suprimió un archivo y la E/S que actualizó los metadatos del sistema de archivos xfs para eliminar la referencia a ese archivo aterrizó en un volumen cercado, la actividad del sistema de archivos se detendría. De este modo se garantiza la integridad del sistema de archivos durante las operaciones cg-snapshot.

Después de configurar el control de escritura en los volúmenes de destino, están listos para la creación de las copias Snapshot. No es necesario crear las copias Snapshot precisamente al mismo tiempo, ya que el estado de los volúmenes se congela desde un punto de vista de escritura dependiente. Para protegerse frente a un defecto en la aplicación que crea las copias cg-snapshots, la barrera de escritura inicial incluye un tiempo de espera configurable en el que ONTAP libera automáticamente la barrera y reanuda el procesamiento de escritura transcurridos un número de segundos definido. Si todas las Snapshot se crean antes de que se agote el tiempo de espera, el conjunto de snapshots resultante es un grupo de coherencia válido.

Orden de escritura dependiente

Desde un punto de vista técnico, la clave para un grupo de consistencia es preservar el orden de escritura y, específicamente, el orden de escritura dependiente. Por ejemplo, una base de datos que escribe en 10 LUN escribe simultáneamente en todas ellas. Muchas escrituras se emiten de forma asíncrona, por lo que el orden en que se completan no es importante y el orden en que se realizan varía según el comportamiento del sistema operativo y de la red.

Algunas operaciones de escritura deben estar presentes en el disco antes de que la base de datos pueda continuar con escrituras adicionales. Estas operaciones de escritura cruciales se denominan escrituras dependientes. La E/S de escritura posterior depende de la presencia de estas escrituras en el disco. Cualquier snapshot, recuperación o replicación de estas 10 LUN debe asegurarse de que la orden de escritura dependiente está garantizada. Las actualizaciones del sistema de archivos son otro ejemplo de escrituras dependientes del orden de escritura. El orden en el que se realizan los cambios en el sistema de archivos debe conservarse o todo el sistema de archivos podría dañarse.

Estrategias

Existen dos enfoques principales para los backups basados en Snapshot:

- Backups coherentes con los fallos
- Backups activos protegidos de Snapshot

Una copia de seguridad coherente con los fallos de una base de datos se refiere a la captura de toda la estructura de la base de datos, incluidos archivos de datos, redo logs y archivos de control, en un único punto en el tiempo. Si la base de datos se almacena en un único volumen, el proceso es sencillo; se puede crear una copia Snapshot en cualquier momento. Si una base de datos abarca volúmenes, debe crearse una snapshot de grupo de coherencia (CG). Existen varias opciones para crear snapshots de CG, como el software NetApp SnapCenter, funciones nativas del grupo de coherencia ONTAP y scripts que se mantienen por el usuario.

Los backups de Snapshot coherentes con los fallos se usan principalmente cuando es suficiente con la recuperación punto del backup. Los registros de archivos se pueden aplicar bajo ciertas circunstancias, pero cuando se requiere una recuperación puntual más granular, es preferible un backup online.

El procedimiento básico para un backup en línea basado en Snapshot es el siguiente:

1. Coloque la base de datos en `backup` modo.
2. Cree una instantánea de todos los volúmenes que alojan archivos de datos.
3. Salga `backup` modo.
4. Ejecute el comando `alter system archive log current` para forzar el archivado de registros.
5. Crear instantáneas de todos los volúmenes que alojan los archive logs.

Este procedimiento produce un juego de instantáneas que contienen archivos de datos en modo de backup y los archive logs críticos generados durante el modo de backup. Estos son los dos requisitos para recuperar una base de datos. Los archivos, como los archivos de control, también deben protegerse por conveniencia, pero el único requisito absoluto es la protección de los archivos de datos y los registros de archivos.

Aunque los diferentes clientes pueden tener estrategias muy diferentes, casi todas estas estrategias se basan en última instancia en los mismos principios descritos a continuación.

Recuperación basada en Snapshot

Al diseñar diseños de volúmenes para bases de datos Oracle, la primera decisión es si utilizar tecnología NetApp SnapRestore basada en volúmenes (VBSR).

El SnapRestore basado en volúmenes permite revertir un volumen casi instantáneamente a un momento específico anterior. Debido a que se revierten todos los datos del volumen, es posible que VBSR no sea apropiado para todos los casos de uso. Por ejemplo, si se almacena una base de datos completa, incluidos archivos de datos, registros de recuperación y registros de archivos, en un solo volumen y este volumen se restaura con VBSR, los datos se pierden porque se descartan los datos de archive log y redo más recientes.

VBSR no se requiere para la restauración. Muchas bases de datos pueden restaurarse utilizando SnapRestore de archivo único (SFSR) basado en archivos o simplemente copiando archivos del snapshot al sistema de archivos activo.

Se prefiere VBSR cuando una base de datos es muy grande o cuando se debe recuperar lo antes posible, y el uso de VBSR requiere aislamiento de los archivos de datos. En un entorno NFS, los archivos de datos de una base de datos determinada deben estar almacenados en volúmenes dedicados que no estén contaminados por ningún otro tipo de archivo. En un entorno SAN, los archivos de datos deben almacenarse en LUN dedicadas en volúmenes dedicados. Si se utiliza un gestor de volúmenes (incluido Oracle Automatic Storage Management [ASM]), el grupo de discos también debe estar dedicado a los archivos de datos.

El aislamiento de archivos de datos de esta manera permite que se reviertan a un estado anterior sin dañar otros sistemas de archivos.

Reserva de Snapshot

Para cada volumen con datos de Oracle en un entorno SAN, el `percent-snapshot-space` Debe establecerse en cero porque reservar espacio para una snapshot en un entorno de LUN no es útil. Si la reserva fraccionaria se establece en 100, una copia snapshot de un volumen con unidades lógicas requiere suficiente espacio libre en el volumen, excluida la reserva de snapshot, para absorber un 100% de renovación de todos los datos. Si la reserva fraccionaria se define en un valor menor, se requiere una cantidad de espacio libre correspondiente menor, pero siempre excluye la reserva de instantáneas. Esto significa que se desperdicia el espacio de reserva de snapshot en un entorno de LUN.

En un entorno NFS, hay dos opciones:

- Ajuste la `percent-snapshot-space` basado en el consumo de espacio esperado de la instantánea.
- Ajuste la `percent-snapshot-space` a cero y gestione el consumo de espacio activo y snapshot de forma colectiva.

Con la primera opción, `percent-snapshot-space` se establece en un valor distinto de cero, normalmente alrededor del 20%. Este espacio se oculta al usuario. Sin embargo, este valor no crea un límite de utilización. Si una base de datos con una reserva del 20% experimenta una rotación del 30%, el espacio de la instantánea puede crecer más allá de los límites de la reserva del 20% y ocupar espacio sin reservar.

La principal ventaja de establecer una reserva en un valor como 20% es verificar que algo de espacio esté siempre disponible para las instantáneas. Por ejemplo, un volumen de 1TB GB con una reserva del 20% solo permitiría que un administrador de bases de datos (DBA) almacene 800GB TB de datos. Esta configuración garantiza al menos 200GB MB de espacio para el consumo de snapshots.

Cuando `percent-snapshot-space` se establece en cero, todo el espacio del volumen está disponible para el usuario final, lo que proporciona una mejor visibilidad. Un administrador de bases de datos debe comprender que, si ve un volumen de 1TB GB que aprovecha las copias Snapshot, este espacio de 1TB TB se compartirá entre los datos activos y la rotación de copias Snapshot.

No hay una preferencia clara entre la opción uno y la opción dos entre los usuarios finales.

Snapshots de ONTAP y de terceros

El ID de documento de Oracle 604683,1 explica los requisitos para la compatibilidad con Snapshot de terceros y las múltiples opciones disponibles para las operaciones de backup y restauración.

El proveedor externo debe garantizar que las copias Snapshot de la empresa cumplen con los requisitos siguientes:

- Las copias Snapshot deben integrarse con las operaciones de restauración y recuperación recomendadas de Oracle.
- Las instantáneas deben ser consistentes con los fallos de la base de datos en el punto de la instantánea.
- El orden de escritura se conserva para cada archivo dentro de una instantánea.

Los productos de gestión de Oracle de ONTAP y NetApp cumplen estos requisitos.

SnapRestore

Restauración de datos rápida en ONTAP a partir de una copia Snapshot realizada por la tecnología NetApp SnapRestore.

Cuando un conjunto de datos críticos no está disponible, las operaciones empresariales fundamentales no funcionan. Las cintas pueden romperse e incluso las restauraciones de backups basados en discos pueden ser lentas para transferirse por la red. SnapRestore evita estos problemas al ofrecer una restauración casi instantánea de conjuntos de datos. Incluso las bases de datos con capacidad de petabytes se pueden restaurar por completo con tan solo unos minutos.

Hay dos formas de SnapRestore: Basado en archivos/LUN y basado en volúmenes.

- Pueden restaurarse archivos o LUN individuales en segundos, tanto si se trata de un LUN de 2TB GB como de un archivo 4KB.
- El contenedor de archivos o LUN se puede restaurar en segundos, ya sea 10GB o 100TB TB de datos.

Un «contenedor de archivos o LUN» normalmente hace referencia a un volumen FlexVol. Por ejemplo, puede tener 10 LUN que componen un grupo de discos LVM en un único volumen o un volumen puede almacenar los directorios iniciales NFS de 1000 usuarios. En lugar de ejecutar una operación de restauración para cada archivo o LUN individuales, puede restaurar el volumen completo como una única operación. Este proceso también funciona con contenedores de escalado horizontal que incluyen múltiples volúmenes, como una FlexGroup o un grupo de consistencia ONTAP.

La razón por la que SnapRestore funciona tan rápido y eficientemente se debe a la naturaleza de una copia Snapshot, que es esencialmente una vista paralela de solo lectura del contenido de un volumen en un momento determinado. Los bloques activos son los bloques reales que se pueden cambiar, mientras que la copia Snapshot es una vista de solo lectura del estado de los bloques que constituyen los archivos y la LUN en el momento de crear la copia Snapshot.

ONTAP solo permite el acceso de solo lectura a los datos de snapshots, pero los datos se pueden reactivar con SnapRestore. La copia de Snapshot se vuelve a habilitar como una vista de lectura y escritura de los datos, lo que devuelve los datos a su estado anterior. SnapRestore puede funcionar a nivel de volumen o archivo. La tecnología es esencialmente la misma con algunas pequeñas diferencias en el comportamiento.

SnapRestore de volumen

La SnapRestore basada en volúmenes devuelve todo el volumen de datos a un estado anterior. Esta operación no requiere el movimiento de datos, lo que significa que el proceso de restauración es esencialmente instantáneo, aunque la operación de la API o la CLI puede tardar unos segundos en procesarse. La restauración de 1GB TB de datos no es más complicada ni requiere más tiempo que restaurar 1PB TB de datos. Esta funcionalidad es el principal motivo por el que muchos clientes empresariales migran a los sistemas de almacenamiento de ONTAP. Proporciona un objetivo de tiempo de recuperación que se mide en segundos incluso para los conjuntos de datos de mayor tamaño.

Una desventaja de la SnapRestore basada en el volumen se debe al hecho de que los cambios dentro de un volumen son acumulativos con el tiempo. Por lo tanto, cada instantánea y los datos del archivo activo dependen de los cambios que conduzcan a ese punto. Revertir un volumen a un estado anterior implica descartar todos los cambios posteriores que se habían realizado en los datos. Sin embargo, lo que no resulta tan obvio es que se incluyen las instantáneas creadas posteriormente. Esto no siempre es deseable.

Por ejemplo, un acuerdo de nivel de servicio de retención de datos puede especificar 30 días de backups nocturnos. Si se restaura un conjunto de datos en una snapshot creada hace cinco días con SnapRestore para volúmenes, se descartarán todas las snapshots creadas en los cinco días anteriores, lo que infringe el acuerdo de nivel de servicio.

Hay varias opciones disponibles para abordar esta limitación:

1. Los datos se pueden copiar a partir de una snapshot anterior, en lugar de realizar una SnapRestore de todo el volumen. Este método funciona mejor con conjuntos de datos más pequeños.
2. Una copia Snapshot puede clonarse en lugar de restaurarse. La limitación de este enfoque es que la copia Snapshot de origen depende del clon. Por lo tanto, no se puede eliminar a menos que también se elimine el clon o se divida en un volumen independiente.
3. Uso de SnapRestore basado en archivos.

SnapRestore de archivos

La SnapRestore basada en archivos es un proceso de restauración más granular basado en Snapshot. En lugar de revertir el estado de un volumen completo, se revierte el estado de un archivo individual o LUN. No es necesario eliminar ninguna instantánea, ni esta operación crea ninguna dependencia de una instantánea anterior. El archivo o el LUN estarán disponibles de inmediato en el volumen activo.

No es necesario mover datos durante una restauración SnapRestore de un archivo o una LUN. Sin embargo, se requieren algunas actualizaciones internas de metadatos para reflejar el hecho de que los bloques subyacentes de un archivo o LUN ahora existen tanto en una snapshot como en el volumen activo. No debería afectar el rendimiento, pero este proceso bloquea la creación de snapshots hasta que se completa. La tasa de procesamiento es de aproximadamente 5Gbps (18TB TB/hora) en función del tamaño total de los archivos restaurados.

Backups en línea

Se necesitan dos conjuntos de datos para proteger y recuperar una base de datos de Oracle en modo de backup. Tenga en cuenta que esta no es la única opción de copia de seguridad de Oracle, pero es la más común.

- Instantánea de los archivos de datos en modo de copia de seguridad
- Los registros de archivos creados mientras los archivos de datos estaban en modo de backup

Si se necesita una recuperación completa, incluidas todas las transacciones confirmadas, se requiere un tercer elemento:

- Juego de redo logs actuales

Existen varias formas de impulsar la recuperación de un backup en línea. Muchos clientes restauran snapshots mediante la interfaz de línea de comandos de ONTAP y, a continuación, usando Oracle RMAN o sqlplus para completar la recuperación. Esto es especialmente habitual en entornos de producción de gran tamaño en los que la probabilidad y frecuencia de las restauraciones de bases de datos es extremadamente baja y cualquier procedimiento de restauración lo gestiona un administrador de bases de datos cualificado. Para obtener una automatización completa, las soluciones como NetApp SnapCenter incluyen un complemento de Oracle con interfaces gráficas y de línea de comandos.

Algunos clientes a gran escala han adoptado un enfoque más simple mediante la configuración de secuencias de comandos básicas en los hosts para colocar las bases de datos en modo de backup en un momento específico de preparación para una copia Snapshot programada. Por ejemplo, programe el comando `alter database begin backup` a las 23:58, `alter database end backup` a las 00:02, y después programe copias snapshot directamente en el sistema de almacenamiento a medianoche. El resultado es una estrategia de backup sencilla y altamente escalable que no requiere software ni licencias externas.

Distribución de datos

El diseño más sencillo es aislar los archivos de datos en uno o varios volúmenes dedicados. No deben estar contaminados por ningún otro tipo de archivo. De este modo, se garantiza que los volúmenes de archivos de datos puedan restaurarse rápidamente mediante una operación SnapRestore sin destruir un registro de recuperación, un archivo de control o un archivo importante.

SAN tiene requisitos similares para aislamiento de archivos de datos en volúmenes dedicados. Con un sistema operativo como Microsoft Windows, un único volumen puede contener varios LUN de archivos de datos, cada uno con un sistema de archivos NTFS. Con otros sistemas operativos, generalmente hay un administrador de volúmenes lógicos. Por ejemplo, con Oracle ASM, la opción más sencilla sería confinar los LUN de un grupo de discos ASM en un único volumen del que se pueda incluir y restaurar como unidad en un backup. Si se necesitan volúmenes adicionales por motivos de rendimiento o gestión de capacidad, crear un grupo de discos adicional en el nuevo volumen simplifica la gestión.

Si se siguen estas directrices, se pueden programar Snapshot directamente en el sistema de almacenamiento sin requisitos para realizar una snapshot de grupo de coherencia. El motivo es que las copias de seguridad de Oracle no necesitan que se realice una copia de seguridad de los archivos de datos al mismo tiempo. El procedimiento de backup online se diseñó para permitir que los archivos de datos sigan actualizándose a medida que se transmiten lentamente a la cinta durante horas.

Se produce una complicación en situaciones como el uso de un grupo de discos de ASM que se distribuye entre volúmenes. En estos casos, se debe realizar una cg-snapshot para garantizar que los metadatos de ASM sean coherentes en todos los volúmenes constituyentes.

Precaución: Verifique que el ASM `spfile` y.. `passwd` los archivos no están en el grupo de discos que aloja los archivos de datos. Esto interfiere con la capacidad de restaurar selectivamente archivos de datos y solo archivos de datos.

Procedimiento de recuperación local: NFS

Este procedimiento se puede realizar manualmente o a través de una aplicación como SnapCenter. El procedimiento básico es el siguiente:

1. Cierre la base de datos.

2. Recupere los volúmenes del archivo de datos en la instantánea inmediatamente antes del punto de restauración deseado.
3. Reproduzca los archive logs en el punto deseado.
4. Reproduzca los redo logs actuales si desea una recuperación completa.

En este procedimiento se asume que los archive logs deseados siguen presentes en el sistema de archivos activo. De lo contrario, se deben restaurar los archive logs o se puede dirigir rman/sqlplus a los datos del directorio de instantáneas.

Además, para bases de datos más pequeñas, un usuario final puede recuperar archivos de datos directamente desde `.snapshot` directorio sin la ayuda de herramientas de automatización o administradores del almacenamiento para ejecutar un `snaprestore` comando.

Procedimiento de recuperación local: San

Este procedimiento se puede realizar manualmente o a través de una aplicación como SnapCenter. El procedimiento básico es el siguiente:

1. Cierre la base de datos.
2. Desactive los grupos de discos que alojan los archivos de datos. El procedimiento varía en función del gestor de volúmenes lógico elegido. Con ASM, el proceso requiere desmontar el grupo de discos. Con Linux, los sistemas de archivos deben desmontarse y los volúmenes lógicos y los grupos de volúmenes deben desactivarse. El objetivo es detener todas las actualizaciones en el grupo de volúmenes objetivo que se va a restaurar.
3. Restaure los grupos de discos de archivos de datos en la instantánea inmediatamente antes del punto de restauración deseado.
4. Vuelva a activar los grupos de discos recién restaurados.
5. Reproduzca los archive logs en el punto deseado.
6. Vuelva a reproducir todos los redo logs si desea realizar una recuperación completa.

En este procedimiento se asume que los archive logs deseados siguen presentes en el sistema de archivos activo. Si no lo son, los registros de archivos se deben restaurar desconectando las LUN del registro de archivos y ejecutando una restauración. Este es también un ejemplo en el que la división de archive logs en volúmenes dedicados es útil. Si los registros de archivos comparten un grupo de volúmenes con registros de recuperación, se deben copiar en otro lugar los registros de recuperación antes de restaurar el conjunto general de LUN. Este paso evita la pérdida de las transacciones registradas finales.

Backups optimizados para Snapshot de almacenamiento

Cuando se lanzó Oracle 12c, ya que no es necesario colocar una base de datos en modo de backup dinámico, se simplificaron aún más las tareas de backup y recuperación basadas en Snapshots. El resultado es la capacidad de programar backups basados en snapshots directamente en un sistema de almacenamiento y mantener la capacidad para realizar una recuperación completa o de un momento específico.

Aunque el procedimiento de recuperación de backup dinámico es más familiar para los administradores de bases de datos, durante mucho tiempo ha sido posible usar snapshots que no se crearon mientras la base de datos estaba en modo de backup dinámico. Oracle 10g y 11g requerían pasos manuales adicionales durante la recuperación para hacer que la base de datos fuera coherente. Con Oracle 12c, `sqlplus` y.. `rman` contienen la lógica adicional para reproducir archive logs en copias de seguridad de archivos de datos que no

estaban en modo de copia de seguridad activa.

Como hemos visto anteriormente, la recuperación de un backup en caliente basado en instantáneas requiere dos conjuntos de datos:

- Instantánea de los archivos de datos creados en modo de backup
- Los registros de archivos generados mientras los archivos de datos estaban en modo de backup dinámico

Durante la recuperación, la base de datos lee los metadatos de los archivos de datos para seleccionar los archive logs requeridos para la recuperación.

La recuperación optimizada para snapshot de almacenamiento requiere conjuntos de datos ligeramente diferentes para lograr los mismos resultados:

- Una instantánea de los archivos de datos, además de un método para identificar la hora a la que se creó la instantánea
- Archive logs desde la hora del punto de control del archivo de datos más reciente hasta la hora exacta de la instantánea

Durante la recuperación, la base de datos lee metadatos de los archivos de datos para identificar el primer archive log necesario. Se puede realizar una recuperación completa o a un momento específico. Al realizar una recuperación puntual, es fundamental conocer la hora de la instantánea de los archivos de datos. El punto de recuperación especificado debe ser posterior a la hora de creación de las instantáneas. NetApp recomienda añadir al menos unos minutos al tiempo de la snapshot para justificar la variación de reloj.

Para obtener más información, consulte la documentación de Oracle sobre el tema «Recuperación mediante la optimización de instantáneas de almacenamiento» disponible en varias versiones de la documentación de Oracle 12c. Además, consulte el ID de documento de Oracle 604683,1 con respecto al soporte de instantáneas de terceros de Oracle.

Distribución de datos

El diseño más sencillo es aislar los archivos de datos en uno o varios volúmenes dedicados. No deben estar contaminados por ningún otro tipo de archivo. De este modo, se garantiza que los volúmenes de archivos de datos se puedan restaurar rápidamente con una operación de SnapRestore sin destruir un registro de recuperación, un archivo de control o un archivo importante.

SAN tiene requisitos similares para aislamiento de archivos de datos en volúmenes dedicados. Con un sistema operativo como Microsoft Windows, un único volumen puede contener varios LUN de archivos de datos, cada uno con un sistema de archivos NTFS. Con otros sistemas operativos, generalmente hay un gestor de volúmenes lógicos también. Por ejemplo, con Oracle ASM, la opción más sencilla sería restringir los grupos de discos en un único volumen del que se pueda realizar un backup y restaurar como unidad. Si se necesitan volúmenes adicionales por motivos de rendimiento o gestión de capacidad, crear un grupo de discos adicional en el nuevo volumen simplifica la gestión.

Si se siguen estas directrices, se pueden programar Snapshot directamente en ONTAP sin requisitos para realizar una snapshot de grupo de coherencia. El motivo es que las copias de seguridad optimizadas para instantáneas no necesitan que se realice una copia de seguridad de los archivos de datos al mismo tiempo.

Se produce una complicación en situaciones como un grupo de discos de ASM que se distribuye entre volúmenes. En estos casos, se debe realizar una cg-snapshot para garantizar que los metadatos de ASM sean coherentes en todos los volúmenes constituyentes.

[Nota]Verifique que los archivos spfile y passwd de ASM no estén en el grupo de discos que aloja los archivos

de datos. Esto interfiere con la capacidad de restaurar selectivamente archivos de datos y solo archivos de datos.

Procedimiento de recuperación local: NFS

Este procedimiento se puede realizar manualmente o a través de una aplicación como SnapCenter. El procedimiento básico es el siguiente:

1. Cierre la base de datos.
2. Recupere los volúmenes del archivo de datos en la instantánea inmediatamente antes del punto de restauración deseado.
3. Reproduzca los archive logs en el punto deseado.

En este procedimiento se asume que los archive logs deseados siguen presentes en el sistema de archivos activo. Si no lo son, se deben restaurar los registros de archivos `rman` o. `sqlplus` se puede dirigir a los datos de la `.snapshot` directorio.

Además, para bases de datos más pequeñas, un usuario final puede recuperar archivos de datos directamente desde `.snapshot` Directorio sin ayuda de las herramientas de automatización o de un administrador del almacenamiento para ejecutar un comando de la SnapRestore.

Procedimiento de recuperación local: San

Este procedimiento se puede realizar manualmente o a través de una aplicación como SnapCenter. El procedimiento básico es el siguiente:

1. Cierre la base de datos.
2. Desactive los grupos de discos que alojan los archivos de datos. El procedimiento varía en función del gestor de volúmenes lógico elegido. Con ASM, el proceso requiere desmontar el grupo de discos. Con Linux, los sistemas de archivos deben desmontarse y los volúmenes lógicos y los grupos de volúmenes están desactivados. El objetivo es detener todas las actualizaciones en el grupo de volúmenes objetivo que se va a restaurar.
3. Restaure los grupos de discos de archivos de datos en la instantánea inmediatamente antes del punto de restauración deseado.
4. Vuelva a activar los grupos de discos recién restaurados.
5. Reproduzca los archive logs en el punto deseado.

En este procedimiento se asume que los archive logs deseados siguen presentes en el sistema de archivos activo. Si no lo son, los registros de archivos se deben restaurar desconectando las LUN del registro de archivos y ejecutando una restauración. Este es también un ejemplo en el que la división de archive logs en volúmenes dedicados es útil. Si los registros de archivos comparten un grupo de volúmenes con redo logs, los redo logs se deben copiar en otro lugar antes de restaurar el conjunto general de LUN para evitar perder las transacciones finales registradas.

Ejemplo de recuperación completa

Supongamos que los archivos de datos se han dañado o destruido y se necesita una recuperación completa. El procedimiento para hacerlo es el siguiente:

```
[oracle@host1 ~]$ sqlplus / as sysdba
Connected to an idle instance.
SQL> startup mount;
ORACLE instance started.
Total System Global Area 1610612736 bytes
Fixed Size                  2924928 bytes
Variable Size            1040191104 bytes
Database Buffers          553648128 bytes
Redo Buffers               13848576 bytes
Database mounted.
SQL> recover automatic;
Media recovery complete.
SQL> alter database open;
Database altered.
SQL>
```

Ejemplo de recuperación a un momento específico

Todo el procedimiento de recuperación es un único comando: `recover automatic`.

Si se requiere una recuperación a un momento específico, es necesario conocer la marca de hora de las instantáneas y se puede identificar de la siguiente manera:

```
Cluster01::> snapshot show -vserver vserver1 -volume NTAP_oradata -fields
create-time
vserver   volume        snapshot   create-time
--------  ------------  ---------  ------------------------
vserver1  NTAP_oradata  my-backup  Thu Mar 09 10:10:06 2017
```

La hora de creación de la copia Snapshot se muestra como 9th de marzo y 10:10:06. Para estar seguro, se añade un minuto a la hora de la copia Snapshot:

```
[oracle@host1 ~]$ sqlplus / as sysdba
Connected to an idle instance.
SQL> startup mount;
ORACLE instance started.
Total System Global Area 1610612736 bytes
Fixed Size                  2924928 bytes
Variable Size            1040191104 bytes
Database Buffers          553648128 bytes
Redo Buffers               13848576 bytes
Database mounted.
SQL> recover database until time '09-MAR-2017 10:44:15' snapshot time '09-
MAR-2017 10:11:00';
```

La recuperación se inicia ahora. Especificó una hora de instantánea de 10:11:00, un minuto después del tiempo registrado para contabilizar la posible variación de reloj y un tiempo de recuperación objetivo de 10:44. A continuación, sqlplus solicita los archive logs necesarios para alcanzar el tiempo de recuperación deseado de 10:44.

```
ORA-00279: change 551760 generated at 03/09/2017 05:06:07 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_31_930813377.dbf
ORA-00280: change 551760 for thread 1 is in sequence #31
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 552566 generated at 03/09/2017 05:08:09 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_32_930813377.dbf
ORA-00280: change 552566 for thread 1 is in sequence #32
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 553045 generated at 03/09/2017 05:10:12 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_33_930813377.dbf
ORA-00280: change 553045 for thread 1 is in sequence #33
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 753229 generated at 03/09/2017 05:15:58 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_34_930813377.dbf
ORA-00280: change 753229 for thread 1 is in sequence #34
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
Log applied.
Media recovery complete.
SQL> alter database open resetlogs;
Database altered.
SQL>
```

Recuperación completa de una base de datos utilizando instantáneas utilizando el `recover automatic` el comando no requiere una licencia específica, sino un uso de recuperación puntual `snapshot time` Necesita la licencia de Oracle Advanced Compression.

Herramientas de automatización y gestión de base de datos

El valor principal de ONTAP en un entorno de bases de datos de Oracle proviene de las tecnologías principales de ONTAP, como las copias Snapshot instantáneas, la replicación simple de SnapMirror y la creación eficiente de los volúmenes FlexClone.

En algunos casos, la simple configuración de estas funciones básicas directamente en ONTAP satisface los requisitos, pero las necesidades más complicadas requieren una capa de orquestación.

SnapCenter

SnapCenter es el producto estrella de protección de datos de NetApp. A un nivel muy bajo, es similar a los

productos de SnapManager en cuanto a cómo se ejecutan backups de bases de datos, pero se creó desde cero para proporcionar un panel único para la gestión de la protección de datos en sistemas de almacenamiento de NetApp.

SnapCenter incluye las funciones básicas, como los backups y restauraciones basados en Snapshot, la replicación de SnapMirror y SnapVault, y otras funciones necesarias para funcionar a escala para grandes empresas. Estas funciones avanzadas incluyen una funcionalidad ampliada de control de acceso basado en roles (RBAC), API RESTful para integrarse con productos de orquestación de terceros, gestión central no disruptiva de complementos de SnapCenter en hosts de bases de datos y una interfaz de usuario diseñada para entornos a escala de cloud.

DESCANSO

ONTAP también contiene un amplio conjunto de API RESTful. Esto permite que 3rd proveedores de partes creen protección de datos y otras aplicaciones de gestión con la profunda integración con ONTAP. Además, los clientes que desean crear sus propios flujos de trabajo y utilidades de automatización pueden consumir fácilmente la API RESTful.

Recuperación ante desastres de Oracle

Descripción general

La recuperación tras desastres se refiere a la restauración de servicios de datos tras un evento catastrófico, como un incendio que destruye un sistema de almacenamiento o incluso un sitio entero.

Esta documentación sustituye a los informes técnicos publicados anteriormente *TR-4591: Oracle Data Protection* y *TR-4592: Oracle en MetroCluster.*

La recuperación tras desastres puede llevarse a cabo mediante la replicación sencilla de datos mediante SnapMirror; por supuesto, muchos clientes actualizan réplicas replicadas cada hora.

Para la mayoría de los clientes, la recuperación ante desastres requiere algo más que poseer una copia remota de datos, requiere la capacidad para usar rápidamente esos datos. NetApp ofrece dos tecnologías para satisfacer esta necesidad: La sincronización activa de MetroCluster y SnapMirror

MetroCluster se refiere a ONTAP en una configuración de hardware que incluye almacenamiento reflejado sincrónico de bajo nivel y numerosas funciones adicionales. Las soluciones integradas como MetroCluster simplifican las complicadas infraestructuras de bases de datos, aplicaciones y virtualización actuales y de escalado horizontal. Reemplaza múltiples productos y estrategias de protección de datos externa por una cabina de almacenamiento simple y central. También proporciona integración de backup, recuperación, recuperación tras siniestros y alta disponibilidad (HA) en un único sistema de almacenamiento en clúster.

La sincronización activa (SM-AS) de SnapMirror se basa en SnapMirror síncrono. Con MetroCluster, cada controladora de ONTAP es responsable de replicar los datos de la unidad en una ubicación remota. Con la sincronización activa de SnapMirror, básicamente cuenta con dos sistemas ONTAP diferentes que mantienen copias independientes de los datos de su unidad lógica, pero que cooperan para presentar una única instancia de esa LUN. Desde el punto de vista del host, se trata de una única entidad de LUN.

Comparación SM-AS y MCC

SM-AS y MetroCluster son similares en cuanto a funcionalidad general, pero hay diferencias importantes en la forma en que se implementó la replicación RPO=0 y cómo se gestiona. La sincronización asíncrona y síncrona

de SnapMirror también se puede utilizar como parte de un plan de recuperación ante desastres, pero no están diseñadas como tecnologías de réplica de alta disponibilidad.

- Una configuración de MetroCluster es más como un clúster integrado con nodos distribuidos por todos los sitios. SM-AS se comporta como dos clústeres independientes que cooperan en el servicio de un objetivo de punto de recuperación seleccionado=0 LUN replicadas de forma síncrona.
- Los datos de una configuración MetroCluster solo son accesibles desde un sitio concreto en un momento dado. Una segunda copia de los datos está presente en el sitio opuesto, pero los datos son pasivos. No es posible acceder a ella sin una conmutación por error del sistema de almacenamiento.
- El mirroring de MetroCluster y SM-AS se produce en diferentes niveles. El mirroring de MetroCluster se realiza en la capa de RAID. Los datos de bajo nivel se almacenan en un formato duplicado mediante SyncMirror. El uso del mirroring es prácticamente invisible en las capas de LUN, volumen y protocolo.
- Por el contrario, la duplicación SM-AS se produce en la capa de protocolo. Los dos clústeres son clústeres independientes en general. Una vez que las dos copias de datos están sincronizadas, los dos clústeres solo tienen que reflejar las escrituras. Cuando se produce una escritura en un clúster, se replica en otro clúster. La escritura solo se reconoce en el host cuando la escritura se ha completado en ambos sitios. Aparte de este comportamiento de división del protocolo, los dos clústeres son clústeres ONTAP normales.
- El rol principal de MetroCluster es la replicación a gran escala. Puede replicar toda una cabina con RPO=0 y RTO casi nulo. Esto simplifica el proceso de conmutación al nodo de respaldo porque solo hay una cosa que conmutar al nodo de respaldo y ofrece una escalabilidad extremadamente buena en cuanto a capacidad e IOPS.
- Un caso de uso clave de SM-AS es la replicación granular. En ocasiones, no desea replicar todos los datos como una sola unidad, o debe poder conmutar al nodo de respaldo de forma selectiva ciertas cargas de trabajo.
- Otro caso de uso clave de SM-AS es en las operaciones activo-activo, donde desea que existan copias de datos totalmente utilizables para estar disponibles en dos clústeres diferentes ubicados en dos ubicaciones diferentes con idénticas características de rendimiento y, si lo desea, no es necesario ampliar la SAN entre los sitios. Puede tener sus aplicaciones ya ejecutándose en ambos sitios, lo que reduce el RTO general durante las operaciones de conmutación al respaldo.

MetroCluster

Recuperación ante desastres con MetroCluster

MetroCluster es una función de ONTAP que puede proteger sus bases de datos de Oracle con RPO=0 mirroring sincrónico entre sitios y se escala verticalmente para admitir cientos de bases de datos en un único sistema de MetroCluster.

También es fácil de usar. El uso de MetroCluster no es necesariamente uno de los factores que contribuyen a aumentar ni cambiar los mejores cursos para el funcionamiento de aplicaciones y bases de datos empresariales.

Siguen siendo aplicables las prácticas recomendadas habituales y, si sus necesidades solo requieren protección de datos con objetivo de punto de recuperación = 0, esta se cumplirá con MetroCluster. Sin embargo, la mayoría de los clientes utilizan MetroCluster no solo para la protección de datos con objetivo de punto de recuperación = 0, sino también para mejorar el objetivo de tiempo de recuperación durante escenarios de desastre, y proporcionar una conmutación por error transparente como parte de las actividades de mantenimiento del sitio.

Arquitectura física

Para comprender el funcionamiento de las bases de datos Oracle en un entorno MetroCluster, es necesario explicar el diseño físico de un sistema MetroCluster.

Esta documentación sustituye al informe técnico *TR-4592 publicado anteriormente: Oracle en MetroCluster.*

MetroCluster está disponible en 3 configuraciones diferentes

- Pares DE ALTA DISPONIBILIDAD con conectividad IP
- Pares DE ALTA DISPONIBILIDAD con conectividad FC
- Controladora única con conectividad FC

El término 'conectividad' hace referencia a la conexión de clúster usada para la replicación entre sitios. No hace referencia a los protocolos de host. Todos los protocolos del lado del host se admiten como de costumbre en una configuración de MetroCluster, independientemente del tipo de conexión utilizada para la comunicación entre clústeres.

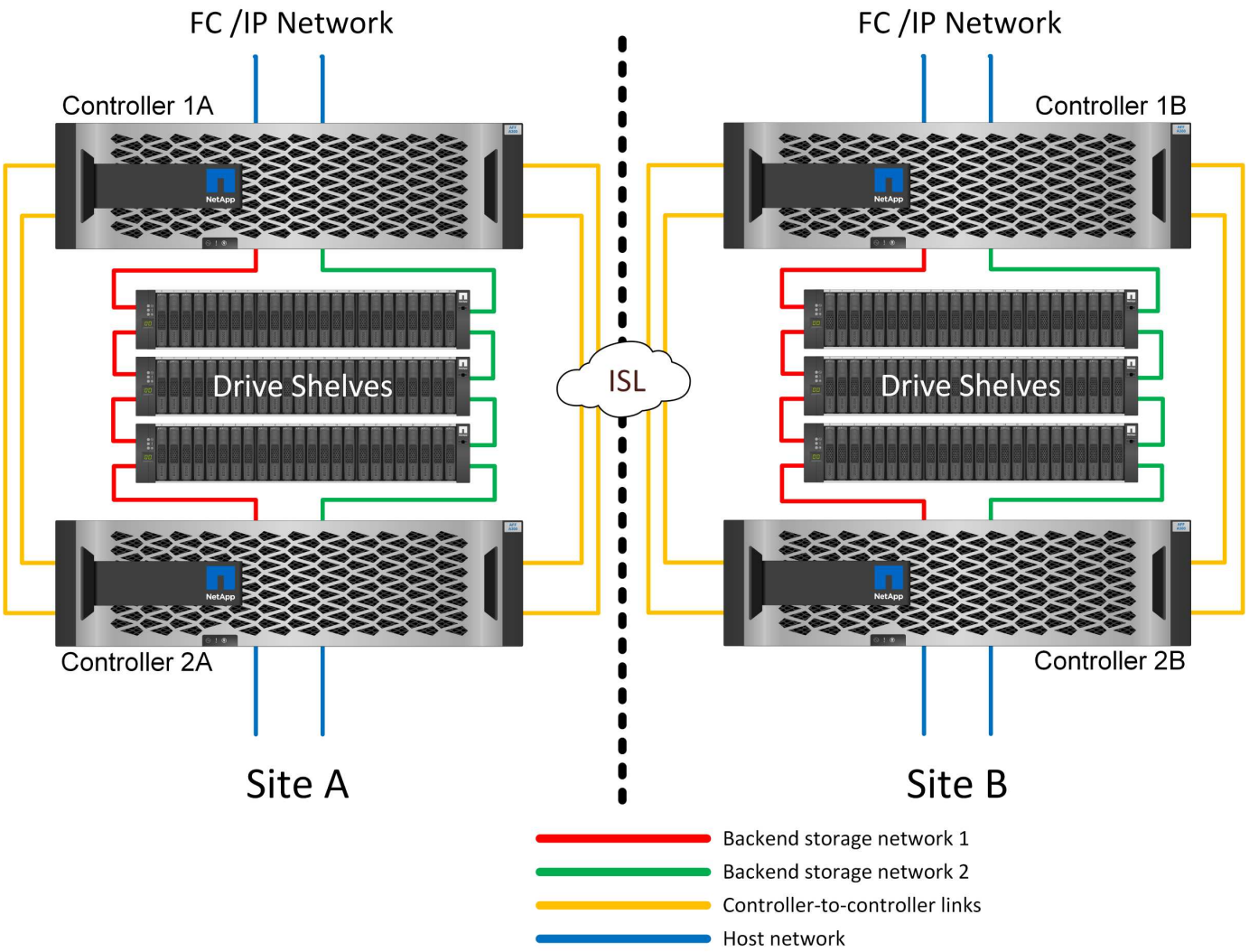
IP de MetroCluster

La configuración IP de MetroCluster para pares de alta disponibilidad utiliza dos o cuatro nodos por sitio. Esta opción de configuración aumenta la complejidad y los costes relacionados con la opción de dos nodos, pero ofrece una ventaja importante: La redundancia dentro del sitio. Un simple fallo de una controladora no requiere acceso a los datos a través de la WAN. El acceso a los datos sigue siendo local a través de la controladora local alternativa.

La mayoría de los clientes eligen la conectividad IP porque los requisitos de infraestructura son más simples. En el pasado, la conectividad entre sitios de alta velocidad solía ser más fácil de aprovisionar mediante switches FC y de fibra oscura; sin embargo, hoy en día los circuitos IP de alta velocidad y baja latencia son más fáciles de obtener.

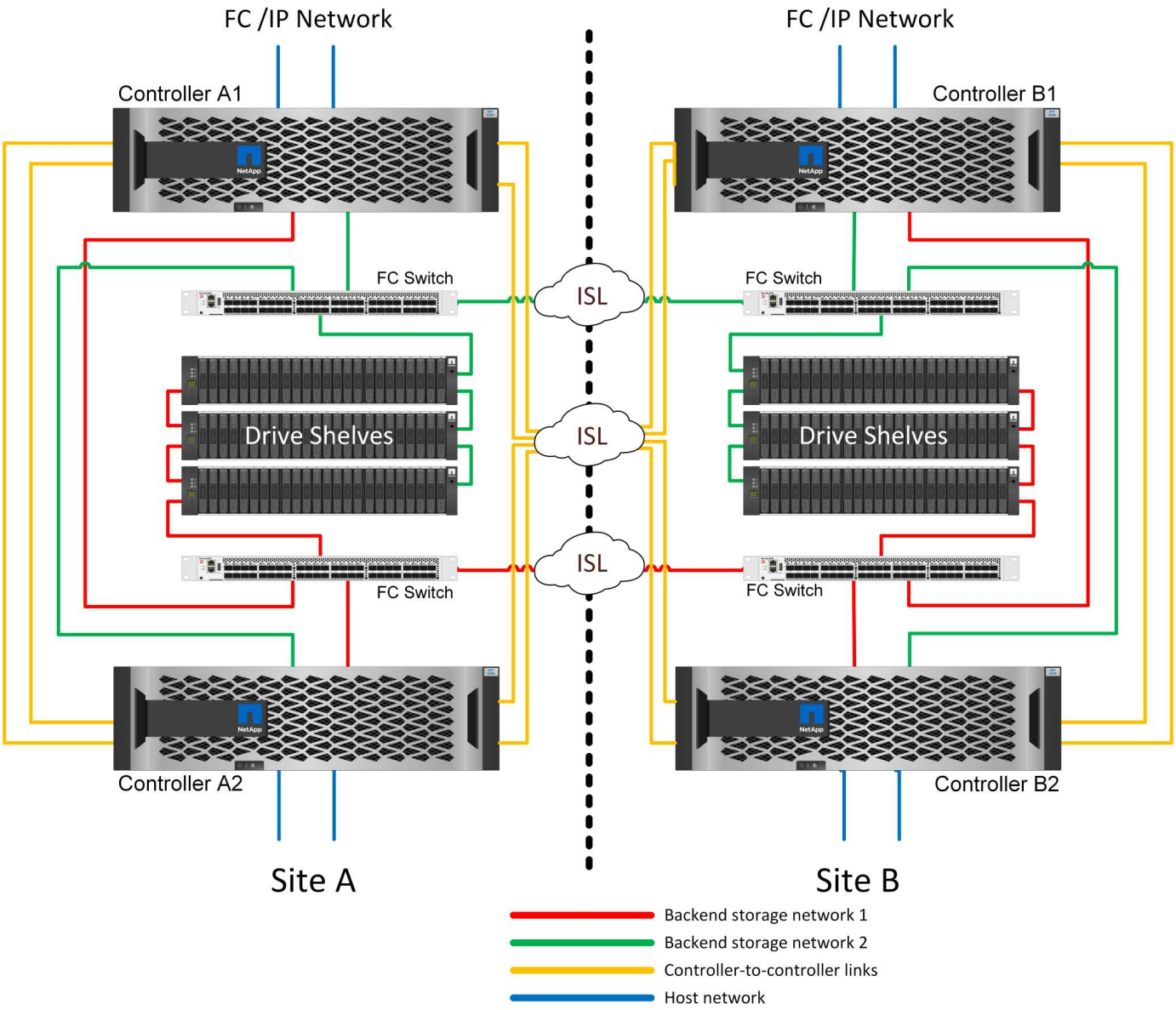
La arquitectura además es más sencilla ya que las únicas conexiones entre sitios son para las controladoras. En MetroCluster conectados a FC SAN, una controladora escribe directamente en las unidades del sitio opuesto y, por lo tanto, requiere conexiones SAN, switches y puentes adicionales. En cambio, una controladora con una configuración IP escribe en las unidades opuestas a través de la controladora.

Para obtener información adicional, consulte la documentación oficial de ONTAP y. "Arquitectura y diseño de la solución MetroCluster IP".



MetroCluster con conexión SAN FC de par de ALTA DISPONIBILIDAD

La configuración MetroCluster FC de par de alta disponibilidad utiliza dos o cuatro nodos por sitio. Esta opción de configuración aumenta la complejidad y los costes relacionados con la opción de dos nodos, pero ofrece una ventaja importante: La redundancia dentro del sitio. Un simple fallo de una controladora no requiere acceso a los datos a través de la WAN. El acceso a los datos sigue siendo local a través de la controladora local alternativa.



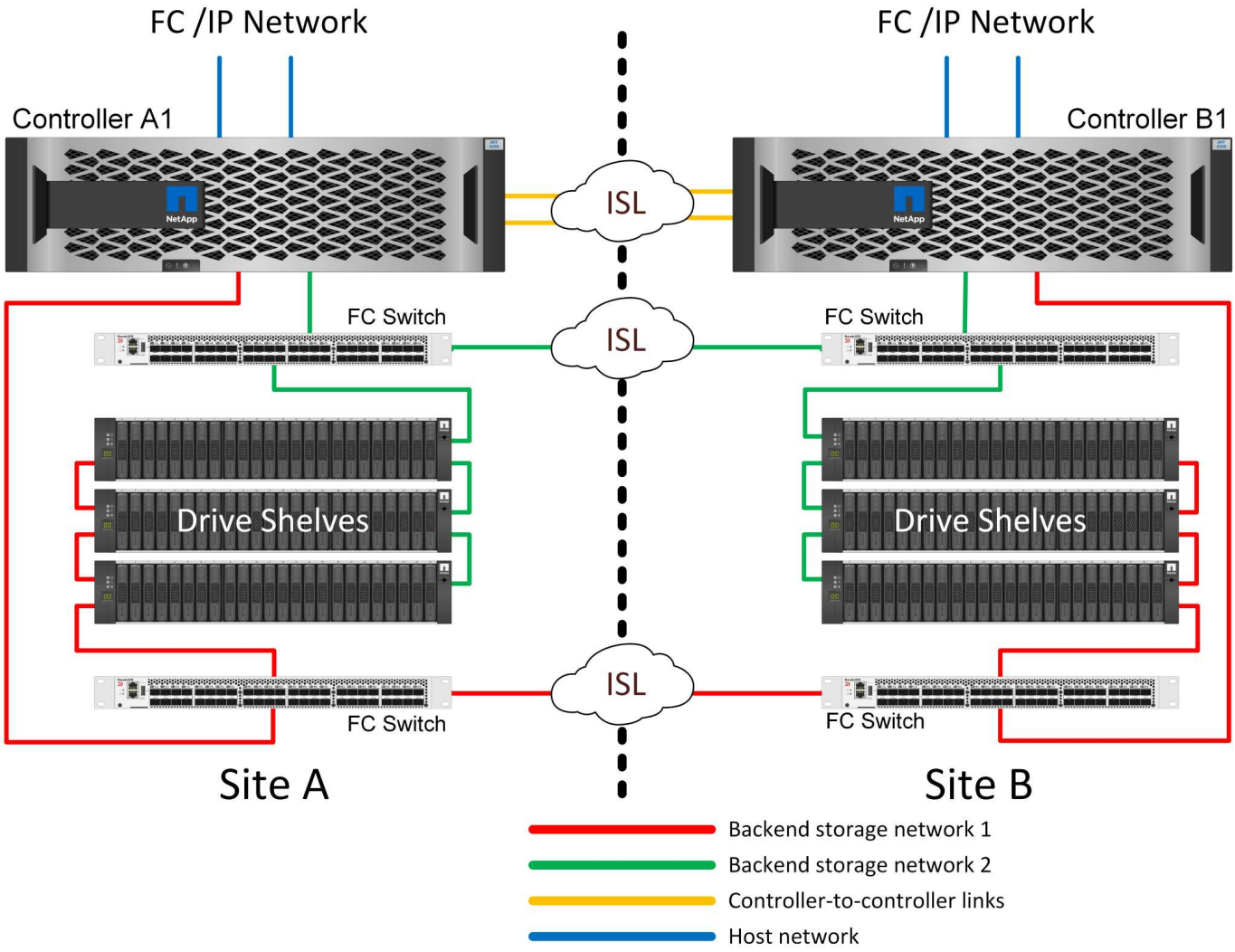
Algunas infraestructuras multisitio no están diseñadas para operaciones activo-activo, sino que se utilizan más como sitio principal y sitio de recuperación de desastres. En esta situación, generalmente es preferible una opción MetroCluster de una pareja de alta disponibilidad por las siguientes razones:

- Aunque un clúster MetroCluster de dos nodos es un sistema de alta disponibilidad, el fallo inesperado de una controladora o de tareas de mantenimiento planificadas requiere que los servicios de datos deban estar online en el sitio opuesto. Si la conectividad de red entre los sitios no puede soportar el ancho de banda requerido, el rendimiento se ve afectado. La única opción sería también conmutar por error los diversos sistemas operativos host y los servicios asociados a la ubicación alternativa. El clúster MetroCluster de la pareja de alta disponibilidad elimina este problema porque la pérdida de una controladora hace que la conmutación al respaldo sea sencilla dentro del mismo sitio.
- Algunas topologías de red no están diseñadas para el acceso entre sitios, sino que utilizan subredes diferentes o SAN FC aisladas. En estos casos, el clúster MetroCluster de dos nodos ya no funciona como un sistema de alta disponibilidad porque la controladora alternativa no puede proporcionar datos a los servidores del sitio opuesto. La opción MetroCluster de par de alta disponibilidad es necesaria para ofrecer una redundancia completa.
- Si se considera una infraestructura de dos sitios como una única infraestructura de alta disponibilidad, la configuración de MetroCluster de dos nodos es adecuada. Sin embargo, si el sistema debe funcionar

durante un largo período de tiempo tras el fallo del sitio, se prefiere un par de alta disponibilidad porque sigue proporcionando alta disponibilidad dentro de un único sitio.

MetroCluster FC de dos nodos conectado a SAN

La configuración de MetroCluster de dos nodos solo utiliza un nodo por sitio. Este diseño es más sencillo que la opción de pareja de alta disponibilidad porque hay menos componentes que configurar y mantener. También ha reducido las demandas de infraestructura en términos de cableado y conmutación FC. Por último, reduce los costes.



El impacto obvio de este diseño es que el fallo de una controladora en un único sitio significa que los datos están disponibles en el sitio opuesto. Esta restricción no es necesariamente un problema. Muchas empresas tienen operaciones de centros de datos multisitio con redes extendidas de alta velocidad y baja latencia que funcionan básicamente como una única infraestructura. En estos casos, la versión de dos nodos de MetroCluster es la configuración preferida. Varios proveedores de servicios utilizan actualmente sistemas de dos nodos a escala de petabytes.

Funcionalidades de resiliencia de MetroCluster

No hay puntos únicos de error en una solución de MetroCluster:

- Cada controladora tiene dos rutas independientes a las bandejas de unidades en el sitio local.

- Cada controladora tiene dos rutas independientes a las bandejas de unidades en el sitio remoto.
- Cada controladora tiene dos rutas independientes a las controladoras del sitio opuesto.
- En la configuración de par de alta disponibilidad, cada controladora tiene dos rutas desde su compañero local.

En resumen, puede eliminarse cualquier componente de la configuración sin poner en riesgo la capacidad de MetroCluster para suministrar datos. La única diferencia en términos de flexibilidad entre las dos opciones es que la versión del par de alta disponibilidad sigue siendo un sistema de almacenamiento de alta disponibilidad global tras un fallo del sitio.

Arquitectura lógica

Comprender el funcionamiento de las bases de datos Oracle en un entorno MetroCluster alsop requiere alguna explicación de la funcionalidad lógica de un sistema MetroCluster.

Protección contra errores del sitio: NVRAM y MetroCluster

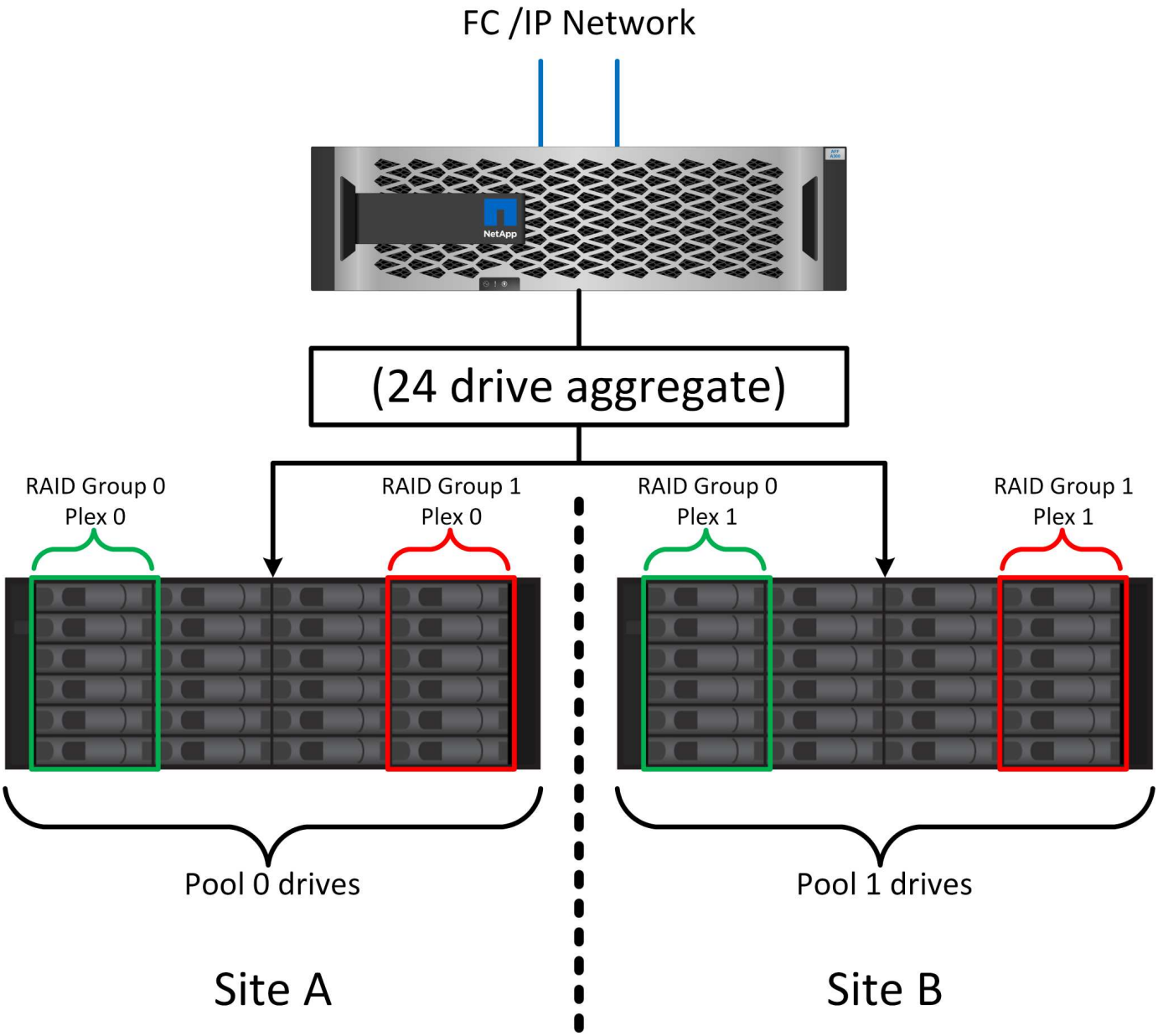
MetroCluster amplía la protección de datos de NVRAM de las siguientes formas:

- En una configuración de dos nodos, los datos de la NVRAM se replican mediante los enlaces Inter-Switch (ISL) al compañero remoto.
- En una configuración de par de alta disponibilidad, los datos de NVRAM se replican tanto en el partner local como en el remoto.
- La escritura no se reconoce hasta que se replica a todos los partners. Esta arquitectura protege la I/O en tránsito de fallos del sitio mediante la replicación de los datos de NVRAM en un partner remoto. Este proceso no está relacionado con la replicación de datos a nivel de unidad. La controladora propietaria de los agregados se encarga de la replicación de datos escribiendo en ambos complejos del agregado, pero seguirá habiendo protección contra la pérdida de I/O en tránsito en caso de pérdida del sitio. Los datos de NVRAM replicados solo se utilizan si una controladora asociada debe asumir el relevo de una controladora que ha fallado.

Protección frente a fallos de sitios y bandejas: SyncMirror y complejos

SyncMirror es una tecnología de mirroring que mejora, pero no sustituye, RAID DP ni RAID-TEC. Refleja el contenido de dos grupos RAID independientes. La configuración lógica es la siguiente:

1. Las unidades se configuran en dos pools según la ubicación. Un pool se compone de todas las unidades en el sitio A, y el segundo pool se compone de todas las unidades en el sitio B.
2. A continuación, se crea un pool de almacenamiento común, conocido como agregado, basado en conjuntos reflejados de grupos RAID. Se extrae un número igual de unidades en cada sitio. Por ejemplo, un agregado SyncMirror de 20 unidades estaría compuesto por 10 unidades del sitio A y 10 unidades del sitio B.
3. Cada conjunto de unidades en un sitio determinado se configura automáticamente como uno o varios grupos RAID DP o RAID-TEC completamente redundantes, independientemente del uso de mirroring. Este uso de RAID debajo del mirroring proporciona protección de datos incluso después de la pérdida de un sitio.



La figura anterior muestra una configuración de SyncMirror de ejemplo. Se creó un agregado de 24 unidades en la controladora con 12 unidades de una bandeja asignada en el sitio A y 12 unidades de una bandeja asignada en el sitio B. Las unidades se agruparon en dos grupos RAID reflejados. El grupo RAID 0 incluye un plex de 6 unidades en el sitio A reflejado en un plex de 6 unidades en el sitio B. Del mismo modo, el grupo RAID 1 incluye un plex de 6 unidades en el sitio A, duplicado en un plex de 6 unidades en el sitio B.

Normalmente, SyncMirror se utiliza para proporcionar mirroring remoto con sistemas MetroCluster, con una copia de los datos de cada sitio. En ocasiones, se ha utilizado para proporcionar un nivel adicional de redundancia en un único sistema. En particular, proporciona redundancia a nivel de bandeja. Una bandeja de unidades ya contiene fuentes de alimentación y controladoras duales y en general es poco más que chapa metálica, pero en algunos casos, la protección adicional puede estar garantizada. Por ejemplo, un cliente de NetApp ha puesto en marcha SyncMirror para una plataforma móvil de análisis en tiempo real que se usa durante las pruebas de automoción. El sistema se separó en dos racks físicos suministrados con fuentes de alimentación independientes y sistemas UPS independientes.

Fallo de redundancia: NVFAIL

Como hemos visto anteriormente, la escritura no se reconoce hasta que se haya iniciado sesión en la NVRAM local y NVRAM en al menos otra controladora. Este método garantiza que un fallo de hardware o una interrupción del suministro eléctrico no provoquen la pérdida de operaciones de I/O en tránsito Si la NVRAM local falla o la conectividad a otros nodos falla, los datos ya no se reflejarían.

Si la NVRAM local informa de un error, el nodo se apaga. Este apagado hace que se conmute al nodo de respaldo a la controladora asociada cuando se utilizan pares de alta disponibilidad. Con MetroCluster, el comportamiento depende de la configuración general elegida, pero puede dar lugar a una conmutación automática por error a la nota remota. En cualquier caso, no se pierden datos porque la controladora que experimenta el fallo no reconoció la operación de escritura.

Un fallo de conectividad entre sitios que bloquea la replicación de NVRAM en nodos remotos es una situación más complicada. Las escrituras ya no se replican en los nodos remotos y, de este modo, se crea la posibilidad de perder datos si se produce un error grave en una controladora. Lo que es más importante, si se intenta conmutar a un nodo diferente durante estas condiciones, se pierden datos.

El factor de control es si NVRAM está sincronizada. Si NVRAM está sincronizada, la conmutación al nodo de respaldo nodo a nodo se realizará de forma segura sin riesgo de pérdida de datos. En una configuración de MetroCluster, si la NVRAM y los complejos de agregado subyacentes están sincronizados, es seguro continuar con la conmutación de sitios sin riesgo de pérdida de datos.

ONTAP no permite una conmutación por error o una conmutación cuando los datos no están sincronizados a menos que se fuercen la conmutación por error o la conmutación. Al forzar un cambio en las condiciones de esta manera, se reconoce que los datos podrían dejarse atrás en la controladora original y que la pérdida de datos es aceptable.

Las bases de datos y otras aplicaciones son especialmente vulnerables a las corrupción si se fuerza una conmutación al respaldo o conmutación por error porque mantienen cachés internos más grandes de datos en el disco. Si se produce un failover forzado o un switchover forzado, los cambios previamente reconocidos se descartan efectivamente. El contenido de la cabina de almacenamiento retrocede efectivamente en el tiempo y el estado de la caché ya no refleja el estado de los datos del disco.

Para evitar esta situación, ONTAP permite configurar volúmenes para una protección especial contra un fallo de NVRAM. Cuando se activa, este mecanismo de protección hace que un volumen entre en un estado denominado NVFAIL. Este estado provoca errores de I/O que provocan un bloqueo de la aplicación. Este bloqueo hace que las aplicaciones se cierren para que no utilicen datos obsoletos. No se deben perder los datos porque los datos de transacción confirmados deben estar presentes en los registros. Los siguientes pasos habituales son para que un administrador apague completamente los hosts antes de volver a poner manualmente los LUN y los volúmenes de nuevo en línea. Aunque estos pasos pueden implicar cierto trabajo, este enfoque es la manera más segura de garantizar la integridad de los datos. No todos los datos requieren esta protección, por lo que el comportamiento NVFAIL se puede configurar volumen por volumen.

Pares DE ALTA disponibilidad y MetroCluster

MetroCluster está disponible en dos configuraciones: De dos nodos y de pareja de alta disponibilidad. La configuración de dos nodos se comporta igual que un par de alta disponibilidad con respecto a NVRAM. En caso de que falle repentinamente, el nodo asociado puede reproducir los datos de NVRAM para hacer que las unidades sean coherentes y asegurarse de que no se ha perdido ninguna escritura reconocida.

La configuración de par de alta disponibilidad replica la NVRAM también en el nodo del partner local. Un fallo de controladora sencillo provoca una reproducción de NVRAM en el nodo de partner, como es el caso con un par de alta disponibilidad independiente sin MetroCluster. En caso de pérdida repentina del sitio completo, el sitio remoto también cuenta con la NVRAM necesaria para hacer que las unidades sean coherentes y

empezar a servir datos.

Un aspecto importante de MetroCluster es que los nodos remotos no tienen acceso a los datos de los partners en condiciones operativas normales. Cada sitio funciona esencialmente como un sistema independiente que puede asumir la personalidad del sitio opuesto. Este proceso es conocido como una conmutación de sitios e incluye una conmutación de sitios planificada en la que las operaciones del sitio se migran de forma no disruptiva al sitio opuesto. También incluye situaciones no planificadas en las que se pierde un sitio y se requiere una conmutación por error manual o automática como parte de la recuperación ante desastres.

Conmutación de sitios y conmutación de estado

Los términos conmutación y conmutación de estado hacen referencia al proceso de transición de volúmenes entre controladoras remotas en una configuración de MetroCluster. Este proceso solo se aplica a los nodos remotos. Cuando MetroCluster se utiliza en una configuración de cuatro volúmenes, la conmutación por error de nodo local es el mismo proceso de toma de control y devolución descrito anteriormente.

Conmutación de sitios y conmutación de estado planificadas

Una conmutación de sitios o conmutación de estado planificada es similar a una toma de control o una conmutación al nodo primario entre nodos. El proceso tiene varios pasos y puede parecer que requiere varios minutos, pero lo que en realidad está sucediendo es una transición fluida multifase de los recursos de red y almacenamiento. El momento en que las transferencias de control se producen mucho más rápido que el tiempo necesario para que se ejecute el comando complete.

La principal diferencia entre toma de control/retorno al nodo primario y conmutación/conmutación de estado afecta a la conectividad SAN FC. Con la toma de control/devolución local, un host experimenta la pérdida de todas las rutas de FC hacia el nodo local y depende de su MPIO nativo para cambiar a las rutas alternativas disponibles. Los puertos no se reubican. Con la conmutación de sitios y la conmutación de estado, los puertos de destino FC virtuales en las controladoras se transfieren al otro sitio. De hecho, dejan de existir en la SAN durante un momento y luego vuelven a aparecer en una controladora alternativa.

Tiempo de espera de SyncMirror

SyncMirror es una tecnología de mirroring de ONTAP que proporciona protección contra fallos de bandeja. Cuando las bandejas se separan a lo largo de una distancia, el resultado es la protección de datos remota.

SyncMirror no ofrece mirroring síncrono universal. El resultado es una mejor disponibilidad. Algunos sistemas de almacenamiento utilizan mirroring constante todo o nada, llamado a veces modo domino. Esta forma de mirroring está limitada en la aplicación porque toda la actividad de escritura debe cesarse si se pierde la conexión con el sitio remoto. De lo contrario, una escritura existiría en un sitio, pero no en el otro. Normalmente, estos entornos están configurados para desconectar las LUN si se pierde la conectividad de sitio a sitio durante más de un breve período (como 30 segundos).

Este comportamiento es deseable para un pequeño subconjunto de entornos. Sin embargo, la mayoría de las aplicaciones requieren una solución que ofrezca replicación síncrona garantizada en condiciones de funcionamiento normales, pero con la posibilidad de suspender la replicación. Con frecuencia, se considera una pérdida total de conectividad entre sitios como una situación próxima a un desastre. Normalmente, estos entornos se mantienen online y proporcionan datos hasta que se repare la conectividad o se tome una decisión formal para desactivar el entorno para proteger los datos. Un requisito para el apagado automático de la aplicación solo debido a un fallo de replicación remota es inusual.

SyncMirror admite los requisitos de mirroring síncrono con la flexibilidad de un tiempo de espera agotado. Si se pierde la conectividad con el controlador remoto y/o plex, comienza la cuenta atrás con un temporizador de 30 segundos. Cuando el contador alcanza los 0, el procesamiento de I/O de escritura se reanuda utilizando los datos locales. La copia remota de los datos se puede utilizar, pero se congela en el tiempo hasta que se

restaure la conectividad. La resincronización aprovecha las copias Snapshot de nivel agregado para que el sistema vuelva al modo síncrono lo más rápido posible.

Cabe destacar que, en muchos casos, este tipo de replicación universal modo domino integral se implementa mejor en el nivel de aplicación. Por ejemplo, Oracle DataGuard incluye el modo de protección máxima, que garantiza la replicación de instancias largas en todas las circunstancias. Si el enlace de replicación falla durante un período que supera un tiempo de espera configurable, las bases de datos se cierran.

Cambio automático desatendido con Fabric Attached MetroCluster

La conmutación de sitios automática desatendida (AUSO) es una función MetroCluster conectada a estructuras que ofrece una forma de alta disponibilidad entre sitios. Como hemos visto anteriormente, MetroCluster está disponible en dos tipos: Una sola controladora en cada sitio o un par de alta disponibilidad en cada sitio. La principal ventaja de la opción de alta disponibilidad es que el apagado planificado o no planificado de la controladora sigue permitiendo que todas las operaciones de I/O sean locales. La ventaja de la opción de un único nodo es la reducción de los costes, la complejidad y la infraestructura.

El principal valor de AUSO es mejorar las funciones de alta disponibilidad de los sistemas MetroCluster Fabric Attached. Cada sitio monitorea el estado del sitio opuesto y, si no quedan nodos para servir datos, AUSO da como resultado un cambio rápido. Este método es especialmente útil en configuraciones de MetroCluster con solo un solo nodo por sitio porque acerca la configuración a un par de alta disponibilidad en términos de disponibilidad.

AUSO no puede ofrecer una supervisión completa a nivel de un par de alta disponibilidad. Un par de alta disponibilidad puede proporcionar una disponibilidad extremadamente alta porque incluye dos cables físicos redundantes para una comunicación directa entre nodos. Además, ambos nodos de un par de alta disponibilidad tienen acceso al mismo conjunto de discos en bucles redundantes, lo cual proporciona otra ruta para un nodo para supervisar el estado de otro.

Los clústeres de MetroCluster existen en todos los sitios en los que tanto la comunicación nodo a nodo como el acceso a disco dependen de la conectividad de red sitio a sitio. La capacidad de supervisar los latidos del resto del clúster es limitada. AUSO tiene que discriminar entre una situación en la que el otro sitio está realmente inactivo en lugar de no disponible debido a un problema de red.

Como resultado, una controladora de un par de alta disponibilidad puede emitir una toma de control si detecta un fallo de controladora que se produjo por un motivo específico, como un motivo de pánico en el sistema. También puede solicitar una toma de control si hay una pérdida completa de conectividad, a veces conocida como latido del corazón perdido.

Un sistema MetroCluster solo puede realizar de forma segura una conmutación automática cuando se detecta una falla específica en el sitio original. Además, la controladora que tome la propiedad del sistema de almacenamiento debe poder garantizar que los datos del disco y NVRAM estén sincronizados. El controlador no puede garantizar la seguridad de un cambio solo porque perdió el contacto con el sitio de origen, que podría estar operativo. Para ver opciones adicionales para automatizar una conmutación de sitios, consulte la información sobre la solución tiebreaker de MetroCluster (MCTB) en la siguiente sección.

Tiebreaker de MetroCluster con MetroCluster estructural

"Tiebreaker de NetApp MetroCluster"El software puede ejecutarse en un tercer sitio para supervisar el estado del entorno de MetroCluster, enviar notificaciones y, opcionalmente, forzar una conmutación de sitios en caso de desastre. Puede encontrar una descripción completa del tiebreaker en la "Sitio de soporte de NetApp", pero el principal objetivo de MetroCluster tiebreaker es detectar la pérdida de sitios. También debe discriminar entre la pérdida del sitio y una pérdida de conectividad. Por ejemplo, la conmutación de sitios no debería ocurrir porque el tiebreaker no pudo llegar al sitio principal, por este motivo, tiebreaker también supervisa la capacidad del sitio remoto para comunicarse con el sitio principal.

El cambio automático con AUSO también es compatible con el MCTB. AUSO reacciona muy rápidamente porque está diseñado para detectar eventos de fallo específicos y luego invocar la conmutación de sitios solo cuando NVRAM y SyncMirror plexes están sincronizados.

Por el contrario, el desempate se encuentra de forma remota y, por lo tanto, debe esperar a que transcurra un temporizador antes de declarar un sitio muerto. El tiebreaker eventualmente detecta el tipo de fallo de la controladora cubierto por AUSO, pero en general AUSO ya ha iniciado la conmutación y posiblemente completado la conmutación antes de que actúe el tiebreaker. Se rechazaría el segundo comando de switchover resultante procedente del tiebreaker.

El software MCTB no verifica que NVRAM WAS y/o los plexes estén sincronizados al forzar un switchover. La conmutación de sitios automática, si se configura, se debe deshabilitar durante actividades de mantenimiento que ocasionen la pérdida de sincronización para complejos de NVRAM o SyncMirror.

Además, es posible que el MCTB no solucione un desastre que lleve a la siguiente secuencia de eventos:

1. La conectividad entre sitios se interrumpe durante más de 30 segundos.
2. Se agota el tiempo de espera de la replicación de SyncMirror y las operaciones continúan en el sitio principal, dejando la réplica remota obsoleta.
3. Se pierde el sitio principal.El resultado es la presencia de cambios no replicados en el sitio principal. Una conmutación de sitios puede ser indeseable por varios motivos, entre los que se incluyen los siguientes:
   - Pueden haber datos cruciales en el sitio principal y esos datos podrían ser recuperables en algún momento. Un cambio que permitiera a la aplicación seguir funcionando descartaría esos datos cruciales.
   - Una aplicación del sitio superviviente que utilizaba recursos de almacenamiento en el sitio principal en el momento de la pérdida del sitio podría haber almacenado datos en caché. Un switchover introduciría una versión obsoleta de los datos que no coincide con la caché.
   - Un sistema operativo del sitio superviviente que utilizaba recursos de almacenamiento en el sitio principal en el momento de la pérdida del sitio podría haber almacenado los datos en caché. Un switchover introduciría una versión obsoleta de los datos que no coincide con la caché. La opción más segura es configurar el tiebreaker para que envíe una alerta si detecta un fallo del sitio y luego hacer que una persona tome una decisión sobre si forzar un cambio. Es posible que las aplicaciones o los sistemas operativos deban apagarse primero para borrar cualquier dato almacenado en caché. Además, la configuración NVFAIL puede usarse para agregar más protección y ayudar a simplificar el proceso de conmutación por error.

Mediador ONTAP con MetroCluster IP

El Mediador ONTAP se utiliza con MetroCluster IP y otras soluciones ONTAP. Funciona como un servicio tradicional de tiebreaker, al igual que el software MetroCluster tiebreaker de referencia anteriormente, pero también incluye una característica crítica, con la posibilidad de realizar una conmutación de sitios automatizada sin supervisión.

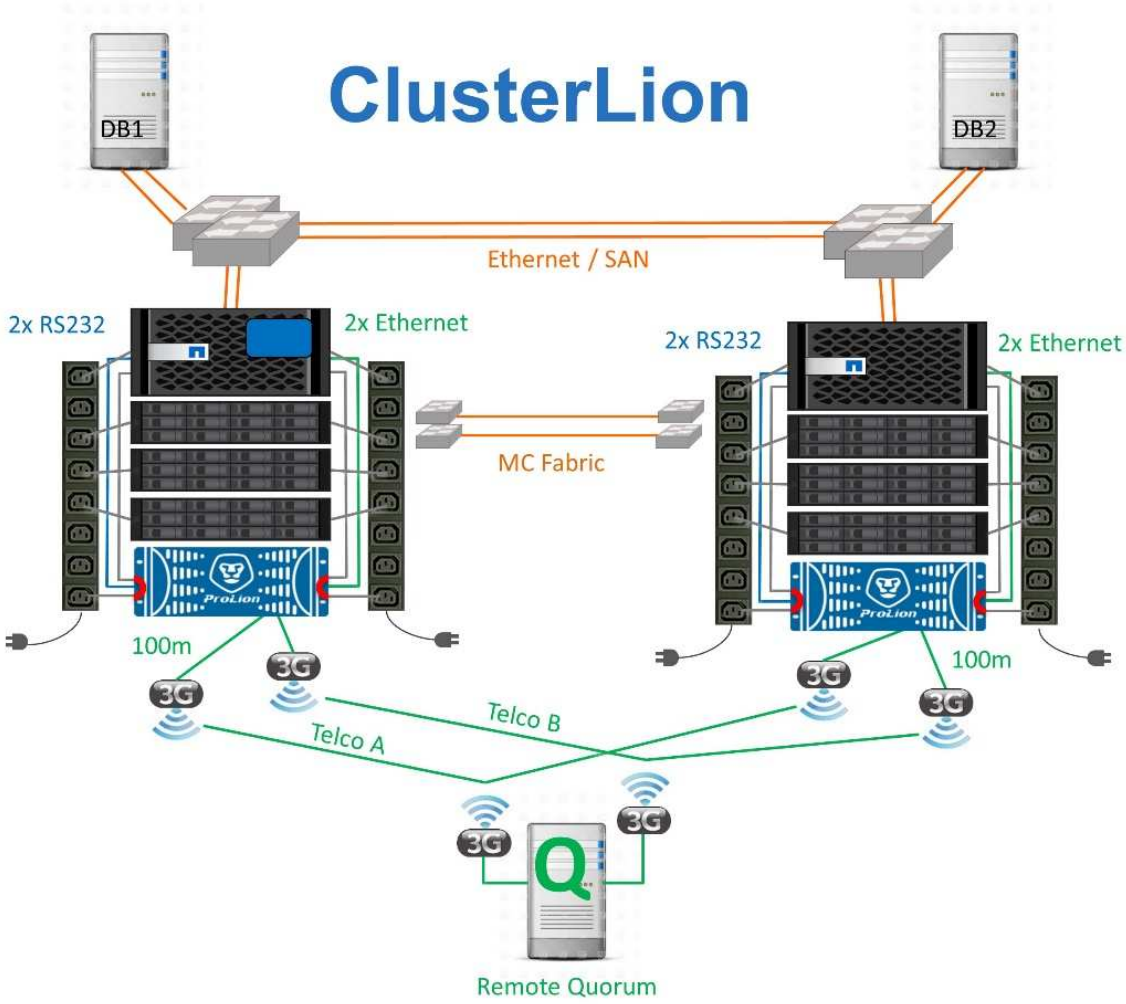
Una MetroCluster conectada a estructura tiene acceso directo a dispositivos de almacenamiento en el sitio opuesto. Esto permite que una controladora MetroCluster supervise el estado de las otras controladoras mediante la lectura de datos de latidos de las unidades. Esto permite que una controladora reconozca el fallo de otra controladora y realizar una conmutación por error.

Por el contrario, la arquitectura IP de MetroCluster enruta todas las I/O de forma exclusiva a través de la conexión del controlador; no hay acceso directo a los dispositivos de almacenamiento en el sitio remoto. Esto limita la capacidad de un controlador para detectar fallos y realizar una conmutación de sitios. Por lo tanto, el

Mediador de ONTAP es necesario como dispositivo tiebreaker para detectar la pérdida del sitio y realizar automáticamente una conmutación.

Tercer sitio virtual con ClusterLion

ClusterLion es un dispositivo de supervisión MetroCluster avanzado que funciona como un tercer sitio virtual. Este enfoque permite implementar MetroCluster de forma segura en una configuración de dos sitios con capacidad de conmutación de sitios totalmente automatizada. Además, ClusterLion puede realizar una supervisión de nivel de red adicional y ejecutar operaciones posteriores a la conmutación. La documentación completa está disponible en ProLion.



- Los dispositivos ClusterLion supervisan el estado de las controladoras con cables Ethernet y serie conectados directamente.
- Los dos aparatos están conectados entre sí con conexiones inalámbricas redundantes de 3G.
- La alimentación al controlador ONTAP se dirige a través de relés internos. En caso de un fallo del sitio, ClusterLion, que contiene un sistema UPS interno, corta las conexiones de alimentación antes de invocar un cambio. Este proceso garantiza que no se produzca ninguna condición cerebral dividida.
- ClusterLion realiza un switchover dentro del tiempo de espera de SyncMirror de 30 segundos o no lo hace en absoluto.
- ClusterLion no realiza una conmutación de sitios a menos que los estados de NVRAM y los complejos SyncMirror estén sincronizados.

- Dado que ClusterLion solo realiza una operación de switchover si MetroCluster está totalmente sincronizado, no es necesario NVFAIL. Esta configuración permite que los entornos de expansión de sitios, como un Oracle RAC ampliado, permanezcan en línea, incluso durante una conmutación de sitios no planificada.
- El soporte incluye MetroCluster FAS e MetroCluster IP

SyncMirror

La base de la protección de datos de Oracle con un sistema MetroCluster es SyncMirror, una tecnología de mirroring síncrono de escalado horizontal y máximo rendimiento.

Protección de datos con SyncMirror

En el nivel más sencillo, la replicación síncrona implica que se debe realizar cualquier cambio en ambas partes del almacenamiento reflejado antes de que se reconozca. Por ejemplo, si una base de datos está escribiendo un registro o se está aplicando la revisión a un invitado VMware, no se debe perder nunca una escritura. Como nivel de protocolo, el sistema de almacenamiento no debe reconocer la escritura hasta que se haya comprometido a medios no volátiles en ambos sitios. Solo entonces es seguro proceder sin el riesgo de pérdida de datos.

El uso de una tecnología de replicación síncrona es el primer paso para diseñar y gestionar una solución de replicación síncrona. Lo más importante es comprender qué podría suceder durante varios escenarios de fallos planificados y no planificados. No todas las soluciones de replicación síncrona ofrecen las mismas funcionalidades. Si necesita una solución que proporcione un objetivo de punto de recuperación (RPO) de cero, lo que significa cero pérdida de datos, deben tenerse en cuenta todos los escenarios de fallo. En particular, ¿cuál es el resultado esperado cuando la replicación es imposible debido a la pérdida de conectividad entre sitios?

Disponibilidad de datos SyncMirror

La replicación de MetroCluster se basa en la tecnología de NetApp SyncMirror, que se ha diseñado para alternar eficientemente entre el modo síncrono y este se sale de él. Esta funcionalidad satisface los requisitos de los clientes que demandan replicación síncrona pero que también necesitan una alta disponibilidad para sus servicios de datos. Por ejemplo, si la conectividad con un sitio remoto se interrumpe, generalmente es preferible que el sistema de almacenamiento siga funcionando en un estado sin replicar.

Muchas soluciones de replicación síncrona solo pueden funcionar en modo síncrono. Este tipo de replicación compuesta por todos o nada se denomina a veces modo domino. Este tipo de sistemas de almacenamiento dejan de servir datos en lugar de permitir que las copias locales y remotas de datos se dessincronicen. Si la replicación se interrumpe de forma forzada, la resincronización puede requerir mucho tiempo y puede dejar al cliente expuesto a la pérdida de datos durante el tiempo que se restablece el mirroring.

SyncMirror no solo puede salir del modo síncrono sin problemas si no se puede acceder al sitio remoto, sino que también puede volver a sincronizar rápidamente con un estado RPO = 0 cuando se restaura la conectividad. La copia obsoleta de los datos en el sitio remoto también se puede conservar en estado utilizable durante la resincronización, lo que garantiza la existencia de copias locales y remotas de los datos en todo momento.

Cuando se requiere el modo domino, NetApp ofrece SnapMirror síncrono (SM-S). También existen opciones de nivel de aplicación, como Oracle DataGuard o SQL Server, grupos de disponibilidad Always On. El mirroring de discos a nivel de sistema operativo puede ser una opción. Consulte con su equipo de cuentas de partner o de NetApp para obtener más información y opciones.

MetroCluster y NVFAIL

NVFAIL es una función general de integridad de los datos en ONTAP que se ha diseñado para maximizar la protección de la integridad de los datos con las bases de datos.

En esta sección se amplía la explicación del NVFAIL básico de ONTAP para tratar temas específicos de MetroCluster.

Con MetroCluster, no se reconoce la escritura hasta que se haya iniciado sesión en la NVRAM y NVRAM locales en al menos otra controladora. Este método garantiza que un fallo de hardware o una interrupción del suministro eléctrico no provoquen la pérdida de operaciones de I/O en tránsito Si la NVRAM local falla o la conectividad a otros nodos falla, los datos ya no se reflejarían.

Si la NVRAM local informa de un error, el nodo se apaga. Este apagado hace que se conmute al nodo de respaldo a la controladora asociada cuando se utilizan pares de alta disponibilidad. Con MetroCluster, el comportamiento depende de la configuración general elegida, pero puede dar lugar a una conmutación automática por error a la nota remota. En cualquier caso, no se pierden datos porque la controladora que experimenta el fallo no reconoció la operación de escritura.

Un fallo de conectividad entre sitios que bloquea la replicación de NVRAM en nodos remotos es una situación más complicada. Las escrituras ya no se replican en los nodos remotos y, de este modo, se crea la posibilidad de perder datos si se produce un error grave en una controladora. Lo que es más importante, si se intenta conmutar a un nodo diferente durante estas condiciones, se pierden datos.

El factor de control es si NVRAM está sincronizada. Si NVRAM está sincronizada, la conmutación al nodo de respaldo nodo a nodo se realizará de forma segura sin riesgo de pérdida de datos. En una configuración de MetroCluster, si la NVRAM y los complejos de agregado subyacentes están sincronizados, es seguro continuar con la conmutación sin el riesgo de perder los datos.

ONTAP no permite una conmutación por error o una conmutación cuando los datos no están sincronizados a menos que se fuercen la conmutación por error o la conmutación. Al forzar un cambio en las condiciones de esta manera, se reconoce que los datos podrían dejarse atrás en la controladora original y que la pérdida de datos es aceptable.

Las bases de datos son especialmente vulnerables a los daños si se fuerza una conmutación por error o una conmutación por error porque las bases de datos mantienen cachés internos mayores de los datos en el disco. Si se produce un failover forzado o un switchover forzado, los cambios previamente reconocidos se descartan efectivamente. El contenido de la cabina de almacenamiento retrocede efectivamente en el tiempo y el estado de la caché de base de datos ya no refleja el estado de los datos del disco.

Para proteger aplicaciones contra esta situación, ONTAP permite configurar volúmenes para obtener protección especial contra un fallo NVRAM. Cuando se activa, este mecanismo de protección hace que un volumen entre en un estado denominado NVFAIL. Este estado provoca errores de I/O que provocan el cierre de la aplicación para que no utilicen datos obsoletos. No se deben perder los datos, ya que aún hay escrituras reconocidas en el sistema de almacenamiento y, con bases de datos, todos los datos de transacciones confirmados deben estar presentes en los registros.

Los siguientes pasos habituales son para que un administrador apague completamente los hosts antes de volver a poner manualmente los LUN y los volúmenes de nuevo en línea. Aunque estos pasos pueden implicar cierto trabajo, este enfoque es la manera más segura de garantizar la integridad de los datos. No todos los datos requieren esta protección, por lo que el comportamiento NVFAIL se puede configurar volumen por volumen.

NVFAIL forzado manualmente

La opción más segura para forzar una conmutación por error con un clúster de aplicaciones (incluido VMware, Oracle RAC y otros) que se distribuye entre los sitios es especificar `-force-nvfail-all` en la línea de comandos. Esta opción está disponible como medida de emergencia para garantizar que todos los datos almacenados en caché están vaciados. Si un host utiliza recursos de almacenamiento ubicados originalmente en el sitio afectado por desastres, recibirá errores de I/O o un identificador de archivos obsoleto (`ESTALE`) error. Las bases de datos de Oracle se bloquean y los sistemas de archivos se desconectan por completo o cambian al modo de sólo lectura.

Una vez finalizada la operación de switchover, el `in-nvfailed-state` La marca debe borrarse y las LUN deben colocarse en línea. Una vez finalizada esta actividad, se puede reiniciar la base de datos. Estas tareas se pueden automatizar para reducir el RTO.

dr-force-nvfail

Como medida de seguridad general, configure el `dr-force-nvfail` marque todos los volúmenes a los que se pueda acceder desde un sitio remoto durante las operaciones normales, lo que significa que se deben usar antes de la conmutación al respaldo. El resultado de esta configuración es que la selección de volúmenes remotos deja de estar disponible cuando se introducen `in-nvfailed-state` durante una conmutación de sitios. Una vez finalizada la operación de switchover, el `in-nvfailed-state` La marca debe borrarse y las LUN deben colocarse en línea. Una vez finalizadas estas actividades, se pueden reiniciar las aplicaciones. Estas tareas se pueden automatizar para reducir el RTO.

El resultado es como usar el `-force-nvfail-all` indicador para conmutadores manuales. Sin embargo, la cantidad de volúmenes afectados puede limitarse a solo los volúmenes que deben protegerse de aplicaciones o sistemas operativos que tienen caché anticuada.

Hay dos requisitos críticos para un entorno que no utiliza `dr-force-nvfail` en volúmenes de aplicaciones:

- Una conmutación de sitios forzada no debe ocurrir más de 30 segundos después de la pérdida del sitio principal.
- Una conmutación de sitios no debe producirse durante las tareas de mantenimiento ni ninguna otra condición en la que los plexes de SyncMirror o la replicación de NVRAM no estén sincronizados. El primer requisito se puede cumplir con el uso de un software tiebreaker configurado para realizar una conmutación de sitios en un plazo de 30 segundos tras un fallo del sitio. Este requisito no significa que el cambio deba realizarse dentro de los 30 segundos posteriores a la detección de un fallo del centro. Esto significa que ya no es seguro forzar un cambio si han transcurrido 30 segundos desde que se confirmó que un sitio está operativo.

El segundo requisito se puede cumplir parcialmente deshabilitando todas las funcionalidades de conmutación automática de sitios cuando se sabe que la configuración de MetroCluster está fuera de sincronización. Mejor opción sería tener una solución tiebreaker que pueda supervisar el estado de la replicación de NVRAM y los plexes de SyncMirror. Si el clúster no está completamente sincronizado, tiebreaker no debería activar una conmutación de sitios.

El software NetApp MCTB no puede supervisar el estado de sincronización, por lo que debe desactivarse cuando MetroCluster no está sincronizado por cualquier motivo. ClusterLion incluye funcionalidades de supervisión de NVRAM y supervisión plex, y se puede configurar para no activar la conmutación de sitios a menos que se haya confirmado que el sistema MetroCluster está totalmente sincronizado.

Instancia única de Oracle

Como se indicó anteriormente, la presencia de un sistema MetroCluster no necesariamente agrega ni cambia ninguna práctica recomendada para el funcionamiento de una base de datos. La mayoría de las bases de datos que se ejecutan actualmente en los sistemas MetroCluster del cliente son de única instancia y sigue las recomendaciones de la documentación de Oracle en ONTAP.

Conmutación al nodo de respaldo con un SO preconfigurado

SyncMirror ofrece una copia síncrona de los datos del sitio de recuperación de desastres, pero para que los datos estén disponibles, requiere un sistema operativo y las aplicaciones asociadas. La automatización básica puede mejorar drásticamente el tiempo de conmutación al nodo de respaldo del entorno global. Los productos de Clusterware, como Veritas Cluster Server (VCS), se utilizan a menudo para crear un clúster en todos los sitios y, en muchos casos, el proceso de conmutación por error se puede llevar a cabo con scripts sencillos.

Si se pierden los nodos primarios, el clusterware (o scripts) se configura para poner las bases de datos en línea en el sitio alternativo. Una opción es crear servidores en espera que estén preconfigurados para los recursos NFS o SAN que componen la base de datos. Si el sitio principal falla, el clusterware o la alternativa con secuencia de comandos realiza una secuencia de acciones similar a las siguientes:

1. Forzar un cambio de MetroCluster
2. Detección de LUN FC (solo SAN)
3. Montaje de sistemas de archivos y/o montaje de grupos de discos ASM
4. Iniciando la base de datos

El requisito principal de este método es un sistema operativo en ejecución instalado en el sitio remoto. Se debe preconfigurar con binarios de Oracle, lo que también significa que las tareas como los parches de Oracle se deben realizar en la ubicación primaria y en espera. Como alternativa, los binarios de Oracle se pueden duplicar en la ubicación remota y montar si se declara un desastre.

El procedimiento de activación real es simple. Los comandos como la detección de LUN sólo requieren unos pocos comandos por puerto FC. El montaje del sistema de archivos no es más que un `mount` Y tanto las bases de datos como ASM se pueden iniciar y parar en la CLI con un único comando. Si los volúmenes y los sistemas de archivos no se están utilizando en el sitio de recuperación de desastres antes de la conmutación de sitios, no es necesario establecerlos `dr-force- nvfail` en los volúmenes.

Conmutación por error con un sistema operativo virtualizado

La conmutación por error de los entornos de base de datos puede ampliarse para incluir el propio sistema operativo. En teoría, esta recuperación tras fallos se puede realizar con las LUN de arranque, pero la mayoría de las veces se realiza con un sistema operativo virtualizado. El procedimiento es similar a los siguientes pasos:

1. Forzar un cambio de MetroCluster
2. Montar los almacenes de datos que alojan las máquinas virtuales del servidor de bases de datos
3. Inicio de las máquinas virtuales
4. Iniciar bases de datos manualmente o configurar las máquinas virtuales para iniciar automáticamente las bases de datos, por ejemplo, un clúster ESX puede abarcar varios sitios. En caso de desastre, los equipos virtuales pueden conectarse en línea en el sitio de recuperación ante desastres después del cambio. Mientras los almacenes de datos que alojan los servidores de bases de datos virtualizadas no estén en

uso en el momento del desastre, no es necesario configurarlos `dr-force- nvfail` en los volúmenes asociados.

Oracle Extended RAC

Muchos clientes optimizan su objetivo de tiempo de recuperación al ampliar un clúster de Oracle RAC en todos los sitios, lo que proporciona una configuración completamente activo-activo. El diseño general se complica porque debe incluir la gestión de quórum de Oracle RAC. Además, se accede a los datos desde ambos sitios, lo que significa que una conmutación por error forzada puede provocar el uso de una copia desactualizada de los datos.

Aunque se encuentra una copia de los datos en ambos sitios, solo la controladora que actualmente posee un agregado puede servir datos. Por lo tanto, con clústeres RAC ampliados, los nodos remotos deben ejecutar operaciones de I/O a través de una conexión de sitio a sitio. El resultado es una latencia de I/O añadida, pero esta latencia no suele ser un problema. La red de interconexión de RAC también debe extenderse entre sitios, lo que significa que se necesita una red de alta velocidad y baja latencia de todos modos. Si la latencia añadida provoca un problema, el clúster se puede operar de una forma activa-pasiva. Luego, las operaciones con un gran volumen de I/O deben dirigirse a los nodos de RAC locales a la controladora propietaria de los agregados. A continuación, los nodos remotos realizan operaciones de E/S más ligeras o se utilizan únicamente como servidores de espera templados.

Si se requiere un RAC extendido activo-activo, se debe considerar la sincronización activa de SnapMirror en lugar de MetroCluster. La replicación de SM-AS permite que se prefiera una réplica específica de los datos. Por lo tanto, se puede crear un clúster RAC ampliado en el que todas las lecturas se realicen localmente. La I/O de lectura nunca se cruza con los sitios, lo que ofrece la menor latencia posible. Toda la actividad de escritura debe seguir transfiriendo la conexión entre sitios, pero dicho tráfico es inevitable con cualquier solución de mirroring síncrono.

> Si se utilizan LUN de inicio, incluidos los discos de inicio virtualizados, con Oracle RAC, es posible que el `misscount` parámetro deba cambiarse. Para obtener más información sobre los parámetros de timeout de RAC, consulte "Oracle RAC con ONTAP".

Configuración de dos sitios

Una configuración de RAC ampliada de dos sitios puede ofrecer servicios de base de datos activa-activa que pueden sobrevivir muchos escenarios de desastres de forma no disruptiva, pero no todos.

Archivos de quorum de RAC

La primera consideración al implementar RAC ampliado en MetroCluster debe ser la gestión del quórum. Oracle RAC tiene dos mecanismos para gestionar el quórum: Latido de disco y latido de red. El latido del disco supervisa el acceso al almacenamiento mediante los archivos de votación. Con una configuración de RAC de un único sitio, un único recurso de votación es suficiente siempre que el sistema de almacenamiento subyacente ofrezca funcionalidades de alta disponibilidad.

En versiones anteriores de Oracle, los archivos de quorum se colocaban en dispositivos de almacenamiento físico, pero en las versiones actuales de Oracle los archivos de quorum se almacenan en grupos de discos de ASM.

Oracle RAC es compatible con NFS. Durante el proceso de instalación de grid, se crea un juego de procesos de ASM para presentar la ubicación NFS utilizada para los archivos de grid como un grupo de discos de ASM. El proceso es prácticamente transparente para el usuario final y no requiere una gestión de ASM en curso una vez finalizada la instalación.

El primer requisito de una configuración de dos ubicaciones es asegurarse de que cada sitio siempre pueda acceder a más de la mitad de los archivos de votación de forma que se garantice un proceso de recuperación ante desastres sin interrupciones. Esta tarea era sencilla antes de que los archivos de votación se almacenaran en grupos de discos de ASM, pero hoy en día los administradores necesitan comprender los principios básicos de la redundancia de ASM.

Los grupos de discos de ASM tienen tres opciones de redundancia `external`, `normal`, y. `high`. En otras palabras, se refleja en 3 direcciones y no reflejado. Una opción más reciente llamada `Flex` también está disponible, pero rara vez se utiliza. El nivel de redundancia y la ubicación de los dispositivos redundantes controlan lo que sucede en escenarios de fallo. Por ejemplo:

- Colocación de los archivos de votación en un `diskgroup` con `external` los recursos de redundancia garantizan el desalojo de un sitio si se pierde la conectividad entre sitios.
- Colocación de los archivos de votación en un `diskgroup` con `normal` La redundancia con un solo disco ASM por sitio garantiza la expulsión de nodos en ambas ubicaciones si se pierde la conectividad entre sitios porque ninguno de los sitios tendría un quórum mayoritario.
- Colocación de los archivos de votación en un `diskgroup` con `high` la redundancia con dos discos en un sitio y un solo disco en el otro sitio permite las operaciones activo-activo cuando ambos sitios están operativos y se puede acceder mutuamente. Sin embargo, si el sitio de un solo disco está aislado de la red, ese sitio se expulsa.

Latido de red RAC

El latido de red de Oracle RAC supervisa la accesibilidad de nodos en la interconexión de cluster. Para permanecer en el clúster, un nodo debe ser capaz de contactar más de la mitad de los otros nodos. En una arquitectura de dos sitios, este requisito crea las siguientes opciones para el recuento de nodos de RAC:

- La colocación de un número igual de nodos por sitio provoca el expulsión en un sitio en caso de que se pierda la conectividad de red.
- La colocación de los nodos N en un sitio y los nodos N+1 en el sitio opuesto garantiza que la pérdida de conectividad entre sitios da lugar al sitio con el mayor número de nodos restantes en el quórum de red y el sitio con menos nodos expulsados.

Antes de Oracle 12cR2, no era posible controlar qué lado experimentaría un desalojo durante la pérdida del sitio. Cuando cada ubicación tiene el mismo número de nodos, el nodo maestro controla la expulsión, que en general es el primer nodo RAC que se inicia.

Oracle 12cR2 introduce la capacidad de ponderación de nodos. Esta capacidad proporciona al administrador más control sobre cómo Oracle resuelve las condiciones de cerebro dividido. Como ejemplo sencillo, el siguiente comando establece la preferencia de un nodo concreto en un RAC:

```
[root@host-a ~]# /grid/bin/crsctl set server css_critical yes
CRS-4416: Server attribute 'CSS_CRITICAL' successfully changed. Restart
Oracle High Availability Services for new value to take effect.
```

Después de reiniciar Oracle High-Availability Services, la configuración tiene el siguiente aspecto:

```
[root@host-a lib]# /grid/bin/crsctl status server -f | egrep
'^NAME|CSS_CRITICAL='
NAME=host-a
CSS_CRITICAL=yes
NAME=host-b
CSS_CRITICAL=no
```

Nodo `host-a` ahora se designa como servidor crítico. Si los dos nodos de RAC están aislados, `host-a` sobrevive, y. `host-b` se expulsa.

Para obtener más información, consulte el white paper de Oracle sobre Oracle Clusterware 12c Versión 2 Technical Overview. ”

Para las versiones de Oracle RAC anteriores a 12cR2, el nodo maestro se puede identificar comprobando los logs de CRS de la siguiente manera:

```
[root@host-a ~]# /grid/bin/crsctl status server -f | egrep
'^NAME|CSS_CRITICAL='
NAME=host-a
CSS_CRITICAL=yes
NAME=host-b
CSS_CRITICAL=no
 [root@host-a ~]# grep -i 'master node' /grid/diag/crs/host-
a/crs/trace/crsd.trc
2017-05-04 04:46:12.261525 :   CRSSE:2130671360: {1:16377:2} Master Change
Event; New Master Node ID:1 This Node's ID:1
2017-05-04 05:01:24.979716 :   CRSSE:2031576832: {1:13237:2} Master Change
Event; New Master Node ID:2 This Node's ID:1
2017-05-04 05:11:22.995707 :   CRSSE:2031576832: {1:13237:221} Master
Change Event; New Master Node ID:1 This Node's ID:1
2017-05-04 05:28:25.797860 :   CRSSE:3336529664: {1:8557:2} Master Change
Event; New Master Node ID:2 This Node's ID:1
```

Este log indica que el nodo maestro es `2` y el nodo `host-a` Tiene un ID de `1`. Este hecho significa eso `host-a` no es el nodo maestro. La identidad del nodo maestro se puede confirmar con el comando `olsnodes -n`.

```
[root@host-a ~]# /grid/bin/olsnodes -n
host-a  1
host-b  2
```

El nodo con un ID de `2` es `host-b`, que es el nodo maestro. En una configuración con el mismo número de nodos en cada sitio, el sitio con `host-b` es el sitio que sobrevive si los dos conjuntos pierden la conectividad

de red por cualquier motivo.

Es posible que la entrada de log que identifica el nodo maestro pueda quedar obsoleta en el sistema. En esta situación, se pueden utilizar las marcas de tiempo de las copias de seguridad de Oracle Cluster Registry (OCR).

```
[root@host-a ~]#  /grid/bin/ocrconfig -showbackup
host-b     2017/05/05 05:39:53     /grid/cdata/host-cluster/backup00.ocr
0
host-b     2017/05/05 01:39:53     /grid/cdata/host-cluster/backup01.ocr
0
host-b     2017/05/04 21:39:52     /grid/cdata/host-cluster/backup02.ocr
0
host-a     2017/05/04 02:05:36     /grid/cdata/host-cluster/day.ocr     0
host-a     2017/04/22 02:05:17     /grid/cdata/host-cluster/week.ocr     0
```

En este ejemplo se muestra que el nodo maestro es `host-b`. También indica un cambio en el nodo maestro desde `host-a` para `host-b` En algún lugar entre las 2:05 y las 21:39 el 4 de mayo. Este método de identificación del nodo maestro sólo es seguro si también se han comprobado los registros de CRS porque es posible que el nodo maestro haya cambiado desde la copia de seguridad de OCR anterior. Si se ha producido este cambio, debería estar visible en los registros de OCR.

La mayoría de los clientes eligen un único grupo de discos de votación que da servicio a todo el entorno y un número igual de nodos de RAC en cada sitio. El grupo de discos se debe colocar en el sitio que contiene la base de datos. El resultado es que la pérdida de conectividad provoca el desalojo en el sitio remoto. El sitio remoto ya no tendría quórum ni tendría acceso a los archivos de la base de datos, pero el sitio local continúa funcionando como de costumbre. Cuando se restaura la conectividad, la instancia remota puede volver a conectarse.

En caso de desastre, se requiere un cambio para poner los archivos de la base de datos y el grupo de discos de votación en línea en el sitio superviviente. Si el desastre permite que AUSO active la conmutación por error, NVFAIL no se activa porque se sabe que el clúster está sincronizado y que los recursos de almacenamiento se conectan de forma normal. AUSO es una operación muy rápida y debe completarse antes de la `disktimeout` el período caduca.

Dado que solo hay dos sitios, no es factible utilizar ningún tipo de software automatizado de tiebreaking externo, lo que significa que la conmutación por error forzada debe ser una operación manual.

Configuraciones en tres sitios

Un clúster RAC ampliado es mucho más fácil de diseñar con tres sitios. Los dos sitios que alojan cada mitad del sistema de MetroCluster también admiten cargas de trabajo de base de datos, mientras que el tercer sitio sirve como desempate tanto para la base de datos como para el sistema de MetroCluster. La configuración de Oracle tiebreaker puede ser tan sencilla como colocar un miembro del grupo de discos de ASM utilizado para votar en un sitio 3rd y también puede incluir una instancia operativa en el sitio 3rd para asegurarse de que hay un número impar de nodos en el cluster RAC.

Consulte la documentación de Oracle sobre el “grupo de fallos de quórum” para obtener información importante sobre el uso de NFS en una configuración RAC ampliada. En resumen, puede que sea necesario modificar las opciones de montaje NFS para incluir la opción soft para garantizar que la pérdida de conectividad con los recursos de quórum del sitio de 3rd que alojan no cuelgue los servidores Oracle principales ni los procesos de Oracle RAC.

SnapMirror síncrono activo

Descripción general

SnapMirror Active Sync le permite crear entornos de base de datos de Oracle de alta disponibilidad donde los LUN están disponibles desde dos clústeres de almacenamiento diferentes.

Con la sincronización activa de SnapMirror, no hay copias «primarias» ni «secundarias» de los datos. Cada clúster puede servir de I/O de lectura a partir de su copia local de los datos y cada clúster replicará una escritura en su compañero. El resultado es un comportamiento de E/S simétrico.

Entre otras opciones, esto permite ejecutar Oracle RAC como un cluster ampliado con instancias operativas en ambas ubicaciones. También podría crear un RPO=0 clusters de bases de datos activo-pasivo en los que las bases de datos de una instancia única se puedan mover de un sitio a otro durante una interrupción del servicio. Este proceso puede automatizarse mediante productos como Pacemaker o VMware HA. La base de todas estas opciones es la replicación síncrona gestionada por SnapMirror Active Sync.

Replicación síncrona

En un funcionamiento normal, la sincronización activa de SnapMirror proporciona una réplica síncrona con un objetivo de punto de recuperación=0 en todo momento, con una excepción. Si los datos no se pueden replicar, ONTAP liberará el requisito para replicar datos y reanudar el servicio de I/O en un sitio mientras las LUN del otro sitio se desconecten.

Hardware de almacenamiento

Al contrario que otras soluciones de recuperación ante desastres del almacenamiento, SnapMirror Active Sync ofrece una flexibilidad de plataforma asimétrica. No es necesario que el hardware de cada sitio sea idéntico. Esta funcionalidad permite ajustar el tamaño adecuado del hardware que se utiliza para dar soporte a SnapMirror de sincronización activa. El sistema de almacenamiento remoto puede ser idéntico al sitio principal si necesita soportar una carga de trabajo de producción completa, pero si un desastre provoca una reducción de I/O, es posible que un sistema más pequeño en el sitio remoto sea más rentable.

Mediador ONTAP

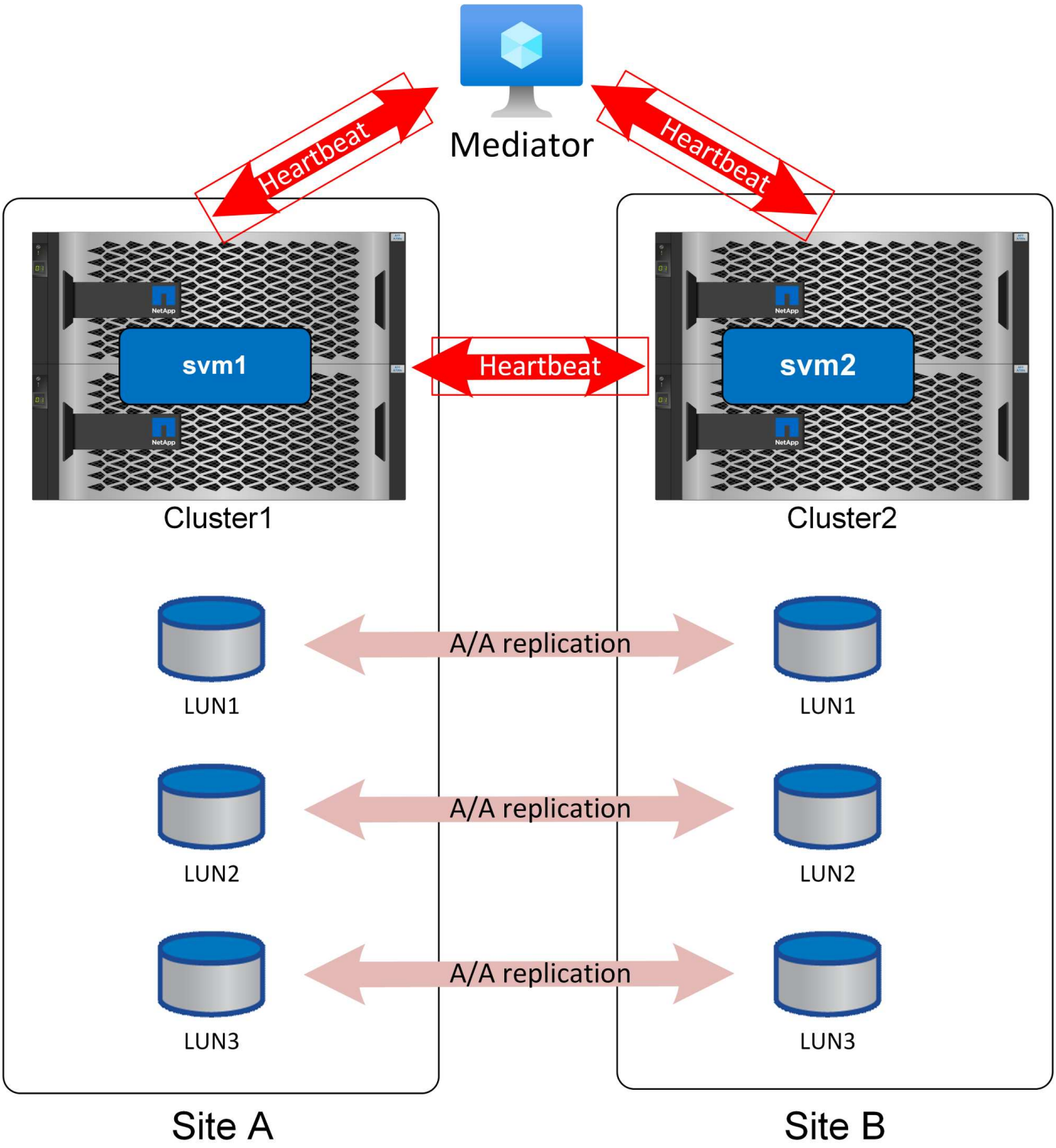
ONTAP Mediator es una aplicación de software que se descarga del soporte técnico de NetApp y que normalmente se implementa en una pequeña máquina virtual. ONTAP Mediator no es un tiebreaker cuando se utiliza con SnapMirror sincronización activa. Es un canal de comunicación alternativo para los dos clústeres que participan en la replicación síncrona activa de SnapMirror. Las operaciones automatizadas son impulsadas por ONTAP en función de las respuestas recibidas del partner a través de conexiones directas y a través del mediador.

Mediador ONTAP

El mediador es necesario para automatizar la conmutación por error de forma segura. Lo ideal sería que se ubicara en un sitio 3rd independiente, pero todavía puede funcionar

para la mayoría de las necesidades si se ubicara con uno de los clústeres que participan en la replicación.

El mediador no es realmente un desempate, aunque esa es efectivamente la función que proporciona. No realiza ninguna acción, sino que proporciona un canal de comunicación alternativo para la comunicación del clúster al clúster.



El desafío #1 con la conmutación automática por error es el problema de cerebro dividido, y ese problema surge si sus dos sitios pierden conectividad entre sí. ¿Qué debería pasar? No desea que dos sitios diferentes

se designen a sí mismos como copias supervivientes de los datos, pero ¿cómo puede un solo sitio diferenciar entre la pérdida real del sitio opuesto y la incapacidad de comunicarse con el sitio opuesto?

Aquí es donde el mediador entra en la imagen. Si se coloca en un sitio 3rd y cada sitio tiene una conexión de red independiente con ese sitio, tiene una ruta adicional para que cada sitio valide el estado del otro. Mire la imagen de arriba otra vez y considere los siguientes escenarios.

- ¿Qué sucede si el mediador falla o es inaccesible desde uno o ambos sitios?
  - Los dos clústeres pueden comunicarse entre sí a través del mismo enlace utilizado para los servicios de replicación.
  - Los datos se siguen ofreciendo con la protección RPO=0
- ¿Qué sucede si falla el sitio A?
  - El sitio B verá que ambos canales de comunicación se caen.
  - El sitio B se hará cargo de los servicios de datos, pero sin el mirroring RPO=0
- ¿Qué sucede si falla el sitio B?
  - El sitio A verá que ambos canales de comunicación se caen.
  - El sitio A se hará cargo de los servicios de datos, pero sin el mirroring RPO=0

Hay otro escenario a considerar: Pérdida del enlace de replicación de datos. Si se pierde el enlace de replicación entre los sitios, obviamente el mirroring RPO=0 se convertirá en imposible. ¿Qué debería pasar entonces?

Esto se controla por el estado de sitio preferido. En una relación SM-AS, uno de los sitios es secundario al otro. Esto no afecta a las operaciones normales y todo el acceso a los datos es simétrico, pero si la replicación se interrumpe, el vínculo tendrá que romperse para reanudar las operaciones. Como resultado, el sitio preferido continuará con las operaciones sin mirroring y el sitio secundario detendrá el procesamiento de I/O hasta que se restaure la comunicación de la replicación.

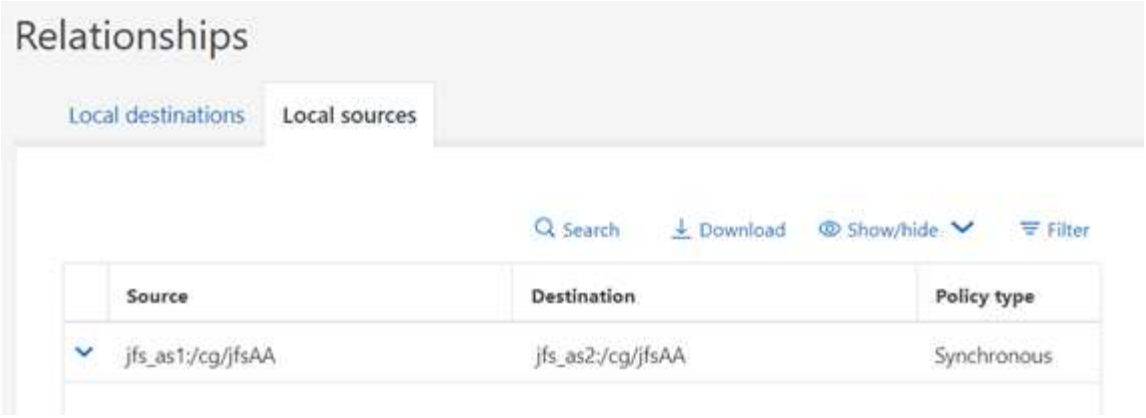
Sitio preferido de sincronización activa de SnapMirror

El comportamiento de sincronización activa de SnapMirror es simétrico, con una excepción importante: La configuración de sitio preferida.

La sincronización activa de SnapMirror considerará que un sitio es el «origen» y el otro el «destino». Esto implica una relación de replicación unidireccional, pero esto no se aplica al comportamiento de E/S. La replicación es bidireccional y simétrica, y los tiempos de respuesta de I/O son los mismos en cualquier lado del espejo.

La `source` designación controla el sitio preferido. Si se pierde el enlace de replicación, las rutas de LUN en la copia de origen seguirán sirviendo datos mientras las rutas de LUN en la copia de destino dejarán de estar disponibles hasta que se restablezca la replicación y SnapMirror vuelva a entrar en un estado síncrono. A continuación, las rutas reanudarán el servicio de datos.

La configuración de origen/destino se puede ver a través de SystemManager:



O en la CLI:

```
Cluster2::> snapmirror show -destination-path jfs_as2:/cg/jfsAA

                           Source Path: jfs_as1:/cg/jfsAA
                      Destination Path: jfs_as2:/cg/jfsAA
                     Relationship Type: XDP
                Relationship Group Type: consistencygroup
                    SnapMirror Schedule: -
                 SnapMirror Policy Type: automated-failover-duplex
                      SnapMirror Policy: AutomatedFailOverDuplex
                            Tries Limit: -
                      Throttle (KB/sec): -
                           Mirror State: Snapmirrored
                    Relationship Status: InSync
```

La clave es que la fuente es la máquina virtual de almacenamiento SVM en cluster1. Tal como se ha mencionado anteriormente, los términos «origen» y «destino» no describen el flujo de los datos replicados. Ambos sitios pueden procesar una escritura y replicarla en el sitio opuesto. De hecho, ambos clústeres son orígenes y destinos. El efecto de designar un clúster como origen simplemente controla qué clúster sobrevive como sistema de almacenamiento de lectura y escritura si se pierde el enlace de replicación.

Topología de red

Acceso uniforme

La conexión de red de acceso uniforme significa que los hosts pueden acceder a las rutas en ambos sitios (o dominios de fallo dentro del mismo sitio).

Una característica importante de SM-AS es la capacidad de configurar los sistemas de almacenamiento para conocer dónde se encuentran los hosts. Cuando asigna las LUN a un host determinado, puede indicar si son proximales o no a un sistema de almacenamiento determinado.

Ajustes de proximidad

La proximidad se refiere a una configuración por clúster que indica que un ID de iniciador de iSCSI o WWN de host particular pertenece a un host local. Es un segundo paso opcional para configurar el acceso a LUN.

El primer paso es la configuración habitual del igroup. Cada LUN debe asignarse a un igroup que contiene los ID WWN/iSCSI de los hosts que necesitan acceder a ese LUN. Este controla el host que tiene *access* a una LUN.

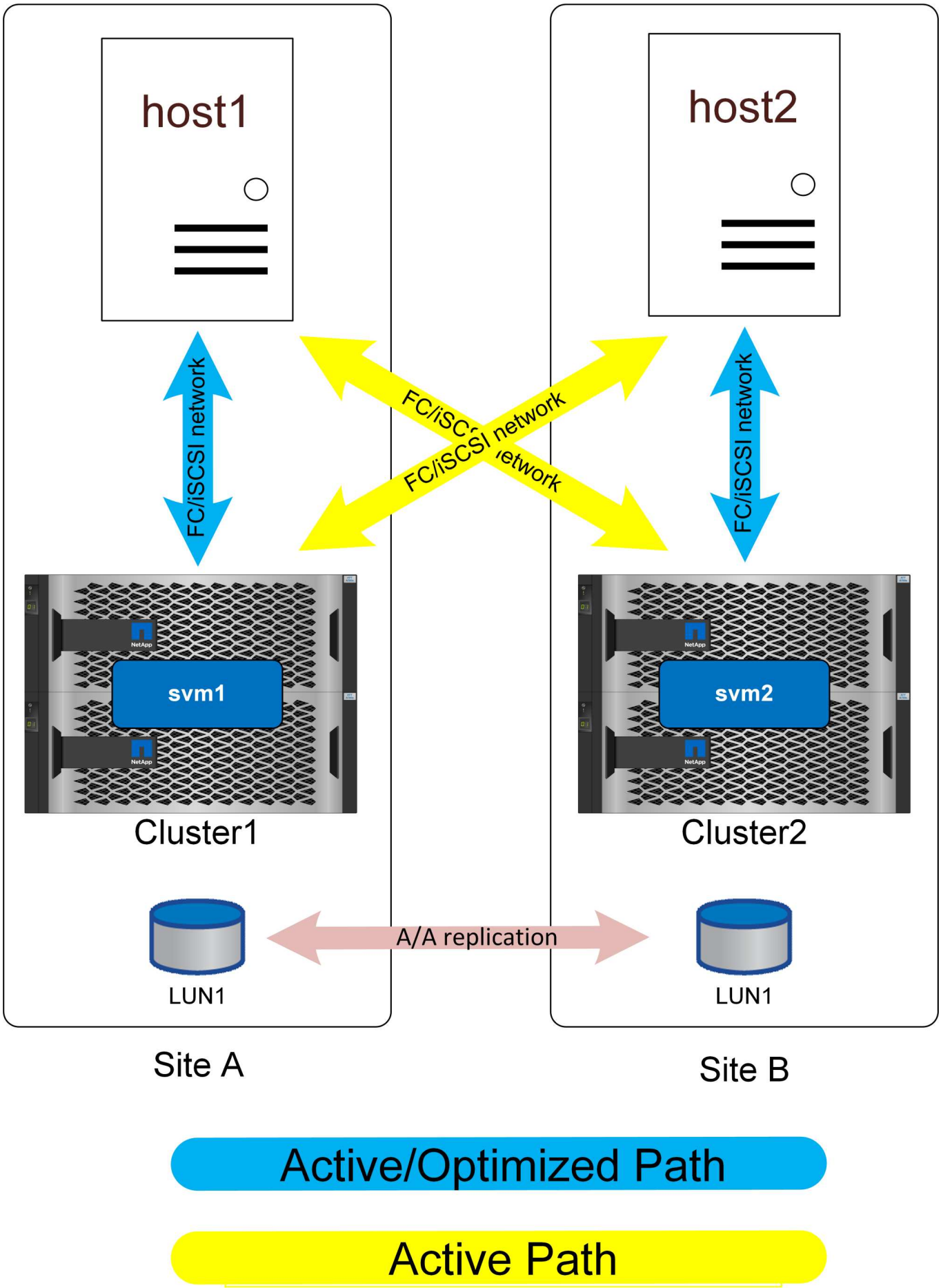
El segundo paso opcional es configurar la proximidad del host. Esto no controla el acceso, controla *priority*.

Por ejemplo, se puede configurar un host del sitio A para acceder a una LUN protegida por sincronización activa de SnapMirror y, como la SAN se extiende a través de los sitios, las rutas están disponibles para ese LUN usando el almacenamiento en el sitio A o el almacenamiento del sitio B.

Sin configuración de proximidad, ese host usará ambos sistemas de almacenamiento por igual porque ambos sistemas de almacenamiento anunciarán rutas activas/optimizadas. Si la latencia SAN o el ancho de banda entre los sitios es limitada, es posible que no sea deseable y puede que desee asegurarse de que durante el funcionamiento normal cada host utilice preferentemente rutas hacia el sistema de almacenamiento local. Esto se configura añadiendo el ID de WWN/iSCSI de host al clúster local como un host proximal. Esto se puede hacer en la CLI o en SystemManager.

AFF

Con un sistema AFF, las rutas aparecerían como se muestra a continuación cuando se configura la proximidad del host.


host1
host2
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
svm1
svm2
Cluster1
Cluster2
A/A replication
LUN1
LUN1
Site A
Site B
Active/Optimized Path
Active Path

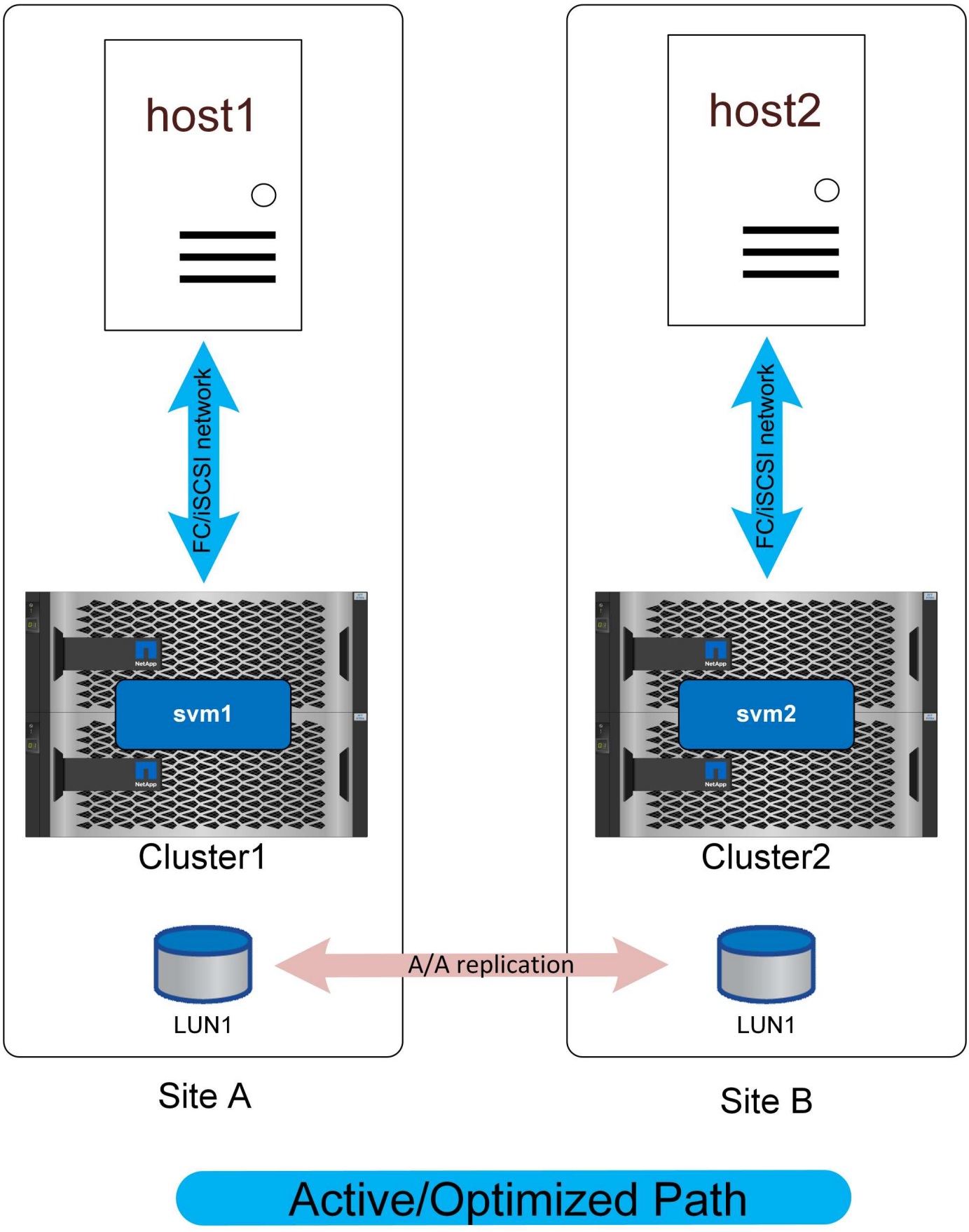
En funcionamiento normal, todas las I/O son locales. Las lecturas y escrituras se sirven desde la cabina de almacenamiento local. Por supuesto, el controlador local también deberá replicar el I/O de escritura en el sistema remoto antes de reconocerlo, pero todas las I/O de lectura se prestarán de servicio local y no incurrirán en latencia adicional atravesando el enlace SAN entre los sitios.

La única vez que se utilizarán las rutas no optimizadas es cuando se pierden todas las rutas activas/optimizadas. Por ejemplo, si se perdiera alimentación toda la cabina en el sitio A, los hosts del sitio A seguirían teniendo acceso a las rutas a la cabina en el sitio B y, por lo tanto, permanecerían operativos, aunque experimentarían una mayor latencia.

Existen rutas redundantes a través del clúster local que no se muestran en estos diagramas para simplificar el proceso. Los sistemas de almacenamiento de ONTAP son por sí mismos de alta disponibilidad, por lo que un fallo de una controladora no debe dar lugar a un fallo del sitio. Simplemente debe dar lugar a un cambio en el que se utilizan las rutas locales en el sitio afectado.

ASA

Los sistemas NetApp ASA ofrecen accesos múltiples activo-activo en todas las rutas de un clúster. Esto también se aplica a las configuraciones SM-AS.



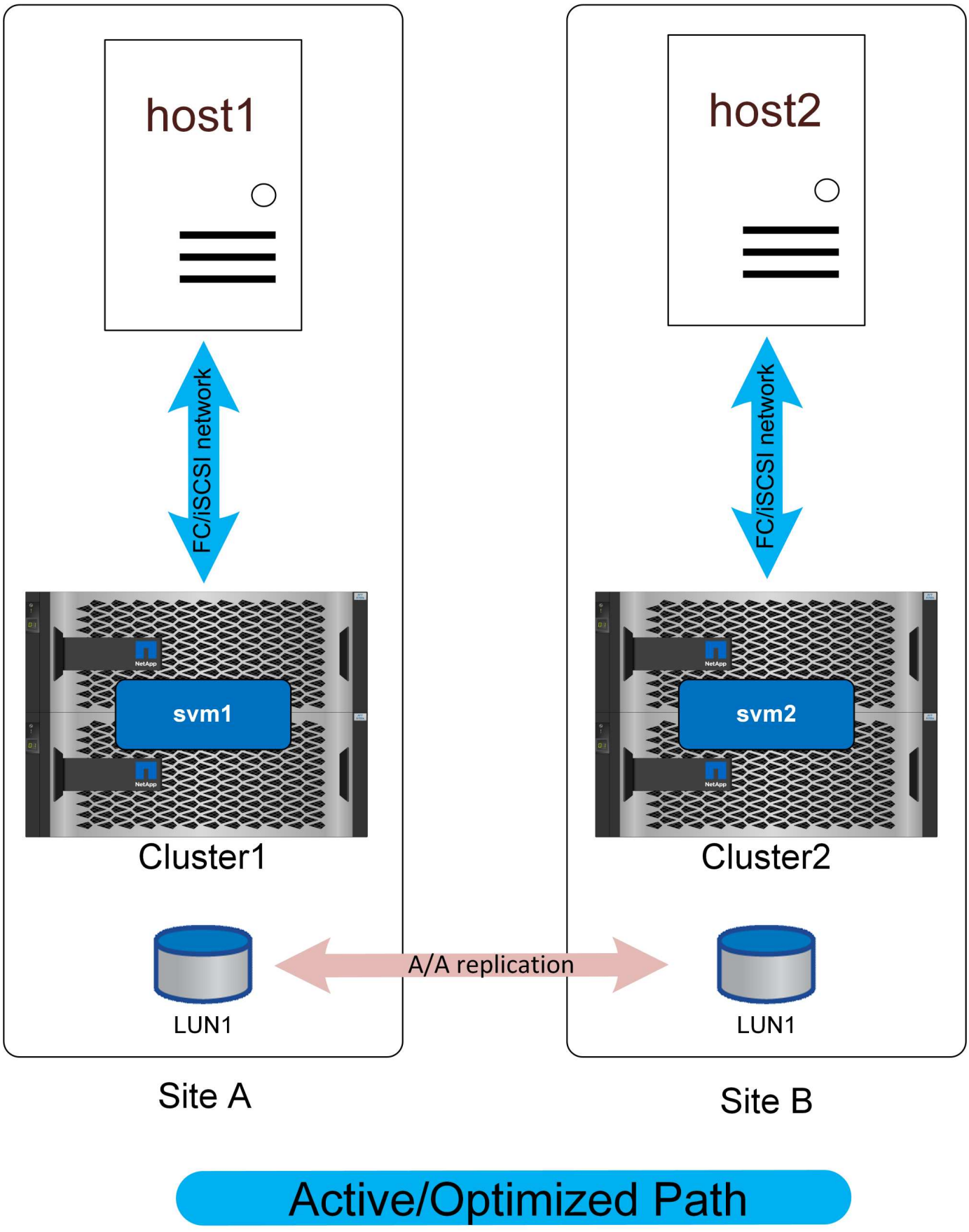
Una configuración de ASA con acceso no uniforme funcionaría en gran medida igual que con AFF. Con un acceso uniforme, IO estaría cruzando la WAN. Esto puede o no ser deseable.

Si los dos sitios estuvieran separados por 100 metros con conectividad de fibra, no debería haber una latencia adicional detectable que cruce la WAN, pero si los sitios estuvieran separados por una distancia larga, el rendimiento de lectura se vería afectado en ambos sitios. Por el contrario, con AFF, dichas rutas de cruce de WAN solo se utilizarían si no hubiera rutas locales disponibles y mejoraría el rendimiento diario, ya que todas las I/O serían locales. ASA con red de acceso no uniforme sería una opción para obtener las ventajas en coste y funciones de ASA sin incurrir en una penalización del acceso a la latencia de varios sitios.

ASA con SM en una configuración de baja latencia ofrece dos ventajas interesantes. En primer lugar, esencialmente * duplica * el rendimiento para cualquier host individual porque IO puede ser atendido por el doble de controladores usando el doble de rutas. En segundo lugar, en un entorno de sitio único ofrece una disponibilidad extrema debido a que se puede perder un sistema de almacenamiento completo sin interrumpir el acceso al host.

Acceso no uniforme

La red de acceso no uniforme significa que cada host solo tiene acceso a los puertos del sistema de almacenamiento local. La SAN no se extiende entre sitios (o dominios de fallos dentro del mismo sitio).



La principal ventaja de este método es la simplicidad en entornos SAN, eliminando la necesidad de extender una SAN por la red. Algunos clientes no tienen una conectividad de baja latencia suficiente entre los sitios o

no disponen de la infraestructura para túnel el tráfico de SAN FC a través de una red intersitio.

La desventaja del acceso no uniforme es que ciertos escenarios de fallo, incluida la pérdida del enlace de replicación, provocarán que algunos hosts pierdan el acceso al almacenamiento. Las aplicaciones que se ejecutan como instancias únicas, como una base de datos sin cluster que inherentemente solo se ejecuta en un único host en cualquier montaje dado, fallarían si se perdiera la conectividad del almacenamiento local. Los datos seguirían estando protegidos, pero el servidor de la base de datos ya no tendría acceso. Deberá reiniciarse en un sitio remoto, preferiblemente mediante un proceso automatizado. Por ejemplo, VMware HA puede detectar una situación de todas las rutas inactivas en un servidor y reiniciar una máquina virtual en otro servidor donde haya rutas disponibles.

Por el contrario, una aplicación en cluster como Oracle RAC puede ofrecer un servicio que esté disponible al mismo tiempo en dos sitios diferentes. Perder un sitio no significa la pérdida del servicio de la aplicación en su conjunto. Las instancias siguen estando disponibles y en ejecución en el sitio superviviente.

En muchos casos, sería inaceptable que la sobrecarga de latencia adicional derivada de una aplicación que accede al almacenamiento a través de un enlace entre sitio y sitio. Esto significa que la disponibilidad mejorada de una red uniforme es mínima, ya que la pérdida de almacenamiento en un sitio llevaría a la necesidad de apagar los servicios en ese sitio que ha fallado de todos modos.

> Existen rutas redundantes a través del clúster local que no se muestran en estos diagramas para simplificar el proceso. Los sistemas de almacenamiento de ONTAP son por sí mismos de alta disponibilidad, por lo que un fallo de una controladora no debe dar lugar a un fallo del sitio. Simplemente debe dar lugar a un cambio en el que se utilizan las rutas locales en el sitio afectado.

Configuraciones de Oracle

Descripción general

El uso de la sincronización activa de SnapMirror no necesariamente agrega ni cambia ninguna práctica recomendada para operar una base de datos.

La mejor arquitectura depende de los requisitos del negocio. Por ejemplo, si el objetivo es contar con una protección RPO=0 frente a la pérdida de datos, pero el objetivo de tiempo de recuperación es relajado, el uso de bases de datos de instancia única de Oracle y la replicación de las LUN con SM-AS podrían ser suficientes y menos costoso desde la creación de licencias de Oracle. Un fallo del sitio remoto no interrumpiría las operaciones, y la pérdida del sitio principal provocaría que las LUN del sitio superviviente estén en línea y listas para utilizarse.

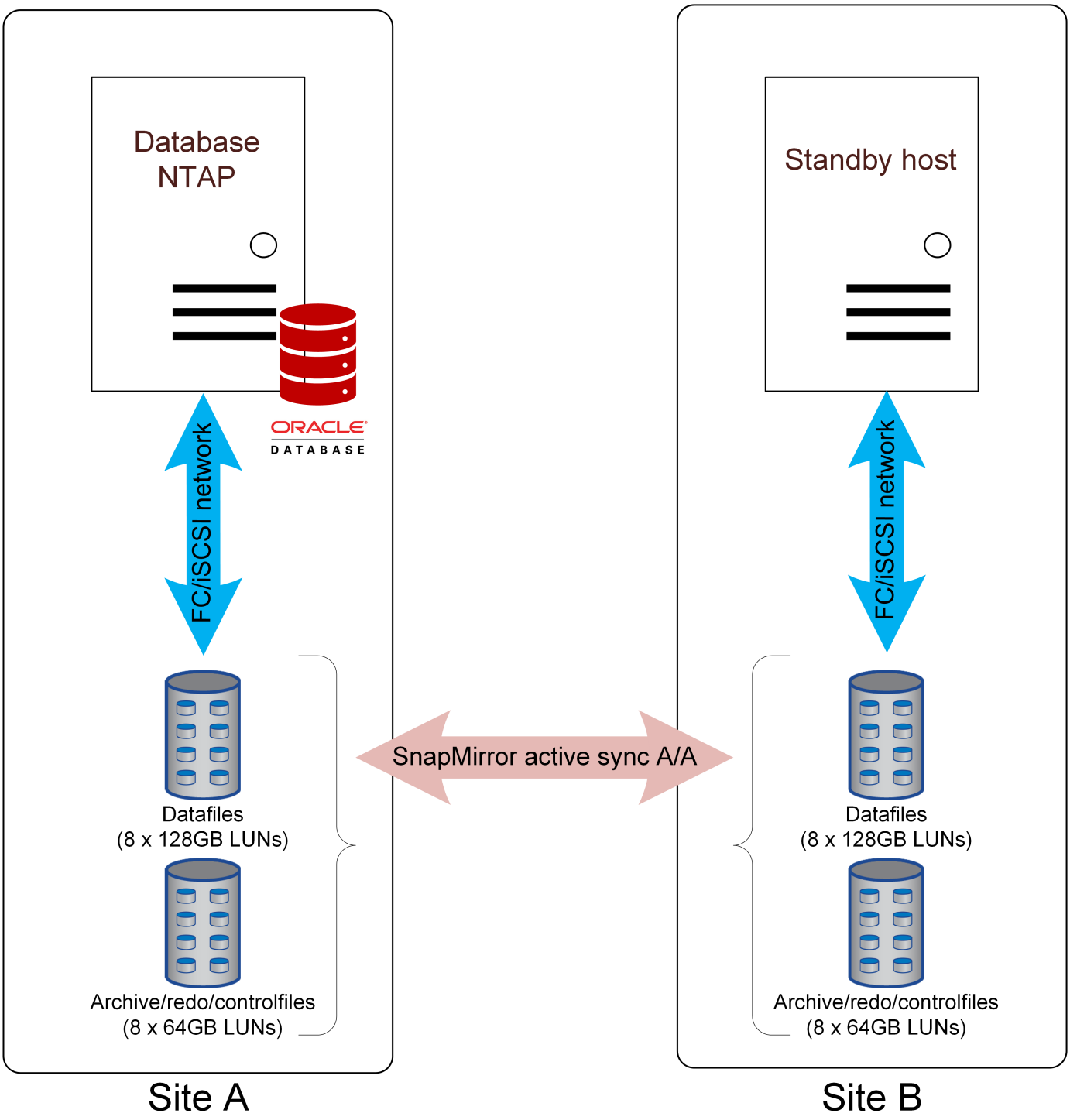
Si el objetivo de tiempo de recuperación fuera más estricto, la automatización activo-pasiva básica mediante scripts o clusterware como Pacemaker o Ansible mejoraría el tiempo de conmutación al nodo de respaldo. Por ejemplo, VMware HA podría configurarse para detectar un fallo de los equipos virtuales en el sitio primario y activar el equipo virtual en el sitio remoto.

Por último, para obtener una conmutación al respaldo extremadamente rápida, Oracle RAC se pudo poner en marcha en diferentes sitios. El RTO sería esencialmente cero porque la base de datos estaría en línea y disponible en ambas ubicaciones en todo momento.

Instancia única de Oracle

Los ejemplos que se explican a continuación muestran algunas de las muchas opciones para desplegar bases de datos de instancia única de Oracle con replicación de

sincronización activa de SnapMirror.



Conmutación al nodo de respaldo con un SO preconfigurado

La sincronización activa de SnapMirror ofrece una copia síncrona de los datos en el sitio de recuperación de desastres, pero para que los datos estén disponibles, es necesario un sistema operativo y las aplicaciones asociadas. La automatización básica puede mejorar drásticamente el tiempo de conmutación al nodo de respaldo del entorno global. Los productos de Clusterware, como Pacemaker, se utilizan a menudo para crear un clúster en todos los sitios y, en muchos casos, el proceso de conmutación por error se puede ejecutar con scripts sencillos.

Si se pierden los nodos primarios, el clusterware (o scripts) pondrá las bases de datos en línea en el sitio alternativo. Una opción es crear servidores en espera preconfigurados para los recursos SAN que componen la base de datos. Si el sitio principal falla, el clusterware o la alternativa con secuencia de comandos realiza una secuencia de acciones similar a las siguientes:

1. Detecte el fallo del sitio principal
2. Realizar detección de LUN FC o iSCSI
3. Montaje de sistemas de archivos y/o montaje de grupos de discos ASM
4. Iniciando la base de datos

El requisito principal de este método es un sistema operativo en ejecución instalado en el sitio remoto. Se debe preconfigurar con binarios de Oracle, lo que también significa que las tareas como los parches de Oracle se deben realizar en la ubicación primaria y en espera. Como alternativa, los binarios de Oracle se pueden duplicar en la ubicación remota y montar si se declara un desastre.

El procedimiento de activación real es simple. Los comandos como la detección de LUN sólo requieren unos pocos comandos por puerto FC. El montaje del sistema de archivos no es más que `mount` un comando, y tanto las bases de datos como ASM se pueden iniciar y detener en la CLI con un único comando.

Conmutación por error con un sistema operativo virtualizado

La conmutación por error de los entornos de base de datos puede ampliarse para incluir el propio sistema operativo. En teoría, esta recuperación tras fallos se puede realizar con las LUN de arranque, pero la mayoría de las veces se realiza con un sistema operativo virtualizado. El procedimiento es similar a los siguientes pasos:

1. Detecte el fallo del sitio principal
2. Montar los almacenes de datos que alojan las máquinas virtuales del servidor de bases de datos
3. Inicio de las máquinas virtuales
4. Iniciar las bases de datos manualmente o configurar las máquinas virtuales para iniciar automáticamente las bases de datos.

Por ejemplo, un clúster ESX podría abarcar sitios. En caso de desastre, los equipos virtuales pueden conectarse en línea en el sitio de recuperación ante desastres después del cambio.

Protección frente a errores de almacenamiento

El diagrama anterior muestra el uso de "acceso no uniforme", donde la SAN no se extiende entre los sitios. Esto puede que sea más sencillo de configurar y, en algunos casos, puede que sea la única opción dadas las funcionalidades SAN actuales, pero también significa que un fallo del sistema de almacenamiento primario provocaría una interrupción en la base de datos hasta que se conmutara al nodo de respaldo de la aplicación.

Para una mayor resiliencia, la solución podría ponerse en marcha con "acceso uniforme". Esto permitiría a las aplicaciones seguir operando utilizando las rutas anunciadas desde el sitio opuesto.

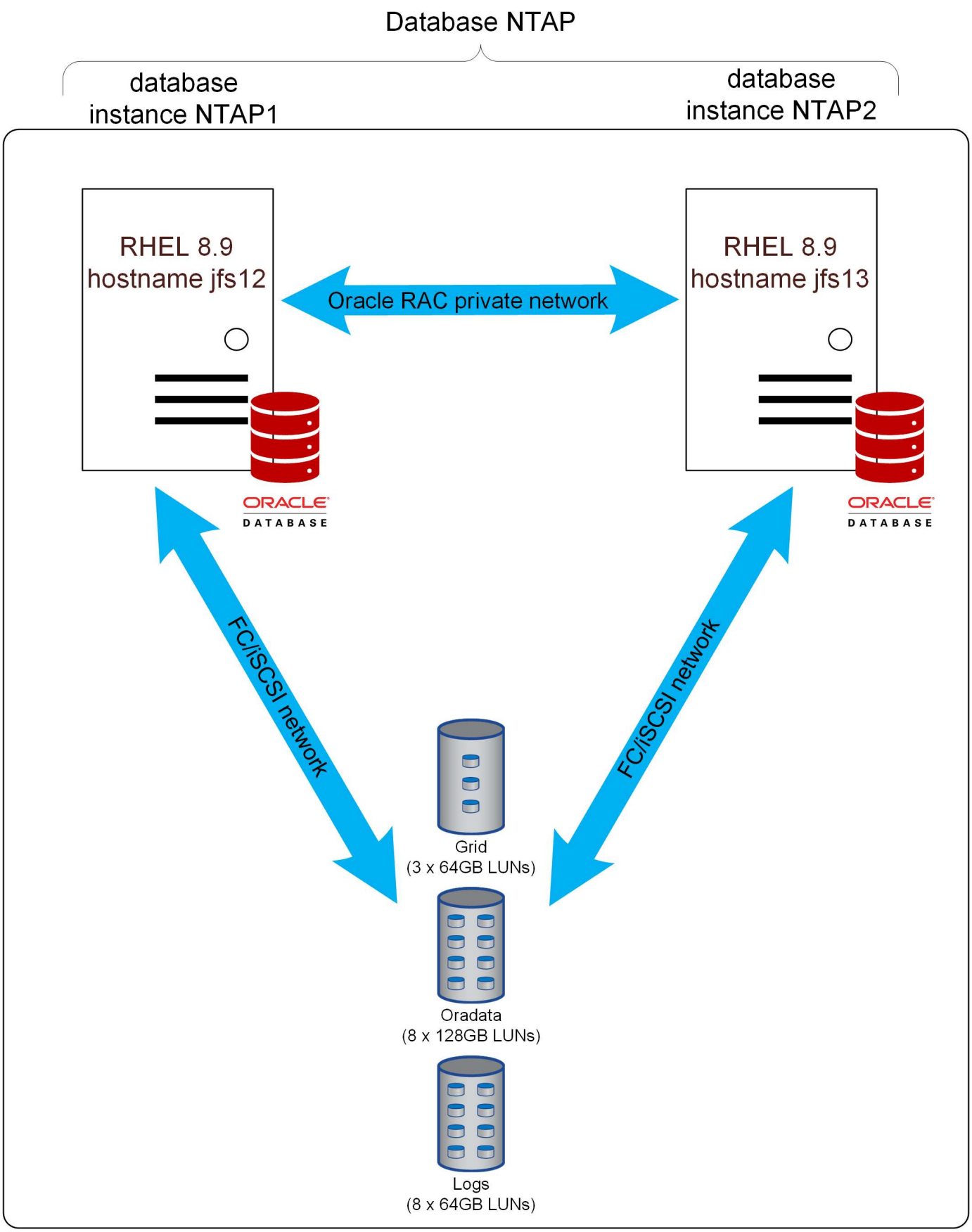
Oracle Extended RAC

Muchos clientes optimizan su objetivo de tiempo de recuperación al ampliar un clúster de Oracle RAC en todos los sitios, lo que proporciona una configuración completamente activo-activo. El diseño general se complica porque debe incluir la gestión de quórum de Oracle RAC.

El cluster de RAC ampliado tradicional confiaba en la duplicación de ASM para proporcionar protección de datos. Este enfoque funciona, pero también requiere muchos pasos de configuración manuales e impone sobrecarga en la infraestructura de red. En cambio, permitir que SnapMirror Active Sync asuma la responsabilidad de la replicación de datos simplifica drásticamente la solución. Además, resulta más sencillo realizar operaciones como la sincronización, la resincronización después de interrupciones, las recuperaciones tras fallos y la gestión del quórum, además de que la SAN no tiene que distribuirse entre sitios, lo que simplifica el diseño y la gestión de SAN.

Replicación

Lo fundamental para comprender la funcionalidad de RAC en la sincronización activa de SnapMirror es ver el almacenamiento como un único conjunto de LUN alojadas en el almacenamiento reflejado. Por ejemplo:



No hay ninguna copia primaria ni copia duplicada. Lógicamente, solo existe una copia única de cada LUN, y esa LUN está disponible en rutas SAN ubicadas en dos sistemas de almacenamiento diferentes. Desde el punto de vista del host, no hay conmutación por error del almacenamiento; en cambio, existen cambios de

ruta. Varios eventos de fallo pueden provocar la pérdida de ciertas rutas a la LUN mientras otras rutas permanecen en línea. La sincronización activa de SnapMirror garantiza que los mismos datos estén disponibles en todas las rutas operativas.

Configuración del almacenamiento

En esta configuración de ejemplo, los discos ASM están configurados de la misma forma que en cualquier configuración de RAC de sitio único en el almacenamiento empresarial. Dado que el sistema de almacenamiento proporciona protección de datos, se utilizaría la redundancia externa de ASM.

Acceso uniforme frente a acceso no informado

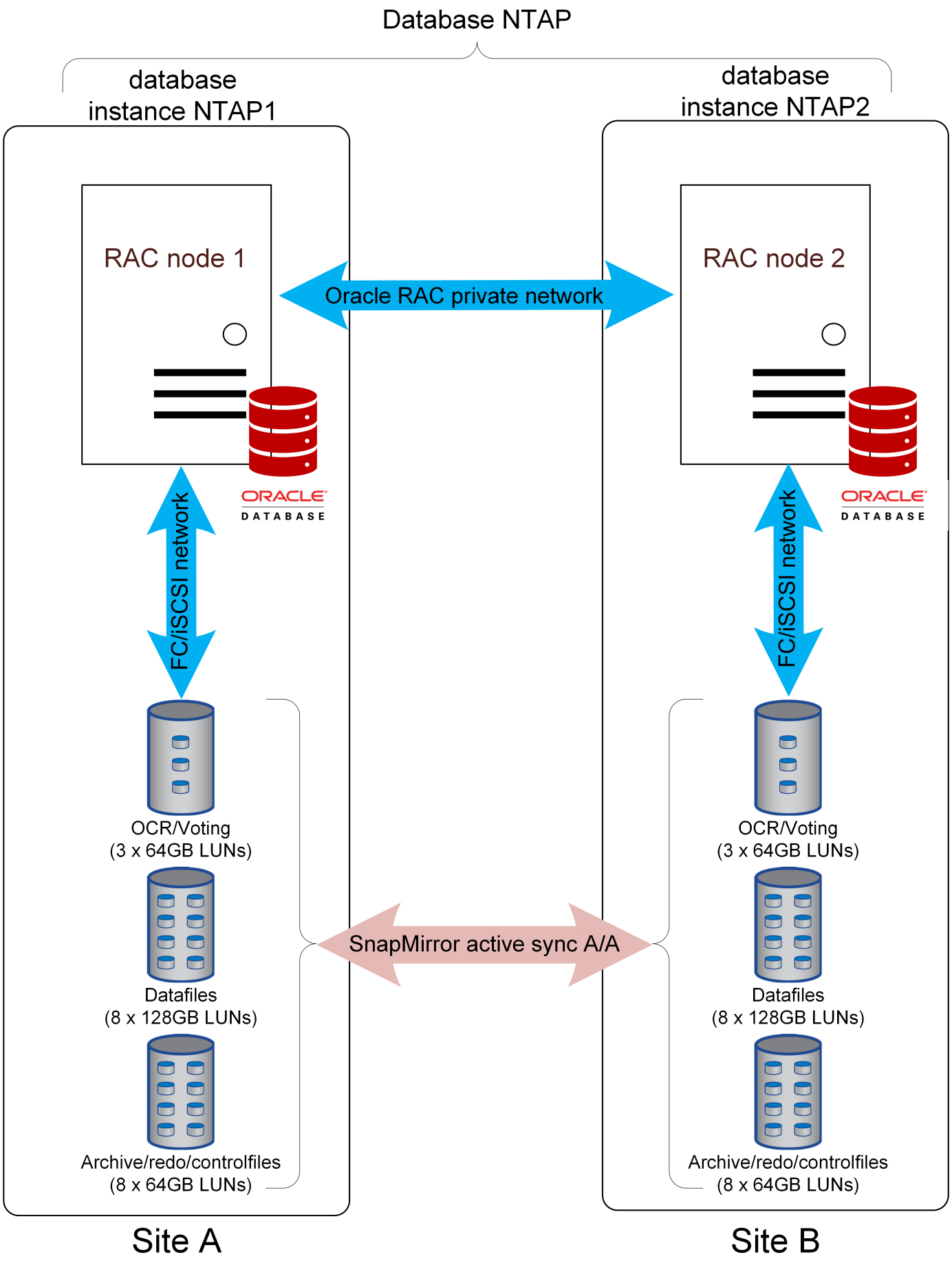
La consideración más importante con Oracle RAC en la sincronización activa de SnapMirror es si se debe utilizar un acceso uniforme o no uniforme.

El acceso uniforme significa que cada host puede ver rutas en ambos clústeres. El acceso no uniforme significa que los hosts solo pueden ver rutas al clúster local.

Ninguna de las opciones se recomienda o desaconseja específicamente. Algunos clientes disponen de fibra oscura disponible en todo momento para conectar sitios, mientras que otros no tienen esta conectividad o su infraestructura SAN no admite ISL de larga distancia.

Acceso no uniforme

El acceso no uniforme es más sencillo de configurar desde la perspectiva de SAN.


Database NTAP
database instance NTAP1
database instance NTAP2
RAC node 1
RAC node 2
Oracle RAC private network
ORACLE DATABASE
ORACLE DATABASE
FC/iSCSI network
FC/iSCSI network
OCR/Voting (3 x 64GB LUNs)
OCR/Voting (3 x 64GB LUNs)
SnapMirror active sync A/A
Datafiles (8 x 128GB LUNs)
Datafiles (8 x 128GB LUNs)
Archive/redo/controlfiles (8 x 64GB LUNs)
Archive/redo/controlfiles (8 x 64GB LUNs)
Site A
Site B

El principal "acceso no uniforme"inconveniente del método es que la pérdida de conectividad con ONTAP entre sitios o la pérdida de un sistema de almacenamiento supondrá la pérdida de instancias de base de datos en un sitio. Obviamente, esto no es deseable, pero puede ser un riesgo aceptable a cambio de una configuración SAN simple.

Acceso uniforme

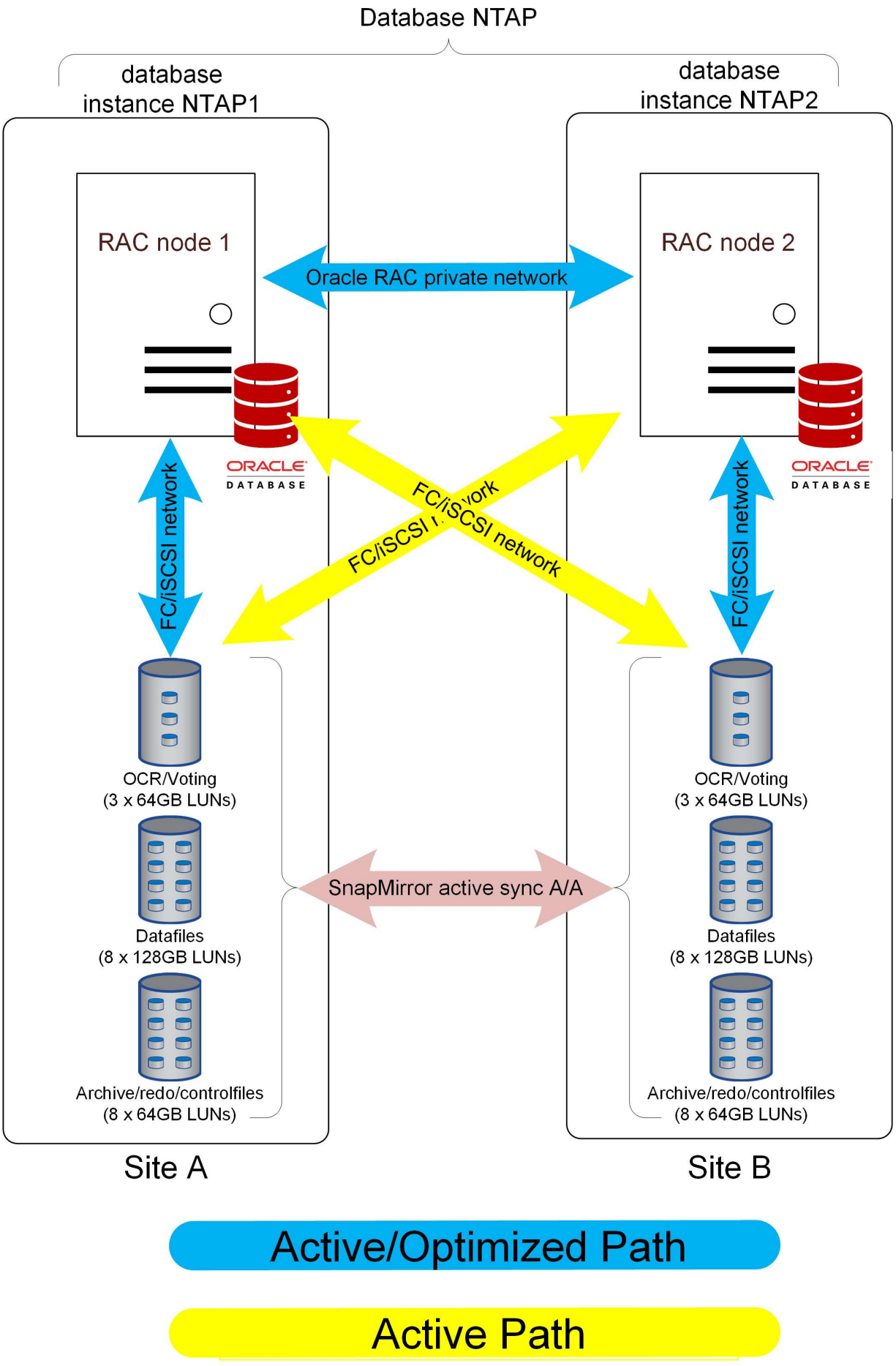
Para el acceso uniforme es necesario ampliar la SAN a través de varios sitios. La ventaja principal es que la pérdida de un sistema de almacenamiento no provocará la pérdida de una instancia de la base de datos. En su lugar, provocaría un cambio de multivía en el que se usan las rutas actualmente.

Hay varias formas de configurar el acceso no uniforme.

> En los diagramas que aparecen a continuación, también existen rutas activas pero no optimizadas que se utilizarán durante los simples fallos de controladoras, pero esas rutas no se muestran en interés de simplificar los diagramas.

AFF con ajustes de proximidad

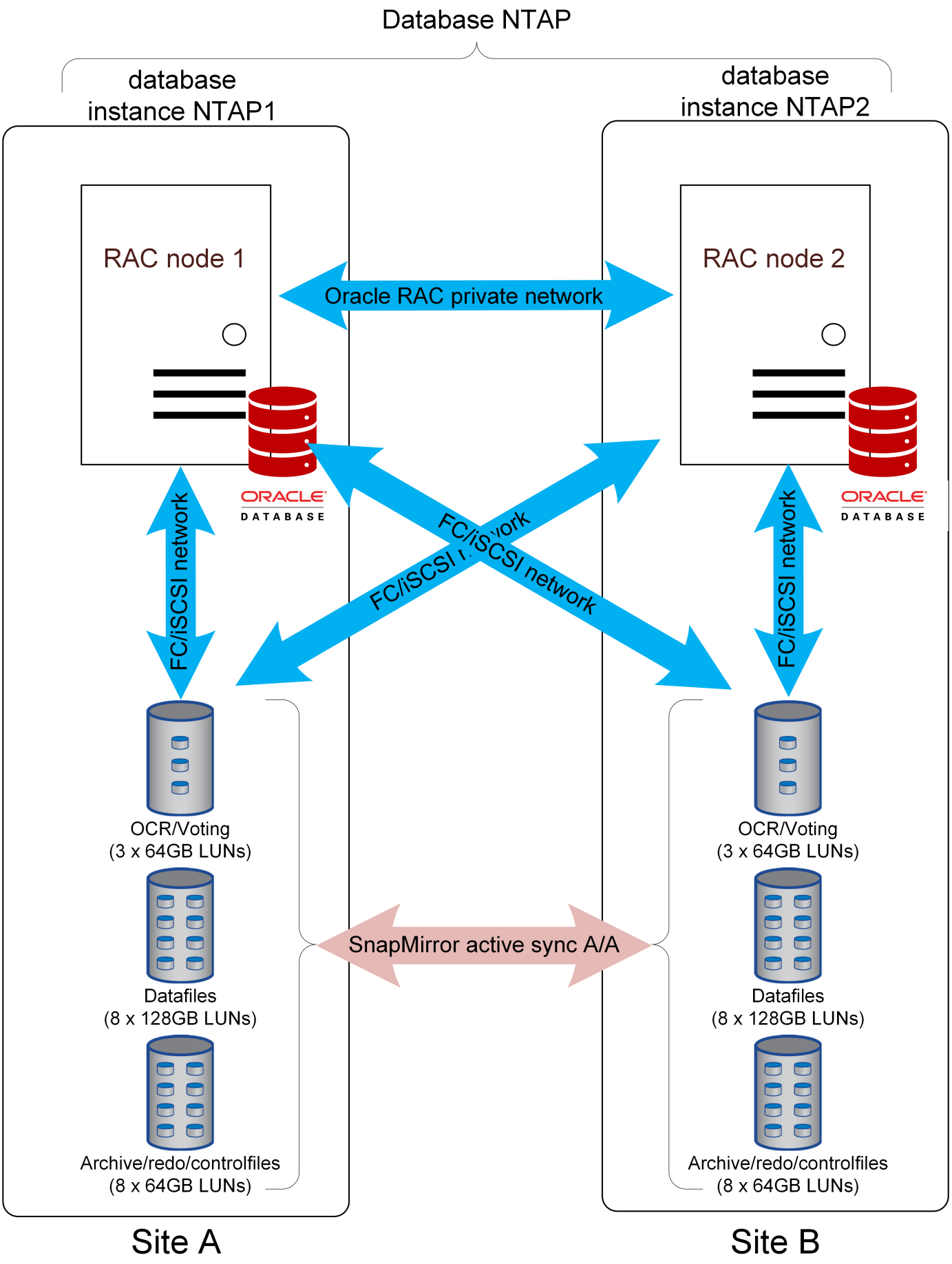
Si hay una latencia significativa entre los sitios, los sistemas AFF se pueden configurar con los ajustes de proximidad del host. Esto permite que cada sistema de almacenamiento tenga en cuenta qué hosts son locales y remotos y asigne prioridades de ruta según corresponda.


Database NTAP
database instance NTAP1
database instance NTAP2
RAC node 1
RAC node 2
Oracle RAC private network
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
ORACLE DATABASE
ORACLE DATABASE
OCR/Voting (3 x 64GB LUNs)
OCR/Voting (3 x 64GB LUNs)
SnapMirror active sync A/A
Datafiles (8 x 128GB LUNs)
Datafiles (8 x 128GB LUNs)
Archive/redo/controlfiles (8 x 64GB LUNs)
Archive/redo/controlfiles (8 x 64GB LUNs)
Site A
Site B
Active/Optimized Path
Active Path

En el funcionamiento normal, cada instancia de Oracle utilizaría preferentemente las rutas de acceso locales activas/optimizadas. El resultado es que la copia local de los bloques suministraría todas las lecturas. Esto proporciona la menor latencia posible. El I/O de escritura se envía de manera similar por rutas a la controladora local. La I/O debe replicarse antes de reconocerse y, por lo tanto, se produciría la latencia adicional al cruzar la red sitio a sitio, pero esto no se puede evitar en una solución de replicación síncrona.

ASA / AFF sin ajustes de proximidad

Si no hay latencia significativa entre los sitios, los sistemas AFF se pueden configurar sin ajustes de proximidad del host o se puede utilizar ASA.


Database NTAP
database instance NTAP1
database instance NTAP2
RAC node 1
RAC node 2
Oracle RAC private network
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
ORACLE DATABASE
ORACLE DATABASE
OCR/Voting (3 x 64GB LUNs)
OCR/Voting (3 x 64GB LUNs)
SnapMirror active sync A/A
Datafiles (8 x 128GB LUNs)
Datafiles (8 x 128GB LUNs)
Archive/redo/controlfiles (8 x 64GB LUNs)
Archive/redo/controlfiles (8 x 64GB LUNs)
Site A
Site B

Cada host podrá utilizar todas las rutas operativas en ambos sistemas de almacenamiento. Esto mejora significativamente el rendimiento, ya que permite que cada host aproveche el potencial de rendimiento de dos clústeres, no solo uno.

Con ASA, no solo todas las rutas a ambos clústeres se considerarían activas y optimizadas, sino que las rutas en las controladoras de los partners también estarían activas. El resultado serían rutas SAN activas en todo el clúster, todo el tiempo.

> Los sistemas ASA también pueden usarse en una configuración de acceso no uniforme. Como no existen rutas entre sitios, no habría impacto en el rendimiento como resultado de I/O al cruzar el ISL.

RAC tiebreaker

Si bien el RAC extendido que usa SnapMirror active sync es una arquitectura simétrica con respecto a E/S, hay una excepción que está conectada a la gestión de cerebro dividido.

¿Qué sucede si el enlace de replicación se pierde y ninguno de los sitios tiene quórum? ¿Qué debería pasar? Esta pregunta se aplica tanto al comportamiento de Oracle RAC como al de ONTAP. Si los cambios no se pueden replicar en todos los sitios y desea reanudar las operaciones, uno de los sitios tendrá que sobrevivir y el otro sitio tendrá que dejar de estar disponible.

El "Mediador ONTAP" resuelve este requisito en la capa ONTAP. Hay varias opciones para RAC tiebreaking.

Oracle tiebreakers

El mejor método para gestionar los riesgos de Oracle RAC de cerebro dividido es utilizar un número impar de nodos de RAC, preferiblemente mediante el uso de un tiebreaker de sitio 3rd. Si un sitio 3rd no está disponible, la instancia de tiebreaker podría colocarse en un sitio de los dos sitios, designándolo efectivamente como un sitio de supervivencia preferido.

Oracle y css_critical

Con un número par de nodos, el comportamiento por defecto de Oracle RAC es que uno de los nodos del cluster se considerará más importante que el resto de nodos. El sitio con ese nodo de mayor prioridad sobrevivirá al aislamiento del sitio mientras que los nodos del otro sitio desalojarán. La priorización se basa en varios factores, pero también puede controlar este comportamiento mediante la `css_critical` configuración.

En la "ejemplo" arquitectura, los nombres de host de los nodos RAC son jfs12 y jfs13. Los ajustes actuales de `css_critical` son los siguientes:

```
[root@jfs12 ~]# /grid/bin/crsctl get server css_critical
CRS-5092: Current value of the server attribute CSS_CRITICAL is no.

[root@jfs13 trace]# /grid/bin/crsctl get server css_critical
CRS-5092: Current value of the server attribute CSS_CRITICAL is no.
```

Si desea que el sitio con jfs12 sea el sitio preferido, cambie este valor a yes en un sitio Un nodo y reinicie los servicios.

```
[root@jfs12 ~]# /grid/bin/crsctl set server css_critical yes
CRS-4416: Server attribute 'CSS_CRITICAL' successfully changed. Restart
Oracle High Availability Services for new value to take effect.

[root@jfs12 ~]# /grid/bin/crsctl stop crs
CRS-2791: Starting shutdown of Oracle High Availability Services-managed
resources on 'jfs12'
CRS-2673: Attempting to stop 'ora.crsd' on 'jfs12'
CRS-2790: Starting shutdown of Cluster Ready Services-managed resources on
server 'jfs12'
CRS-2673: Attempting to stop 'ora.ntap.ntappdb1.pdb' on 'jfs12'
…
CRS-2673: Attempting to stop 'ora.gipcd' on 'jfs12'
CRS-2677: Stop of 'ora.gipcd' on 'jfs12' succeeded
CRS-2793: Shutdown of Oracle High Availability Services-managed resources
on 'jfs12' has completed
CRS-4133: Oracle High Availability Services has been stopped.

[root@jfs12 ~]# /grid/bin/crsctl start crs
CRS-4123: Oracle High Availability Services has been started.
```

Escenarios de fallo

Descripción general

La planificación de una arquitectura completa de aplicaciones de sincronización activa de SnapMirror requiere comprender cómo SM-AS responderá en varias situaciones de conmutación por error planificadas e imprevistas.

Para los siguientes ejemplos, supongamos que el sitio A está configurado como el sitio preferido.

Pérdida de conectividad de replicación

Si se interrumpe la replicación de SM-AS, la E/S de escritura no se puede completar porque sería imposible que un clúster replique los cambios en el sitio opuesto.

Sitio A (Sitio preferido)

El resultado de un fallo del enlace de replicación en el sitio preferido será una pausa de aproximadamente 15 segundos en el procesamiento de I/O de escritura, ya que ONTAP reintenta las operaciones de escritura replicadas antes de que determine que el enlace de replicación es realmente inaccesible. Una vez transcurridos los 15 segundos, el sistema del sitio A reanuda el procesamiento de E/S de lectura y escritura. Las rutas de SAN no se modificarán y los LUN permanecerán en línea.

Centro B

Dado que el sitio B no es el sitio preferido de sincronización activa de SnapMirror, sus rutas de LUN dejarán de estar disponibles después de unos 15 segundos.

Fallo del sistema de almacenamiento

El resultado de un fallo del sistema de almacenamiento es casi idéntico al de perder el enlace de replicación. El sitio superviviente debería experimentar una pausa de IO de aproximadamente 15 segundos. Una vez transcurrido ese período de 15 segundos, IO se reanudará en ese sitio como de costumbre.

Pérdida del mediador

El servicio de mediador no controla directamente las operaciones de almacenamiento. Funciona como una ruta de control alternativa entre los clústeres. Existe principalmente para automatizar la conmutación al nodo de respaldo sin el riesgo de un escenario de cerebro dividido. En un funcionamiento normal, cada clúster está replicando los cambios en su compañero y, por lo tanto, cada clúster puede verificar que el clúster asociado esté en línea y sirviendo datos. Si el enlace de replicación falla, la replicación se detendría.

El motivo por el que se necesita un mediador para una conmutación por error automatizada segura es que, de otro modo, sería imposible que un clúster de almacenamiento pueda determinar si la pérdida de comunicación bidireccional se debió a una interrupción de la red o a un error real de almacenamiento.

El mediador proporciona una ruta alternativa para que cada clúster compruebe el estado de su compañero. Los escenarios son los siguientes:

- Si un clúster puede ponerse en contacto directamente con su socio, los servicios de replicación están operativos. No se requiere ninguna acción.
- Si un sitio preferido no puede ponerse en contacto con su partner directamente o a través del mediador, se asumirá que el partner no está disponible o que se ha aislado y ha desconectado las rutas de LUN. El sitio preferido procederá a liberar el estado RPO=0 y continuará procesando las I/O de lectura y escritura.
- Si un sitio no preferido no puede ponerse en contacto directamente con su socio, pero puede contactarlo a través del mediador, tomará sus rutas fuera de línea y esperará la devolución de la conexión de replicación.
- Si un sitio no preferido no puede contactar a su partner directamente o a través de un mediador operativo, asumirá que el partner no está disponible o que se ha aislado y ha desconectado las rutas de LUN. El sitio no preferido continuará liberando el estado RPO=0 y continuará procesando las I/O de lectura y escritura. Asumirá el rol del origen de replicación y se convertirá en el nuevo sitio preferido.

Si el mediador no está totalmente disponible:

- El fallo en los servicios de replicación por cualquier motivo, incluido el fallo del sitio o del sistema de almacenamiento no preferido, provocará que el sitio preferido libere el estado RPO=0 y reanude el procesamiento de I/O de lectura y escritura. El sitio no preferido desconectará sus rutas.
- Un fallo del sitio preferido provocará una interrupción porque el sitio no preferido no podrá verificar que el sitio opuesto esté realmente fuera de línea y, por lo tanto, no sería seguro para el sitio no preferido reanudar los servicios.

Restauración de servicios

Tras resolver un fallo, como restaurar la conectividad de sitio a sitio o encender un sistema fallido, los extremos de sincronización activa de SnapMirror detectan automáticamente la presencia de una relación de replicación defectuosa y la devuelven a un estado RPO=0. Una vez que se restablece la replicación síncrona, las rutas fallidas volverán a conectarse.

En muchos casos, las aplicaciones en clúster detectan automáticamente el retorno de las rutas fallidas, y dichas aplicaciones también volverán a estar online. En otros casos, puede ser necesario un análisis SAN a nivel de host o es posible que las aplicaciones deban volver a conectarse manualmente. Depende de la

aplicación y cómo se configura, y en general tales tareas se pueden automatizar fácilmente. El propio ONTAP se repara automáticamente y no debería requerir la intervención del usuario para reanudar las operaciones de almacenamiento RPO=0.

Recuperación manual tras fallos

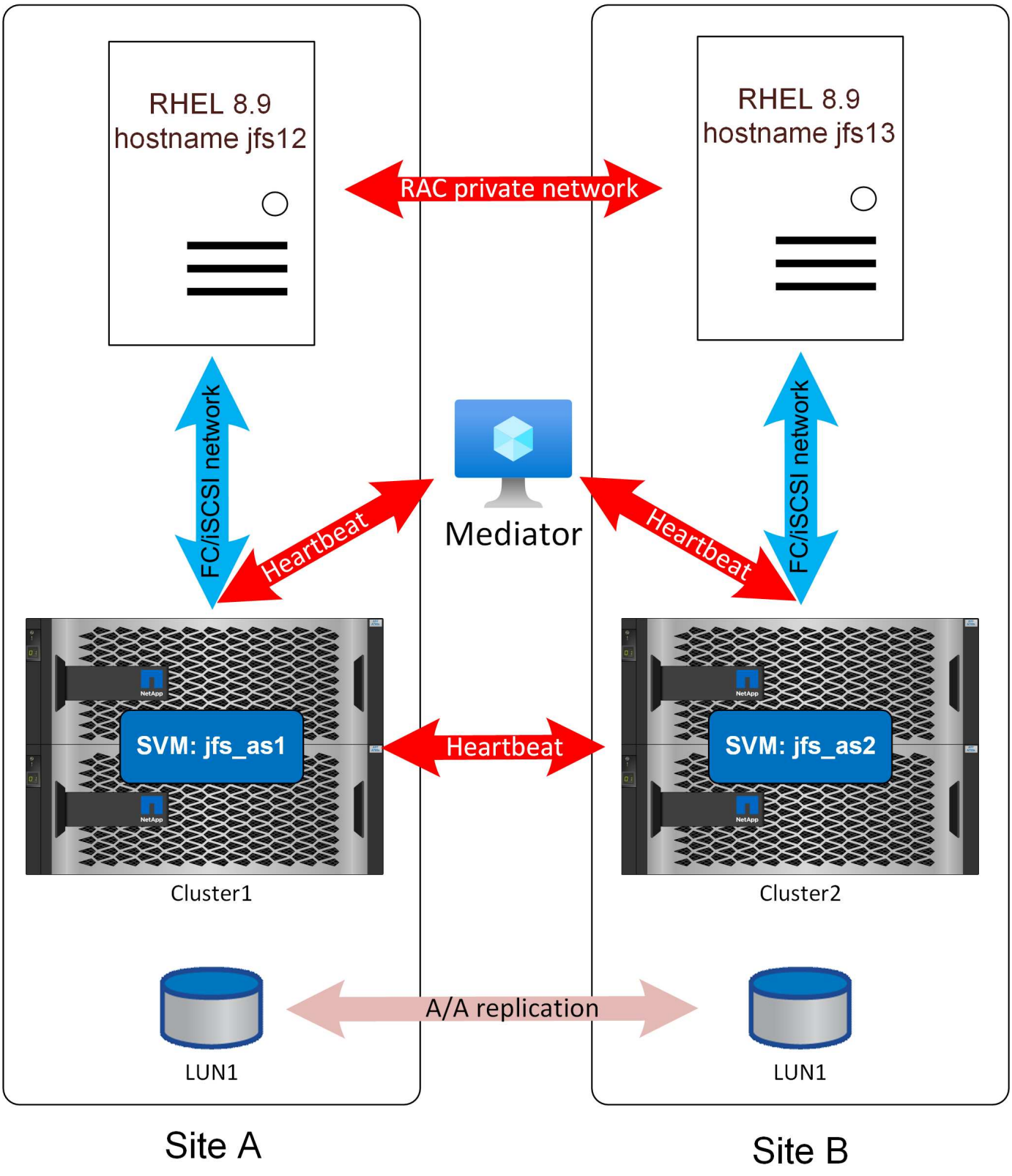
Cambiar el sitio preferido requiere una operación simple. I/O se detendrá durante un segundo o dos como autoridad sobre los cambios en el comportamiento de replicación entre los clústeres, pero I/O de otro modo no se verá afectado.

Arquitectura de ejemplo

Los ejemplos de fallos detallados que se muestran en estas secciones se basan en la arquitectura que se muestra a continuación.

> Esta es solo una de las muchas opciones para bases de datos Oracle en sincronización activa de SnapMirror. Este diseño fue elegido porque ilustra algunos de los escenarios más complicados.

En este diseño, asuma que el sitio A se establece en el "sitio preferido".



Fallo de interconexión de RAC

La pérdida del enlace de replicación de Oracle RAC producirá un resultado similar a la pérdida de conectividad de SnapMirror, excepto que los tiempos de espera serán más cortos por defecto. En la configuración predeterminada, un nodo de Oracle RAC

esperará 200 segundos después de la pérdida de conectividad de almacenamiento antes de expulsarlo, pero solo esperará 30 segundos después de la pérdida del latido de la red de RAC.

Los mensajes de CRS son similares a los que se muestran a continuación. Puede ver el lapso de tiempo de espera de 30 segundos. Dado que css_critical se estableció en jfs12, ubicado en el sitio A, ese será el sitio para sobrevivir y jfs13 en el sitio B será desalojado.

```
2024-09-12 10:56:44.047 [ONMD(3528)]CRS-1611: Network communication with
node jfs13 (2) has been missing for 75% of the timeout interval.  If this
persists, removal of this node from cluster will occur in 6.980 seconds
2024-09-12 10:56:48.048 [ONMD(3528)]CRS-1610: Network communication with
node jfs13 (2) has been missing for 90% of the timeout interval.  If this
persists, removal of this node from cluster will occur in 2.980 seconds
2024-09-12 10:56:51.031 [ONMD(3528)]CRS-1607: Node jfs13 is being evicted
in cluster incarnation 621599354; details at (:CSSNM00007:) in
/gridbase/diag/crs/jfs12/crs/trace/onmd.trc.
2024-09-12 10:56:52.390 [CRSD(6668)]CRS-7503: The Oracle Grid
Infrastructure process 'crsd' observed communication issues between node
'jfs12' and node 'jfs13', interface list of local node 'jfs12' is
'192.168.30.1:33194;', interface list of remote node 'jfs13' is
'192.168.30.2:33621;'.
2024-09-12 10:56:55.683 [ONMD(3528)]CRS-1601: CSSD Reconfiguration
complete. Active nodes are jfs12 .
2024-09-12 10:56:55.722 [CRSD(6668)]CRS-5504: Node down event reported for
node 'jfs13'.
2024-09-12 10:56:57.222 [CRSD(6668)]CRS-2773: Server 'jfs13' has been
removed from pool 'Generic'.
2024-09-12 10:56:57.224 [CRSD(6668)]CRS-2773: Server 'jfs13' has been
removed from pool 'ora.NTAP'.
```

Fallo de comunicación de SnapMirror

Si el enlace de replicación de sincronización activa de SnapMirror, el I/O de escritura no se puede completar porque sería imposible que un clúster replique los cambios en el sitio opuesto.

Centro a

El resultado en el sitio A de un fallo de enlace de replicación será una pausa de aproximadamente 15 segundos en el procesamiento de E/S de escritura, ya que ONTAP intenta replicar las escrituras antes de determinar que el enlace de replicación es realmente inoperable. Después de transcurridos 15 segundos, el clúster de ONTAP en el sitio A reanuda el procesamiento de I/O de lectura y escritura. Las rutas de SAN no se modificarán y los LUN permanecerán en línea.

Centro B

Dado que el sitio B no es el sitio preferido de sincronización activa de SnapMirror, sus rutas de LUN dejarán de estar disponibles después de unos 15 segundos.

El enlace de replicación se cortó en la marca de tiempo 15:19:44. La primera advertencia de Oracle RAC llega 100 segundos después cuando se acerca el timeout de 200 segundos (controlado por el parámetro de Oracle RAC disktimeout).

```
2024-09-10 15:21:24.702 [ONMD(2792)]CRS-1615: No I/O has completed after
50% of the maximum interval. If this persists, voting file
/dev/mapper/grid2 will be considered not functional in 99340 milliseconds.
2024-09-10 15:22:14.706 [ONMD(2792)]CRS-1614: No I/O has completed after
75% of the maximum interval. If this persists, voting file
/dev/mapper/grid2 will be considered not functional in 49330 milliseconds.
2024-09-10 15:22:44.708 [ONMD(2792)]CRS-1613: No I/O has completed after
90% of the maximum interval. If this persists, voting file
/dev/mapper/grid2 will be considered not functional in 19330 milliseconds.
2024-09-10 15:23:04.710 [ONMD(2792)]CRS-1604: CSSD voting file is offline:
/dev/mapper/grid2; details at (:CSSNM00058:) in
/gridbase/diag/crs/jfs13/crs/trace/onmd.trc.
2024-09-10 15:23:04.710 [ONMD(2792)]CRS-1606: The number of voting files
available, 0, is less than the minimum number of voting files required, 1,
resulting in CSSD termination to ensure data integrity; details at
(:CSSNM00018:) in /gridbase/diag/crs/jfs13/crs/trace/onmd.trc
2024-09-10 15:23:04.716 [ONMD(2792)]CRS-1699: The CSS daemon is
terminating due to a fatal error from thread:
clssnmvDiskPingMonitorThread; Details at (:CSSSC00012:) in
/gridbase/diag/crs/jfs13/crs/trace/onmd.trc
2024-09-10 15:23:04.731 [OCSSD(2794)]CRS-1652: Starting clean up of CRSD
resources.
```

Una vez alcanzado el tiempo de espera del disco de quorum de 200 segundos, este nodo de Oracle RAC se expulsará del cluster y se reiniciará.

Fallo total de interconexión de red

Si el enlace de replicación entre las ubicaciones se pierde por completo, se interrumpirán tanto la conectividad de SnapMirror Active Sync como la de Oracle RAC.

La detección de cerebro dividido de Oracle RAC depende de los latidos del corazón del almacenamiento de Oracle RAC. Si la pérdida de conectividad de sitio a sitio provoca una pérdida simultánea de los latidos de la red de RAC y de los servicios de replicación de almacenamiento, el resultado es que los sitios de RAC no podrán comunicarse entre sitios ni a través de la interconexión de RAC ni de los discos de quorum de RAC. El resultado de un conjunto de nodos de numeración uniforme puede ser la expulsión de ambos sitios en la configuración predeterminada. El comportamiento exacto dependerá de la secuencia de eventos y del tiempo de la red RAC y de los sondeos de latidos del disco.

El riesgo de una interrupción del servicio de 2 sitios puede abordarse de dos maneras. En primer lugar, se

puede utilizar una "tiebreaker" configuración.

Si no hay un sitio 3rd disponible, este riesgo se puede solucionar ajustando el parámetro misscount en el cluster RAC. Bajo los valores predeterminados, el tiempo de espera de latido de la red RAC es de 30 segundos. RAC lo utiliza normalmente para identificar los nodos de RAC fallidos y quitarlos del cluster. También tiene una conexión con el latido del disco de votación.

Si, por ejemplo, un retroexcavador corta el conducto que transporta el tráfico entre sitios tanto para Oracle RAC como para los servicios de replicación de almacenamiento, comenzará la cuenta atrás de 30 segundos de recuento de errores. Si el nodo de sitio preferido de RAC no puede restablecer el contacto con el sitio opuesto en 30 segundos, y tampoco puede utilizar los discos de votación para confirmar que el sitio opuesto está caído dentro de la misma ventana de 30 segundos, entonces los nodos de sitio preferidos también expulsarán. El resultado es una interrupción completa de la base de datos.

Dependiendo de cuándo se produzca el sondeo de recuento incorrecto, es posible que 30 segundos no sean suficientes para que se agote el tiempo de espera de la sincronización activa de SnapMirror y que el almacenamiento del sitio preferido reanude los servicios antes de que caduque la ventana de 30 segundos. Esta ventana de 30 segundos se puede aumentar.

```
[root@jfs12 ~]# /grid/bin/crsctl set css misscount 100
CRS-4684: Successful set of parameter misscount to 100 for Cluster
Synchronization Services.
```

Este valor permite que el sistema de almacenamiento del sitio preferido reanude las operaciones antes de que se agote el tiempo de espera del recuento erróneo. A continuación, el resultado solo se expulsará de los nodos del sitio donde se quitaron las rutas de LUN. Ejemplo a continuación:

```
2024-09-12 09:50:59.352 [ONMD(681360)]CRS-1612: Network communication with
node jfs13 (2) has been missing for 50% of the timeout interval.  If this
persists, removal of this node from cluster will occur in 49.570 seconds
2024-09-12 09:51:10.082 [CRSD(682669)]CRS-7503: The Oracle Grid
Infrastructure process 'crsd' observed communication issues between node
'jfs12' and node 'jfs13', interface list of local node 'jfs12' is
'192.168.30.1:46039;', interface list of remote node 'jfs13' is
'192.168.30.2:42037;'.
2024-09-12 09:51:24.356 [ONMD(681360)]CRS-1611: Network communication with
node jfs13 (2) has been missing for 75% of the timeout interval.  If this
persists, removal of this node from cluster will occur in 24.560 seconds
2024-09-12 09:51:39.359 [ONMD(681360)]CRS-1610: Network communication with
node jfs13 (2) has been missing for 90% of the timeout interval.  If this
persists, removal of this node from cluster will occur in 9.560 seconds
2024-09-12 09:51:47.527 [OHASD(680884)]CRS-8011: reboot advisory message
from host: jfs13, component: cssagent, with time stamp: L-2024-09-12-
09:51:47.451
2024-09-12 09:51:47.527 [OHASD(680884)]CRS-8013: reboot advisory message
text: oracssdagent is about to reboot this node due to unknown reason as
it did not receive local heartbeats for 10470 ms amount of time
2024-09-12 09:51:48.925 [ONMD(681360)]CRS-1632: Node jfs13 is being
removed from the cluster in cluster incarnation 621596607
```

Los Servicios de Soporte Oracle no recomiendan modificar los parámetros misscount o disktimeout para resolver problemas de configuración. Sin embargo, los cambios de estos parámetros pueden garantizarse e evitarse en muchos casos, incluido el arranque SAN, la virtualización y las configuraciones de replicación del almacenamiento. Si, por ejemplo, tenía problemas de estabilidad con una red SAN o IP que provocaba expulsiones de RAC, debería corregir el problema subyacente y no cargar los valores del recuento de errores o el tiempo de espera del disco. Cambiar los tiempos de espera para corregir los errores de configuración es enmascarar un problema, no resolver un problema. Cambiar estos parámetros para configurar correctamente un entorno RAC basado en aspectos de diseño de la infraestructura subyacente es diferente y es coherente con las sentencias de soporte de Oracle. Con el arranque SAN, es común ajustar misscount hasta 200 para que coincida con el tiempo de espera del disco. Consulte "este enlace" para obtener información adicional.

Error en el centro

El resultado de un fallo del sistema de almacenamiento o del sitio es casi idéntico al resultado de perder el enlace de replicación. El sitio superviviente debería experimentar una pausa de I/O de aproximadamente 15 segundos en las escrituras. Una vez transcurrido ese período de 15 segundos, IO se reanudará en ese sitio como de costumbre.

Si solo el sistema de almacenamiento se vio afectado, el nodo de Oracle RAC del sitio donde se ha producido el fallo perderá los servicios de almacenamiento e introducirá la misma cuenta atrás con un tiempo de espera de disco de 200 segundos antes de su expulsión y reinicio posterior.

```
2024-09-11 13:44:38.613 [ONMD(3629)]CRS-1615: No I/O has completed after
50% of the maximum interval. If this persists, voting file
/dev/mapper/grid2 will be considered not functional in 99750 milliseconds.
2024-09-11 13:44:51.202 [ORAAGENT(5437)]CRS-5011: Check of resource "NTAP"
failed: details at "(:CLSN00007:)" in
"/gridbase/diag/crs/jfs13/crs/trace/crsd_oraagent_oracle.trc"
2024-09-11 13:44:51.798 [ORAAGENT(75914)]CRS-8500: Oracle Clusterware
ORAAGENT process is starting with operating system process ID 75914
2024-09-11 13:45:28.626 [ONMD(3629)]CRS-1614: No I/O has completed after
75% of the maximum interval. If this persists, voting file
/dev/mapper/grid2 will be considered not functional in 49730 milliseconds.
2024-09-11 13:45:33.339 [ORAAGENT(76328)]CRS-8500: Oracle Clusterware
ORAAGENT process is starting with operating system process ID 76328
2024-09-11 13:45:58.629 [ONMD(3629)]CRS-1613: No I/O has completed after
90% of the maximum interval. If this persists, voting file
/dev/mapper/grid2 will be considered not functional in 19730 milliseconds.
2024-09-11 13:46:18.630 [ONMD(3629)]CRS-1604: CSSD voting file is offline:
/dev/mapper/grid2; details at (:CSSNM00058:) in
/gridbase/diag/crs/jfs13/crs/trace/onmd.trc.
2024-09-11 13:46:18.631 [ONMD(3629)]CRS-1606: The number of voting files
available, 0, is less than the minimum number of voting files required, 1,
resulting in CSSD termination to ensure data integrity; details at
(:CSSNM00018:) in /gridbase/diag/crs/jfs13/crs/trace/onmd.trc
2024-09-11 13:46:18.638 [ONMD(3629)]CRS-1699: The CSS daemon is
terminating due to a fatal error from thread:
clssnmvDiskPingMonitorThread; Details at (:CSSSC00012:) in
/gridbase/diag/crs/jfs13/crs/trace/onmd.trc
2024-09-11 13:46:18.651 [OCSSD(3631)]CRS-1652: Starting clean up of CRSD
resources.
```

El estado de la ruta de SAN en el nodo RAC que ha perdido los servicios de almacenamiento se parece a este:

```
oradata7 (3600a0980383041334a3f55676c697347) dm-20 NETAPP,LUN C-Mode
size=128G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|-+- policy='service-time 0' prio=0 status=enabled
| `- 34:0:0:18 sdam 66:96  failed faulty running
`-+- policy='service-time 0' prio=0 status=enabled
  `- 33:0:0:18 sdaj 66:48  failed faulty running
```

El host linux detectó la pérdida de las rutas mucho más rápido que 200 segundos, pero desde el punto de vista de la base de datos, las conexiones del cliente al host en el sitio con errores se seguirán congelando durante 200 segundos en la configuración predeterminada de Oracle RAC. Las operaciones de base de datos completa solo se reanudarán una vez que se complete el expulsión.

Mientras tanto, el nodo de Oracle RAC en la ubicación opuesta registrará la pérdida del otro nodo de RAC. De lo contrario, sigue funcionando como de costumbre.

```
2024-09-11 13:46:34.152 [ONMD(3547)]CRS-1612: Network communication with
node jfs13 (2) has been missing for 50% of the timeout interval.  If this
persists, removal of this node from cluster will occur in 14.020 seconds
2024-09-11 13:46:41.154 [ONMD(3547)]CRS-1611: Network communication with
node jfs13 (2) has been missing for 75% of the timeout interval.  If this
persists, removal of this node from cluster will occur in 7.010 seconds
2024-09-11 13:46:46.155 [ONMD(3547)]CRS-1610: Network communication with
node jfs13 (2) has been missing for 90% of the timeout interval.  If this
persists, removal of this node from cluster will occur in 2.010 seconds
2024-09-11 13:46:46.470 [OHASD(1705)]CRS-8011: reboot advisory message
from host: jfs13, component: cssmonit, with time stamp: L-2024-09-11-
13:46:46.404
2024-09-11 13:46:46.471 [OHASD(1705)]CRS-8013: reboot advisory message
text: At this point node has lost voting file majority access and
oracssdmonitor is rebooting the node due to unknown reason as it did not
receive local hearbeats for 28180 ms amount of time
2024-09-11 13:46:48.173 [ONMD(3547)]CRS-1632: Node jfs13 is being removed
from the cluster in cluster incarnation 621516934
```

Fallo del mediador

El servicio de mediador no controla directamente las operaciones de almacenamiento. Funciona como una ruta de control alternativa entre los clústeres. Existe principalmente para automatizar la conmutación al nodo de respaldo sin el riesgo de un escenario de cerebro dividido.

En un funcionamiento normal, cada clúster está replicando los cambios en su compañero y, por lo tanto, cada clúster puede verificar que el clúster asociado esté en línea y sirviendo datos. Si el enlace de replicación falla, la replicación se detendría.

El motivo por el que se necesita un mediador para llevar a cabo operaciones automatizadas seguras es que, de otro modo, sería imposible que los clústeres de almacenamiento puedan determinar si la pérdida de comunicación bidireccional se debió a una interrupción de la red o a un error real de almacenamiento.

El mediador proporciona una ruta alternativa para que cada clúster compruebe el estado de su compañero. Los escenarios son los siguientes:

- Si un clúster puede ponerse en contacto directamente con su socio, los servicios de replicación están operativos. No se requiere ninguna acción.
- Si un sitio preferido no puede ponerse en contacto con su partner directamente o a través del mediador, se asumirá que el partner no está disponible o que se ha aislado y ha desconectado las rutas de LUN. El sitio preferido procederá a liberar el estado RPO=0 y continuará procesando las I/O de lectura y escritura.
- Si un sitio no preferido no puede ponerse en contacto directamente con su socio, pero puede contactarlo a través del mediador, tomará sus rutas fuera de línea y esperará la devolución de la conexión de replicación.

- Si un sitio no preferido no puede contactar a su partner directamente o a través de un mediador operativo, asumirá que el partner no está disponible o que se ha aislado y ha desconectado las rutas de LUN. El sitio no preferido continuará liberando el estado RPO=0 y continuará procesando las I/O de lectura y escritura. Asumirá el rol del origen de replicación y se convertirá en el nuevo sitio preferido.

Si el mediador no está totalmente disponible:

- Un fallo en los servicios de replicación por cualquier motivo provocará que el sitio preferido publique el estado RPO=0 y reanude el procesamiento de I/O de lectura y escritura. El sitio no preferido desconectará sus rutas.
- Un fallo del sitio preferido provocará una interrupción porque el sitio no preferido no podrá verificar que el sitio opuesto esté realmente fuera de línea y, por lo tanto, no sería seguro para el sitio no preferido reanudar los servicios.

Restauración del servicio

SnapMirror es reparación automática. La sincronización activa de SnapMirror detecta automáticamente la presencia de una relación de replicación defectuosa y la devuelve a un estado RPO=0. Una vez que se restablece la replicación síncrona, las rutas volverán a conectarse.

En muchos casos, las aplicaciones en clúster detectan automáticamente el retorno de las rutas fallidas, y dichas aplicaciones también volverán a estar online. En otros casos, puede ser necesario un análisis SAN a nivel de host o es posible que las aplicaciones deban volver a conectarse manualmente.

Depende de la aplicación y de cómo se configura, y en general tales tareas se pueden automatizar fácilmente. La sincronización activa de SnapMirror es autocorregida y no debería requerir la intervención del usuario para reanudar las operaciones de almacenamiento RPO=0 una vez que se restablezcan la alimentación y la conectividad.

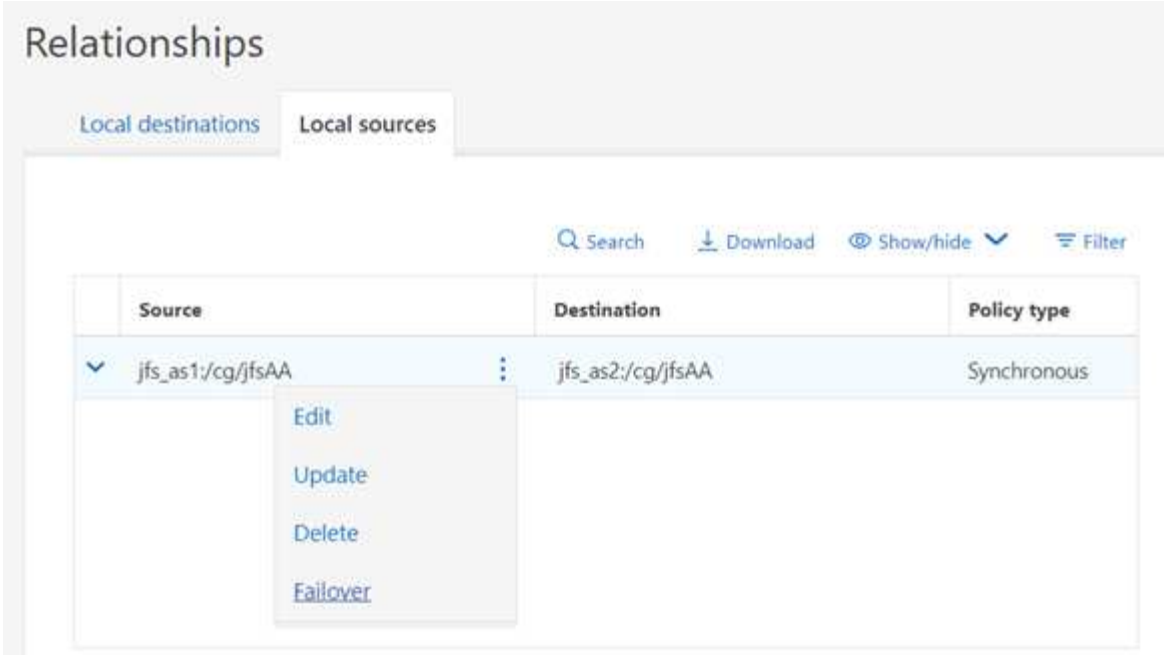
Recuperación manual tras fallos

El término «conmutación por error» no hace referencia a la dirección de la replicación con el servicio de sincronización activa de SnapMirror porque es una tecnología de replicación bidireccional. En su lugar, la recuperación tras fallos hace referencia al sistema de almacenamiento en el sitio preferido en caso de fallo.

Por ejemplo, puede que desee realizar una conmutación al respaldo para cambiar el sitio preferido antes de apagar un sitio por mantenimiento o antes de realizar una prueba de recuperación ante desastres.

Cambiar el sitio preferido requiere una operación simple. I/O se detendrá durante un segundo o dos como autoridad sobre los cambios en el comportamiento de replicación entre los clústeres, pero I/O de otro modo no se verá afectado.

Ejemplo de interfaz gráfica de usuario:



Ejemplo de cambio a través de la CLI:

```
Cluster2::> snapmirror failover start -destination-path jfs_as2:/cg/jfsAA
[Job 9575] Job is queued: SnapMirror failover for destination
"jfs_as2:/cg/jfsAA                        ".

Cluster2::> snapmirror failover show

Source    Destination                                            Error
Path      Path        Type     Status    start-time end-time    Reason
--------- ----------  -------- --------- ---------- ---------- ----------
jfs_as1:/cg/jfsAA
          jfs_as2:/cg/jfsAA
                      planned  completed 9/11/2024  9/11/2024
                                         09:29:22   09:29:32

The new destination path can be verified as follows:


Cluster1::> snapmirror show -destination-path jfs_as1:/cg/jfsAA

                           Source Path: jfs_as2:/cg/jfsAA
                        Destination Path: jfs_as1:/cg/jfsAA
                      Relationship Type: XDP
                Relationship Group Type: consistencygroup
                 SnapMirror Policy Type: automated-failover-duplex
                      SnapMirror Policy: AutomatedFailOverDuplex
                            Tries Limit: -
                           Mirror State: Snapmirrored
                    Relationship Status: InSync
```

Migración de bases de datos de Oracle

Descripción general

El aprovechamiento de las funciones de una nueva plataforma de almacenamiento tiene un requisito inevitable: Los datos deben estar situados en el nuevo sistema de almacenamiento. ONTAP simplifica el proceso de migración, lo que incluye migraciones y actualizaciones de ONTAP a ONTAP, importaciones de LUN externas y procedimientos para utilizar directamente el sistema operativo del host o el software de base de datos de Oracle.

Esta documentación sustituye al informe técnico *TR-4534: Migración de bases de datos de Oracle a sistemas de almacenamiento de NetApp*

En el caso de un nuevo proyecto de base de datos, no se trata de un problema, ya que los entornos de bases de datos y aplicaciones están construidos in situ. Sin embargo, la migración plantea desafíos especiales con

respecto a la interrupción del negocio, el tiempo necesario para completar la migración, las habilidades necesarias y la minimización de riesgos.

Scripts

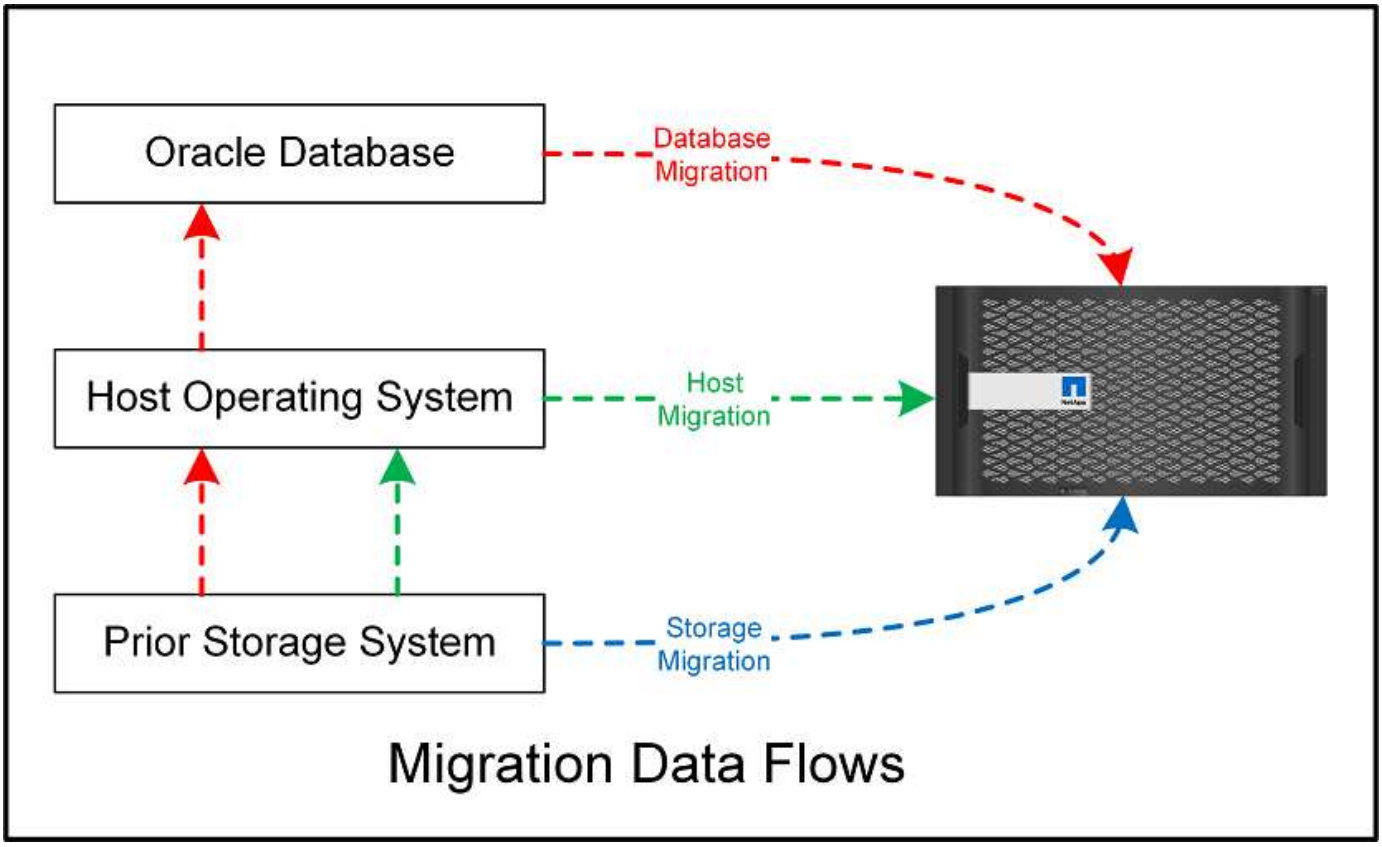
En esta documentación se proporcionan secuencias de comandos de ejemplo. Estos scripts proporcionan métodos de ejemplo de automatización de diversos aspectos de la migración para reducir la posibilidad de errores de usuario. Las secuencias de comandos pueden reducir las demandas generales sobre el PERSONAL DE TI responsable de la migración y pueden acelerar el proceso general. Todos estos scripts se extraen de los proyectos de migración reales realizados por los servicios profesionales de NetApp y los partners de NetApp. A lo largo de esta documentación se muestran ejemplos de su uso.

Planificación de migración

La migración de datos de Oracle puede producirse en uno de tres niveles: La base de datos, el host o la cabina de almacenamiento.

Las diferencias residen en qué componente de la solución general es responsable del movimiento de datos: La base de datos, el sistema operativo del host o el sistema de almacenamiento.

La siguiente figura muestra un ejemplo de los niveles de migración y el flujo de datos. En el caso de la migración a nivel de base de datos, los datos se mueven desde el sistema de almacenamiento original a través de las capas de base de datos y host al nuevo entorno. La migración al nivel de host es similar, pero los datos no pasan a través de la capa de aplicaciones y, en su lugar, se escriben en la nueva ubicación mediante procesos de host. Por último, con la migración a nivel del almacenamiento, una cabina como un sistema NetApp FAS es responsable del movimiento de datos.



Una migración a nivel de base de datos generalmente hace referencia al uso del envío de logs de Oracle a través de una base de datos en espera para completar una migración en la capa de Oracle. Las migraciones a

nivel de host se realizan utilizando la capacidad nativa de la configuración del sistema operativo host. Esta configuración incluye operaciones de copia de archivos mediante comandos como cp, tar y Oracle Recovery Manager (RMAN) o mediante un gestor de volúmenes lógicos (LVM) para reubicar los bytes subyacentes de un sistema de archivos. Oracle Automatic Storage Management (ASM) se clasifica como una capacidad de nivel de host porque se ejecuta por debajo del nivel de la aplicación de base de datos. ASM sustituye al administrador de volúmenes lógicos habitual en un host. Por último, los datos pueden migrarse a nivel de cabina de almacenamiento, lo cual significa que se encuentra debajo del nivel del sistema operativo.

Consideraciones DE PLANIFICACIÓN

La mejor opción para la migración depende de una combinación de factores, como la escala del entorno que se va a migrar, la necesidad de evitar el tiempo de inactividad y el esfuerzo general requerido para realizar la migración. Obviamente, las bases de datos grandes requieren más tiempo y esfuerzo para la migración, pero la complejidad de estas migraciones es mínima. Las bases de datos pequeñas se pueden migrar rápidamente, pero, si hay miles que migrar, la escala del esfuerzo puede crear complicaciones. Por último, cuanto mayor sea la base de datos, más probabilidades hay de que sea crítica para el negocio, lo cual da lugar a la necesidad de minimizar los tiempos de inactividad a la vez que se conserva una ruta de back-out.

Aquí se tratan algunas de las consideraciones para planificar una estrategia de migración.

Tamaño de datos

Los tamaños de las bases de datos que se migrarán afectan obviamente a la planificación de la migración, aunque el tamaño no afecta necesariamente al tiempo de transición. Cuando es necesario migrar una gran cantidad de datos, la principal cuestión es el ancho de banda. Las operaciones de copia suelen realizarse con I/O secuenciales eficientes Según estimaciones conservadoras, asuma el aprovechamiento del 50% del ancho de banda de red disponible para operaciones de copia. Por ejemplo, un puerto FC de 8GB Gb puede transferir aproximadamente 800Mbps Gb en teoría. Suponiendo una utilización del 50%, se puede copiar una base de datos a una velocidad de aproximadamente 400Mbps KB. Por lo tanto, una base de datos de 10TB TB se puede copiar en unas siete horas a esta velocidad.

La migración a distancias más largas generalmente requiere un enfoque más creativo, como el proceso de envío de registros explicado en "Movimiento de archivos de datos en línea". Las redes IP de larga distancia rara vez tienen ancho de banda en cualquier lugar cercano a las velocidades LAN o SAN. En un caso, NetApp ayudó en la migración a larga distancia de una base de datos de 220TB con tasas muy altas de generación de registros de archivo. El enfoque elegido para la transferencia de datos era el envío diario de cintas, ya que este método ofrecía el máximo ancho de banda posible.

Recuento de bases de datos

En muchos casos, el problema de mover una gran cantidad de datos no es el tamaño de los datos, sino la complejidad de la configuración que soporta la base de datos. No basta con saber que deben migrarse 50TB TB de bases de datos. Podría ser una única base de datos de misión crítica de 50TB TB, una colección de 4, 000 bases de datos heredadas o una combinación de datos de producción y no de producción. En algunos casos, gran parte de los datos se componen de clones de una base de datos de origen. Estos clones no tienen que migrarse de ninguna manera, ya que pueden volver a crearse fácilmente, especialmente cuando la nueva arquitectura está diseñada para aprovechar los volúmenes FlexClone de NetApp.

Para la planificación de la migración, hay que entender cuántas bases de datos están incluidas y cómo deben priorizarse. A medida que aumenta el número de bases de datos, la opción de migración preferida tiende a ser más baja y más baja en la pila. Por ejemplo, la copia de una única base de datos se puede realizar fácilmente con RMAN y una interrupción breve. Es la replicación a nivel de host.

Si hay bases de datos 50, es posible que sea más fácil evitar configurar una nueva estructura del sistema de archivos para recibir una copia de RMAN y, en su lugar, mover los datos. Este proceso puede realizarse

aprovechando la migración de LVM basada en host para reubicar datos de las LUN antiguas a nuevas LUN. De este modo, se traslada la responsabilidad del equipo del administrador de la base de datos (DBA) al equipo del sistema operativo y, como resultado, los datos se migran de forma transparente con respecto a la base de datos. La configuración del sistema de archivos no cambia.

Por último, si es necesario migrar 500 bases de datos en 200 servidores, pueden utilizarse opciones basadas en almacenamiento como la funcionalidad Importación de LUN externas (FLI) de ONTAP para realizar una migración directa de las LUN.

Vuelva a crear los requisitos de la arquitectura

Normalmente, el diseño de un archivo de base de datos debe modificarse para aprovechar las funciones de la nueva cabina de almacenamiento; sin embargo, esto no siempre es así. Por ejemplo, las funciones de las cabinas all-flash EF-Series se dirigen principalmente al rendimiento SAN y la fiabilidad de SAN. En la mayoría de los casos, las bases de datos pueden migrarse a una cabina EF-Series sin tener en cuenta ninguna necesidad de distribución de los datos. Los únicos requisitos son el alto nivel de IOPS, la baja latencia y la sólida fiabilidad. Aunque existen prácticas recomendadas en relación con factores como la configuración de RAID o los pools de discos dinámicos, los proyectos EF-Series rara vez requieren cambios significativos en la arquitectura general de almacenamiento para aprovechar estas funciones.

Por el contrario, la migración a ONTAP generalmente requiere tener en cuenta el diseño de la base de datos para asegurarse de que la configuración final aporta el máximo valor. Por sí mismo, ONTAP ofrece muchas funciones para un entorno de base de datos, incluso sin ningún esfuerzo de arquitectura específico. Y lo que es más importante, ofrece la capacidad de migrar sin interrupciones a un nuevo hardware cuando el hardware actual llega al final de su vida útil. En términos generales, una migración a ONTAP es la última migración que se debería realizar. Se actualiza el hardware subsiguiente in situ y los datos se migran a los nuevos medios de forma no disruptiva.

Con un poco de planificación, aún hay más beneficios disponibles. Las consideraciones más importantes rodean el uso de instantáneas. Las copias Snapshot son la base para realizar backups, restauraciones de datos y operaciones de clonado casi instantáneas. Como ejemplo del potencial de las copias Snapshot, el uso más grande conocido es con una única base de datos de 996TB TB que se ejecuta en unas 250 LUN en 6 controladoras. Puede realizarse backup de esta base de datos en 2 minutos, restaurarse en 2 minutos y clonarse en 15 minutos. Entre otras ventajas, se incluyen la capacidad de mover datos por el clúster en respuesta a los cambios en la carga de trabajo y la aplicación de controles de calidad de servicio para proporcionar un buen rendimiento constante en un entorno multibase de datos.

Tecnologías como los controles de calidad de servicio, la reubicación de datos, las snapshots y el clonado funcionan en prácticamente cualquier configuración. Sin embargo, generalmente se requiere algo de pensamiento para maximizar los beneficios. En algunos casos, la distribución del almacenamiento de la base de datos puede requerir cambios en el diseño para maximizar la inversión en la nueva cabina de almacenamiento. Estos cambios de diseño pueden afectar a la estrategia de migración, ya que las migraciones basadas en host o basadas en almacenamiento replican la distribución de datos original. Podrían ser necesarios pasos adicionales para completar la migración y ofrecer una distribución de datos optimizada para ONTAP. Los procedimientos que se muestran en la "Descripción general de los procedimientos de migración de Oracle" y más tarde, mostrar algunos de los métodos no solo para migrar una base de datos, sino para migrarla al diseño final óptimo con el mínimo esfuerzo.

Tiempo de transición

Se debe determinar la interrupción máxima permitida del servicio durante la transición. Es un error común asumir que todo el proceso de migración provoca interrupciones. Muchas tareas pueden completarse antes de que comience cualquier interrupción del servicio y muchas opciones permiten completar la migración sin interrupciones ni interrupciones del servicio. Incluso cuando resulte imposible evitar las interrupciones, debe definir la interrupción del servicio máxima permitida, puesto que la duración del tiempo de transición varía de

un procedimiento a otro.

Por ejemplo, la copia de una base de datos de 10TB GB normalmente requiere aproximadamente siete horas para completarse. Si su empresa necesita permitir un fallo de siete horas, la copia de archivos es una opción fácil y segura para la migración. Si cinco horas son inaceptables, un simple proceso de envío de registros (consulte "Envío de registros de Oracle") puede configurarse con un esfuerzo mínimo para reducir el tiempo de transición a aproximadamente 15 minutos. Durante este tiempo, un administrador de la base de datos puede completar el proceso. Si 15 minutos son inaceptables, el proceso final de transición se puede automatizar mediante secuencias de comandos para reducir el tiempo de transición a tan solo unos minutos. Siempre se puede acelerar la migración, pero hacerlo conlleva un coste de tiempo y esfuerzo. Los objetivos de tiempo de transición deben basarse en lo que sea aceptable para la empresa.

Ruta de retroceso

Ninguna migración está completamente exenta de riesgos. Incluso si la tecnología funciona perfectamente, siempre existe la posibilidad de error del usuario. El riesgo asociado a una ruta de migración elegida debe tenerse en cuenta junto con las consecuencias de una migración fallida. Por ejemplo, la capacidad transparente de migración de almacenamiento en línea de Oracle ASM es una de sus funciones clave, y este método es una de las más fiables conocidas. Sin embargo, los datos se copian de forma irreversible con este método. En el caso muy poco probable de que se produzca un problema con ASM, no hay una ruta de salida fácil. La única opción es restaurar el entorno original o utilizar ASM para revertir la migración de nuevo a las LUN originales. El riesgo puede minimizarse, pero no eliminarse, realizando un backup del tipo snapshot en el sistema de almacenamiento original, asumiendo que el sistema sea capaz de realizar dicha operación.

Ensayo

Algunos procedimientos de migración deben verificarse por completo antes de la ejecución. La necesidad de migración y ensayo del proceso de transición es una solicitud común con bases de datos críticas para la misión para la que la migración debe tener éxito y se debe minimizar el tiempo de inactividad. Además, las pruebas de aceptación del usuario se incluyen con frecuencia como parte del trabajo posterior a la migración y el sistema en general solo puede volver a la producción una vez que se hayan completado estas pruebas.

Si hay una necesidad de ensayo, varias capacidades de ONTAP pueden hacer el proceso mucho más fácil. En particular, las copias Snapshot pueden restablecer un entorno de prueba y crear rápidamente varias copias con gestión eficiente del espacio de un entorno de base de datos.

Procedimientos

Descripción general

Hay muchos procedimientos disponibles para la base de datos de migración de Oracle. El correcto depende de las necesidades de su empresa.

En muchos casos, los administradores de sistemas y los administradores de bases de datos cuentan con sus propios métodos preferidos para reubicar datos de volúmenes físicos, realizar mirroring y desduplicación o utilizar Oracle RMAN para copiar datos.

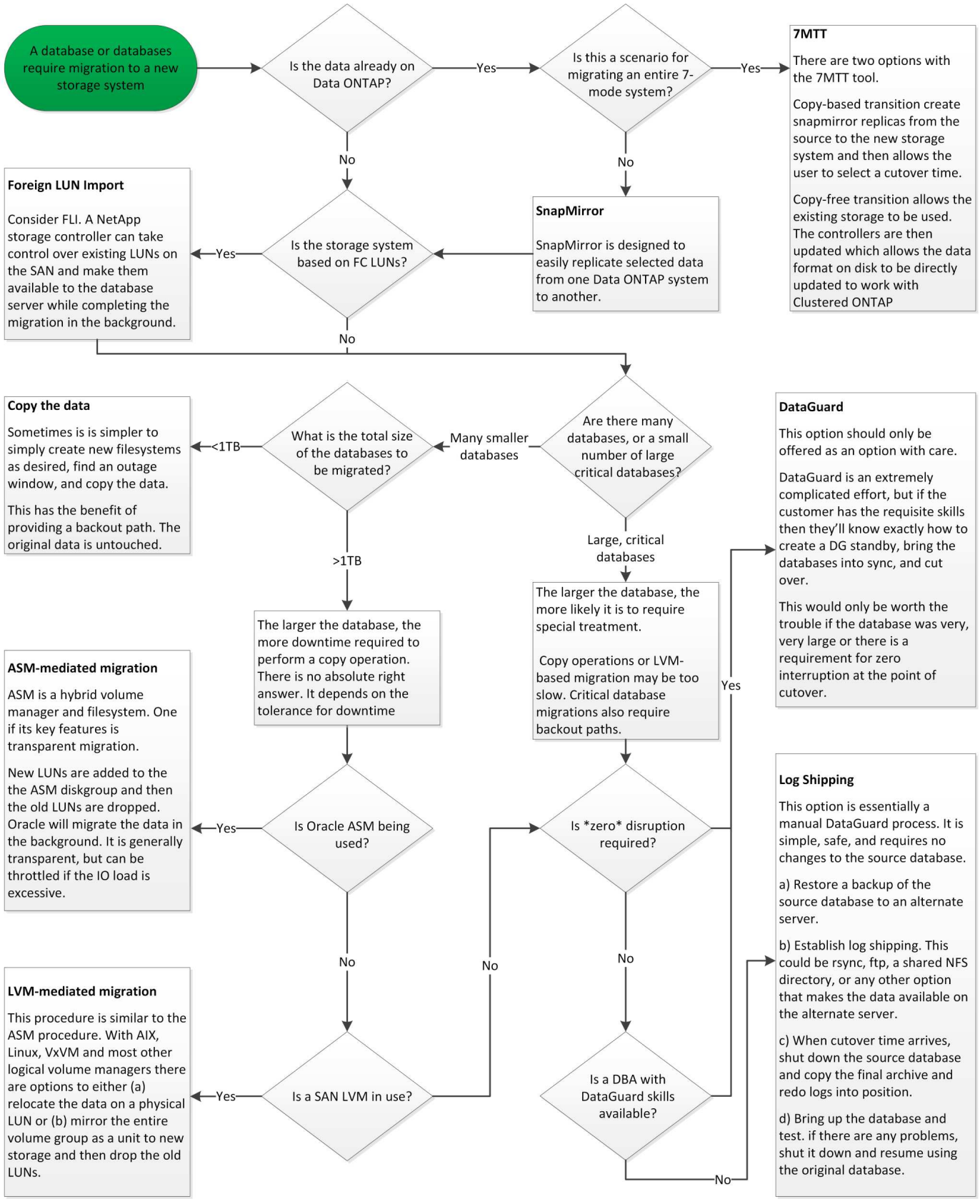
Estos procedimientos se proporcionan principalmente como orientación para el PERSONAL DE TI menos familiarizado con algunas de las opciones disponibles. Además, los procedimientos muestran las tareas, los requisitos de tiempo y las demandas de habilidades para cada método de migración. De este modo, otras partes como NetApp y los servicios profesionales de partners o el equipo de gestión de TI pueden apreciar de forma más completa los requisitos de cada procedimiento.

No existe una práctica recomendada única para crear una estrategia de migración. La creación de un plan

requiere primero comprender las opciones de disponibilidad y luego seleccionar el método que mejor se adapte a las necesidades del negocio. La siguiente figura ilustra las consideraciones básicas y las conclusiones típicas de los clientes, pero no es universalmente aplicable a todas las situaciones.

Por ejemplo, un paso plantea el problema del tamaño total de la base de datos. El siguiente paso depende de si la base de datos es mayor o menor que 1TB. Los pasos recomendados son simplemente eso: Recomendaciones basadas en las prácticas típicas del cliente. La mayoría de los clientes no utilizarían DataGuard para copiar una base de datos pequeña, pero algunos podrían. La mayoría de los clientes no intentarían copiar una base de datos de 50TB GB debido al tiempo necesario, pero algunos pueden tener una ventana de mantenimiento lo suficientemente grande como para permitir dicha operación.

El siguiente diagrama de flujo muestra los tipos de consideraciones sobre la ruta de migración que es mejor. Puede hacer clic con el botón derecho en la imagen y abrirla en una nueva pestaña para mejorar la legibilidad.



.

Movimiento de archivos de datos en línea

Oracle 12cR1 y las versiones superiores incluyen la capacidad de mover un archivo de datos mientras la base de datos permanece en línea. Además, funciona entre diferentes tipos de sistemas de archivos. Por ejemplo,

un archivo de datos se puede reubicar de un sistema de archivos xfs a ASM. Este método no se utiliza generalmente a escala debido al número de operaciones de movimiento de archivos de datos individuales que serían necesarias, pero es una opción que vale la pena considerar con bases de datos más pequeñas con menos archivos de datos.

Además, simplemente mover un archivo de datos es una buena opción para migrar partes de bases de datos existentes. Por ejemplo, los archivos de datos menos activos podrían reubicarse en un almacenamiento más rentable, como un volumen FabricPool que pueda almacenar bloques inactivos en el almacén de objetos.

Migración a nivel de base de datos

La migración a nivel de base de datos implica permitir que la base de datos vuelva a ubicar los datos. Específicamente, esto significa el envío de registros. Tecnologías como RMAN y ASM son productos de Oracle, pero, para la migración, funcionan en el nivel de host en el que copian archivos y gestionan volúmenes.

Trasvase de registros

La base para la migración a nivel de base de datos es el archive log de Oracle, que contiene un log de los cambios realizados en la base de datos. La mayoría de las veces, un registro de archivo forma parte de una estrategia de backup y recuperación. El proceso de recuperación comienza con la restauración de una base de datos y luego la reproducción de uno o más registros de archivos para que la base de datos alcance el estado deseado. Esta misma tecnología básica se puede usar para realizar una migración con poca o ninguna interrupción de las operaciones. Y lo que es más importante, esta tecnología permite la migración sin modificar la base de datos original, lo que mantiene un camino de back-out.

El proceso de migración comienza con la restauración de un backup de base de datos a un servidor secundario. Puede hacerlo de varias formas, pero la mayoría de los clientes utilizan su aplicación de backup normal para restaurar los archivos de datos. Después de restaurar los archivos de datos, los usuarios establecen un método para el envío de registros. El objetivo es crear una fuente constante de los archive logs generados por la base de datos primaria y reproducirlos en la base de datos restaurada para mantenerlos cerca del mismo estado. Cuando llega el tiempo de transposición, la base de datos de origen se cierra por completo y los archive logs finales, y en algunos casos los redo logs, se copian y se vuelven a reproducir. Es fundamental que los redo logs también se tengan en cuenta porque pueden contener algunas de las transacciones finales confirmadas.

Después de transferir y reproducir estos registros, ambas bases de datos son coherentes entre sí. En este momento, la mayoría de los clientes realizan algunas pruebas básicas. Si se produce algún error durante el proceso de migración, la reproducción de log debe informar de los errores y fallar. Aún es aconsejable realizar algunas pruebas rápidas basadas en consultas conocidas o actividades controladas por aplicaciones para verificar que la configuración es óptima. También es una práctica común crear una tabla de prueba final antes de cerrar la base de datos original para verificar si está presente en la base de datos migrada. Este paso garantiza que no se hayan producido errores durante la sincronización del registro final.

Una simple migración de envío de registros se puede configurar fuera de banda con respecto a la base de datos original, lo que la hace particularmente útil para las bases de datos de misión crítica. No se requieren cambios de configuración para la base de datos de origen, y la restauración y configuración inicial del entorno de migración no afectan a las operaciones de producción. Después de configurar el envío de registros, coloca algunas demandas de E/S en los servidores de producción. Sin embargo, el envío de registros consiste en lecturas secuenciales simples de los archive logs, lo que es poco probable que afecte al rendimiento de la base de datos de producción.

El envío de registros ha demostrado ser particularmente útil para proyectos de migración de larga distancia y alta tasa de cambio. En un ejemplo, una sola base de datos de 220TB TB se migró a una nueva ubicación aproximadamente a 500 kilómetros de distancia. La tasa de cambio fue extremadamente alta y las

restricciones de seguridad impidieron el uso de una conexión de red. El envío de registros se realizó mediante cinta y mensajería. Se restauró inicialmente una copia de la base de datos de origen mediante los procedimientos descritos a continuación. A continuación, los registros se enviaron semanalmente por mensajería hasta el momento de la transición, cuando se entregó el conjunto final de cintas y se aplicaron los registros a la base de datos de réplica.

Oracle DataGuard

En algunos casos, se garantiza un entorno DataGuard completo. No es correcto utilizar el término DataGuard para hacer referencia a cualquier envío de log o configuración de base de datos en espera. Oracle DataGuard es un marco completo para gestionar la replicación de bases de datos, pero no es una tecnología de replicación. La principal ventaja de un entorno DataGuard completo en un esfuerzo de migración es el switchover transparente de una base de datos a otra. DATAGUARD también permite un switchover transparente a la base de datos original si se detecta un problema, como un problema de rendimiento o conectividad de red con el nuevo entorno. Un entorno DataGuard completamente configurado requiere la configuración no sólo de la capa de base de datos, sino también de las aplicaciones, de modo que las aplicaciones puedan detectar un cambio en la ubicación de la base de datos primaria. En general, no es necesario utilizar DataGuard para completar una migración, pero algunos clientes tienen una amplia experiencia en DataGuard interna y ya dependen de ella para el trabajo de migración.

Vuelva a diseñar la arquitectura

Como hemos visto anteriormente, aprovechar las funciones avanzadas de las cabinas de almacenamiento en ocasiones requiere cambiar el diseño de la base de datos. Además, un cambio en el protocolo de almacenamiento, como migrar de ASM a un sistema de archivos NFS, altera necesariamente la distribución del sistema de archivos.

Una de las principales ventajas de los métodos de envío de registros, incluido DataGuard, es que el destino de replicación no tiene que coincidir con el origen. No hay problemas con el uso de un enfoque de envío de logs para migrar de ASM a un sistema de archivos normal o viceversa. El diseño preciso de los archivos de datos se puede cambiar en el destino para optimizar el uso de la tecnología de base de datos conectable (PDB) o para establecer controles de QoS de forma selectiva en ciertos archivos. En otras palabras, un proceso de migración basado en el envío de registros le permite optimizar el diseño de almacenamiento de la base de datos de forma fácil y segura.

Recursos del servidor

La necesidad de un segundo servidor es una limitación para la migración a nivel de base de datos. Hay dos maneras de usar este segundo servidor:

1. Puede utilizar el segundo servidor como nuevo directorio raíz permanente para la base de datos.
2. Puede utilizar el segundo servidor como servidor temporal. Una vez completada y probada la migración de datos a la nueva cabina de almacenamiento, los sistemas de archivos LUN o NFS se desconectan del servidor provisional y se vuelven a conectar al servidor original.

La primera opción es la más fácil, pero su uso podría no ser factible en entornos muy grandes que requieran servidores muy potentes. La segunda opción requiere trabajo adicional para volver a ubicar los sistemas de archivos en la ubicación original. Esta operación puede ser sencilla en la que NFS se utiliza como protocolo de almacenamiento, ya que los sistemas de archivos se pueden desmontar del servidor de almacenamiento provisional y volver a montarse en el servidor original.

Los sistemas de archivos basados en bloques requieren trabajo adicional para actualizar la división en zonas de FC o los iniciadores de iSCSI. Con la mayoría de los administradores de volúmenes lógicos (incluido ASM), los LUN se detectan automáticamente y se conectan después de que estén disponibles en el servidor original.

Sin embargo, algunas implementaciones de sistemas de archivos y LVM pueden requerir más trabajo para exportar e importar los datos. El procedimiento preciso puede variar, pero generalmente es fácil establecer un procedimiento simple y repetible para completar la migración y volver a alojar los datos en el servidor original.

Aunque es posible configurar el envío de logs y replicar una base de datos en un entorno de servidor único, la nueva instancia debe tener un SID de proceso diferente para reproducir los logs. Es posible traer temporalmente la base de datos bajo un juego diferente de IDs de proceso con un SID diferente y cambiarla más tarde. Sin embargo, esta operación puede resultar en una gran cantidad de actividades de gestión complicadas y pone en riesgo al entorno de bases de datos de que se produzcan errores por parte del usuario.

Migración de nivel de host

Migrar datos a nivel de host significa utilizar el sistema operativo del host y las utilidades asociadas para completar la migración. Este proceso incluye cualquier utilidad que copie datos, incluidos Oracle RMAN y Oracle ASM.

Copiado de datos

No se debe subestimar el valor de una operación de copia simple. Las infraestructuras de red modernas pueden transferir datos a velocidades medidas en gigabytes por segundo y las operaciones de copia de archivos se basan en una eficiente E/S de lectura y escritura secuencial Una operación de copia de host no puede evitar más interrupciones cuando se compara con el envío de registros, pero una migración supone algo más que movimiento de datos. Por lo general, incluye cambios en las redes, el tiempo de reinicio de la base de datos y las pruebas posteriores a la migración.

El tiempo real necesario para copiar los datos puede no ser significativo. Además, una operación de copia conserva una ruta de back-out garantizada, ya que los datos originales permanecen sin tocar. Si se produce algún problema durante el proceso de migración, se pueden volver a activar los sistemas de archivos originales con los datos originales.

Cambio de la plataforma

El cambio de plataforma hace referencia a un cambio en el tipo de CPU. Cuando una base de datos se migra desde una plataforma tradicional Solaris, AIX o HP-UX a x86 Linux, los datos se deben volver a formatear debido a los cambios en la arquitectura de la CPU. Las CPU SPARC, IA64 y POWER se conocen como procesadores big endian, mientras que las arquitecturas x86 y x86_64 se conocen como little endian. Como resultado, algunos datos de los archivos de datos de Oracle se ordenan de forma diferente dependiendo del procesador en uso.

Tradicionalmente, los clientes utilizaban DataPump para replicar datos entre plataformas. DataPump es una utilidad que crea un tipo especial de exportación de datos lógicos que se puede importar más rápidamente en la base de datos destino. Debido a que crea una copia lógica de los datos, DataPump deja atrás las dependencias de endianness del procesador. Algunos clientes siguen utilizando DataPump para la transformación de plataformas, pero se ha puesto a disposición una opción más rápida con los tablespaces transportables multiplataforma de Oracle 11g:. Este avance permite que un tablespace se convierta a un formato endian diferente. Se trata de una transformación física que ofrece un mejor rendimiento que una exportación de DataPump, que debe convertir bytes físicos en datos lógicos y luego volver a convertir a bytes físicos.

No se trata completamente de la NetApp documentación de DataPump y los espacios de tablas transportables. No obstante, NetApp cuenta con algunas recomendaciones basadas en nuestra experiencia al ayudar a los clientes durante la migración a un nuevo registro de cabina de almacenamiento con una nueva arquitectura de CPU:

- Si se utiliza DataPump, el tiempo necesario para completar la migración se debe medir en un entorno de prueba. A veces, los clientes se sorprenden por el momento necesario para completar la migración. Este tiempo de inactividad adicional inesperado puede provocar una interrupción.
- Muchos clientes creen erróneamente que los tablespaces transportables entre plataformas no requieren conversión de datos. Cuando se utiliza una CPU con un endian diferente, un RMAN `convert` la operación debe realizarse en los archivos de datos de antemano. No se trata de una operación instantánea. En algunos casos, el proceso de conversión se puede acelerar al tener varios subprocesos que funcionan en diferentes archivos de datos, pero el proceso de conversión no se puede evitar.

Migración controlada por el gestor de volúmenes lógicos

Los LVM funcionan tomando un grupo de uno o más LUN y dividiéndolos en unidades pequeñas que normalmente se conocen como extensiones. El pool de extensiones se utiliza entonces como origen para crear volúmenes lógicos que están esencialmente virtualizados. Esta capa de virtualización proporciona valor de varias formas:

- Los volúmenes lógicos pueden utilizar extensiones extraídas de varios LUN. Cuando se crea un sistema de archivos en un volumen lógico, puede utilizar todas las funcionalidades de rendimiento de todas las LUN. También promueve la carga uniforme de todas las LUN en el grupo de volúmenes, lo que ofrece un rendimiento más previsible.
- Los volúmenes lógicos se pueden cambiar de tamaño agregando y, en algunos casos, eliminando extensiones. Cambiar el tamaño de un sistema de archivos en un volumen lógico suele ser no disruptivo.
- Los volúmenes lógicos pueden migrarse de forma no disruptiva moviendo las extensiones subyacentes.

La migración mediante un LVM funciona de dos maneras: Mover una extensión o duplicar/desactivar una extensión. La migración de LVM utiliza I/O secuencial de grandes bloques y solo rara vez crea preocupación sobre el rendimiento. Si esto se convierte en un problema, normalmente existen opciones para reducir la tasa de I/O. Hacerlo, aumenta el tiempo necesario para completar la migración pero reduce la carga de I/O en el host y los sistemas de almacenamiento.

Retrovisor y retrovisor

Algunos administradores de volúmenes, como AIX LVM, permiten al usuario especificar el número de copias para cada extensión y controlar qué dispositivos alojan cada copia. La migración se lleva a cabo tomando un volumen lógico existente, reflejando las extensiones subyacentes a los nuevos volúmenes, esperando a que se sincronicen las copias y borrando la antigua. Si se desea una ruta de retroceso, se puede crear una instantánea de los datos originales antes del punto en el que se descarta la copia de duplicación. También puede apagar el servidor brevemente para enmascarar las LUN originales antes de eliminar forzosamente las copias de duplicación contenidas. De este modo se conserva una copia recuperable de los datos en su ubicación original.

Migración de extensiones

Casi todos los gestores de volúmenes permiten migrar extensiones y, a veces, existen varias opciones. Por ejemplo, algunos administradores de volúmenes permiten que un administrador reubique las extensiones individuales de un volumen lógico específico, de almacenamiento antiguo a nuevo. Los gestores de volúmenes, como Linux LVM2, ofrecen el `pvmove` Comando, que reubica todas las extensiones del dispositivo LUN especificado en una LUN nueva. Después de evacuar la LUN antigua, puede quitarse.

El principal riesgo para las operaciones es la eliminación de LUN antiguas y no utilizadas de la configuración. Debe tenerse mucho cuidado al cambiar la división en zonas de FC y eliminar los dispositivos LUN obsoletos.

Gestión Automática de Almacenamiento de Oracle

Oracle ASM es un gestor de volúmenes lógicos y un sistema de archivos combinados. En un nivel superior, Oracle ASM toma una colección de LUN, los divide en pequeñas unidades de asignación y los presenta como un único volumen conocido como grupo de discos ASM. ASM también incluye la capacidad de reflejar el grupo de discos mediante la definición del nivel de redundancia. Un volumen puede estar no reflejado (redundancia externa), reflejado (redundancia normal) o reflejado en tres direcciones (alta redundancia). Se debe tener cuidado al configurar el nivel de redundancia porque no se puede cambiar después de la creación.

ASM también proporciona la funcionalidad del sistema de archivos. Aunque el sistema de archivos no está visible directamente desde el host, la base de datos Oracle puede crear, mover y suprimir archivos y directorios en un grupo de discos ASM. Además, la estructura puede ser navegada usando la utilidad asmcmd.

Al igual que con otras implementaciones de LVM, Oracle ASM optimiza el rendimiento de E/S mediante la segmentación y el equilibrio de carga de E/S de cada archivo en todas las LUN disponibles. En segundo lugar, las extensiones subyacentes se pueden reubicar para permitir tanto el cambio de tamaño del grupo de discos de ASM como la migración. Oracle ASM automatiza el proceso mediante la operación de reequilibrio. Se agregan nuevos LUN a un grupo de discos ASM y se eliminan LUN antiguas, lo que activa la reubicación de extensiones y la posterior caída de la LUN evacuada del grupo de discos. Este proceso es uno de los métodos de migración más probados, y la fiabilidad de ASM a la hora de proporcionar una migración transparente es posiblemente su característica más importante.

Como el nivel de mirroring de Oracle ASM es fijo, no se puede utilizar con el método de migración mirror y demirror.

Migración de nivel de almacenamiento

La migración al nivel de almacenamiento significa realizar la migración por debajo tanto del nivel de aplicación como del sistema operativo. Anteriormente, esto suponía el uso de dispositivos especializados que copiaban LUN a nivel de red, pero estas funcionalidades ahora se encuentran de forma nativa en ONTAP.

SnapMirror

La migración de bases de datos desde sistemas NetApp se realiza casi universalmente con el software de replicación de datos SnapMirror de NetApp. El proceso implica configurar una relación de mirroring para los volúmenes que se migrarán, lo que permite que se sincronicen y luego esperar la ventana de transposición. Cuando llega, la base de datos de origen se cierra, se realiza una actualización de duplicación final y se interrumpe la duplicación. A continuación, los volúmenes de réplica están listos para su uso, ya sea montando un directorio de sistema de archivos NFS contenido o detectando los LUN contenidos e iniciando la base de datos.

La reubicación de volúmenes dentro de un único clúster de ONTAP no se considera una migración, sino una rutina `volume move` funcionamiento. SnapMirror se utiliza como motor de replicación de datos en el clúster. Este proceso está totalmente automatizado. No hay otros pasos de migración que se deben realizar cuando atributos del volumen, como la asignación de LUN o los permisos de exportación de NFS, se mueven con el propio volumen. La reubicación no provoca interrupciones en las operaciones del host. En algunos casos, el acceso a la red debe actualizarse para garantizar que se accede a los datos recién reubicados de la forma más eficiente posible, pero estas tareas también no producen interrupciones.

Importación de LUN externa (FLI)

FLI es una función que permite que un sistema Data ONTAP que ejecuta 8,3 o superior migre un LUN existente desde otra cabina de almacenamiento. El procedimiento es simple: El sistema ONTAP se divide en

zonas en la cabina de almacenamiento existente como si fuera cualquier otro host SAN. A continuación, Data ONTAP toma el control de las LUN heredadas deseadas y migra los datos subyacentes. Además, el proceso de importación utiliza la configuración de eficiencia del volumen nuevo a medida que se migran los datos, lo que significa que los datos se pueden comprimir y deduplicar online durante el proceso de migración.

La primera implementación de FLI en Data ONTAP 8,3 solo permitía la migración sin conexión. Esta transferencia fue extremadamente rápida, pero seguía significando que los datos de la LUN no estaban disponibles hasta que se completó la migración. La migración en línea se introdujo en Data ONTAP 8,3.1. Este tipo de migración minimiza las interrupciones al permitir que ONTAP sirva datos de LUN durante el proceso de transferencia. Se produce una breve interrupción mientras se vuelve a dividir en zonas el host para usar los LUN a través de ONTAP. No obstante, tan pronto como se realicen estos cambios, los datos volverán a estar accesibles y seguirán siendo accesibles durante todo el proceso de migración.

La I/O de lectura se proxy mediante ONTAP hasta que se completa la operación de copia, mientras que la I/O de escritura se escribe de forma síncrona en el LUN externo y en el LUN de ONTAP. Las dos copias LUN se mantienen sincronizadas de esta manera hasta que el administrador ejecuta una transposición completa que libera la LUN externa y ya no replica las escrituras.

FLI está diseñado para funcionar con FC, pero si se desea cambiar a iSCSI, el LUN migrado puede volver a asignarse fácilmente como LUN iSCSI una vez finalizada la migración.

Entre las características de FLI se encuentra la detección y ajuste automático de alineación. En este contexto, el término alineación hace referencia a una partición en un dispositivo LUN. Para un rendimiento óptimo es necesario alinear las E/S con bloques de 4K KB. Si una partición se coloca en un desplazamiento que no es múltiplo de 4K, el rendimiento se ve afectado.

Hay un segundo aspecto de la alineación que no se puede corregir ajustando un desplazamiento de partición: El tamaño del bloque del sistema de archivos. Por ejemplo, un sistema de archivos ZFS generalmente toma por defecto un tamaño de bloque interno de 512 bytes. Otros clientes que usan AIX han creado ocasionalmente sistemas de archivos JFS2 con un tamaño de bloque de 512 o 1, 024 bytes. Aunque es posible que el sistema de archivos esté alineado con un límite de 4K KB, los archivos creados dentro de ese sistema de archivos no lo están y el rendimiento se resienta.

FLI no debe utilizarse en estas circunstancias. Aunque se puede acceder a los datos tras la migración, el resultado son sistemas de archivos con serias limitaciones de rendimiento. Como principio general, cualquier sistema de archivos que admita una carga de trabajo de sobrescritura aleatoria en ONTAP debería utilizar un tamaño de bloque de 4K KB. Esto es aplicable principalmente a cargas de trabajo como los archivos de datos de bases de datos e implementaciones de VDI. El tamaño de bloque se puede identificar mediante los comandos del sistema operativo del host relevantes.

Por ejemplo, en AIX, el tamaño de bloque se puede ver con `lsfs -q`. Con Linux, `xfs_info` y.. `tune2fs` se puede utilizar para `xfs` y.. `ext3/ext4`, respectivamente. Con `zfs`, el comando es `zdb -C`.

El parámetro que controla el tamaño del bloque es `ashift` y, por lo general, el valor predeterminado es 9, lo que significa 2^9, o 512 bytes. Para un rendimiento óptimo, el `ashift` El valor debe ser 12 (2^12=4K). Este valor se define en el momento en que se crea zpool y no se puede cambiar, lo que significa que los datos zpools con un `ashift` los datos que no sean 12 se deben migrar copiando a un zpool recién creado.

Oracle ASM no tiene un tamaño de bloque fundamental. El único requisito es que la partición en la que se crea el disco de ASM esté alineada correctamente.

Herramienta de transición de 7-Mode

La herramienta de transición de 7-Mode (7MTT) es una utilidad de automatización que se usa para migrar configuraciones de 7- Mode de gran tamaño a ONTAP. La mayoría de los clientes de bases de datos

encuentran otros métodos más sencillos, en parte, debido a que suelen migrar la base de datos de sus entornos por base de datos en lugar de reubicar todo el espacio físico de almacenamiento. Además, normalmente las bases de datos solo forman parte de un entorno de almacenamiento de mayor tamaño. Por tanto, las bases de datos suelen migrarse de forma individual y entonces el entorno restante puede moverse con el 7MTT.

Hay un número pequeño pero significativo de clientes que disponen de sistemas de almacenamiento dedicados a entornos de bases de datos complicados. Estos entornos pueden contener numerosos volúmenes, copias Snapshot y numerosos detalles de configuración, como permisos de exportación, grupos de iniciadores de LUN, permisos de usuario y configuración de protocolo ligero de acceso a directorios. En tales casos, las capacidades de automatización de 7MTT pueden simplificar una migración.

7MTT puede funcionar en uno de dos modos:

- **Transición basada en copia (CBT).** 7MTT Con CBT se configuran los volúmenes de SnapMirror a partir de un sistema 7-Mode existente en el nuevo entorno. Una vez que los datos están sincronizados, 7MTT orquesta el proceso de transición.
- **Transición sin copia (CFT).** 7MTT con CFT se basa en la conversión in situ de las bandejas de discos 7-Mode existentes. No se copian datos y las bandejas de discos existentes pueden volver a utilizarse. La configuración existente de la protección de datos y la eficiencia del almacenamiento se conserva.

La principal diferencia entre estas dos opciones es que la transición sin copias es un método muy importante, en el que todas las bandejas de discos conectadas al par de alta disponibilidad 7- Mode original deben reubicarse en el nuevo entorno. No existe una opción para mover un subconjunto de bandejas. El enfoque basado en copia permite mover los volúmenes seleccionados. También hay potencialmente un periodo de transición más largo con una transición sin copias debido al vínculo necesario para volver a conectar las bandejas de discos y convertir los metadatos. Según la experiencia práctica, NetApp recomienda permitir 1 hora para reubicar y reconectar las bandejas de discos, y entre 15 minutos y 2 horas para la conversión de metadatos.

Migración de archivos de datos

Los archivos de datos de Oracle individuales se pueden mover con un solo comando.

Por ejemplo, el siguiente comando mueve el archivo de datos IOPST.dbf del sistema de archivos `/oradata2` al sistema de archivos `/oradata3`.

```
SQL> alter database move datafile  '/oradata2/NTAP/IOPS002.dbf' to
'/oradata3/NTAP/IOPS002.dbf';
Database altered.
```

Mover un archivo de datos con este método puede ser lento, pero normalmente no debería producir suficientes E/S que interfiera con las cargas de trabajo diarias de la base de datos. Por el contrario, la migración a través del reequilibrio de ASM puede ejecutarse mucho más rápido, pero a costa de ralentizar la base de datos general mientras se mueven los datos.

El tiempo necesario para mover archivos de datos se puede medir fácilmente creando un archivo de datos de prueba y moviéndolo después. El tiempo transcurrido para la operación se registra en los datos de v$session:

```
SQL> set linesize 300;
SQL> select elapsed_seconds||':'||message from v$session_longops;
ELAPSED_SECONDS||':'||MESSAGE
------------------------------------------------------------------------
---------------
351:Online data file move: data file 8: 22548578304 out of 22548578304
bytes done
SQL> select bytes / 1024 / 1024 /1024 as GB from dba_data_files where
FILE_ID = 8;
        GB
----------
        21
```

En este ejemplo, el archivo que se movió era el archivo de datos 8, que tenía un tamaño de 21GB GB y requería unos 6 minutos para migrar. El tiempo necesario depende obviamente de las funcionalidades del sistema de almacenamiento, la red de almacenamiento y la actividad general de las bases de datos que se produzca en el momento de la migración.

Trasvase de registros

El objetivo de una migración mediante el envío de registros es crear una copia de los archivos de datos originales en una nueva ubicación y, a continuación, establecer un método de envío de cambios en el nuevo entorno.

Una vez establecido, el envío y la reproducción de registros se pueden automatizar para mantener la base de datos de réplicas en gran medida sincronizada con la fuente. Por ejemplo, se puede programar un trabajo cron para (a) copiar los logs más recientes en la nueva ubicación y (b) reproducirlos cada 15 minutos. De este modo, se genera una interrupción mínima en el momento de la transición, ya que no se deben volver a reproducir más de 15 minutos de registros de archivo.

El procedimiento que se muestra a continuación también es esencialmente una operación de clonado de base de datos. La lógica mostrada es similar al motor de NetApp SnapManager para Oracle (SMO) y el plugin para Oracle de NetApp SnapCenter. Algunos clientes han utilizado el procedimiento mostrado en los flujos de trabajo de WFA o en los scripts para operaciones de clonado personalizadas. Aunque este procedimiento es más manual que usar SMO o SnapCenter, todavía dispone de secuencias de comandos sencillas y las API de gestión de datos en ONTAP simplifican aún más el proceso.

Envío de registros: Sistema de archivos al sistema de archivos

Este ejemplo muestra la migración de una base de datos denominada WAFFLE de un sistema de archivos ordinario a otro sistema de archivos ordinario ubicado en un servidor diferente. También ilustra el uso de SnapMirror para realizar una copia rápida de los archivos de datos, pero esto no forma parte integral del procedimiento general.

Crear copia de seguridad de base de datos

El primer paso es crear una copia de seguridad de la base de datos. En concreto, este procedimiento requiere un juego de archivos de datos que se pueda utilizar para la reproducción del archive log.

Entorno Oracle

En este ejemplo, la base de datos de origen se encuentra en un sistema ONTAP. El método más sencillo para crear un backup de una base de datos es mediante una instantánea. La base de datos se coloca en modo de backup dinámico durante unos segundos mientras a. `snapshot create` la operación se ejecuta en el volumen que aloja los archivos de datos.

```
SQL> alter database begin backup;
Database altered.
```

```
Cluster01::*> snapshot create -vserver vserver1 -volume jfsc1_oradata
hotbackup
Cluster01::*>
```

```
SQL> alter database end backup;
Database altered.
```

El resultado es una instantánea en disco llamada `hotbackup` que contiene una imagen de los archivos de datos mientras se encuentra en modo de copia de seguridad activa. Si se combinan con los archive logs adecuados para que los archivos de datos sean coherentes, se pueden utilizar los datos de esta copia Snapshot como base de la restauración o el clon. En este caso, se replica en el nuevo servidor.

Restauración al nuevo entorno

La copia de seguridad se debe restaurar ahora en el nuevo entorno. Esto puede realizarse de varias maneras, incluida Oracle RMAN, restauración desde una aplicación de backup como NetBackup o una operación de copia sencilla de archivos de datos ubicados en modo de backup dinámico.

En este ejemplo, se usa SnapMirror para replicar el backup en caliente de la copia Snapshot en una nueva ubicación.

1. Cree un volumen nuevo para recibir los datos de las snapshots. Inicialice el mirroring a partir de `jfsc1_oradata` para `vol_oradata`.

   ```
   Cluster01::*> volume create -vserver vserver1 -volume vol_oradata
   -aggregate data_01 -size 20g -state online -type DP -snapshot-policy
   none -policy jfsc3
   [Job 833] Job succeeded: Successful
   ```

```
Cluster01::*> snapmirror initialize -source-path vserver1:jfsc1_oradata
-destination-path vserver1:vol_oradata
Operation is queued: snapmirror initialize of destination
"vserver1:vol_oradata".
Cluster01::*> volume mount -vserver vserver1 -volume vol_oradata
-junction-path /vol_oradata
Cluster01::*>
```

2. Una vez definido el estado mediante SnapMirror, que indica que la sincronización está completada, actualice el mirror según la snapshot que desee.

```
Cluster01::*> snapmirror show -destination-path vserver1:vol_oradata
-fields state
source-path             destination-path        state
----------------------- ----------------------- ------------
vserver1:jfsc1_oradata vserver1:vol_oradata SnapMirrored
```

```
Cluster01::*> snapmirror update -destination-path vserver1:vol_oradata
-source-snapshot hotbackup
Operation is queued: snapmirror update of destination
"vserver1:vol_oradata".
```

3. La sincronización correcta se puede verificar en el `newest-snapshot` en el volumen de reflejo.

```
Cluster01::*> snapmirror show -destination-path vserver1:vol_oradata
-fields newest-snapshot
source-path             destination-path        newest-snapshot
----------------------- ----------------------- ---------------
vserver1:jfsc1_oradata vserver1:vol_oradata hotbackup
```

4. El espejo puede romperse.

```
Cluster01::> snapmirror break -destination-path vserver1:vol_oradata
Operation succeeded: snapmirror break for destination
"vserver1:vol_oradata".
Cluster01::>
```

5. Monte el nuevo sistema de archivos.Con los sistemas de archivos basados en bloques, los procedimientos precisos varían según el LVM en uso. Debe configurarse la división en zonas de FC o las conexiones iSCSI. Después de establecer la conectividad a las LUN, comandos como Linux `pvscan` Puede que sea necesario detectar qué grupos de volúmenes o LUN tienen que estar correctamente configurados para que ASM pueda detectar.

En este ejemplo, se utiliza un sistema de archivos NFS simple. Este sistema de archivos se puede montar directamente.

```
fas8060-nfs1:/vol_oradata        19922944   1639360   18283584   9%
/oradata
fas8060-nfs1:/vol_logs            9961472       128    9961344   1%
/logs
```

Crear plantilla de creación de archivo de control

A continuación, debe crear una plantilla de archivo de control. La `backup controlfile to trace` command crea comandos de texto para volver a crear un archivo de control. Esta función puede ser útil para restaurar una base de datos a partir de un backup bajo determinadas circunstancias, y se suele utilizar con scripts que realizan tareas como la clonación de bases de datos.

1. La salida del siguiente comando se utiliza para recrear los controlfiles para la base de datos migrada.

```
SQL> alter database backup controlfile to trace as '/tmp/waffle.ctrl';
Database altered.
```

2. Después de crear los archivos de control, copie el archivo en el nuevo servidor.

```
[oracle@jfsc3 tmp]$ scp oracle@jfsc1:/tmp/waffle.ctrl /tmp/
oracle@jfsc1's password:
waffle.ctrl                                           100% 5199
5.1KB/s   00:00
```

Archivo de parámetros de copia de seguridad

También se necesita un archivo de parámetros en el nuevo entorno. El método más simple es crear un pfile a partir del spfile o pfile actual. En este ejemplo, la base de datos de origen está utilizando un spfile.

```
SQL> create pfile='/tmp/waffle.tmp.pfile' from spfile;
File created.
```

Crear entrada oratab

La creación de una entrada oratab es necesaria para el correcto funcionamiento de utilidades como oraenv. Para crear una entrada de oratab, realice el siguiente paso.

```
WAFFLE:/orabin/product/12.1.0/dbhome_1:N
```

Preparar la estructura de directorios

Si los directorios necesarios no estaban presentes, debe crearlos o el procedimiento de inicio de la base de datos falla. Para preparar la estructura de directorios, complete los siguientes requisitos mínimos.

```
[oracle@jfsc3 ~]$ . oraenv
ORACLE_SID = [oracle] ? WAFFLE
The Oracle base has been set to /orabin
[oracle@jfsc3 ~]$ cd $ORACLE_BASE
[oracle@jfsc3 orabin]$ cd admin
[oracle@jfsc3 admin]$ mkdir WAFFLE
[oracle@jfsc3 admin]$ cd WAFFLE
[oracle@jfsc3 WAFFLE]$ mkdir adump dpdump pfile scripts xdb_wallet
```

Actualizaciones de archivos de parámetros

1. Para copiar el archivo de parámetros en el nuevo servidor, ejecute los siguientes comandos. La ubicación predeterminada es la `$ORACLE_HOME/dbs` directorio. En este caso, el archivo pfile se puede colocar en cualquier lugar. Sólo se utiliza como paso intermedio en el proceso de migración.

```
[oracle@jfsc3 admin]$ scp oracle@jfsc1:/tmp/waffle.tmp.pfile
$ORACLE_HOME/dbs/waffle.tmp.pfile
oracle@jfsc1's password:
waffle.pfile                                          100%  916
0.9KB/s   00:00
```

1. Edite el archivo según sea necesario. Por ejemplo, si la ubicación del archive log ha cambiado, el archivo pfile debe modificarse para reflejar la nueva ubicación. En este ejemplo, sólo se reubican los archivos de control, en parte para distribuirlos entre los sistemas de archivos de registro y de datos.

```
[root@jfsc1 tmp]# cat waffle.pfile
WAFFLE.__data_transfer_cache_size=0
WAFFLE.__db_cache_size=507510784
WAFFLE.__java_pool_size=4194304
WAFFLE.__large_pool_size=20971520
WAFFLE.__oracle_base='/orabin'#ORACLE_BASE set from environment
WAFFLE.__pga_aggregate_target=268435456
WAFFLE.__sga_target=805306368
WAFFLE.__shared_io_pool_size=29360128
WAFFLE.__shared_pool_size=234881024
WAFFLE.__streams_pool_size=0
*.audit_file_dest='/orabin/admin/WAFFLE/adump'
*.audit_trail='db'
*.compatible='12.1.0.2.0'
*.control_files='/oradata//WAFFLE/control01.ctl','/oradata//WAFFLE/contr
ol02.ctl'
*.control_files='/oradata/WAFFLE/control01.ctl','/logs/WAFFLE/control02.
ctl'
*.db_block_size=8192
*.db_domain=''
*.db_name='WAFFLE'
*.diagnostic_dest='/orabin'
*.dispatchers='(PROTOCOL=TCP) (SERVICE=WAFFLEXDB)'
*.log_archive_dest_1='LOCATION=/logs/WAFFLE/arch'
*.log_archive_format='%t_%s_%r.dbf'
*.open_cursors=300
*.pga_aggregate_target=256m
*.processes=300
*.remote_login_passwordfile='EXCLUSIVE'
*.sga_target=768m
*.undo_tablespace='UNDOTBS1'
```

2. Una vez finalizadas las ediciones, cree un archivo spfile basado en este archivo pfile.

```
SQL> create spfile from pfile='waffle.tmp.pfile';
File created.
```

Vuelva a crear los archivos de control

En un paso anterior, la salida de `backup controlfile to trace` se ha copiado en el nuevo servidor. La parte específica de la salida necesaria es la `controlfile recreation` comando. Esta información se puede encontrar en el archivo bajo la sección marcada `Set #1. NORESETLOGS`. Comienza con la línea `create controlfile reuse database` y debe incluir la palabra `noresetlogs`. Termina con el carácter de punto y coma (;).

1. En este procedimiento de ejemplo, el archivo se lee de la siguiente manera.

```
CREATE CONTROLFILE REUSE DATABASE "WAFFLE" NORESETLOGS  ARCHIVELOG
    MAXLOGFILES 16
    MAXLOGMEMBERS 3
    MAXDATAFILES 100
    MAXINSTANCES 8
    MAXLOGHISTORY 292
LOGFILE
  GROUP 1 '/logs/WAFFLE/redo/redo01.log'  SIZE 50M BLOCKSIZE 512,
  GROUP 2 '/logs/WAFFLE/redo/redo02.log'  SIZE 50M BLOCKSIZE 512,
  GROUP 3 '/logs/WAFFLE/redo/redo03.log'  SIZE 50M BLOCKSIZE 512
-- STANDBY LOGFILE
DATAFILE
  '/oradata/WAFFLE/system01.dbf',
  '/oradata/WAFFLE/sysaux01.dbf',
  '/oradata/WAFFLE/undotbs01.dbf',
  '/oradata/WAFFLE/users01.dbf'
CHARACTER SET WE8MSWIN1252
;
```

2. Edite este script como desee para reflejar la nueva ubicación de los distintos archivos. Por ejemplo, algunos archivos de datos conocidos por admitir una gran I/O podrían redirigirse a un sistema de archivos en un nivel de almacenamiento de alto rendimiento. En otros casos, los cambios podrían ser únicamente por motivos de administrador, como el aislamiento de los archivos de datos de una PDB determinada en volúmenes dedicados.
3. En este ejemplo, la `DATAFILE` stanza se deja sin cambios, pero los redo logs se mueven a una nueva ubicación en `/redo` en lugar de compartir espacio con archive logs `/logs`.

```
CREATE CONTROLFILE REUSE DATABASE "WAFFLE" NORESETLOGS  ARCHIVELOG
    MAXLOGFILES 16
    MAXLOGMEMBERS 3
    MAXDATAFILES 100
    MAXINSTANCES 8
    MAXLOGHISTORY 292
LOGFILE
  GROUP 1 '/redo/redo01.log'  SIZE 50M BLOCKSIZE 512,
  GROUP 2 '/redo/redo02.log'  SIZE 50M BLOCKSIZE 512,
  GROUP 3 '/redo/redo03.log'  SIZE 50M BLOCKSIZE 512
-- STANDBY LOGFILE
DATAFILE
  '/oradata/WAFFLE/system01.dbf',
  '/oradata/WAFFLE/sysaux01.dbf',
  '/oradata/WAFFLE/undotbs01.dbf',
  '/oradata/WAFFLE/users01.dbf'
CHARACTER SET WE8MSWIN1252
;
```

```
SQL> startup nomount;
ORACLE instance started.
Total System Global Area  805306368 bytes
Fixed Size                  2929552 bytes
Variable Size             331353200 bytes
Database Buffers          465567744 bytes
Redo Buffers                5455872 bytes
SQL> CREATE CONTROLFILE REUSE DATABASE "WAFFLE" NORESETLOGS  ARCHIVELOG
  2      MAXLOGFILES 16
  3      MAXLOGMEMBERS 3
  4      MAXDATAFILES 100
  5      MAXINSTANCES 8
  6      MAXLOGHISTORY 292
  7  LOGFILE
  8    GROUP 1 '/redo/redo01.log'  SIZE 50M BLOCKSIZE 512,
  9    GROUP 2 '/redo/redo02.log'  SIZE 50M BLOCKSIZE 512,
 10    GROUP 3 '/redo/redo03.log'  SIZE 50M BLOCKSIZE 512
 11  -- STANDBY LOGFILE
 12  DATAFILE
 13    '/oradata/WAFFLE/system01.dbf',
 14    '/oradata/WAFFLE/sysaux01.dbf',
 15    '/oradata/WAFFLE/undotbs01.dbf',
 16    '/oradata/WAFFLE/users01.dbf'
 17  CHARACTER SET WE8MSWIN1252
 18  ;
Control file created.
SQL>
```

Si alguno de los archivos está mal ubicado o los parámetros están mal configurados, se generan errores que indican lo que debe corregirse. La base de datos está montada, pero aún no está abierta y no se puede abrir porque los archivos de datos en uso siguen marcados como en modo de copia de seguridad en caliente. Los archive logs deben aplicarse primero para que la base de datos sea coherente.

Replicación de registro inicial

Se necesita al menos una operación de respuesta de log para que los archivos de datos sean consistentes. Hay muchas opciones disponibles para reproducir logs. En algunos casos, la ubicación original del archive log en el servidor original se puede compartir a través de NFS, y la respuesta del log se puede realizar directamente. En otros casos, los archive logs deben copiarse.

Por ejemplo, un simple `scp` la operación puede copiar todos los registros actuales del servidor de origen al servidor de migración:

```
[oracle@jfsc3 arch]$ scp jfsc1:/logs/WAFFLE/arch/* ./
oracle@jfsc1's password:
1_22_912662036.dbf                                          100%   47MB
47.0MB/s   00:01
1_23_912662036.dbf                                          100%   40MB
40.4MB/s   00:00
1_24_912662036.dbf                                          100%   45MB
45.4MB/s   00:00
1_25_912662036.dbf                                          100%   41MB
40.9MB/s   00:01
1_26_912662036.dbf                                          100%   39MB
39.4MB/s   00:00
1_27_912662036.dbf                                          100%   39MB
38.7MB/s   00:00
1_28_912662036.dbf                                          100%   40MB
40.1MB/s   00:01
1_29_912662036.dbf                                          100%   17MB
16.9MB/s   00:00
1_30_912662036.dbf                                          100%  636KB
636.0KB/s   00:00
```

Reproducción de log inicial

Una vez que los archivos están en la ubicación del archive log, se pueden reproducir emitiendo el comando `recover database until cancel` seguido de la respuesta `AUTO` para reproducir automáticamente todos los logs disponibles.

```
SQL> recover database until cancel;
ORA-00279: change 382713 generated at 05/24/2016 09:00:54 needed for
thread 1
ORA-00289: suggestion : /logs/WAFFLE/arch/1_23_912662036.dbf
ORA-00280: change 382713 for thread 1 is in sequence #23
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
AUTO
ORA-00279: change 405712 generated at 05/24/2016 15:01:05 needed for
thread 1
ORA-00289: suggestion : /logs/WAFFLE/arch/1_24_912662036.dbf
ORA-00280: change 405712 for thread 1 is in sequence #24
ORA-00278: log file '/logs/WAFFLE/arch/1_23_912662036.dbf' no longer
needed for
this recovery
...
ORA-00279: change 713874 generated at 05/26/2016 04:26:43 needed for
thread 1
ORA-00289: suggestion : /logs/WAFFLE/arch/1_31_912662036.dbf
ORA-00280: change 713874 for thread 1 is in sequence #31
ORA-00278: log file '/logs/WAFFLE/arch/1_30_912662036.dbf' no longer
needed for
this recovery
ORA-00308: cannot open archived log '/logs/WAFFLE/arch/1_31_912662036.dbf'
ORA-27037: unable to obtain file status
Linux-x86_64 Error: 2: No such file or directory
Additional information: 3
```

La respuesta final del archive log informa de un error, pero esto es normal. El registro lo indica `sqlplus` estaba buscando un archivo de registro en particular y no lo encontró. La razón es, lo más probable, que el archivo log no existe aún.

Si la base de datos de origen se puede cerrar antes de copiar archive logs, este paso debe realizarse una sola vez. Los archive logs se copian y se reproducen y, a continuación, el proceso puede continuar directamente con el proceso de transposición que replica los redo logs críticos.

Replicación y repetición de log incremental

En la mayoría de los casos, la migración no se realiza de forma inmediata. Pueden pasar días o incluso semanas antes de que se complete el proceso de migración, lo que significa que los registros deben enviarse continuamente a la base de datos de réplica y reproducirse. Por lo tanto, al llegar la transición, es necesario transferir y reproducir unos datos mínimos.

Al hacerlo se puede ejecutar un script de muchas maneras, pero uno de los métodos más populares es usar rsync, una utilidad común de replicación de archivos. La forma más segura de utilizar esta utilidad es configurarla como daemon. Por ejemplo, la `rsyncd.conf` el siguiente archivo muestra cómo crear un recurso llamado `waffle.arch` Al que se accede con las credenciales de usuario de Oracle y se asigna a. `/logs/WAFFLE/arch`. Lo que es más importante, el recurso se establece en solo lectura, lo que permite que los datos de producción se lean, pero no se alteren.

```
[root@jfsc1 arch]# cat /etc/rsyncd.conf
[waffle.arch]
   uid=oracle
   gid=dba
   path=/logs/WAFFLE/arch
   read only = true
[root@jfsc1 arch]# rsync --daemon
```

El siguiente comando sincroniza el destino del archive log del nuevo servidor con el recurso rsync `waffle.arch` en el servidor original. La `t` argumento en `rsync - potg` hace que la lista de archivos se compare en función de la marca de tiempo, y solo se copian los archivos nuevos. Este proceso proporciona una actualización incremental del nuevo servidor. Este comando también se puede programar en cron para que se ejecute de forma regular.

```
[oracle@jfsc3 arch]$ rsync -potg --stats --progress jfsc1::waffle.arch/*
/logs/WAFFLE/arch/
1_31_912662036.dbf
      650240 100%  124.02MB/s    0:00:00 (xfer#1, to-check=8/18)
1_32_912662036.dbf
     4873728 100%  110.67MB/s    0:00:00 (xfer#2, to-check=7/18)
1_33_912662036.dbf
     4088832 100%   50.64MB/s    0:00:00 (xfer#3, to-check=6/18)
1_34_912662036.dbf
     8196096 100%   54.66MB/s    0:00:00 (xfer#4, to-check=5/18)
1_35_912662036.dbf
    19376128 100%   57.75MB/s    0:00:00 (xfer#5, to-check=4/18)
1_36_912662036.dbf
       71680 100%  201.15kB/s    0:00:00 (xfer#6, to-check=3/18)
1_37_912662036.dbf
     1144320 100%    3.06MB/s    0:00:00 (xfer#7, to-check=2/18)
1_38_912662036.dbf
    35757568 100%   63.74MB/s    0:00:00 (xfer#8, to-check=1/18)
1_39_912662036.dbf
      984576 100%    1.63MB/s    0:00:00 (xfer#9, to-check=0/18)
Number of files: 18
Number of files transferred: 9
Total file size: 399653376 bytes
Total transferred file size: 75143168 bytes
Literal data: 75143168 bytes
Matched data: 0 bytes
File list size: 474
File list generation time: 0.001 seconds
File list transfer time: 0.000 seconds
Total bytes sent: 204
Total bytes received: 75153219
sent 204 bytes  received 75153219 bytes  150306846.00 bytes/sec
total size is 399653376  speedup is 5.32
```

Una vez recibidos los registros, deben reproducirse. Ejemplos anteriores muestran el uso de sqlplus para ejecutar manualmente `recover database until cancel`, un proceso que se puede automatizar fácilmente. El ejemplo que se muestra aquí utiliza el script descrito en "Reproducir Logs en Base de Datos". Los scripts aceptan un argumento que especifica la base de datos que necesita una operación de reproducción. Esto permite utilizar el mismo script en un esfuerzo de migración de varias bases de datos.

```
[oracle@jfsc3 logs]$ ./replay.logs.pl WAFFLE
ORACLE_SID = [WAFFLE] ? The Oracle base remains unchanged with value
/orabin
SQL*Plus: Release 12.1.0.2.0 Production on Thu May 26 10:47:16 2016
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit
Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
SQL> ORA-00279: change 713874 generated at 05/26/2016 04:26:43 needed for
thread 1
ORA-00289: suggestion : /logs/WAFFLE/arch/1_31_912662036.dbf
ORA-00280: change 713874 for thread 1 is in sequence #31
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 814256 generated at 05/26/2016 04:52:30 needed for
thread 1
ORA-00289: suggestion : /logs/WAFFLE/arch/1_32_912662036.dbf
ORA-00280: change 814256 for thread 1 is in sequence #32
ORA-00278: log file '/logs/WAFFLE/arch/1_31_912662036.dbf' no longer
needed for
this recovery
ORA-00279: change 814780 generated at 05/26/2016 04:53:04 needed for
thread 1
ORA-00289: suggestion : /logs/WAFFLE/arch/1_33_912662036.dbf
ORA-00280: change 814780 for thread 1 is in sequence #33
ORA-00278: log file '/logs/WAFFLE/arch/1_32_912662036.dbf' no longer
needed for
this recovery
...
ORA-00279: change 1120099 generated at 05/26/2016 09:59:21 needed for
thread 1
ORA-00289: suggestion : /logs/WAFFLE/arch/1_40_912662036.dbf
ORA-00280: change 1120099 for thread 1 is in sequence #40
ORA-00278: log file '/logs/WAFFLE/arch/1_39_912662036.dbf' no longer
needed for
this recovery
ORA-00308: cannot open archived log '/logs/WAFFLE/arch/1_40_912662036.dbf'
ORA-27037: unable to obtain file status
Linux-x86_64 Error: 2: No such file or directory
Additional information: 3
SQL> Disconnected from Oracle Database 12c Enterprise Edition Release
12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
```

Transición

Cuando esté listo para realizar la transición al nuevo entorno, debe realizar una sincronización final que incluya tanto archive logs como redo logs. Si la ubicación de redo log original no se conoce todavía, se puede identificar de la siguiente manera:

```
SQL> select member from v$logfile;
MEMBER
-------------------------------------------------------------------------------
------
/logs/WAFFLE/redo/redo01.log
/logs/WAFFLE/redo/redo02.log
/logs/WAFFLE/redo/redo03.log
```

1. Cierre la base de datos de origen.
2. Realice una sincronización final de los archive logs en el nuevo servidor con el método deseado.
3. Los redo logs de origen se deben copiar en el nuevo servidor. En este ejemplo, los redo logs se reubicaron en un nuevo directorio en `/redo`.

   ```
   [oracle@jfsc3 logs]$ scp jfsc1:/logs/WAFFLE/redo/* /redo/
   oracle@jfsc1's password:
   redo01.log
   100%   50MB  50.0MB/s   00:01
   redo02.log
   100%   50MB  50.0MB/s   00:00
   redo03.log
   100%   50MB  50.0MB/s   00:00
   ```

4. En esta etapa, el nuevo entorno de base de datos contiene todos los archivos necesarios para llevarlo al mismo estado que el origen. Los registros de archivos se deben reproducir por última vez.

```
SQL> recover database until cancel;
ORA-00279: change 1120099 generated at 05/26/2016 09:59:21 needed for
thread 1
ORA-00289: suggestion : /logs/WAFFLE/arch/1_40_912662036.dbf
ORA-00280: change 1120099 for thread 1 is in sequence #40
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
AUTO
ORA-00308: cannot open archived log
'/logs/WAFFLE/arch/1_40_912662036.dbf'
ORA-27037: unable to obtain file status
Linux-x86_64 Error: 2: No such file or directory
Additional information: 3
ORA-00308: cannot open archived log
'/logs/WAFFLE/arch/1_40_912662036.dbf'
ORA-27037: unable to obtain file status
Linux-x86_64 Error: 2: No such file or directory
Additional information: 3
```

5. Una vez finalizado, los redo logs se deben volver a reproducir. Si el mensaje `Media recovery complete` se devuelve, el proceso se realiza correctamente y las bases de datos se sincronizan y se pueden abrir.

```
SQL> recover database;
Media recovery complete.
SQL> alter database open;
Database altered.
```

Envío de registros: ASM al sistema de archivos

Este ejemplo muestra el uso de Oracle RMAN para migrar una base de datos. Es muy similar al ejemplo anterior del envío de registros del sistema de archivos al sistema de archivos, pero los archivos de ASM no son visibles para el host. La única opción para migrar datos ubicados en dispositivos ASM es mediante la reubicación del LUN de ASM o mediante Oracle RMAN para realizar las operaciones de copia.

Aunque RMAN es un requisito para copiar archivos de Oracle ASM, el uso de RMAN no se limita a ASM. RMAN se puede utilizar para migrar de cualquier tipo de almacenamiento a cualquier otro tipo.

Este ejemplo muestra la reubicación de una base de datos llamada PANCAKE del almacenamiento de ASM a un sistema de archivos normal ubicado en un servidor diferente en las rutas de acceso `/oradata` y.. `/logs`.

Crear copia de seguridad de base de datos

El primer paso es crear una copia de seguridad de la base de datos que se migrará a un servidor alternativo. Dado que el origen utiliza Oracle ASM, se debe utilizar RMAN. Se puede realizar una copia de seguridad simple de RMAN del siguiente modo. Este método crea una copia de seguridad etiquetada que RMAN puede identificar fácilmente más adelante en el procedimiento.

El primer comando define el tipo de destino para la copia de seguridad y la ubicación que se utilizará. El segundo inicia la copia de seguridad de los archivos de datos solamente.

```
RMAN> configure channel device type disk format '/rman/pancake/%U';
using target database control file instead of recovery catalog
old RMAN configuration parameters:
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT   '/rman/pancake/%U';
new RMAN configuration parameters:
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT   '/rman/pancake/%U';
new RMAN configuration parameters are successfully stored
RMAN> backup database tag 'ONTAP_MIGRATION';
Starting backup at 24-MAY-16
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=251 device type=DISK
channel ORA_DISK_1: starting full datafile backup set
channel ORA_DISK_1: specifying datafile(s) in backup set
input datafile file number=00001 name=+ASM0/PANCAKE/system01.dbf
input datafile file number=00002 name=+ASM0/PANCAKE/sysaux01.dbf
input datafile file number=00003 name=+ASM0/PANCAKE/undotbs101.dbf
input datafile file number=00004 name=+ASM0/PANCAKE/users01.dbf
channel ORA_DISK_1: starting piece 1 at 24-MAY-16
channel ORA_DISK_1: finished piece 1 at 24-MAY-16
piece handle=/rman/pancake/1gr6c161_1_1 tag=ONTAP_MIGRATION comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:03
channel ORA_DISK_1: starting full datafile backup set
channel ORA_DISK_1: specifying datafile(s) in backup set
including current control file in backup set
including current SPFILE in backup set
channel ORA_DISK_1: starting piece 1 at 24-MAY-16
channel ORA_DISK_1: finished piece 1 at 24-MAY-16
piece handle=/rman/pancake/1hr6c164_1_1 tag=ONTAP_MIGRATION comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:01
Finished backup at 24-MAY-16
```

Copia de seguridad del archivo de control

Se necesita un archivo de control de copia de seguridad más adelante en el procedimiento del `duplicate database` funcionamiento.

```
RMAN> backup current controlfile format '/rman/pancake/ctrl.bkp';
Starting backup at 24-MAY-16
using channel ORA_DISK_1
channel ORA_DISK_1: starting full datafile backup set
channel ORA_DISK_1: specifying datafile(s) in backup set
including current control file in backup set
channel ORA_DISK_1: starting piece 1 at 24-MAY-16
channel ORA_DISK_1: finished piece 1 at 24-MAY-16
piece handle=/rman/pancake/ctrl.bkp tag=TAG20160524T032651 comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:01
Finished backup at 24-MAY-16
```

Archivo de parámetros de copia de seguridad

También se necesita un archivo de parámetros en el nuevo entorno. El método más simple es crear un pfile a partir del spfile o pfile actual. En este ejemplo, la base de datos de origen utiliza un spfile.

```
RMAN> create pfile='/rman/pancake/pfile' from spfile;
Statement processed
```

Script de cambio de nombre de archivo de ASM

Varias ubicaciones de archivos definidas actualmente en los controlfiles cambian cuando se mueve la base de datos. El siguiente archivo de comandos crea un archivo de comandos de RMAN para facilitar el proceso. Este ejemplo muestra una base de datos con un número muy pequeño de archivos de datos, pero normalmente las bases de datos contienen cientos o incluso miles de archivos de datos.

Este script se puede encontrar en "Conversión de ASM a Nombre de Sistema de Archivos" y hace dos cosas.

En primer lugar, crea un parámetro para redefinir las ubicaciones de redo log llamadas `log_file_name_convert`. Es esencialmente una lista de campos alternos. El primer campo es la ubicación de un redo log actual y el segundo campo es la ubicación del nuevo servidor. El patrón se repite entonces.

La segunda función consiste en proporcionar una plantilla para el cambio de nombre del archivo de datos. El archivo de comandos pasa por los archivos de datos, extrae la información del nombre y el número de archivo y lo formatea como un archivo de comandos de RMAN. A continuación, hace lo mismo con los archivos temporales. El resultado es un script de rman simple que se puede editar como se desee para asegurarse de que los archivos se restauran en la ubicación deseada.

```
SQL> @/rman/mk.rename.scripts.sql
Parameters for log file conversion:
*.log_file_name_convert = '+ASM0/PANCAKE/redo01.log',
'/NEW_PATH/redo01.log','+ASM0/PANCAKE/redo02.log',
'/NEW_PATH/redo02.log','+ASM0/PANCAKE/redo03.log', '/NEW_PATH/redo03.log'
rman duplication script:
run
{
set newname for datafile 1 to '+ASM0/PANCAKE/system01.dbf';
set newname for datafile 2 to '+ASM0/PANCAKE/sysaux01.dbf';
set newname for datafile 3 to '+ASM0/PANCAKE/undotbs101.dbf';
set newname for datafile 4 to '+ASM0/PANCAKE/users01.dbf';
set newname for tempfile 1 to '+ASM0/PANCAKE/temp01.dbf';
duplicate target database for standby backup location INSERT_PATH_HERE;
}
PL/SQL procedure successfully completed.
```

Captura la salida de esta pantalla. La `log_file_name_convert` el parámetro se coloca en el archivo pfile como se describe a continuación. El archivo de datos RENAME y el archivo de comandos DUPLICATE de RMAN se deben editar en consecuencia para colocar los archivos de datos en las ubicaciones deseadas. En este ejemplo, se colocan todos `/oradata/pancake`.

```
run
{
set newname for datafile 1 to '/oradata/pancake/pancake.dbf';
set newname for datafile 2 to '/oradata/pancake/sysaux.dbf';
set newname for datafile 3 to '/oradata/pancake/undotbs1.dbf';
set newname for datafile 4 to '/oradata/pancake/users.dbf';
set newname for tempfile 1 to '/oradata/pancake/temp.dbf';
duplicate target database for standby backup location '/rman/pancake';
}
```

Preparar la estructura de directorios

Los scripts están casi listos para ejecutarse, pero primero debe estar la estructura de directorios en su lugar. Si los directorios necesarios no están ya presentes, se deben crear o el procedimiento de inicio de la base de datos falla. El ejemplo siguiente refleja los requisitos mínimos.

```
[oracle@jfsc2 ~]$ mkdir /oradata/pancake
[oracle@jfsc2 ~]$ mkdir /logs/pancake
[oracle@jfsc2 ~]$ cd /orabin/admin
[oracle@jfsc2 admin]$ mkdir PANCAKE
[oracle@jfsc2 admin]$ cd PANCAKE
[oracle@jfsc2 PANCAKE]$ mkdir adump dpdump pfile scripts xdb_wallet
```

Crear entrada oratab

El siguiente comando es necesario para que utilidades como oraenv funcionen correctamente.

```
PANCAKE:/orabin/product/12.1.0/dbhome_1:N
```

Actualizaciones de parámetros

El archivo pfile guardado se debe actualizar para reflejar cualquier cambio de ruta en el nuevo servidor. El script de duplicación de RMAN modifica los cambios de la ruta de acceso del archivo de datos y casi todas las bases de datos requieren cambios en el `control_files` y.. `log_archive_dest` parámetros. Es posible que también haya ubicaciones de archivos de auditoría que deban modificarse y parámetros como `db_create_file_dest` Puede que no sea relevante fuera de ASM. Un DBA con experiencia debe revisar cuidadosamente los cambios propuestos antes de continuar.

En este ejemplo, los cambios clave son las ubicaciones del archivo de control, el destino del archivo de registro y la adición del `log_file_name_convert` parámetro.

```
PANCAKE.__data_transfer_cache_size=0
PANCAKE.__db_cache_size=545259520
PANCAKE.__java_pool_size=4194304
PANCAKE.__large_pool_size=25165824
PANCAKE.__oracle_base='/orabin'#ORACLE_BASE set from environment
PANCAKE.__pga_aggregate_target=268435456
PANCAKE.__sga_target=805306368
PANCAKE.__shared_io_pool_size=29360128
PANCAKE.__shared_pool_size=192937984
PANCAKE.__streams_pool_size=0
*.audit_file_dest='/orabin/admin/PANCAKE/adump'
*.audit_trail='db'
*.compatible='12.1.0.2.0'
*.control_files='+ASM0/PANCAKE/control01.ctl','+ASM0/PANCAKE/control02.ctl
'
*.control_files='/oradata/pancake/control01.ctl','/logs/pancake/control02.
ctl'
*.db_block_size=8192
*.db_domain=''
*.db_name='PANCAKE'
*.diagnostic_dest='/orabin'
*.dispatchers='(PROTOCOL=TCP) (SERVICE=PANCAKEXDB)'
*.log_archive_dest_1='LOCATION=+ASM1'
*.log_archive_dest_1='LOCATION=/logs/pancake'
*.log_archive_format='%t_%s_%r.dbf'
'/logs/path/redo02.log'
*.log_file_name_convert = '+ASM0/PANCAKE/redo01.log',
'/logs/pancake/redo01.log', '+ASM0/PANCAKE/redo02.log',
'/logs/pancake/redo02.log', '+ASM0/PANCAKE/redo03.log',
'/logs/pancake/redo03.log'
*.open_cursors=300
*.pga_aggregate_target=256m
*.processes=300
*.remote_login_passwordfile='EXCLUSIVE'
*.sga_target=768m
*.undo_tablespace='UNDOTBS1'
```

Después de confirmar los nuevos parámetros, los parámetros deben ponerse en vigor. Existen varias opciones, pero la mayoría de los clientes crean un spfile basado en el archivo pfile de texto.

```
bash-4.1$ sqlplus / as sysdba
SQL*Plus: Release 12.1.0.2.0 Production on Fri Jan 8 11:17:40 2016
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to an idle instance.
SQL> create spfile from pfile='/rman/pancake/pfile';
File created.
```

Inicio nomount

El último paso antes de replicar la base de datos es abrir los procesos de la base de datos pero no montar los archivos. En este paso, los problemas con el spfile pueden hacerse evidentes. Si la `startup nomount` el comando falla debido a un error de parámetro, es fácil de cerrar, corregir la plantilla pfile, recargarla como spfile e intentarlo de nuevo.

```
SQL> startup nomount;
ORACLE instance started.
Total System Global Area  805306368 bytes
Fixed Size                  2929552 bytes
Variable Size             373296240 bytes
Database Buffers          423624704 bytes
Redo Buffers                5455872 bytes
```

Duplique la base de datos

La restauración de la copia de seguridad de RMAN anterior en la nueva ubicación consume más tiempo que otros pasos de este proceso. La base de datos se debe duplicar sin cambiar el identificador de base de datos (DBID) ni restablecer los logs. Esto evita que se apliquen los logs, lo que es un paso necesario para sincronizar completamente las copias.

Conéctese a la base de datos con RMAN como aux y emita el comando DUPLICATE DATABASE mediante el script creado en un paso anterior.

```
[oracle@jfsc2 pancake]$ rman auxiliary /
Recovery Manager: Release 12.1.0.2.0 - Production on Tue May 24 03:04:56
2016
Copyright (c) 1982, 2014, Oracle and/or its affiliates.  All rights
reserved.
connected to auxiliary database: PANCAKE (not mounted)
RMAN> run
2> {
3> set newname for datafile 1 to '/oradata/pancake/pancake.dbf';
4> set newname for datafile 2 to '/oradata/pancake/sysaux.dbf';
5> set newname for datafile 3 to '/oradata/pancake/undotbs1.dbf';
6> set newname for datafile 4 to '/oradata/pancake/users.dbf';
7> set newname for tempfile 1 to '/oradata/pancake/temp.dbf';
```

```
8> duplicate target database for standby backup location '/rman/pancake';
9> }
executing command: SET NEWNAME
executing command: SET NEWNAME
executing command: SET NEWNAME
executing command: SET NEWNAME
executing command: SET NEWNAME
Starting Duplicate Db at 24-MAY-16
contents of Memory Script:
{
   restore clone standby controlfile from  '/rman/pancake/ctrl.bkp';
}
executing Memory Script
Starting restore at 24-MAY-16
allocated channel: ORA_AUX_DISK_1
channel ORA_AUX_DISK_1: SID=243 device type=DISK
channel ORA_AUX_DISK_1: restoring control file
channel ORA_AUX_DISK_1: restore complete, elapsed time: 00:00:01
output file name=/oradata/pancake/control01.ctl
output file name=/logs/pancake/control02.ctl
Finished restore at 24-MAY-16
contents of Memory Script:
{
   sql clone 'alter database mount standby database';
}
executing Memory Script
sql statement: alter database mount standby database
released channel: ORA_AUX_DISK_1
allocated channel: ORA_AUX_DISK_1
channel ORA_AUX_DISK_1: SID=243 device type=DISK
contents of Memory Script:
{
   set newname for tempfile  1 to
 "/oradata/pancake/temp.dbf";
   switch clone tempfile all;
   set newname for datafile  1 to
 "/oradata/pancake/pancake.dbf";
   set newname for datafile  2 to
 "/oradata/pancake/sysaux.dbf";
   set newname for datafile  3 to
 "/oradata/pancake/undotbs1.dbf";
   set newname for datafile  4 to
 "/oradata/pancake/users.dbf";
   restore
   clone database
   ;
```

```
}
executing Memory Script
executing command: SET NEWNAME
renamed tempfile 1 to /oradata/pancake/temp.dbf in control file
executing command: SET NEWNAME
executing command: SET NEWNAME
executing command: SET NEWNAME
executing command: SET NEWNAME
Starting restore at 24-MAY-16
using channel ORA_AUX_DISK_1
channel ORA_AUX_DISK_1: starting datafile backup set restore
channel ORA_AUX_DISK_1: specifying datafile(s) to restore from backup set
channel ORA_AUX_DISK_1: restoring datafile 00001 to
/oradata/pancake/pancake.dbf
channel ORA_AUX_DISK_1: restoring datafile 00002 to
/oradata/pancake/sysaux.dbf
channel ORA_AUX_DISK_1: restoring datafile 00003 to
/oradata/pancake/undotbs1.dbf
channel ORA_AUX_DISK_1: restoring datafile 00004 to
/oradata/pancake/users.dbf
channel ORA_AUX_DISK_1: reading from backup piece
/rman/pancake/1gr6c161_1_1
channel ORA_AUX_DISK_1: piece handle=/rman/pancake/1gr6c161_1_1
tag=ONTAP_MIGRATION
channel ORA_AUX_DISK_1: restored backup piece 1
channel ORA_AUX_DISK_1: restore complete, elapsed time: 00:00:07
Finished restore at 24-MAY-16
contents of Memory Script:
{
   switch clone datafile all;
}
executing Memory Script
datafile 1 switched to datafile copy
input datafile copy RECID=5 STAMP=912655725 file
name=/oradata/pancake/pancake.dbf
datafile 2 switched to datafile copy
input datafile copy RECID=6 STAMP=912655725 file
name=/oradata/pancake/sysaux.dbf
datafile 3 switched to datafile copy
input datafile copy RECID=7 STAMP=912655725 file
name=/oradata/pancake/undotbs1.dbf
datafile 4 switched to datafile copy
input datafile copy RECID=8 STAMP=912655725 file
name=/oradata/pancake/users.dbf
Finished Duplicate Db at 24-MAY-16
```

Replicación de registro inicial

Ahora debe enviar los cambios de la base de datos de origen a una nueva ubicación. Si lo hace, puede que sea necesario realizar una combinación de pasos. El método más sencillo sería tener RMAN en la base de datos de origen escribir archive logs en una conexión de red compartida. Si una ubicación compartida no está disponible, un método alternativo es utilizar RMAN para escribir en un sistema de archivos local y, a continuación, utilizar rcp o rsync para copiar los archivos.

En este ejemplo, la `/rman` Directory es un recurso compartido NFS que está disponible tanto para la base de datos original como para la migrada.

Una cuestión importante aquí es la `disk format` cláusula. El formato de disco del backup es `%h_%e_%a.dbf`, Lo que significa que debe utilizar el formato de número de hilo, número de secuencia e identificador de activación para la base de datos. Aunque las letras son diferentes, esto coincide con `log_archive_format='%t_%s_%r.dbf` en el pfile. Este parámetro también especifica archive logs en el formato de Núm. De thread, Núm. De secuencia e ID de activación. El resultado final es que los backups de los archivos de registro del origen utilizan una convención de nomenclatura que espera la base de datos. Al hacerlo, se realizan operaciones como `recover database` mucho más sencillo porque sqlplus anticipa correctamente los nombres de los archive logs que se van a reproducir.

```
RMAN> configure channel device type disk format
'/rman/pancake/logship/%h_%e_%a.dbf';
old RMAN configuration parameters:
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT
'/rman/pancake/arch/%h_%e_%a.dbf';
new RMAN configuration parameters:
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT
'/rman/pancake/logship/%h_%e_%a.dbf';
new RMAN configuration parameters are successfully stored
released channel: ORA_DISK_1
RMAN> backup as copy archivelog from time 'sysdate-2';
Starting backup at 24-MAY-16
current log archived
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=373 device type=DISK
channel ORA_DISK_1: starting archived log copy
input archived log thread=1 sequence=54 RECID=70 STAMP=912658508
output file name=/rman/pancake/logship/1_54_912576125.dbf RECID=123
STAMP=912659482
channel ORA_DISK_1: archived log copy complete, elapsed time: 00:00:01
channel ORA_DISK_1: starting archived log copy
input archived log thread=1 sequence=41 RECID=29 STAMP=912654101
output file name=/rman/pancake/logship/1_41_912576125.dbf RECID=124
STAMP=912659483
channel ORA_DISK_1: archived log copy complete, elapsed time: 00:00:01
...
channel ORA_DISK_1: starting archived log copy
input archived log thread=1 sequence=45 RECID=33 STAMP=912654688
output file name=/rman/pancake/logship/1_45_912576125.dbf RECID=152
STAMP=912659514
channel ORA_DISK_1: archived log copy complete, elapsed time: 00:00:01
channel ORA_DISK_1: starting archived log copy
input archived log thread=1 sequence=47 RECID=36 STAMP=912654809
output file name=/rman/pancake/logship/1_47_912576125.dbf RECID=153
STAMP=912659515
channel ORA_DISK_1: archived log copy complete, elapsed time: 00:00:01
Finished backup at 24-MAY-16
```

Reproducción de log inicial

Una vez que los archivos están en la ubicación del archive log, se pueden reproducir emitiendo el comando `recover database until cancel` seguido de la respuesta `AUTO` para reproducir automáticamente todos los logs disponibles. El archivo de parámetros está dirigiendo los archive logs al `/logs/archive`, Pero esto no coincide con la ubicación en la que se utilizó RMAN para guardar registros. La ubicación se puede redirigir temporalmente de la siguiente manera antes de recuperar la base de datos.

```
SQL> alter system set log_archive_dest_1='LOCATION=/rman/pancake/logship'
scope=memory;
System altered.
SQL> recover standby database until cancel;
ORA-00279: change 560224 generated at 05/24/2016 03:25:53 needed for
thread 1
ORA-00289: suggestion : /rman/pancake/logship/1_49_912576125.dbf
ORA-00280: change 560224 for thread 1 is in sequence #49
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
AUTO
ORA-00279: change 560353 generated at 05/24/2016 03:29:17 needed for
thread 1
ORA-00289: suggestion : /rman/pancake/logship/1_50_912576125.dbf
ORA-00280: change 560353 for thread 1 is in sequence #50
ORA-00278: log file '/rman/pancake/logship/1_49_912576125.dbf' no longer
needed
for this recovery
...
ORA-00279: change 560591 generated at 05/24/2016 03:33:56 needed for
thread 1
ORA-00289: suggestion : /rman/pancake/logship/1_54_912576125.dbf
ORA-00280: change 560591 for thread 1 is in sequence #54
ORA-00278: log file '/rman/pancake/logship/1_53_912576125.dbf' no longer
needed
for this recovery
ORA-00308: cannot open archived log
'/rman/pancake/logship/1_54_912576125.dbf'
ORA-27037: unable to obtain file status
Linux-x86_64 Error: 2: No such file or directory
Additional information: 3
```

La respuesta final del archive log informa de un error, pero esto es normal. El error indica que sqlplus estaba buscando un archivo log en particular y no lo encontró. La razón es más probable que el archivo log no exista aún.

Si la base de datos de origen se puede cerrar antes de copiar archive logs, este paso debe realizarse una sola vez. Los archive logs se copian y se reproducen y, a continuación, el proceso puede continuar directamente con el proceso de transposición que replica los redo logs críticos.

Replicación y repetición de log incremental

En la mayoría de los casos, la migración no se realiza de forma inmediata. Pueden pasar días o incluso semanas antes de que se complete el proceso de migración, lo que significa que los registros deben enviarse continuamente a la base de datos de réplica y reproducirse. Al hacerlo, se garantiza que se deban transferir y reproducir unos datos mínimos al llegar la transición.

Este proceso se puede programar fácilmente. Por ejemplo, el siguiente comando se puede programar en la base de datos original para asegurarse de que la ubicación utilizada para el envío de registros se actualiza

continuamente.

```
[oracle@jfsc1 pancake]$ cat copylogs.rman
configure channel device type disk format
'/rman/pancake/logship/%h_%e_%a.dbf';
backup as copy archivelog from time 'sysdate-2';
```

```
[oracle@jfsc1 pancake]$ rman target / cmdfile=copylogs.rman
Recovery Manager: Release 12.1.0.2.0 - Production on Tue May 24 04:36:19
2016
Copyright (c) 1982, 2014, Oracle and/or its affiliates.  All rights
reserved.
connected to target database: PANCAKE (DBID=3574534589)
RMAN> configure channel device type disk format
'/rman/pancake/logship/%h_%e_%a.dbf';
2> backup as copy archivelog from time 'sysdate-2';
3>
4>
using target database control file instead of recovery catalog
old RMAN configuration parameters:
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT
'/rman/pancake/logship/%h_%e_%a.dbf';
new RMAN configuration parameters:
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT
'/rman/pancake/logship/%h_%e_%a.dbf';
new RMAN configuration parameters are successfully stored
Starting backup at 24-MAY-16
current log archived
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=369 device type=DISK
channel ORA_DISK_1: starting archived log copy
input archived log thread=1 sequence=54 RECID=123 STAMP=912659482
RMAN-03009: failure of backup command on ORA_DISK_1 channel at 05/24/2016
04:36:22
ORA-19635: input and output file names are identical:
/rman/pancake/logship/1_54_912576125.dbf
continuing other job steps, job failed will not be re-run
channel ORA_DISK_1: starting archived log copy
input archived log thread=1 sequence=41 RECID=124 STAMP=912659483
RMAN-03009: failure of backup command on ORA_DISK_1 channel at 05/24/2016
04:36:23
ORA-19635: input and output file names are identical:
/rman/pancake/logship/1_41_912576125.dbf
continuing other job steps, job failed will not be re-run
...
```

```
channel ORA_DISK_1: starting archived log copy
input archived log thread=1 sequence=45 RECID=152 STAMP=912659514
RMAN-03009: failure of backup command on ORA_DISK_1 channel at 05/24/2016
04:36:55
ORA-19635: input and output file names are identical:
/rman/pancake/logship/1_45_912576125.dbf
continuing other job steps, job failed will not be re-run
channel ORA_DISK_1: starting archived log copy
input archived log thread=1 sequence=47 RECID=153 STAMP=912659515
RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
RMAN-03009: failure of backup command on ORA_DISK_1 channel at 05/24/2016
04:36:57
ORA-19635: input and output file names are identical:
/rman/pancake/logship/1_47_912576125.dbf
Recovery Manager complete.
```

Una vez recibidos los registros, deben reproducirse. Ejemplos anteriores mostraron el uso de sqlplus para ejecutar manualmente `recover database until cancel`, que se puede automatizar fácilmente. El ejemplo que se muestra aquí utiliza el script descrito en "Logs de Reproducción en Base de Datos en Espera". El script acepta un argumento que especifica la base de datos que necesita una operación de reproducción. Este proceso permite utilizar el mismo script en un esfuerzo de migración de varias bases de datos.

```
[root@jfsc2 pancake]# ./replaylogs.pl PANCAKE
ORACLE_SID = [oracle] ? The Oracle base has been set to /orabin
SQL*Plus: Release 12.1.0.2.0 Production on Tue May 24 04:47:10 2016
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit
Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
SQL> ORA-00279: change 560591 generated at 05/24/2016 03:33:56 needed for
thread 1
ORA-00289: suggestion : /rman/pancake/logship/1_54_912576125.dbf
ORA-00280: change 560591 for thread 1 is in sequence #54
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 562219 generated at 05/24/2016 04:15:08 needed for
thread 1
ORA-00289: suggestion : /rman/pancake/logship/1_55_912576125.dbf
ORA-00280: change 562219 for thread 1 is in sequence #55
ORA-00278: log file '/rman/pancake/logship/1_54_912576125.dbf' no longer
needed for this recovery
ORA-00279: change 562370 generated at 05/24/2016 04:19:18 needed for
thread 1
ORA-00289: suggestion : /rman/pancake/logship/1_56_912576125.dbf
ORA-00280: change 562370 for thread 1 is in sequence #56
ORA-00278: log file '/rman/pancake/logship/1_55_912576125.dbf' no longer
needed for this recovery
...
ORA-00279: change 563137 generated at 05/24/2016 04:36:20 needed for
thread 1
ORA-00289: suggestion : /rman/pancake/logship/1_65_912576125.dbf
ORA-00280: change 563137 for thread 1 is in sequence #65
ORA-00278: log file '/rman/pancake/logship/1_64_912576125.dbf' no longer
needed for this recovery
ORA-00308: cannot open archived log
'/rman/pancake/logship/1_65_912576125.dbf'
ORA-27037: unable to obtain file status
Linux-x86_64 Error: 2: No such file or directory
Additional information: 3
SQL> Disconnected from Oracle Database 12c Enterprise Edition Release
12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
```

Transición

Cuando esté listo para pasar al nuevo entorno, debe realizar una sincronización final. Cuando se trabaja con sistemas de archivos normales, es fácil asegurarse de que la base de datos migrada esté sincronizada al 100% con la original, ya que los redo logs originales se copian y se vuelven a reproducir. No hay una buena forma de hacerlo con ASM. Sólo los archive logs se pueden volver a copiar fácilmente. Para asegurarse de que no se pierden datos, el cierre final de la base de datos original debe realizarse con cuidado.

1. En primer lugar, la base de datos debe estar en modo inactivo, asegurándose de que no se realicen cambios. Esta desactivación puede incluir la desactivación de las operaciones programadas, el cierre de listeners y/o el cierre de aplicaciones.
2. Después de realizar este paso, la mayoría de los DBA crean una tabla ficticia que sirve como marcador del cierre.
3. Forzar un archivo log para asegurarse de que la creación de la tabla ficticia se registra en los archive logs. Para ello, ejecute los siguientes comandos:

```
SQL> create table cutovercheck as select * from dba_users;
Table created.
SQL> alter system archive log current;
System altered.
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
```

4. Para copiar el último de los archive logs, ejecute los siguientes comandos. La base de datos debe estar disponible pero no abierta.

```
SQL> startup mount;
ORACLE instance started.
Total System Global Area  805306368 bytes
Fixed Size                  2929552 bytes
Variable Size             331353200 bytes
Database Buffers          465567744 bytes
Redo Buffers                5455872 bytes
Database mounted.
```

5. Para copiar los archive logs, ejecute los siguientes comandos:

```
RMAN> configure channel device type disk format
'/rman/pancake/logship/%h_%e_%a.dbf';
2> backup as copy archivelog from time 'sysdate-2';
3>
4>
using target database control file instead of recovery catalog
old RMAN configuration parameters:
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT
'/rman/pancake/logship/%h_%e_%a.dbf';
new RMAN configuration parameters:
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT
'/rman/pancake/logship/%h_%e_%a.dbf';
new RMAN configuration parameters are successfully stored
Starting backup at 24-MAY-16
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=8 device type=DISK
channel ORA_DISK_1: starting archived log copy
input archived log thread=1 sequence=54 RECID=123 STAMP=912659482
RMAN-03009: failure of backup command on ORA_DISK_1 channel at
05/24/2016 04:58:24
ORA-19635: input and output file names are identical:
/rman/pancake/logship/1_54_912576125.dbf
continuing other job steps, job failed will not be re-run
...
channel ORA_DISK_1: starting archived log copy
input archived log thread=1 sequence=45 RECID=152 STAMP=912659514
RMAN-03009: failure of backup command on ORA_DISK_1 channel at
05/24/2016 04:58:58
ORA-19635: input and output file names are identical:
/rman/pancake/logship/1_45_912576125.dbf
continuing other job steps, job failed will not be re-run
channel ORA_DISK_1: starting archived log copy
input archived log thread=1 sequence=47 RECID=153 STAMP=912659515
RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
RMAN-03009: failure of backup command on ORA_DISK_1 channel at
05/24/2016 04:59:00
ORA-19635: input and output file names are identical:
/rman/pancake/logship/1_47_912576125.dbf
```

6. Por último, vuelva a reproducir los archive logs restantes en el nuevo servidor.

```
[root@jfsc2 pancake]# ./replaylogs.pl PANCAKE
ORACLE_SID = [oracle] ? The Oracle base has been set to /orabin
SQL*Plus: Release 12.1.0.2.0 Production on Tue May 24 05:00:53 2016
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit
Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
SQL> ORA-00279: change 563137 generated at 05/24/2016 04:36:20 needed
for thread 1
ORA-00289: suggestion : /rman/pancake/logship/1_65_912576125.dbf
ORA-00280: change 563137 for thread 1 is in sequence #65
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 563629 generated at 05/24/2016 04:55:20 needed for
thread 1
ORA-00289: suggestion : /rman/pancake/logship/1_66_912576125.dbf
ORA-00280: change 563629 for thread 1 is in sequence #66
ORA-00278: log file '/rman/pancake/logship/1_65_912576125.dbf' no longer
needed
for this recovery
ORA-00308: cannot open archived log
'/rman/pancake/logship/1_66_912576125.dbf'
ORA-27037: unable to obtain file status
Linux-x86_64 Error: 2: No such file or directory
Additional information: 3
SQL> Disconnected from Oracle Database 12c Enterprise Edition Release
12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
```

7. En esta fase, replique todos los datos. La base de datos está lista para convertirse de una base de datos en espera a una base de datos operativa activa y, a continuación, abrirse.

```
SQL> alter database activate standby database;
Database altered.
SQL> alter database open;
Database altered.
```

8. Confirme la presencia de la tabla ficticia y, a continuación, suéltela.

```
SQL> desc cutovercheck
 Name                                      Null?    Type
 ----------------------------------------- --------
----------------------------
 USERNAME                                  NOT NULL VARCHAR2(128)
 USER_ID                                   NOT NULL NUMBER
 PASSWORD                                           VARCHAR2(4000)
 ACCOUNT_STATUS                            NOT NULL VARCHAR2(32)
 LOCK_DATE                                          DATE
 EXPIRY_DATE                                        DATE
 DEFAULT_TABLESPACE                        NOT NULL VARCHAR2(30)
 TEMPORARY_TABLESPACE                      NOT NULL VARCHAR2(30)
 CREATED                                   NOT NULL DATE
 PROFILE                                   NOT NULL VARCHAR2(128)
 INITIAL_RSRC_CONSUMER_GROUP                        VARCHAR2(128)
 EXTERNAL_NAME                                      VARCHAR2(4000)
 PASSWORD_VERSIONS                                  VARCHAR2(12)
 EDITIONS_ENABLED                                   VARCHAR2(1)
 AUTHENTICATION_TYPE                                VARCHAR2(8)
 PROXY_ONLY_CONNECT                                 VARCHAR2(1)
 COMMON                                             VARCHAR2(3)
 LAST_LOGIN                                         TIMESTAMP(9) WITH
TIME ZONE
 ORACLE_MAINTAINED                                  VARCHAR2(1)
SQL> drop table cutovercheck;
Table dropped.
```

Migración de redo log no disruptiva

Hay veces en las que una base de datos está correctamente organizada en general con la excepción de los redo logs. Esto puede ocurrir por muchos motivos, el más común de los cuales está relacionado con las copias Snapshot. Productos como SnapManager para Oracle, SnapCenter y el marco de gestión de almacenamiento Snap Creator de NetApp permiten la recuperación casi instantánea de una base de datos, pero únicamente si revierte el estado de los volúmenes de archivos de datos. Si los redo logs comparten espacio con los archivos de datos, la reversión no se puede realizar de forma segura porque podría provocar la destrucción de los redo logs, lo que probablemente significa pérdida de datos. Por lo tanto, los redo logs deben reubicarse.

Este procedimiento es sencillo y puede realizarse sin interrupciones.

Configuración actual de redo log

1. Identifique el Núm. De grupos de redo logs y sus respectivos Núm.s de grupo.

```
SQL> select group#||' '||member from v$logfile;
GROUP#||''||MEMBER
--------------------------------------------------------------------------------
--------
1 /redo0/NTAP/redo01a.log
1 /redo1/NTAP/redo01b.log
2 /redo0/NTAP/redo02a.log
2 /redo1/NTAP/redo02b.log
3 /redo0/NTAP/redo03a.log
3 /redo1/NTAP/redo03b.log
rows selected.
```

2. Introduzca el tamaño de los redo logs.

```
SQL> select group#||' '||bytes from v$log;
GROUP#||''||BYTES
--------------------------------------------------------------------------------
--------
1 524288000
2 524288000
3 524288000
```

Crear nuevos logs

1. Para cada redo log, cree un nuevo grupo con un tamaño y un Núm. De miembros coincidentes.

```
SQL> alter database add logfile ('/newredo0/redo01a.log',
'/newredo1/redo01b.log') size 500M;
Database altered.
SQL> alter database add logfile ('/newredo0/redo02a.log',
'/newredo1/redo02b.log') size 500M;
Database altered.
SQL> alter database add logfile ('/newredo0/redo03a.log',
'/newredo1/redo03b.log') size 500M;
Database altered.
SQL>
```

2. Verifique la nueva configuración.

```
SQL> select group#||' '||member from v$logfile;
GROUP#||''||MEMBER
--------------------------------------------------------------------------------
--------
1 /redo0/NTAP/redo01a.log
1 /redo1/NTAP/redo01b.log
2 /redo0/NTAP/redo02a.log
2 /redo1/NTAP/redo02b.log
3 /redo0/NTAP/redo03a.log
3 /redo1/NTAP/redo03b.log
4 /newredo0/redo01a.log
4 /newredo1/redo01b.log
5 /newredo0/redo02a.log
5 /newredo1/redo02b.log
6 /newredo0/redo03a.log
6 /newredo1/redo03b.log
12 rows selected.
```

Borre los registros antiguos

1. Borre los registros antiguos (grupos 1, 2 y 3).

```
SQL> alter database drop logfile group 1;
Database altered.
SQL> alter database drop logfile group 2;
Database altered.
SQL> alter database drop logfile group 3;
Database altered.
```

2. Si encuentra un error que le impide borrar un log activo, fuerce un cambio al siguiente log para liberar el bloqueo y forzar un punto de control global. Vea el siguiente ejemplo de este proceso. Se ha denegado el intento de borrar el grupo de archivos de registro 2, que se encontraba en la ubicación anterior, porque todavía había datos activos en este archivo de registro.

```
SQL> alter database drop logfile group 2;
alter database drop logfile group 2
*
ERROR at line 1:
ORA-01623: log 2 is current log for instance NTAP (thread 1) - cannot
drop
ORA-00312: online log 2 thread 1: '/redo0/NTAP/redo02a.log'
ORA-00312: online log 2 thread 1: '/redo1/NTAP/redo02b.log'
```

3. Un archivo log seguido de un punto de control permite borrar el archivo log.

```
SQL> alter system archive log current;
System altered.
SQL> alter system checkpoint;
System altered.
SQL> alter database drop logfile group 2;
Database altered.
```

4. A continuación, elimine los registros del sistema de archivos. Debe realizar este proceso con extremo cuidado.

Copiado de datos de host

Al igual que sucede con la migración a nivel de base de datos, la migración en la capa de host proporciona un enfoque independiente del proveedor de almacenamiento.

En otras palabras, en algún momento “solo copiar los archivos” es la mejor opción.

Aunque este enfoque de baja tecnología puede parecer demasiado básico, ofrece beneficios significativos porque no se requiere ningún software especial y los datos originales permanecen intactos de forma segura durante el proceso. La principal limitación es el hecho de que una migración de datos de copia de archivos es un proceso disruptivo, ya que la base de datos debe cerrarse antes de que comience la operación de copia. No hay una buena manera de sincronizar los cambios dentro de un archivo, por lo que los archivos deben estar completamente desactivados antes de que comience la copia.

Si el cierre necesario para una operación de copia no es deseable, la siguiente mejor opción basada en host es utilizar un gestor de volúmenes lógicos (LVM). Existen muchas opciones de LVM, incluido Oracle ASM, todas con capacidades similares, pero también con algunas limitaciones que deben tenerse en cuenta. En la mayoría de los casos, la migración se puede realizar sin tiempos de inactividad ni interrupciones.

Copiando sistema de archivos al sistema de archivos

La utilidad de una operación de copia simple no debe subestimarse. Esta operación requiere un tiempo de inactividad durante el proceso de copia, pero es un proceso muy fiable y no requiere experiencia especial en sistemas operativos, bases de datos o sistemas de almacenamiento. Además, es muy seguro porque no afecta a los datos originales. Normalmente, un administrador de sistemas cambia los sistemas de archivos de origen para montarse como de solo lectura y luego reinicia un servidor para garantizar que nada pueda dañar los datos actuales. El proceso de copia se puede programar para asegurarse de que se ejecuta lo más rápido posible sin riesgo de error por parte del usuario. Dado que el tipo de I/O es una transferencia secuencial simple de datos, es altamente eficiente del ancho de banda.

El siguiente ejemplo muestra una opción para una migración segura y rápida.

Entorno Oracle

El entorno que se va a migrar es el siguiente:

- Sistemas de archivos actuales

```
ontap-nfs1:/host1_oradata       52428800  16196928  36231872  31%
/oradata
ontap-nfs1:/host1_logs          49807360    548032  49259328   2% /logs
```

- Sistemas de archivos nuevos

```
ontap-nfs1:/host1_logs_new      49807360       128  49807232   1%
/new/logs
ontap-nfs1:/host1_oradata_new   49807360       128  49807232   1%
/new/oradata
```

Descripción general

El DBA puede migrar la base de datos simplemente cerrando la base de datos y copiando los archivos, pero el proceso se ejecuta fácilmente en la secuencia de comandos si se deben migrar muchas bases de datos o si se minimiza el tiempo de inactividad es crítico. El uso de scripts también reduce la posibilidad de errores de los usuarios.

Los scripts de ejemplo que se muestran automatizan las siguientes operaciones:

- Cerrando la base de datos
- Convertir los sistemas de archivos existentes a un estado de sólo lectura
- Copia de todos los datos de los sistemas de archivos de origen a los de destino, lo que conserva todos los permisos de archivos
- Desmontaje de los sistemas de archivos antiguos y nuevos
- Volver a montar los nuevos sistemas de archivos en las mismas rutas que los sistemas de archivos anteriores

Procedimiento

1. Cierre la base de datos.

```
[root@host1 current]# ./dbshut.pl NTAP
ORACLE_SID = [oracle] ? The Oracle base has been set to /orabin
SQL*Plus: Release 12.1.0.2.0 Production on Thu Dec 3 15:58:48 2015
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit
Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
SQL> Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> Disconnected from Oracle Database 12c Enterprise Edition Release
12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
NTAP shut down
```

2. Convierta los sistemas de archivos a sólo lectura. Esto se puede hacer más rápidamente usando un script, como se muestra en "Convertir sistema de archivos a Sólo lectura".

```
[root@host1 current]# ./mk.fs.readonly.pl /oradata
/oradata unmounted
/oradata mounted read-only
[root@host1 current]# ./mk.fs.readonly.pl /logs
/logs unmounted
/logs mounted read-only
```

3. Confirme que los sistemas de archivos ahora son de sólo lectura.

```
ontap-nfs1:/host1_oradata on /oradata type nfs
(ro,bg,vers=3,rsize=65536,wsize=65536,addr=172.20.101.10)
ontap-nfs1:/host1_logs on /logs type nfs
(ro,bg,vers=3,rsize=65536,wsize=65536,addr=172.20.101.10)
```

4. Sincronice el contenido del sistema de archivos con `rsync` comando.

```
[root@host1 current]# rsync -rlpogt --stats --progress
--exclude=.snapshot /oradata/ /new/oradata/
sending incremental file list
./
NTAP/
NTAP/IOPS.dbf
```

```
 10737426432 100%  153.50MB/s    0:01:06 (xfer#1, to-check=10/13)
NTAP/iops.dbf.zip
    22823573 100%   12.09MB/s    0:00:01 (xfer#2, to-check=9/13)
...
NTAP/undotbs02.dbf
  1073750016 100%  131.60MB/s    0:00:07 (xfer#10, to-check=1/13)
NTAP/users01.dbf
     5251072 100%    3.95MB/s    0:00:01 (xfer#11, to-check=0/13)
Number of files: 13
Number of files transferred: 11
Total file size: 18570092218 bytes
Total transferred file size: 18570092218 bytes
Literal data: 18570092218 bytes
Matched data: 0 bytes
File list size: 277
File list generation time: 0.001 seconds
File list transfer time: 0.000 seconds
Total bytes sent: 18572359828
Total bytes received: 228
sent 18572359828 bytes  received 228 bytes  162204017.96 bytes/sec
total size is 18570092218  speedup is 1.00
[root@host1 current]# rsync -rlpogt --stats --progress
--exclude=.snapshot /logs/ /new/logs/
sending incremental file list
./
NTAP/
NTAP/1_22_897068759.dbf
    45523968 100%   95.98MB/s    0:00:00 (xfer#1, to-check=15/18)
NTAP/1_23_897068759.dbf
    40601088 100%   49.45MB/s    0:00:00 (xfer#2, to-check=14/18)
...
NTAP/redo/redo02.log
    52429312 100%   44.68MB/s    0:00:01 (xfer#12, to-check=1/18)
NTAP/redo/redo03.log
    52429312 100%   68.03MB/s    0:00:00 (xfer#13, to-check=0/18)
Number of files: 18
Number of files transferred: 13
Total file size: 527032832 bytes
Total transferred file size: 527032832 bytes
Literal data: 527032832 bytes
Matched data: 0 bytes
File list size: 413
File list generation time: 0.001 seconds
File list transfer time: 0.000 seconds
Total bytes sent: 527098156
Total bytes received: 278
```

```
sent 527098156 bytes  received 278 bytes  95836078.91 bytes/sec
total size is 527032832  speedup is 1.00
```

5. Desmonte los sistemas de archivos antiguos y reubique los datos copiados. Esto se puede hacer más rápidamente usando un script, como se muestra en "Reemplazar sistema de archivos".

```
[root@host1 current]# ./swap.fs.pl /logs,/new/logs
/new/logs unmounted
/logs unmounted
Updated /logs mounted
[root@host1 current]# ./swap.fs.pl /oradata,/new/oradata
/new/oradata unmounted
/oradata unmounted
Updated /oradata mounted
```

6. Confirme que los nuevos sistemas de archivos están en posición.

```
ontap-nfs1:/host1_logs_new on /logs type nfs
(rw,bg,vers=3,rsize=65536,wsize=65536,addr=172.20.101.10)
ontap-nfs1:/host1_oradata_new on /oradata type nfs
(rw,bg,vers=3,rsize=65536,wsize=65536,addr=172.20.101.10)
```

7. Inicie la base de datos.

```
[root@host1 current]# ./dbstart.pl NTAP
ORACLE_SID = [oracle] ? The Oracle base has been set to /orabin
SQL*Plus: Release 12.1.0.2.0 Production on Thu Dec 3 16:10:07 2015
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to an idle instance.
SQL> ORACLE instance started.
Total System Global Area  805306368 bytes
Fixed Size                  2929552 bytes
Variable Size             390073456 bytes
Database Buffers          406847488 bytes
Redo Buffers                5455872 bytes
Database mounted.
Database opened.
SQL> Disconnected from Oracle Database 12c Enterprise Edition Release
12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
NTAP started
```

Transición totalmente automatizada

Este script de ejemplo acepta argumentos del SID de la base de datos seguidos de pares de sistemas de archivos delimitados comúnmente. Para el ejemplo mostrado anteriormente, el comando se emite del siguiente modo:

```
[root@host1 current]# ./migrate.oracle.fs.pl NTAP /logs,/new/logs
/oradata,/new/oradata
```

Cuando se ejecuta, el script de ejemplo intenta realizar la siguiente secuencia. Termina si encuentra un error en cualquier paso:

1. Cierre la base de datos.
2. Convierta los sistemas de archivos actuales al estado de sólo lectura.
3. Utilice cada par delimitado por comas de argumentos del sistema de archivos y sincronice el primer sistema de archivos con el segundo.
4. Desmonte los sistemas de archivos anteriores.
5. Actualice el `/etc/fstab` el archivo es el siguiente:
   a. Cree un backup en `/etc/fstab.bak`.
   b. Comente las entradas anteriores de los sistemas de archivos anteriores y nuevos.
   c. Cree una nueva entrada para el nuevo sistema de archivos que utilice el antiguo punto de montaje.
6. Monte los sistemas de archivos.
7. Inicie la base de datos.

El siguiente texto proporciona un ejemplo de ejecución para este script:

```
[root@host1 current]# ./migrate.oracle.fs.pl NTAP /logs,/new/logs
/oradata,/new/oradata
ORACLE_SID = [oracle] ? The Oracle base has been set to /orabin
SQL*Plus: Release 12.1.0.2.0 Production on Thu Dec 3 17:05:50 2015
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit
Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
SQL> Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> Disconnected from Oracle Database 12c Enterprise Edition Release
12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
NTAP shut down
```

```
sending incremental file list
./
NTAP/
NTAP/1_22_897068759.dbf
    45523968 100%  185.40MB/s    0:00:00 (xfer#1, to-check=15/18)
NTAP/1_23_897068759.dbf
    40601088 100%   81.34MB/s    0:00:00 (xfer#2, to-check=14/18)
...
NTAP/redo/redo02.log
    52429312 100%   70.42MB/s    0:00:00 (xfer#12, to-check=1/18)
NTAP/redo/redo03.log
    52429312 100%   47.08MB/s    0:00:01 (xfer#13, to-check=0/18)
Number of files: 18
Number of files transferred: 13
Total file size: 527032832 bytes
Total transferred file size: 527032832 bytes
Literal data: 527032832 bytes
Matched data: 0 bytes
File list size: 413
File list generation time: 0.001 seconds
File list transfer time: 0.000 seconds
Total bytes sent: 527098156
Total bytes received: 278
sent 527098156 bytes  received 278 bytes  150599552.57 bytes/sec
total size is 527032832  speedup is 1.00
Succesfully replicated filesystem /logs to /new/logs
sending incremental file list
./
NTAP/
NTAP/IOPS.dbf
 10737426432 100%  176.55MB/s    0:00:58 (xfer#1, to-check=10/13)
NTAP/iops.dbf.zip
    22823573 100%    9.48MB/s    0:00:02 (xfer#2, to-check=9/13)
... NTAP/undotbs01.dbf
   309338112 100%   70.76MB/s    0:00:04 (xfer#9, to-check=2/13)
NTAP/undotbs02.dbf
  1073750016 100%  187.65MB/s    0:00:05 (xfer#10, to-check=1/13)
NTAP/users01.dbf
     5251072 100%    5.09MB/s    0:00:00 (xfer#11, to-check=0/13)
Number of files: 13
Number of files transferred: 11
Total file size: 18570092218 bytes
Total transferred file size: 18570092218 bytes
Literal data: 18570092218 bytes
Matched data: 0 bytes
File list size: 277
```

```
File list generation time: 0.001 seconds
File list transfer time: 0.000 seconds
Total bytes sent: 18572359828
Total bytes received: 228
sent 18572359828 bytes  received 228 bytes  177725933.55 bytes/sec
total size is 18570092218  speedup is 1.00
Succesfully replicated filesystem /oradata to /new/oradata
swap 0 /logs /new/logs
/new/logs unmounted
/logs unmounted
Mounted updated /logs
Swapped filesystem /logs for /new/logs
swap 1 /oradata /new/oradata
/new/oradata unmounted
/oradata unmounted
Mounted updated /oradata
Swapped filesystem /oradata for /new/oradata
ORACLE_SID = [oracle] ? The Oracle base has been set to /orabin
SQL*Plus: Release 12.1.0.2.0 Production on Thu Dec 3 17:08:59 2015
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to an idle instance.
SQL> ORACLE instance started.
Total System Global Area  805306368 bytes
Fixed Size                  2929552 bytes
Variable Size             390073456 bytes
Database Buffers          406847488 bytes
Redo Buffers                5455872 bytes
Database mounted.
Database opened.
SQL> Disconnected from Oracle Database 12c Enterprise Edition Release
12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
NTAP started
[root@host1 current]#
```

Migración de Oracle ASM spfile y passwd

Una dificultad para completar la migración que implica ASM es el spfile específico de ASM y el archivo de contraseñas. Por defecto, estos archivos de metadatos críticos se crean en el primer grupo de discos de ASM definido. Si se debe evacuar y eliminar un grupo de discos de ASM concreto, se debe reubicar el archivo spfile y de contraseñas que rigen dicha instancia de ASM.

Otro caso de uso en el que es posible que sea necesario reubicar estos archivos es durante un despliegue de software de gestión de base de datos como SnapManager para Oracle o el complemento de Oracle de SnapCenter. Una de las características de estos productos es restaurar rápidamente una base de datos mediante la reversión del estado de las LUN de ASM que alojan los archivos de datos. Para hacerlo, es necesario desconectar el grupo de discos de ASM antes de realizar una restauración. Esto no es un problema

siempre que los archivos de datos de una base de datos determinada estén aislados en un grupo de discos de ASM dedicado.

Cuando ese grupo de discos también contiene el archivo spfile/passwd de ASM, la única forma en que el grupo de discos se puede poner fuera de línea es cerrar toda la instancia de ASM. Este es un proceso disruptivo, lo que significa que el archivo spfile/passwd tendría que ser reubicado.

Entorno Oracle

1. SID de base de datos = TOAST
2. Archivos de datos actuales en `+DATA`
3. Archivos log y archivos de control actuales en `+LOGS`
4. Se han establecido nuevos grupos de discos de ASM como `+NEWDATA` y.. `+NEWLOGS`

Ubicaciones de archivos spfile/passwd de ASM

La reubicación de estos archivos puede realizarse de forma no disruptiva. Sin embargo, por motivos de seguridad, NetApp recomienda cerrar el entorno de la base de datos para que pueda estar seguro de que los archivos se han reubicado y que la configuración se ha actualizado correctamente. Este procedimiento se debe repetir si hay varias instancias de ASM presentes en un servidor.

Identificar instancias de ASM

Identifique las instancias de ASM en función de los datos registrados en la `oratab` archivo. Las instancias de ASM se indican con un símbolo +.

```
-bash-4.1$ cat /etc/oratab | grep '^+'
+ASM:/orabin/grid:N             # line added by Agent
```

Hay una instancia de ASM denominada +ASM en este servidor.

Asegúrese de que todas las bases de datos están cerradas

El único proceso smon visible debe ser smon para la instancia de ASM en uso. La presencia de otro proceso smon indica que una base de datos todavía está en ejecución.

```
-bash-4.1$ ps -ef | grep smon
oracle     857     1  0 18:26 ?        00:00:00 asm_smon_+ASM
```

El único proceso smon es la propia instancia de ASM. Esto significa que no se ejecuta ninguna otra base de datos y es seguro continuar sin riesgo de interrumpir las operaciones de la base de datos.

Localizar archivos

Identifique la ubicación actual del archivo spfile y de contraseña de ASM mediante `spget` y.. `pwget` comandos.

```
bash-4.1$ asmcmd
ASMCMD> spget
+DATA/spfile.ora
```

```
ASMCMD> pwget --asm
+DATA/orapwasm
```

Los archivos se encuentran en la base del `+DATA` grupo de discos.

Copiar archivos

Copie los archivos en el nuevo grupo de discos de ASM con `spcopy` y.. `pwcopy` comandos. Si el nuevo grupo de discos se ha creado recientemente y está vacío actualmente, es posible que tenga que montarlo primero.

```
ASMCMD> mount NEWDATA
```

```
ASMCMD> spcopy +DATA/spfile.ora +NEWDATA/spfile.ora
copying +DATA/spfile.ora -> +NEWDATA/spfilea.ora
```

```
ASMCMD> pwcopy +DATA/orapwasm +NEWDATA/orapwasm
copying +DATA/orapwasm -> +NEWDATA/orapwasm
```

Los archivos se han copiado ahora de `+DATA` para `+NEWDATA`.

Actualizar instancia de ASM

La instancia de ASM debe actualizarse para reflejar el cambio de ubicación. La `spset` y.. `pwset` Los comandos actualizan los metadatos de ASM necesarios para iniciar el grupo de discos de ASM.

```
ASMCMD> spset +NEWDATA/spfile.ora
ASMCMD> pwset --asm +NEWDATA/orapwasm
```

Active ASM con archivos actualizados

En este punto, la instancia de ASM sigue utilizando las ubicaciones anteriores de estos archivos. La instancia se debe reiniciar para forzar una nueva lectura de los archivos desde sus nuevas ubicaciones y liberar bloqueos en los archivos anteriores.

```
-bash-4.1$ sqlplus / as sysasm
SQL> shutdown immediate;
ASM diskgroups volume disabled
ASM diskgroups dismounted
ASM instance shutdown
```

```
SQL> startup
ASM instance started
Total System Global Area 1140850688 bytes
Fixed Size                  2933400 bytes
Variable Size            1112751464 bytes
ASM Cache                  25165824 bytes
ORA-15032: not all alterations performed
ORA-15017: diskgroup "NEWDATA" cannot be mounted
ORA-15013: diskgroup "NEWDATA" is already mounted
```

Elimine los archivos de contraseña y spfile antiguos

Si el procedimiento se ha realizado correctamente, los archivos anteriores ya no se bloquean y ahora se pueden eliminar.

```
-bash-4.1$ asmcmd
ASMCMD> rm +DATA/spfile.ora
ASMCMD> rm +DATA/orapwasm
```

Copia de Oracle ASM en ASM

Oracle ASM es esencialmente un gestor de volúmenes combinado ligero y un sistema de archivos. Dado que el sistema de archivos no se puede ver fácilmente, se debe utilizar RMAN para realizar operaciones de copia. A pesar de que un proceso de migración basado en copias es seguro y sencillo, el resultado es cierto tipo de interrupciones. La interrupción puede minimizarse, pero no eliminarse por completo.

Si desea una migración no disruptiva de una base de datos basada en ASM, la mejor opción es aprovechar la capacidad de ASM para reequilibrar las extensiones de ASM a nuevos LUN y borrar los LUN antiguos. Hacerlo resulta generalmente seguro y no disruptivo para las operaciones, pero no ofrece ningún camino de retroceso. Si se encuentran problemas funcionales o de rendimiento, la única opción es volver a migrar los datos al origen.

Este riesgo puede evitarse copiando la base de datos a la nueva ubicación en lugar de mover los datos, de modo que los datos originales queden intactos. La base de datos se puede probar completamente en su nueva ubicación antes de comenzar a funcionar, y la base de datos original está disponible como opción de reserva si se encuentran problemas.

Este procedimiento es una de las muchas opciones que implica RMAN. Está diseñado para permitir un proceso de dos pasos en el que se crea la copia de seguridad inicial y, a continuación, se sincroniza a través de la reproducción de log. Este proceso es deseable minimizar los tiempos de inactividad, ya que permite que la base de datos permanezca operativa y sirviendo datos durante la copia básica inicial.

Copiar base de datos

Oracle RMAN crea una copia de nivel 0 (completa) de la base de datos de origen ubicada actualmente en el grupo de discos de ASM `+DATA` a la nueva ubicación en `+NEWDATA`.

```
-bash-4.1$ rman target /
Recovery Manager: Release 12.1.0.2.0 - Production on Sun Dec 6 17:40:03
2015
Copyright (c) 1982, 2014, Oracle and/or its affiliates.  All rights
reserved.
connected to target database: TOAST (DBID=2084313411)
RMAN> backup as copy incremental level 0 database format '+NEWDATA' tag
'ONTAP_MIGRATION';
Starting backup at 06-DEC-15
using target database control file instead of recovery catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=302 device type=DISK
channel ORA_DISK_1: starting datafile copy
input datafile file number=00001
name=+DATA/TOAST/DATAFILE/system.262.897683141
...
input datafile file number=00004
name=+DATA/TOAST/DATAFILE/users.264.897683151
output file name=+NEWDATA/TOAST/DATAFILE/users.258.897759623
tag=ONTAP_MIGRATION RECID=5 STAMP=897759622
channel ORA_DISK_1: datafile copy complete, elapsed time: 00:00:01
channel ORA_DISK_1: starting incremental level 0 datafile backup set
channel ORA_DISK_1: specifying datafile(s) in backup set
including current SPFILE in backup set
channel ORA_DISK_1: starting piece 1 at 06-DEC-15
channel ORA_DISK_1: finished piece 1 at 06-DEC-15
piece
handle=+NEWDATA/TOAST/BACKUPSET/2015_12_06/nnsnn0_ontap_migration_0.262.89
7759623 tag=ONTAP_MIGRATION comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:01
Finished backup at 06-DEC-15
```

Forzar el cambio de archive log

Debe forzar un cambio de archive log para asegurarse de que los archive logs contienen todos los datos necesarios para que la copia sea totalmente coherente. Sin este comando, es posible que los datos clave sigan presentes en los redo logs.

```
RMAN> sql 'alter system archive log current';
sql statement: alter system archive log current
```

Cierre la base de datos de origen

La interrupción comienza en este paso porque la base de datos se cierra y se coloca en un modo de solo lectura de acceso limitado. Para cerrar la base de datos de origen, ejecute los siguientes comandos:

```
RMAN> shutdown immediate;
using target database control file instead of recovery catalog
database closed
database dismounted
Oracle instance shut down
RMAN> startup mount;
connected to target database (not started)
Oracle instance started
database mounted
Total System Global Area     805306368 bytes
Fixed Size                     2929552 bytes
Variable Size                390073456 bytes
Database Buffers             406847488 bytes
Redo Buffers                   5455872 bytes
```

Backup de CONTROLFILE

Debe realizar una copia de seguridad del archivo de control en caso de que deba anular la migración y volver a la ubicación de almacenamiento original. Una copia del archivo de control de copia de seguridad no es 100% necesaria, pero hace que el proceso de restablecer las ubicaciones de los archivos de base de datos a la ubicación original sea más fácil.

```
RMAN> backup as copy current controlfile format '/tmp/TOAST.ctrl';
Starting backup at 06-DEC-15
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=358 device type=DISK
channel ORA_DISK_1: starting datafile copy
copying current control file
output file name=/tmp/TOAST.ctrl tag=TAG20151206T174753 RECID=6
STAMP=897760073
channel ORA_DISK_1: datafile copy complete, elapsed time: 00:00:01
Finished backup at 06-DEC-15
```

Actualizaciones de parámetros

El spfile actual contiene referencias a los archivos de control en sus ubicaciones actuales dentro del antiguo grupo de discos de ASM. Debe editarse, lo cual se hace fácilmente editando una versión pfile intermedia.

```
RMAN> create pfile='/tmp/pfile' from spfile;
Statement processed
```

Actualizar archivo pfile

Actualice los parámetros que hagan referencia a los grupos de discos de ASM antiguos para reflejar los nuevos nombres de grupos de discos de ASM. A continuación, guarde el archivo pfile actualizado. Compruebe que la `db_create` los parámetros están presentes.

En el ejemplo siguiente, las referencias a. `+DATA` eso fue cambiado a. `+NEWDATA` se resaltan en amarillo. Dos parámetros clave son el `db_create` parámetros que crean cualquier archivo nuevo en la ubicación correcta.

```
*.compatible='12.1.0.2.0'
*.control_files='+NEWLOGS/TOAST/CONTROLFILE/current.258.897683139'
*.db_block_size=8192
*. db_create_file_dest='+NEWDATA'
*. db_create_online_log_dest_1='+NEWLOGS'
*.db_domain=''
*.db_name='TOAST'
*.diagnostic_dest='/orabin'
*.dispatchers='(PROTOCOL=TCP) (SERVICE=TOASTXDB)'
*.log_archive_dest_1='LOCATION=+NEWLOGS'
*.log_archive_format='%t_%s_%r.dbf'
```

Actualice el archivo init.ora

La mayoría de las bases de datos basadas en ASM utilizan un `init.ora` archivo ubicado en la `$ORACLE_HOME/dbs` Directorio, que es un punto a spfile en el grupo de discos de ASM. Este archivo se debe redirigir a una ubicación en el nuevo grupo de discos de ASM.

```
-bash-4.1$ cd $ORACLE_HOME/dbs
-bash-4.1$ cat initTOAST.ora
SPFILE='+DATA/TOAST/spfileTOAST.ora'
```

Cambie este archivo de la siguiente manera:

```
SPFILE=+NEWLOGS/TOAST/spfileTOAST.ora
```

Recreación del archivo de parámetros

El archivo spfile ya está listo para ser rellenado por los datos del archivo pfile editado.

```
RMAN> create spfile from pfile='/tmp/pfile';
Statement processed
```

Inicie la base de datos para empezar a utilizar el nuevo spfile

Inicie la base de datos para asegurarse de que ahora utiliza el spfile recién creado y de que cualquier otro cambio en los parámetros del sistema se registra correctamente.

```
RMAN> startup nomount;
connected to target database (not started)
Oracle instance started
Total System Global Area     805306368 bytes
Fixed Size                     2929552 bytes
Variable Size                373296240 bytes
Database Buffers             423624704 bytes
Redo Buffers                   5455872 bytes
```

Restaure el archivo de control

RMAN también puede restaurar el archivo de control de copia de seguridad creado por RMAN directamente en la ubicación especificada en el nuevo spfile.

```
RMAN> restore controlfile from
'+DATA/TOAST/CONTROLFILE/current.258.897683139';
Starting restore at 06-DEC-15
using target database control file instead of recovery catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=417 device type=DISK
channel ORA_DISK_1: copied control file copy
output file name=+NEWLOGS/TOAST/CONTROLFILE/current.273.897761061
Finished restore at 06-DEC-15
```

Monte la base de datos y verifique el uso del nuevo archivo de control.

```
RMAN> alter database mount;
using target database control file instead of recovery catalog
Statement processed
```

```
SQL> show parameter control_files;
NAME                                 TYPE        VALUE
------------------------------------ -----------
------------------------------
control_files                        string
+NEWLOGS/TOAST/CONTROLFILE/cur
                                                 rent.273.897761061
```

Reproducción de registro

La base de datos utiliza actualmente los archivos de datos en la ubicación antigua. Antes de poder utilizar la copia, deben sincronizarse. Ha transcurrido tiempo durante el proceso de copia inicial y los cambios se han registrado principalmente en los archive logs. Estos cambios se replican de la siguiente manera:

1. Realice una copia de seguridad incremental de RMAN, que contiene los archive logs.

```
RMAN> backup incremental level 1 format '+NEWLOGS' for recover of copy
with tag 'ONTAP_MIGRATION' database;
Starting backup at 06-DEC-15
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=62 device type=DISK
channel ORA_DISK_1: starting incremental level 1 datafile backup set
channel ORA_DISK_1: specifying datafile(s) in backup set
input datafile file number=00001
name=+DATA/TOAST/DATAFILE/system.262.897683141
input datafile file number=00002
name=+DATA/TOAST/DATAFILE/sysaux.260.897683143
input datafile file number=00003
name=+DATA/TOAST/DATAFILE/undotbs1.257.897683145
input datafile file number=00004
name=+DATA/TOAST/DATAFILE/users.264.897683151
channel ORA_DISK_1: starting piece 1 at 06-DEC-15
channel ORA_DISK_1: finished piece 1 at 06-DEC-15
piece
handle=+NEWLOGS/TOAST/BACKUPSET/2015_12_06/nnndn1_ontap_migration_0.268.
897762693 tag=ONTAP_MIGRATION comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:01
channel ORA_DISK_1: starting incremental level 1 datafile backup set
channel ORA_DISK_1: specifying datafile(s) in backup set
including current control file in backup set
including current SPFILE in backup set
channel ORA_DISK_1: starting piece 1 at 06-DEC-15
channel ORA_DISK_1: finished piece 1 at 06-DEC-15
piece
handle=+NEWLOGS/TOAST/BACKUPSET/2015_12_06/ncsnn1_ontap_migration_0.267.
897762697 tag=ONTAP_MIGRATION comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:01
Finished backup at 06-DEC-15
```

2. Vuelva a reproducir el log.

```
RMAN> recover copy of database with tag 'ONTAP_MIGRATION';
Starting recover at 06-DEC-15
using channel ORA_DISK_1
channel ORA_DISK_1: starting incremental datafile backup set restore
channel ORA_DISK_1: specifying datafile copies to recover
recovering datafile copy file number=00001
name=+NEWDATA/TOAST/DATAFILE/system.259.897759609
recovering datafile copy file number=00002
name=+NEWDATA/TOAST/DATAFILE/sysaux.263.897759615
recovering datafile copy file number=00003
name=+NEWDATA/TOAST/DATAFILE/undotbs1.264.897759619
recovering datafile copy file number=00004
name=+NEWDATA/TOAST/DATAFILE/users.258.897759623
channel ORA_DISK_1: reading from backup piece
+NEWLOGS/TOAST/BACKUPSET/2015_12_06/nnndn1_ontap_migration_0.268.8977626
93
channel ORA_DISK_1: piece
handle=+NEWLOGS/TOAST/BACKUPSET/2015_12_06/nnndn1_ontap_migration_0.268.
897762693 tag=ONTAP_MIGRATION
channel ORA_DISK_1: restored backup piece 1
channel ORA_DISK_1: restore complete, elapsed time: 00:00:01
Finished recover at 06-DEC-15
```

Activación

El archivo de control que se restauró sigue haciendo referencia a los archivos de datos en la ubicación original y también contiene la información de ruta de acceso para los archivos de datos copiados.

1. Para cambiar los archivos de datos activos, ejecute el `switch database to copy` comando.

```
RMAN> switch database to copy;
datafile 1 switched to datafile copy
"+NEWDATA/TOAST/DATAFILE/system.259.897759609"
datafile 2 switched to datafile copy
"+NEWDATA/TOAST/DATAFILE/sysaux.263.897759615"
datafile 3 switched to datafile copy
"+NEWDATA/TOAST/DATAFILE/undotbs1.264.897759619"
datafile 4 switched to datafile copy
"+NEWDATA/TOAST/DATAFILE/users.258.897759623"
```

   Los archivos de datos activos son ahora los archivos de datos copiados, pero es posible que haya cambios en los redo logs finales.

2. Para reproducir todos los logs restantes, ejecute el `recover database` comando. Si el mensaje `media recovery complete` aparece, el proceso se ha realizado correctamente.

```
RMAN> recover database;
Starting recover at 06-DEC-15
using channel ORA_DISK_1
starting media recovery
media recovery complete, elapsed time: 00:00:01
Finished recover at 06-DEC-15
```

Este proceso solo cambió la ubicación de los archivos de datos normales. Se debe cambiar el nombre de los archivos de datos temporales, pero no es necesario copiarlos porque solo son temporales. La base de datos está inactiva, por lo que no hay datos activos en los archivos de datos temporales.

3. Para reubicar los archivos de datos temporales, primero identifique su ubicación.

```
RMAN> select file#||' '||name from v$tempfile;
FILE#||''||NAME
--------------------------------------------------------------------------------
--------
1 +DATA/TOAST/TEMPFILE/temp.263.897683145
```

4. Reubicar los archivos de datos temporales mediante un comando de RMAN que define el nuevo nombre para cada archivo de datos. Con Oracle Managed Files (OMF), el nombre completo no es necesario; el grupo de discos de ASM es suficiente. Cuando se abre la base de datos, OMF se enlaza a la ubicación adecuada en el grupo de discos de ASM. Para reubicar archivos, ejecute los siguientes comandos:

```
run {
set newname for tempfile 1 to '+NEWDATA';
switch tempfile all;
}
```

```
RMAN> run {
2> set newname for tempfile 1 to '+NEWDATA';
3> switch tempfile all;
4> }
executing command: SET NEWNAME
renamed tempfile 1 to +NEWDATA in control file
```

Migración de redo log

El proceso de migración está casi completo, pero los redo logs siguen estando en el grupo de discos de ASM original. Los redo logs no se pueden reubicar directamente. En su lugar, se crea un nuevo juego de redo logs y se agrega a la configuración, seguido de un borrado de los antiguos logs.

1. Identifique el Núm. De grupos de redo logs y sus respectivos Núm.s de grupo.

```
RMAN> select group#||' '||member from v$logfile;
GROUP#||''||MEMBER
--------------------------------------------------------------------------------
--------
1 +DATA/TOAST/ONLINELOG/group_1.261.897683139
2 +DATA/TOAST/ONLINELOG/group_2.259.897683139
3 +DATA/TOAST/ONLINELOG/group_3.256.897683139
```

2. Introduzca el tamaño de los redo logs.

```
RMAN> select group#||' '||bytes from v$log;
GROUP#||''||BYTES
--------------------------------------------------------------------------------
--------
1 52428800
2 52428800
3 52428800
```

3. Para cada redo log, cree un nuevo grupo con una configuración coincidente. Si no utiliza OMF, debe especificar la ruta completa. Este es también un ejemplo que utiliza `db_create_online_log` parámetros. Como se mostró anteriormente, este parámetro se estableció en +NEWLOGS. Esta configuración permite utilizar los siguientes comandos para crear nuevos logs en línea sin necesidad de especificar una ubicación de archivo o incluso un grupo de discos de ASM específico.

```
RMAN> alter database add logfile size 52428800;
Statement processed
RMAN> alter database add logfile size 52428800;
Statement processed
RMAN> alter database add logfile size 52428800;
Statement processed
```

4. Abra la base de datos.

```
SQL> alter database open;
Database altered.
```

5. Borre los registros antiguos.

```
RMAN> alter database drop logfile group 1;
Statement processed
```

6. Si encuentra un error que le impide borrar un log activo, fuerce un cambio al siguiente log para liberar el

bloqueo y forzar un punto de control global. A continuación se muestra un ejemplo. Se ha denegado el intento de borrar el grupo de archivos de registro 3, que se encontraba en la ubicación anterior, porque todavía había datos activos en este archivo de registro. Un archivo de registro después de un punto de control le permite suprimir el archivo de registro.

```
RMAN> alter database drop logfile group 3;
RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
RMAN-03002: failure of sql statement command at 12/08/2015 20:23:51
ORA-01623: log 3 is current log for instance TOAST (thread 4) - cannot
drop
ORA-00312: online log 3 thread 1:
'+LOGS/TOAST/ONLINELOG/group_3.259.897563549'
RMAN> alter system switch logfile;
Statement processed
RMAN> alter system checkpoint;
Statement processed
RMAN> alter database drop logfile group 3;
Statement processed
```

7. Revise el entorno para asegurarse de que todos los parámetros basados en la ubicación estén actualizados.

```
SQL> select name from v$datafile;
SQL> select member from v$logfile;
SQL> select name from v$tempfile;
SQL> show parameter spfile;
SQL> select name, value from v$parameter where value is not null;
```

8. El siguiente script muestra cómo simplificar este proceso:

```
[root@host1 current]# ./checkdbdata.pl TOAST
TOAST datafiles:
+NEWDATA/TOAST/DATAFILE/system.259.897759609
+NEWDATA/TOAST/DATAFILE/sysaux.263.897759615
+NEWDATA/TOAST/DATAFILE/undotbs1.264.897759619
+NEWDATA/TOAST/DATAFILE/users.258.897759623
TOAST redo logs:
+NEWLOGS/TOAST/ONLINELOG/group_4.266.897763123
+NEWLOGS/TOAST/ONLINELOG/group_5.265.897763125
+NEWLOGS/TOAST/ONLINELOG/group_6.264.897763125
TOAST temp datafiles:
+NEWDATA/TOAST/TEMPFILE/temp.260.897763165
TOAST spfile
spfile                                string
+NEWDATA/spfiletoast.ora
TOAST key parameters
control_files +NEWLOGS/TOAST/CONTROLFILE/current.273.897761061
log_archive_dest_1 LOCATION=+NEWLOGS
db_create_file_dest +NEWDATA
db_create_online_log_dest_1 +NEWLOGS
```

9. Si los grupos de discos de ASM se evacuaron por completo, ahora se pueden desmontar con `asmcmd`. Sin embargo, en muchos casos, los archivos que pertenecen a otras bases de datos o al archivo spfile/passwd de ASM pueden estar presentes.

```
-bash-4.1$ . oraenv
ORACLE_SID = [TOAST] ? +ASM
The Oracle base remains unchanged with value /orabin
-bash-4.1$ asmcmd
ASMCMD> umount DATA
ASMCMD>
```

Oracle ASM a la copia del sistema de archivos

El procedimiento de copia del sistema de archivos de Oracle ASM a es muy similar al procedimiento de copia de ASM a ASM, con ventajas y restricciones similares. La diferencia principal es la sintaxis de los distintos comandos y parámetros de configuración cuando se utiliza un sistema de archivos visible en lugar de un grupo de discos de ASM.

Copiar base de datos

Oracle RMAN se utiliza para crear una copia de nivel 0 (completa) de la base de datos de origen ubicada actualmente en el grupo de discos de ASM `+DATA` a la nueva ubicación en `/oradata`.

```
RMAN> backup as copy incremental level 0 database format
'/oradata/TOAST/%U' tag 'ONTAP_MIGRATION';
Starting backup at 13-MAY-16
using target database control file instead of recovery catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=377 device type=DISK
channel ORA_DISK_1: starting datafile copy
input datafile file number=00001 name=+ASM0/TOAST/system01.dbf
output file name=/oradata/TOAST/data_D-TOAST_I-2098173325_TS-SYSTEM_FNO-
1_01r5fhjg tag=ONTAP_MIGRATION RECID=1 STAMP=911722099
channel ORA_DISK_1: datafile copy complete, elapsed time: 00:00:07
channel ORA_DISK_1: starting datafile copy
input datafile file number=00002 name=+ASM0/TOAST/sysaux01.dbf
output file name=/oradata/TOAST/data_D-TOAST_I-2098173325_TS-SYSAUX_FNO-
2_02r5fhjo tag=ONTAP_MIGRATION RECID=2 STAMP=911722106
channel ORA_DISK_1: datafile copy complete, elapsed time: 00:00:07
channel ORA_DISK_1: starting datafile copy
input datafile file number=00003 name=+ASM0/TOAST/undotbs101.dbf
output file name=/oradata/TOAST/data_D-TOAST_I-2098173325_TS-UNDOTBS1_FNO-
3_03r5fhjt tag=ONTAP_MIGRATION RECID=3 STAMP=911722113
channel ORA_DISK_1: datafile copy complete, elapsed time: 00:00:07
channel ORA_DISK_1: starting datafile copy
copying current control file
output file name=/oradata/TOAST/cf_D-TOAST_id-2098173325_04r5fhk5
tag=ONTAP_MIGRATION RECID=4 STAMP=911722118
channel ORA_DISK_1: datafile copy complete, elapsed time: 00:00:01
channel ORA_DISK_1: starting datafile copy
input datafile file number=00004 name=+ASM0/TOAST/users01.dbf
output file name=/oradata/TOAST/data_D-TOAST_I-2098173325_TS-USERS_FNO-
4_05r5fhk6 tag=ONTAP_MIGRATION RECID=5 STAMP=911722118
channel ORA_DISK_1: datafile copy complete, elapsed time: 00:00:01
channel ORA_DISK_1: starting incremental level 0 datafile backup set
channel ORA_DISK_1: specifying datafile(s) in backup set
including current SPFILE in backup set
channel ORA_DISK_1: starting piece 1 at 13-MAY-16
channel ORA_DISK_1: finished piece 1 at 13-MAY-16
piece handle=/oradata/TOAST/06r5fhk7_1_1 tag=ONTAP_MIGRATION comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:01
Finished backup at 13-MAY-16
```

Forzar el cambio de archive log

Es necesario forzar el cambio de archive log para asegurarse de que los archive logs contienen todos los datos necesarios para que la copia sea totalmente coherente. Sin este comando, es posible que los datos clave sigan presentes en los redo logs. Para forzar un cambio de archive log, ejecute el siguiente comando:

```
RMAN> sql 'alter system archive log current';
sql statement: alter system archive log current
```

Cierre la base de datos de origen

La interrupción comienza en este paso porque la base de datos se cierra y se coloca en un modo de solo lectura de acceso limitado. Para cerrar la base de datos de origen, ejecute los siguientes comandos:

```
RMAN> shutdown immediate;
using target database control file instead of recovery catalog
database closed
database dismounted
Oracle instance shut down
RMAN> startup mount;
connected to target database (not started)
Oracle instance started
database mounted
Total System Global Area     805306368 bytes
Fixed Size                     2929552 bytes
Variable Size                331353200 bytes
Database Buffers             465567744 bytes
Redo Buffers                   5455872 bytes
```

Backup de CONTROLFILE

Realice una copia de seguridad de controlfiles en caso de que deba cancelar la migración y volver a la ubicación de almacenamiento original. Una copia del archivo de control de copia de seguridad no es 100% necesaria, pero hace que el proceso de restablecer las ubicaciones de los archivos de base de datos a la ubicación original sea más fácil.

```
RMAN> backup as copy current controlfile format '/tmp/TOAST.ctrl';
Starting backup at 08-DEC-15
using channel ORA_DISK_1
channel ORA_DISK_1: starting datafile copy
copying current control file
output file name=/tmp/TOAST.ctrl tag=TAG20151208T194540 RECID=30
STAMP=897939940
channel ORA_DISK_1: datafile copy complete, elapsed time: 00:00:01
Finished backup at 08-DEC-15
```

Actualizaciones de parámetros

```
RMAN> create pfile='/tmp/pfile' from spfile;
Statement processed
```

Actualizar archivo pfile

Todos los parámetros que hagan referencia a grupos de discos de ASM antiguos deben actualizarse y, en algunos casos, suprimirse cuando ya no sean relevantes. Actualícelos para reflejar las nuevas rutas del sistema de archivos y guardar el archivo pfile actualizado. Asegúrese de que se muestra la ruta de destino completa. Para actualizar estos parámetros, ejecute los siguientes comandos:

```
*.audit_file_dest='/orabin/admin/TOAST/adump'
*.audit_trail='db'
*.compatible='12.1.0.2.0'
*.control_files='/logs/TOAST/arch/control01.ctl','/logs/TOAST/redo/control
02.ctl'
*.db_block_size=8192
*.db_domain=''
*.db_name='TOAST'
*.diagnostic_dest='/orabin'
*.dispatchers='(PROTOCOL=TCP) (SERVICE=TOASTXDB)'
*.log_archive_dest_1='LOCATION=/logs/TOAST/arch'
*.log_archive_format='%t_%s_%r.dbf'
*.open_cursors=300
*.pga_aggregate_target=256m
*.processes=300
*.remote_login_passwordfile='EXCLUSIVE'
*.sga_target=768m
*.undo_tablespace='UNDOTBS1'
```

Desactive el archivo init.ora original

Este archivo se encuentra en la `$ORACLE_HOME/dbs` Directory AND se encuentra normalmente en un archivo pfile que sirve como puntero al spfile en el grupo de discos de ASM. Para asegurarse de que el spfile original ya no se utiliza, cámbiele el nombre. Sin embargo, no lo elimine porque este archivo es necesario si se debe cancelar la migración.

```
[oracle@jfsc1 ~]$ cd $ORACLE_HOME/dbs
[oracle@jfsc1 dbs]$ cat initTOAST.ora
SPFILE='+ASM0/TOAST/spfileTOAST.ora'
[oracle@jfsc1 dbs]$ mv initTOAST.ora initTOAST.ora.prev
[oracle@jfsc1 dbs]$
```

Recreación del archivo de parámetros

Este es el último paso en la reubicación de spfile. El spfile original ya no se utiliza y la base de datos se inicia actualmente (pero no se monta) mediante el archivo intermedio. El contenido de este archivo se puede escribir en la nueva ubicación spfile de la siguiente manera:

```
RMAN> create spfile from pfile='/tmp/pfile';
Statement processed
```

Inicie la base de datos para empezar a utilizar el nuevo spfile

Debe iniciar la base de datos para liberar los bloqueos en el archivo intermedio e iniciar la base de datos utilizando sólo el nuevo archivo spfile. El inicio de la base de datos también demuestra que la nueva ubicación spfile es correcta y que sus datos son válidos.

```
RMAN> shutdown immediate;
Oracle instance shut down
RMAN> startup nomount;
connected to target database (not started)
Oracle instance started
Total System Global Area     805306368 bytes
Fixed Size                     2929552 bytes
Variable Size                331353200 bytes
Database Buffers             465567744 bytes
Redo Buffers                   5455872 bytes
```

Restaure el archivo de control

Se creó un archivo de control de copia de seguridad en la ruta `/tmp/TOAST.ctrl` anteriormente en el procedimiento. El nuevo spfile define las ubicaciones del archivo de control como `/logfs/TOAST/ctrl/ctrlfile1.ctrl` y.. `/logfs/TOAST/redo/ctrlfile2.ctrl`. Sin embargo, esos archivos aún no existen.

1. Este comando restaura los datos del archivo de control a las rutas definidas en spfile.

   ```
   RMAN> restore controlfile from '/tmp/TOAST.ctrl';
   Starting restore at 13-MAY-16
   using channel ORA_DISK_1
   channel ORA_DISK_1: copied control file copy
   output file name=/logs/TOAST/arch/control01.ctl
   output file name=/logs/TOAST/redo/control02.ctl
   Finished restore at 13-MAY-16
   ```

2. Emita el comando mount para que los archivos de control se detecten correctamente y contengan datos válidos.

```
RMAN> alter database mount;
Statement processed
released channel: ORA_DISK_1
```

Para validar el `control_files` parámetro, ejecute el siguiente comando:

```
SQL> show parameter control_files;
NAME                                 TYPE        VALUE
------------------------------------ -----------
------------------------------
control_files                        string
/logs/TOAST/arch/control01.ctl
                                                 ,
/logs/TOAST/redo/control02.c
                                                 tl
```

Reproducción de registro

La base de datos está utilizando actualmente los archivos de datos en la ubicación antigua. Para poder utilizar la copia, es necesario sincronizar los archivos de datos. El tiempo transcurrido durante el proceso de copia inicial y los cambios se registraron principalmente en los registros de archivos. Estos cambios se replican en los dos pasos siguientes.

1. Realice una copia de seguridad incremental de RMAN, que contiene los archive logs.

```
RMAN>  backup incremental level 1 format '/logs/TOAST/arch/%U' for
recover of copy with tag 'ONTAP_MIGRATION' database;
Starting backup at 13-MAY-16
using target database control file instead of recovery catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=124 device type=DISK
channel ORA_DISK_1: starting incremental level 1 datafile backup set
channel ORA_DISK_1: specifying datafile(s) in backup set
input datafile file number=00001 name=+ASM0/TOAST/system01.dbf
input datafile file number=00002 name=+ASM0/TOAST/sysaux01.dbf
input datafile file number=00003 name=+ASM0/TOAST/undotbs101.dbf
input datafile file number=00004 name=+ASM0/TOAST/users01.dbf
channel ORA_DISK_1: starting piece 1 at 13-MAY-16
channel ORA_DISK_1: finished piece 1 at 13-MAY-16
piece handle=/logs/TOAST/arch/09r5fj8i_1_1 tag=ONTAP_MIGRATION
comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:01
Finished backup at 13-MAY-16
RMAN-06497: WARNING: control file is not current, control file
AUTOBACKUP skipped
```

2. Vuelva a reproducir los registros.

```
RMAN> recover copy of database with tag 'ONTAP_MIGRATION';
Starting recover at 13-MAY-16
using channel ORA_DISK_1
channel ORA_DISK_1: starting incremental datafile backup set restore
channel ORA_DISK_1: specifying datafile copies to recover
recovering datafile copy file number=00001 name=/oradata/TOAST/data_D-
TOAST_I-2098173325_TS-SYSTEM_FNO-1_01r5fhjg
recovering datafile copy file number=00002 name=/oradata/TOAST/data_D-
TOAST_I-2098173325_TS-SYSAUX_FNO-2_02r5fhjo
recovering datafile copy file number=00003 name=/oradata/TOAST/data_D-
TOAST_I-2098173325_TS-UNDOTBS1_FNO-3_03r5fhjt
recovering datafile copy file number=00004 name=/oradata/TOAST/data_D-
TOAST_I-2098173325_TS-USERS_FNO-4_05r5fhk6
channel ORA_DISK_1: reading from backup piece
/logs/TOAST/arch/09r5fj8i_1_1
channel ORA_DISK_1: piece handle=/logs/TOAST/arch/09r5fj8i_1_1
tag=ONTAP_MIGRATION
channel ORA_DISK_1: restored backup piece 1
channel ORA_DISK_1: restore complete, elapsed time: 00:00:01
Finished recover at 13-MAY-16
RMAN-06497: WARNING: control file is not current, control file
AUTOBACKUP skipped
```

Activación

El archivo de control que se restauró sigue haciendo referencia a los archivos de datos en la ubicación original y también contiene la información de ruta de acceso para los archivos de datos copiados.

1. Para cambiar los archivos de datos activos, ejecute el `switch database to copy` comando:

```
RMAN> switch database to copy;
datafile 1 switched to datafile copy "/oradata/TOAST/data_D-TOAST_I-
2098173325_TS-SYSTEM_FNO-1_01r5fhjg"
datafile 2 switched to datafile copy "/oradata/TOAST/data_D-TOAST_I-
2098173325_TS-SYSAUX_FNO-2_02r5fhjo"
datafile 3 switched to datafile copy "/oradata/TOAST/data_D-TOAST_I-
2098173325_TS-UNDOTBS1_FNO-3_03r5fhjt"
datafile 4 switched to datafile copy "/oradata/TOAST/data_D-TOAST_I-
2098173325_TS-USERS_FNO-4_05r5fhk6"
```

2. Aunque los archivos de datos deben ser totalmente coherentes, se necesita un paso final para reproducir los cambios restantes registrados en los redo logs en línea. Utilice la `recover database` comando para reproducir estos cambios y hacer que la copia sea 100% idéntica a la original. Sin embargo, la copia aún no está abierta.

```
RMAN> recover database;
Starting recover at 13-MAY-16
using channel ORA_DISK_1
starting media recovery
archived log for thread 1 with sequence 28 is already on disk as file
+ASM0/TOAST/redo01.log
archived log file name=+ASM0/TOAST/redo01.log thread=1 sequence=28
media recovery complete, elapsed time: 00:00:00
Finished recover at 13-MAY-16
```

Reubicar archivos de datos temporales

1. Identifique la ubicación de los archivos de datos temporales que aún se están utilizando en el grupo de discos original.

```
RMAN> select file#||' '||name from v$tempfile;
FILE#||''||NAME
-------------------------------------------------------------------------
--------
1 +ASM0/TOAST/temp01.dbf
```

2. Para reubicar los archivos de datos, ejecute los siguientes comandos. Si hay muchos archivos temporales, utilice un editor de texto para crear el comando RMAN y, a continuación, córtelo y péguelo.

```
RMAN> run {
2> set newname for tempfile 1 to '/oradata/TOAST/temp01.dbf';
3> switch tempfile all;
4> }
executing command: SET NEWNAME
renamed tempfile 1 to /oradata/TOAST/temp01.dbf in control file
```

Migración de redo log

El proceso de migración está casi completo, pero los redo logs siguen estando en el grupo de discos de ASM original. Los redo logs no se pueden reubicar directamente. En su lugar, se crea un nuevo juego de redo logs y se agrega a la configuración, luego se borran los logs antiguos.

1. Identifique el Núm. De grupos de redo logs y sus respectivos Núm.s de grupo.

```
RMAN> select group#||' '||member from v$logfile;
GROUP#||''||MEMBER
--------------------------------------------------------------------------------
--------
1 +ASM0/TOAST/redo01.log
2 +ASM0/TOAST/redo02.log
3 +ASM0/TOAST/redo03.log
```

2. Introduzca el tamaño de los redo logs.

```
RMAN> select group#||' '||bytes from v$log;
GROUP#||''||BYTES
--------------------------------------------------------------------------------
--------
1 52428800
2 52428800
3 52428800
```

3. Para cada redo log, cree un nuevo grupo utilizando el mismo tamaño que el grupo de redo logs actual mediante la nueva ubicación del sistema de archivos.

```
RMAN> alter database add logfile '/logs/TOAST/redo/log00.rdo' size
52428800;
Statement processed
RMAN> alter database add logfile '/logs/TOAST/redo/log01.rdo' size
52428800;
Statement processed
RMAN> alter database add logfile '/logs/TOAST/redo/log02.rdo' size
52428800;
Statement processed
```

4. Elimine los grupos de archivos de registro antiguos que aún se encuentran en el almacenamiento anterior.

```
RMAN> alter database drop logfile group 4;
Statement processed
RMAN> alter database drop logfile group 5;
Statement processed
RMAN> alter database drop logfile group 6;
Statement processed
```

5. Si se detecta un error que bloquea el borrado de un log activo, fuerce un cambio al siguiente log para liberar el bloqueo y forzar un punto de control global. A continuación se muestra un ejemplo. Se ha denegado el intento de borrar el grupo de archivos de registro 3, que se encontraba en la ubicación

anterior, porque todavía había datos activos en este archivo de registro. Un archivo log seguido de un punto de control permite la supresión de archivos log.

```
RMAN> alter database drop logfile group 4;
RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
RMAN-03002: failure of sql statement command at 12/08/2015 20:23:51
ORA-01623: log 4 is current log for instance TOAST (thread 4) - cannot
drop
ORA-00312: online log 4 thread 1:
'+NEWLOGS/TOAST/ONLINELOG/group_4.266.897763123'
RMAN> alter system switch logfile;
Statement processed
RMAN> alter system checkpoint;
Statement processed
RMAN> alter database drop logfile group 4;
Statement processed
```

6. Revise el entorno para asegurarse de que todos los parámetros basados en la ubicación estén actualizados.

```
SQL> select name from v$datafile;
SQL> select member from v$logfile;
SQL> select name from v$tempfile;
SQL> show parameter spfile;
SQL> select name, value from v$parameter where value is not null;
```

7. El siguiente script muestra cómo facilitar este proceso.

```
[root@jfsc1 current]# ./checkdbdata.pl TOAST
TOAST datafiles:
/oradata/TOAST/data_D-TOAST_I-2098173325_TS-SYSTEM_FNO-1_01r5fhjg
/oradata/TOAST/data_D-TOAST_I-2098173325_TS-SYSAUX_FNO-2_02r5fhjo
/oradata/TOAST/data_D-TOAST_I-2098173325_TS-UNDOTBS1_FNO-3_03r5fhjt
/oradata/TOAST/data_D-TOAST_I-2098173325_TS-USERS_FNO-4_05r5fhk6
TOAST redo logs:
/logs/TOAST/redo/log00.rdo
/logs/TOAST/redo/log01.rdo
/logs/TOAST/redo/log02.rdo
TOAST temp datafiles:
/oradata/TOAST/temp01.dbf
TOAST spfile
spfile                                string
/orabin/product/12.1.0/dbhome_
                                                    1/dbs/spfileTOAST.ora
TOAST key parameters
control_files /logs/TOAST/arch/control01.ctl,
/logs/TOAST/redo/control02.ctl
log_archive_dest_1 LOCATION=/logs/TOAST/arch
```

8. Si los grupos de discos de ASM se evacuaron por completo, ahora se pueden desmontar con `asmcmd`. En muchos casos, los archivos que pertenecen a otras bases de datos o al archivo spfile/passwd de ASM pueden seguir presentes.

```
-bash-4.1$ . oraenv
ORACLE_SID = [TOAST] ? +ASM
The Oracle base remains unchanged with value /orabin
-bash-4.1$ asmcmd
ASMCMD> umount DATA
ASMCMD>
```

Procedimiento de limpieza del archivo de datos

El proceso de migración puede dar lugar a archivos de datos con sintaxis larga o críptica, según cómo se haya utilizado Oracle RMAN. En el ejemplo que se muestra aquí, la copia de seguridad se realizó con el formato de archivo de `/oradata/TOAST/%U`. `%U` Indica que RMAN debe crear un nombre único por defecto para cada archivo de datos. El resultado es similar al que se muestra en el siguiente texto. Los nombres tradicionales de los archivos de datos están incrustados en los nombres. Esto se puede limpiar utilizando el enfoque con guión que se muestra en la "Limpieza de Migración de ASM".

```
[root@jfsc1 current]# ./fixuniquenames.pl TOAST
#sqlplus Commands
shutdown immediate;
startup mount;
host mv /oradata/TOAST/data_D-TOAST_I-2098173325_TS-SYSTEM_FNO-1_01r5fhjg
/oradata/TOAST/system.dbf
host mv /oradata/TOAST/data_D-TOAST_I-2098173325_TS-SYSAUX_FNO-2_02r5fhjo
/oradata/TOAST/sysaux.dbf
host mv /oradata/TOAST/data_D-TOAST_I-2098173325_TS-UNDOTBS1_FNO-
3_03r5fhjt /oradata/TOAST/undotbs1.dbf
host mv /oradata/TOAST/data_D-TOAST_I-2098173325_TS-USERS_FNO-4_05r5fhk6
/oradata/TOAST/users.dbf
alter database rename file '/oradata/TOAST/data_D-TOAST_I-2098173325_TS-
SYSTEM_FNO-1_01r5fhjg' to '/oradata/TOAST/system.dbf';
alter database rename file '/oradata/TOAST/data_D-TOAST_I-2098173325_TS-
SYSAUX_FNO-2_02r5fhjo' to '/oradata/TOAST/sysaux.dbf';
alter database rename file '/oradata/TOAST/data_D-TOAST_I-2098173325_TS-
UNDOTBS1_FNO-3_03r5fhjt' to '/oradata/TOAST/undotbs1.dbf';
alter database rename file '/oradata/TOAST/data_D-TOAST_I-2098173325_TS-
USERS_FNO-4_05r5fhk6' to '/oradata/TOAST/users.dbf';
alter database open;
```

Reequilibrio de Oracle ASM

Como se ha explicado anteriormente, un grupo de discos de Oracle ASM se puede migrar de forma transparente a un nuevo sistema de almacenamiento mediante el proceso de reequilibrio. En resumen, el proceso de reequilibrio requiere la adición de LUN de igual tamaño al grupo existente de LUN seguido de una operación de eliminación del LUN anterior. Oracle ASM reubica automáticamente los datos subyacentes en un nuevo almacenamiento en un diseño óptimo y, al finalizar, libera las LUN antiguas.

El proceso de migración utiliza I/O secuencial eficiente y no suele provocar interrupciones en el rendimiento, pero la tasa de migración puede acelerarse cuando es necesario.

Identifique los datos que se van a migrar

```
SQL> select name||' '||group_number||' '||total_mb||' '||path||'
'||header_status from v$asm_disk;
NEWDATA_0003 1 10240 /dev/mapper/3600a090038303537762b47594c315864 MEMBER
NEWDATA_0002 1 10240 /dev/mapper/3600a090038303537762b47594c315863 MEMBER
NEWDATA_0000 1 10240 /dev/mapper/3600a090038303537762b47594c315861 MEMBER
NEWDATA_0001 1 10240 /dev/mapper/3600a090038303537762b47594c315862 MEMBER
SQL> select group_number||' '||name from v$asm_diskgroup;
1 NEWDATA
```

Cree nuevas LUN

Cree nuevas LUN del mismo tamaño y establezca la pertenencia de usuarios y grupos como sea necesario. Las LUN deben aparecer como `CANDIDATE` discos.

```
SQL> select name||' '||group_number||' '||total_mb||' '||path||'
'||header_status from v$asm_disk;
 0 0 /dev/mapper/3600a098038303537762b47594c31586b CANDIDATE
 0 0 /dev/mapper/3600a098038303537762b47594c315869 CANDIDATE
 0 0 /dev/mapper/3600a098038303537762b47594c315858 CANDIDATE
 0 0 /dev/mapper/3600a098038303537762b47594c31586a CANDIDATE
NEWDATA_0003 1 10240 /dev/mapper/3600a098038303537762b47594c315864 MEMBER
NEWDATA_0002 1 10240 /dev/mapper/3600a098038303537762b47594c315863 MEMBER
NEWDATA_0000 1 10240 /dev/mapper/3600a098038303537762b47594c315861 MEMBER
NEWDATA_0001 1 10240 /dev/mapper/3600a098038303537762b47594c315862 MEMBER
```

Agregar NUEVAS LUN

Aunque las operaciones de agregar y soltar se pueden realizar de forma conjunta, generalmente es más sencillo añadir nuevas LUN en dos pasos. En primer lugar, agregue las nuevas LUN al grupo de discos. Este paso hace que la mitad de las extensiones se migren de las LUN de ASM actuales a las nuevas LUN.

La potencia de reequilibrio indica la velocidad a la que se transfieren los datos. Cuanto mayor sea el número, mayor será el paralelismo de la transferencia de datos. La migración se realiza con eficientes operaciones de I/O secuenciales que es poco probable que provoquen problemas de rendimiento. Sin embargo, si lo desea, la potencia de reequilibrio de una migración continua se puede ajustar con el `alter diskgroup [name] rebalance power [level]` comando. Las migraciones típicas utilizan un valor de 5.

```
SQL> alter diskgroup NEWDATA add disk
'/dev/mapper/3600a098038303537762b47594c31586b' rebalance power 5;
Diskgroup altered.
SQL> alter diskgroup NEWDATA add disk
'/dev/mapper/3600a098038303537762b47594c315869' rebalance power 5;
Diskgroup altered.
SQL> alter diskgroup NEWDATA add disk
'/dev/mapper/3600a098038303537762b47594c315858' rebalance power 5;
Diskgroup altered.
SQL> alter diskgroup NEWDATA add disk
'/dev/mapper/3600a098038303537762b47594c31586a' rebalance power 5;
Diskgroup altered.
```

Supervise el funcionamiento

Una operación de reequilibrio puede supervisarse y gestionarse de varias maneras. Utilizamos el siguiente comando para este ejemplo.

```
SQL> select group_number,operation,state from v$asm_operation;
GROUP_NUMBER OPERA STAT
------------ ----- ----
           1 REBAL RUN
           1 REBAL WAIT
```

Una vez finalizada la migración, no se informan las operaciones de reequilibrio.

```
SQL> select group_number,operation,state from v$asm_operation;
no rows selected
```

Borre las LUN antiguas

La migración se ha completado a mitad de camino. Podría ser deseable realizar algunas pruebas de rendimiento básicas para asegurarse de que el entorno está en buen estado. Después de la confirmación, se pueden reubicar los datos restantes eliminando las LUN antiguas. Tenga en cuenta que esto no provoca una versión inmediata de las LUN. La operación de borrado indica a Oracle ASM que reubique primero las extensiones y, a continuación, libere el LUN.

```
sqlplus / as sysasm
SQL> alter diskgroup NEWDATA drop disk NEWDATA_0000 rebalance power 5;
Diskgroup altered.
SQL> alter diskgroup NEWDATA drop disk NEWDATA_0001 rebalance power 5;
Diskgroup altered.
SQL> alter diskgroup newdata drop disk NEWDATA_0002 rebalance power 5;
Diskgroup altered.
SQL> alter diskgroup newdata drop disk NEWDATA_0003 rebalance power 5;
Diskgroup altered.
```

Supervise el funcionamiento

La operación de reequilibrio se puede supervisar y gestionar de varias maneras. Utilizamos el siguiente comando para este ejemplo:

```
SQL> select group_number,operation,state from v$asm_operation;
GROUP_NUMBER OPERA STAT
------------ ----- ----
           1 REBAL RUN
           1 REBAL WAIT
```

Una vez finalizada la migración, no se informan las operaciones de reequilibrio.

```
SQL> select group_number,operation,state from v$asm_operation;
no rows selected
```

Quite las LUN antiguas

Antes de quitar las LUN antiguas del grupo de discos, debe realizar una comprobación final del estado del encabezado. Después de liberar una LUN desde ASM, ya no aparece un nombre y el estado de la cabecera aparece como `FORMER`. Esto indica que estas LUN se pueden eliminar de forma segura del sistema.

```
SQL> select name||' '||group_number||' '||total_mb||' '||path||'
'||header_status from v$asm_disk;
NAME||''||GROUP_NUMBER||''||TOTAL_MB||''||PATH||''||HEADER_STATUS
------------------------------------------------------------------------
------
 0 0 /dev/mapper/3600a098038303537762b47594c315863 FORMER
 0 0 /dev/mapper/3600a098038303537762b47594c315864 FORMER
 0 0 /dev/mapper/3600a098038303537762b47594c315861 FORMER
 0 0 /dev/mapper/3600a098038303537762b47594c315862 FORMER
NEWDATA_0005 1 10240 /dev/mapper/3600a098038303537762b47594c315869 MEMBER
NEWDATA_0007 1 10240 /dev/mapper/3600a098038303537762b47594c31586a MEMBER
NEWDATA_0004 1 10240 /dev/mapper/3600a098038303537762b47594c31586b MEMBER
NEWDATA_0006 1 10240 /dev/mapper/3600a098038303537762b47594c315858 MEMBER
8 rows selected.
```

Migración de LVM

El procedimiento que se presenta aquí muestra los principios de una migración basada en LVM de un grupo de volúmenes llamado `datavg`. Los ejemplos se extraen del LVM de Linux, pero los principios se aplican por igual a AIX, HP-UX y VxVM. Los comandos precisos pueden variar.

1. Identifique las LUN actualmente en el `datavg` grupo de volúmenes.

```
[root@host1 ~]# pvdisplay -C | grep datavg
  /dev/mapper/3600a098038303537762b47594c31582f datavg lvm2 a--  10.00g
10.00g
  /dev/mapper/3600a098038303537762b47594c31585a datavg lvm2 a--  10.00g
10.00g
  /dev/mapper/3600a098038303537762b47594c315859 datavg lvm2 a--  10.00g
10.00g
  /dev/mapper/3600a098038303537762b47594c31586c datavg lvm2 a--  10.00g
10.00g
```

2. Cree nuevas LUN del mismo tamaño físico o ligeramente mayor y definiéndolas como volúmenes físicos.

```
[root@host1 ~]# pvcreate /dev/mapper/3600a098038303537762b47594c315864
  Physical volume "/dev/mapper/3600a098038303537762b47594c315864"
successfully created
[root@host1 ~]# pvcreate /dev/mapper/3600a098038303537762b47594c315863
  Physical volume "/dev/mapper/3600a098038303537762b47594c315863"
successfully created
[root@host1 ~]# pvcreate /dev/mapper/3600a098038303537762b47594c315862
  Physical volume "/dev/mapper/3600a098038303537762b47594c315862"
successfully created
[root@host1 ~]# pvcreate /dev/mapper/3600a098038303537762b47594c315861
  Physical volume "/dev/mapper/3600a098038303537762b47594c315861"
successfully created
```

3. Añada los volúmenes nuevos al grupo de volúmenes.

```
[root@host1 tmp]# vgextend datavg
/dev/mapper/3600a098038303537762b47594c315864
  Volume group "datavg" successfully extended
[root@host1 tmp]# vgextend datavg
/dev/mapper/3600a098038303537762b47594c315863
  Volume group "datavg" successfully extended
[root@host1 tmp]# vgextend datavg
/dev/mapper/3600a098038303537762b47594c315862
  Volume group "datavg" successfully extended
[root@host1 tmp]# vgextend datavg
/dev/mapper/3600a098038303537762b47594c315861
  Volume group "datavg" successfully extended
```

4. Emita el `pvmove` Comando para reubicar las extensiones de cada LUN actual en la nueva LUN. La `-i [seconds]` argument supervisa el progreso de la operación.

```
[root@host1 tmp]# pvmove -i 10
/dev/mapper/3600a098038303537762b47594c31582f
/dev/mapper/3600a098038303537762b47594c315864
  /dev/mapper/3600a098038303537762b47594c31582f: Moved: 0.0%
  /dev/mapper/3600a098038303537762b47594c31582f: Moved: 14.2%
  /dev/mapper/3600a098038303537762b47594c31582f: Moved: 28.4%
  /dev/mapper/3600a098038303537762b47594c31582f: Moved: 42.5%
  /dev/mapper/3600a098038303537762b47594c31582f: Moved: 57.1%
  /dev/mapper/3600a098038303537762b47594c31582f: Moved: 72.3%
  /dev/mapper/3600a098038303537762b47594c31582f: Moved: 87.3%
  /dev/mapper/3600a098038303537762b47594c31582f: Moved: 100.0%
[root@host1 tmp]# pvmove -i 10
/dev/mapper/3600a098038303537762b47594c31585a
/dev/mapper/3600a098038303537762b47594c315863
  /dev/mapper/3600a098038303537762b47594c31585a: Moved: 0.0%
  /dev/mapper/3600a098038303537762b47594c31585a: Moved: 14.9%
  /dev/mapper/3600a098038303537762b47594c31585a: Moved: 29.9%
  /dev/mapper/3600a098038303537762b47594c31585a: Moved: 44.8%
  /dev/mapper/3600a098038303537762b47594c31585a: Moved: 60.1%
  /dev/mapper/3600a098038303537762b47594c31585a: Moved: 75.8%
  /dev/mapper/3600a098038303537762b47594c31585a: Moved: 90.9%
  /dev/mapper/3600a098038303537762b47594c31585a: Moved: 100.0%
[root@host1 tmp]# pvmove -i 10
/dev/mapper/3600a098038303537762b47594c315859
/dev/mapper/3600a098038303537762b47594c315862
  /dev/mapper/3600a098038303537762b47594c315859: Moved: 0.0%
  /dev/mapper/3600a098038303537762b47594c315859: Moved: 14.8%
  /dev/mapper/3600a098038303537762b47594c315859: Moved: 29.8%
  /dev/mapper/3600a098038303537762b47594c315859: Moved: 45.5%
  /dev/mapper/3600a098038303537762b47594c315859: Moved: 61.1%
  /dev/mapper/3600a098038303537762b47594c315859: Moved: 76.6%
  /dev/mapper/3600a098038303537762b47594c315859: Moved: 91.7%
  /dev/mapper/3600a098038303537762b47594c315859: Moved: 100.0%
[root@host1 tmp]# pvmove -i 10
/dev/mapper/3600a098038303537762b47594c31586c
/dev/mapper/3600a098038303537762b47594c315861
  /dev/mapper/3600a098038303537762b47594c31586c: Moved: 0.0%
  /dev/mapper/3600a098038303537762b47594c31586c: Moved: 15.0%
  /dev/mapper/3600a098038303537762b47594c31586c: Moved: 30.4%
  /dev/mapper/3600a098038303537762b47594c31586c: Moved: 46.0%
  /dev/mapper/3600a098038303537762b47594c31586c: Moved: 61.4%
  /dev/mapper/3600a098038303537762b47594c31586c: Moved: 77.2%
  /dev/mapper/3600a098038303537762b47594c31586c: Moved: 92.3%
  /dev/mapper/3600a098038303537762b47594c31586c: Moved: 100.0%
```

5. Cuando finalice este proceso, borre las LUN antiguas del grupo de volúmenes mediante el `vgreduce` comando. Si es correcto, la LUN ahora se puede quitar de forma segura del sistema.

```
[root@host1 tmp]# vgreduce datavg
/dev/mapper/3600a098038303537762b47594c31582f
Removed "/dev/mapper/3600a098038303537762b47594c31582f" from volume
group "datavg"
[root@host1 tmp]# vgreduce datavg
/dev/mapper/3600a098038303537762b47594c31585a
  Removed "/dev/mapper/3600a098038303537762b47594c31585a" from volume
group "datavg"
[root@host1 tmp]# vgreduce datavg
/dev/mapper/3600a098038303537762b47594c315859
  Removed "/dev/mapper/3600a098038303537762b47594c315859" from volume
group "datavg"
[root@host1 tmp]# vgreduce datavg
/dev/mapper/3600a098038303537762b47594c31586c
  Removed "/dev/mapper/3600a098038303537762b47594c31586c" from volume
group "datavg"
```

Importación LUN externo

Planificación

Los procedimientos para migrar recursos SAN mediante FLI se documentan en NetApp "Documentación de importación de LUN externa de ONTAP" .

Desde un punto de vista de base de datos y host, no se requieren pasos especiales. Después de actualizar las zonas de FC y de que los LUN estén disponibles en ONTAP, LVM debería poder leer los metadatos de LVM de los LUN. Además, los grupos de volúmenes están listos para usarse sin más pasos de configuración. En raras ocasiones, los entornos pueden incluir archivos de configuración que se codificaron de forma fija con referencias a la cabina de almacenamiento anterior. Por ejemplo, un sistema Linux que incluyó `/etc/multipath.conf` Las reglas que hacen referencia a un WWN de un dispositivo determinado se deben actualizar para reflejar los cambios introducidos por FLI.

> Consulte la Matriz de compatibilidad de NetApp para obtener información sobre las configuraciones admitidas. Si su entorno no está incluido, póngase en contacto con su representante de NetApp para obtener ayuda.

Este ejemplo muestra la migración de LUN de ASM y LVM alojadas en un servidor Linux. FLI es compatible con otros sistemas operativos y, aunque los comandos del lado del host pueden ser diferentes, los principios son los mismos y los procedimientos de ONTAP son idénticos.

Identifique las LUN de LVM

El primer paso de preparación es identificar las LUN que se van a migrar. En el ejemplo que se muestra aquí, hay dos sistemas de archivos basados en SAN montados en `/orabin` y.. `/backups`.

```
[root@host1 ~]# df -k
Filesystem                          1K-blocks      Used Available Use%
Mounted on
/dev/mapper/rhel-root                52403200   8811464  43591736  17% /
devtmpfs                             65882776         0  65882776   0% /dev
...
fas8060-nfs-public:/install         199229440 119368128  79861312  60%
/install
/dev/mapper/sanvg-lvorabin           20961280  12348476   8612804  59%
/orabin
/dev/mapper/sanvg-lvbackups          73364480  62947536  10416944  86%
/backups
```

El nombre del grupo de volúmenes se puede extraer del nombre del dispositivo, que utiliza el formato (nombre del grupo de volúmenes)-(nombre del volumen lógico). En este caso, se denomina al grupo de volúmenes `sanvg`.

La `pvdisplay` El comando se puede utilizar de la siguiente manera para identificar las LUN que admiten este grupo de volúmenes. En este caso, hay 10 LUN que componen el `sanvg` grupo de volúmenes.

```
[root@host1 ~]# pvdisplay -C -o pv_name,pv_size,pv_fmt,vg_name
  PV                                                    PSize   VG
  /dev/mapper/3600a0980383030445424487556574266  10.00g sanvg
  /dev/mapper/3600a0980383030445424487556574267  10.00g sanvg
  /dev/mapper/3600a0980383030445424487556574268  10.00g sanvg
  /dev/mapper/3600a0980383030445424487556574269  10.00g sanvg
  /dev/mapper/3600a098038303044542448755657426a  10.00g sanvg
  /dev/mapper/3600a098038303044542448755657426b  10.00g sanvg
  /dev/mapper/3600a098038303044542448755657426c  10.00g sanvg
  /dev/mapper/3600a098038303044542448755657426d  10.00g sanvg
  /dev/mapper/3600a098038303044542448755657426e  10.00g sanvg
  /dev/mapper/3600a098038303044542448755657426f  10.00g sanvg
  /dev/sda2                                             278.38g rhel
```

Identificar LUN de ASM

Las LUN de ASM también se deben migrar. Para obtener el número de rutas de LUN y LUN desde sqlplus como usuario sysasm, ejecute el siguiente comando:

```
SQL> select path||' '||os_mb from v$asm_disk;
PATH||''||OS_MB
--------------------------------------------------------------------------------
------
/dev/oracleasm/disks/ASM0 10240
/dev/oracleasm/disks/ASM9 10240
/dev/oracleasm/disks/ASM8 10240
/dev/oracleasm/disks/ASM7 10240
/dev/oracleasm/disks/ASM6 10240
/dev/oracleasm/disks/ASM5 10240
/dev/oracleasm/disks/ASM4 10240
/dev/oracleasm/disks/ASM1 10240
/dev/oracleasm/disks/ASM3 10240
/dev/oracleasm/disks/ASM2 10240
10 rows selected.
SQL>
```

Cambios de red FC

El entorno actual contiene 20 LUN que se van a migrar. Actualice la SAN actual para que ONTAP pueda acceder a los LUN actuales. Los datos aún no se han migrado, pero ONTAP debe leer la información de configuración de las LUN actuales para crear el nuevo directorio raíz de los datos.

Como mínimo, se debe configurar al menos un puerto HBA en el sistema AFF/FAS como puerto iniciador. Además, deben actualizarse las zonas de FC para que ONTAP pueda acceder a los LUN en la cabina de almacenamiento externa. Algunas cabinas de almacenamiento tienen configurado el enmascaramiento de LUN, lo que limita los nombres WWN que pueden acceder a una LUN determinada. En tales casos, el enmascaramiento de LUN también debe actualizarse para conceder acceso a los WWN de ONTAP.

Cuando se completa este paso, ONTAP debe poder ver la cabina de almacenamiento externa con el `storage array show` comando. El campo clave que devuelve es el prefijo que se utiliza para identificar la LUN externa en el sistema. En el siguiente ejemplo, las LUN de la cabina externa `FOREIGN_1` Aparece en ONTAP con el prefijo de `FOR-1`.

Identifique la cabina externa

```
Cluster01::> storage array show -fields name,prefix
name          prefix
------------- ------
FOREIGN_1     FOR-1
Cluster01::>
```

Identificar LUN externas

Las LUN se pueden enumerar pasando el `array-name` para la `storage disk show` comando. Se hace referencia a los datos devueltos varias veces durante el procedimiento de migración.

```
Cluster01::> storage disk show -array-name FOREIGN_1 -fields disk,serial
disk     serial-number
-------- -------------
FOR-1.1  800DT$HuVWBX
FOR-1.2  800DT$HuVWBZ
FOR-1.3  800DT$HuVWBW
FOR-1.4  800DT$HuVWBY
FOR-1.5  800DT$HuVWB/
FOR-1.6  800DT$HuVWBa
FOR-1.7  800DT$HuVWBd
FOR-1.8  800DT$HuVWBb
FOR-1.9  800DT$HuVWBc
FOR-1.10 800DT$HuVWBe
FOR-1.11 800DT$HuVWBf
FOR-1.12 800DT$HuVWBg
FOR-1.13 800DT$HuVWBi
FOR-1.14 800DT$HuVWBh
FOR-1.15 800DT$HuVWBj
FOR-1.16 800DT$HuVWBk
FOR-1.17 800DT$HuVWBm
FOR-1.18 800DT$HuVWBl
FOR-1.19 800DT$HuVWBo
FOR-1.20 800DT$HuVWBn
20 entries were displayed.
Cluster01::>
```

Registre LUN de cabina externa como candidatos para importar

Las LUN externas inicialmente se clasifican como cualquier tipo de LUN específico. Antes de poder importar los datos, las LUN deben etiquetarse como externas y, por lo tanto, candidatas para el proceso de importación. Este paso se completa pasando el número de serie al `storage disk modify` command, tal y como se muestra en el siguiente ejemplo. Tenga en cuenta que este proceso solo etiqueta la LUN como externa en ONTAP. No se escriben datos en la propia LUN externa.

```
Cluster01::*> storage disk modify {-serial-number 800DT$HuVWBW} -is
-foreign true
Cluster01::*> storage disk modify {-serial-number 800DT$HuVWBX} -is
-foreign true
...
Cluster01::*> storage disk modify {-serial-number 800DT$HuVWBn} -is
-foreign true
Cluster01::*> storage disk modify {-serial-number 800DT$HuVWBo} -is
-foreign true
Cluster01::*>
```

Crear volúmenes para alojar LUN migradas

Se necesita un volumen para alojar los LUN migrados. La configuración exacta de volúmenes depende del plan general para aprovechar las funciones de ONTAP. En este ejemplo, las LUN de ASM se colocan en un volumen y las LUN de LVM se colocan en un segundo volumen. Esto le permite gestionar las LUN como grupos independientes para fines como organización en niveles, creación de snapshots o configuración de controles de calidad de servicio.

Ajuste la `snapshot-policy `to `none`. El proceso de migración puede incluir un alto volumen de cambios de datos. Por lo tanto, es posible que se produzca un gran aumento en el consumo de espacio si las instantáneas se crean por accidente porque se capturan datos no deseados en las copias Snapshot.

```
Cluster01::> volume create -volume new_asm -aggregate data_02 -size 120G
-snapshot-policy none
[Job 1152] Job succeeded: Successful
Cluster01::> volume create -volume new_lvm -aggregate data_02 -size 120G
-snapshot-policy none
[Job 1153] Job succeeded: Successful
Cluster01::>
```

Crear LUN de ONTAP

Después de crear los volúmenes, es necesario crear las nuevas LUN. Normalmente, la creación de una LUN requiere que el usuario especifique dicha información como el tamaño de LUN, pero en este caso el argumento de disco externo se pasa al comando. Como resultado, ONTAP replica los datos de configuración de LUN actuales del número de serie especificado. También utiliza la geometría de la LUN y los datos de la tabla de particiones para ajustar la alineación de la LUN y establecer un rendimiento óptimo.

En este paso, se deben hacer referencias cruzadas de los números de serie a la cabina externa para asegurarse de que la LUN externa correcta coincida con la nueva LUN correcta.

```
Cluster01::*> lun create -vserver vserver1 -path /vol/new_asm/LUN0 -ostype
linux -foreign-disk 800DT$HuVWBW
Created a LUN of size 10g (10737418240)
Cluster01::*> lun create -vserver vserver1 -path /vol/new_asm/LUN1 -ostype
linux -foreign-disk 800DT$HuVWBX
Created a LUN of size 10g (10737418240)
...
Created a LUN of size 10g (10737418240)
Cluster01::*> lun create -vserver vserver1 -path /vol/new_lvm/LUN8 -ostype
linux -foreign-disk 800DT$HuVWBn
Created a LUN of size 10g (10737418240)
Cluster01::*> lun create -vserver vserver1 -path /vol/new_lvm/LUN9 -ostype
linux -foreign-disk 800DT$HuVWBo
Created a LUN of size 10g (10737418240)
```

Crear relaciones de importación

Las LUN ahora se han creado, pero no se configuran como destino de replicación. Antes de poder realizar este paso, las LUN deben colocarse primero sin conexión. Este paso adicional está diseñado para proteger los datos de los errores de los usuarios. Si ONTAP permitiera realizar una migración a una LUN online, supondría el riesgo de que un error tipográfico pudiera provocar la sobrescritura de los datos activos. El paso adicional de obligar al usuario a desconectar primero una LUN ayuda a verificar que se utiliza la LUN de destino correcta como destino de migración.

```
Cluster01::*> lun offline -vserver vserver1 -path /vol/new_asm/LUN0
Warning: This command will take LUN "/vol/new_asm/LUN0" in Vserver
         "vserver1" offline.
Do you want to continue? {y|n}: y
Cluster01::*> lun offline -vserver vserver1 -path /vol/new_asm/LUN1
Warning: This command will take LUN "/vol/new_asm/LUN1" in Vserver
         "vserver1" offline.
Do you want to continue? {y|n}: y
...
Warning: This command will take LUN "/vol/new_lvm/LUN8" in Vserver
         "vserver1" offline.
Do you want to continue? {y|n}: y
Cluster01::*> lun offline -vserver vserver1 -path /vol/new_lvm/LUN9
Warning: This command will take LUN "/vol/new_lvm/LUN9" in Vserver
         "vserver1" offline.
Do you want to continue? {y|n}: y
```

Después de que las LUN estén sin conexión, puede establecer la relación de importación pasando el número de serie de la LUN externa al `lun import create` comando.

```
Cluster01::*> lun import create -vserver vserver1 -path /vol/new_asm/LUN0
-foreign-disk 800DT$HuVWBW
Cluster01::*> lun import create -vserver vserver1 -path /vol/new_asm/LUN1
-foreign-disk 800DT$HuVWBX
...
Cluster01::*> lun import create -vserver vserver1 -path /vol/new_lvm/LUN8
-foreign-disk 800DT$HuVWBn
Cluster01::*> lun import create -vserver vserver1 -path /vol/new_lvm/LUN9
-foreign-disk 800DT$HuVWBo
Cluster01::*>
```

Una vez establecidas todas las relaciones de importación, las LUN pueden volver a colocarse en línea.

```
Cluster01::*> lun online -vserver vserver1 -path /vol/new_asm/LUN0
Cluster01::*> lun online -vserver vserver1 -path /vol/new_asm/LUN1
...
Cluster01::*> lun online -vserver vserver1 -path /vol/new_lvm/LUN8
Cluster01::*> lun online -vserver vserver1 -path /vol/new_lvm/LUN9
Cluster01::*>
```

Cree el iGroup

Un igroup forma parte de la arquitectura de enmascaramiento LUN de ONTAP. No es posible acceder a un LUN recién creado a menos que se conceda acceso en primer lugar a un host. Para ello, cree un igroup que enumere los nombres de iniciadores iSCSI o WWN de FC a los que se debe otorgar acceso. Cuando se escribió este informe, FLI solo se admitía para los LUN FC. Sin embargo, la conversión a iSCSI posterior a la migración es una tarea sencilla, como se muestra en la "Conversión de protocolos".

En este ejemplo, se crea un igroup que contiene dos WWN que corresponden a los dos puertos disponibles en el HBA del host.

```
Cluster01::*> igroup create linuxhost -protocol fcp -ostype linux
-initiator 21:00:00:0e:1e:16:63:50 21:00:00:0e:1e:16:63:51
```

Asignar nuevas LUN al host

Después de la creación del igroup, las LUN se asignan al igroup definido. Estos LUN solo están disponibles para los WWN incluidos en este igroup. NetApp asume que en esta etapa del proceso de migración no se ha zonificado el host en ONTAP. Esto es importante porque si se divide en zonas el host simultáneamente en la cabina externa y el nuevo sistema ONTAP, existe el riesgo de que LUN con el mismo número de serie se puedan detectar en cada cabina. Esta situación podría provocar fallos de funcionamiento de varias rutas o daños en los datos.

```
Cluster01::*> lun map -vserver vserver1 -path /vol/new_asm/LUN0 -igroup
linuxhost
Cluster01::*> lun map -vserver vserver1 -path /vol/new_asm/LUN1 -igroup
linuxhost
...
Cluster01::*> lun map -vserver vserver1 -path /vol/new_lvm/LUN8 -igroup
linuxhost
Cluster01::*> lun map -vserver vserver1 -path /vol/new_lvm/LUN9 -igroup
linuxhost
Cluster01::*>
```

Transición

No es posible evitar alguna interrupción durante una importación de LUN externa debido a la necesidad de cambiar la configuración de red FC. Sin embargo, la interrupción no tiene que durar mucho más del tiempo requerido para reiniciar el entorno de bases de

datos y actualizar la división en zonas de FC para cambiar la conectividad de FC de host desde el LUN externo a ONTAP.

Este proceso se puede resumir de la siguiente manera:

1. Desactive toda la actividad de LUN en las LUN externas.
2. Redirija las conexiones host FC al nuevo sistema ONTAP.
3. Active el proceso de importación.
4. Vuelva a detectar las LUN.
5. Reinicie la base de datos.

No es necesario esperar hasta que finalice el proceso de migración. Tan pronto como comience la migración de una LUN determinada, está disponible en ONTAP y puede servir datos mientras continúa el proceso de copia de datos. Todas las lecturas se pasan a través del LUN externo y todas las escrituras se escriben sincrónicamente en ambas cabinas. La operación de copia es muy rápida y la sobrecarga que conlleva redirigir el tráfico FC es mínima, por lo que cualquier impacto sobre el rendimiento debe ser temporal y mínimo. Si existe algún problema, puede retrasar el reinicio del entorno hasta que se complete el proceso de migración y se eliminen las relaciones de importación.

Cierre la base de datos

El primer paso para desactivar el entorno en este ejemplo es cerrar la base de datos.

```
[oracle@host1 bin]$ . oraenv
ORACLE_SID = [oracle] ? FLIDB
The Oracle base remains unchanged with value /orabin
[oracle@host1 bin]$ sqlplus / as sysdba
SQL*Plus: Release 12.1.0.2.0
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit
Production
With the Partitioning, Automatic Storage Management, OLAP, Advanced
Analytics
and Real Application Testing options
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL>
```

Cierre los servicios de red

Uno de los sistemas de archivos basados en SAN que se están migrando también incluye los servicios de Oracle ASM. Para desactivar las LUN subyacentes es necesario desmontar los sistemas de archivos, lo que, a su vez, significa detener cualquier proceso con archivos abiertos en este sistema de archivos.

```
[oracle@host1 bin]$ ./crsctl stop has -f
CRS-2791: Starting shutdown of Oracle High Availability Services-managed
resources on 'host1'
CRS-2673: Attempting to stop 'ora.evmd' on 'host1'
CRS-2673: Attempting to stop 'ora.DATA.dg' on 'host1'
CRS-2673: Attempting to stop 'ora.LISTENER.lsnr' on 'host1'
CRS-2677: Stop of 'ora.DATA.dg' on 'host1' succeeded
CRS-2673: Attempting to stop 'ora.asm' on 'host1'
CRS-2677: Stop of 'ora.LISTENER.lsnr' on 'host1' succeeded
CRS-2677: Stop of 'ora.evmd' on 'host1' succeeded
CRS-2677: Stop of 'ora.asm' on 'host1' succeeded
CRS-2673: Attempting to stop 'ora.cssd' on 'host1'
CRS-2677: Stop of 'ora.cssd' on 'host1' succeeded
CRS-2793: Shutdown of Oracle High Availability Services-managed resources
on 'host1' has completed
CRS-4133: Oracle High Availability Services has been stopped.
[oracle@host1 bin]$
```

Desmonte los sistemas de archivos

Si todos los procesos se cierran, la operación umount se realiza correctamente. Si se deniega el permiso, debe haber un proceso con un bloqueo en el sistema de archivos. La `fuser` command puede ayudar a identificar estos procesos.

```
[root@host1 ~]# umount /orabin
[root@host1 ~]# umount /backups
```

Desactivar los grupos de volúmenes

Una vez que se han desmontado todos los sistemas de archivos de un grupo de volúmenes determinado, el grupo de volúmenes puede desactivarse.

```
[root@host1 ~]# vgchange --activate n sanvg
  0 logical volume(s) in volume group "sanvg" now active
[root@host1 ~]#
```

Cambios de red FC

Ahora las zonas de FC se pueden actualizar para eliminar todo el acceso del host a la cabina externa y establecer acceso a ONTAP.

Inicie el proceso de importación

Para iniciar los procesos de importación de LUN, ejecute el `lun import start` comando.

```
Cluster01::lun import*> lun import start -vserver vserver1 -path
/vol/new_asm/LUN0
Cluster01::lun import*> lun import start -vserver vserver1 -path
/vol/new_asm/LUN1
...
Cluster01::lun import*> lun import start -vserver vserver1 -path
/vol/new_lvm/LUN8
Cluster01::lun import*> lun import start -vserver vserver1 -path
/vol/new_lvm/LUN9
Cluster01::lun import*>
```

Supervise el progreso de la importación

La operación de importación se puede supervisar con el `lun import show` comando. Como se muestra a continuación, la importación de todas las 20 LUN está en curso, lo que significa que ahora se puede acceder a los datos a través de ONTAP aunque la operación de copia de datos aún progresa.

```
Cluster01::lun import*> lun import show -fields path,percent-complete
vserver   foreign-disk path              percent-complete
--------- ------------ ----------------- ----------------
vserver1  800DT$HuVWB/ /vol/new_asm/LUN4 5
vserver1  800DT$HuVWBW /vol/new_asm/LUN0 5
vserver1  800DT$HuVWBX /vol/new_asm/LUN1 6
vserver1  800DT$HuVWBY /vol/new_asm/LUN2 6
vserver1  800DT$HuVWBZ /vol/new_asm/LUN3 5
vserver1  800DT$HuVWBa /vol/new_asm/LUN5 4
vserver1  800DT$HuVWBb /vol/new_asm/LUN6 4
vserver1  800DT$HuVWBc /vol/new_asm/LUN7 4
vserver1  800DT$HuVWBd /vol/new_asm/LUN8 4
vserver1  800DT$HuVWBe /vol/new_asm/LUN9 4
vserver1  800DT$HuVWBf /vol/new_lvm/LUN0 5
vserver1  800DT$HuVWBg /vol/new_lvm/LUN1 4
vserver1  800DT$HuVWBh /vol/new_lvm/LUN2 4
vserver1  800DT$HuVWBi /vol/new_lvm/LUN3 3
vserver1  800DT$HuVWBj /vol/new_lvm/LUN4 3
vserver1  800DT$HuVWBk /vol/new_lvm/LUN5 3
vserver1  800DT$HuVWBl /vol/new_lvm/LUN6 4
vserver1  800DT$HuVWBm /vol/new_lvm/LUN7 3
vserver1  800DT$HuVWBn /vol/new_lvm/LUN8 2
vserver1  800DT$HuVWBo /vol/new_lvm/LUN9 2
20 entries were displayed.
```

Si necesita un proceso sin conexión, retrase la detección o el reinicio de servicios hasta que el `lun import show` comando indique que toda la migración se ha realizado correctamente y se ha completado. A continuación, puede completar el proceso de migración como se describe en "Importación de LUN externa:

Completado".

Si necesita una migración en línea, continúe con la detección de las LUN en su nuevo directorio raíz y obtenga los servicios.

Busque cambios en el dispositivo SCSI

En la mayoría de los casos, la opción más sencilla para volver a detectar nuevos LUN es reiniciar el host. Al hacerlo, se eliminan automáticamente los dispositivos obsoletos antiguos, se detectan correctamente todas las LUN nuevas y se crean dispositivos asociados como dispositivos multivía. El ejemplo aquí muestra un proceso totalmente en línea con fines de demostración.

Precaución: Antes de reiniciar un host, asegúrese de que todas las entradas en `/etc/fstab` Que se comentan los recursos SAN migrados de referencia. Si no se realiza y hay problemas con el acceso a la LUN, es posible que el sistema operativo no arranque. Esta situación no daña los datos. Sin embargo, puede ser muy incómodo arrancar en modo de rescate o un modo similar y corregir el `/etc/fstab` Para que el sistema operativo se pueda iniciar y permitir la solución de problemas.

Las LUN de la versión de Linux utilizada en este ejemplo se pueden volver a analizar con el `rescan-scsi-bus.sh` comando. Si el comando se realiza correctamente, cada ruta de LUN debería aparecer en el resultado. El resultado puede ser difícil de interpretar, pero, si la configuración de división en zonas y igroup es correcta, deberían aparecer muchas LUN que incluyan un `NETAPP` cadena de proveedor.

```
[root@host1 /]# rescan-scsi-bus.sh
Scanning SCSI subsystem for new devices
Scanning host 0 for  SCSI target IDs  0 1 2 3 4 5 6 7, all LUNs
 Scanning for device 0 2 0 0 ...
OLD: Host: scsi0 Channel: 02 Id: 00 Lun: 00
      Vendor: LSI      Model: RAID SAS 6G 0/1  Rev: 2.13
      Type:   Direct-Access                    ANSI SCSI revision: 05
Scanning host 1 for  SCSI target IDs  0 1 2 3 4 5 6 7, all LUNs
 Scanning for device 1 0 0 0 ...
OLD: Host: scsi1 Channel: 00 Id: 00 Lun: 00
      Vendor: Optiarc  Model: DVD RW AD-7760H  Rev: 1.41
      Type:   CD-ROM                           ANSI SCSI revision: 05
Scanning host 2 for  SCSI target IDs  0 1 2 3 4 5 6 7, all LUNs
Scanning host 3 for  SCSI target IDs  0 1 2 3 4 5 6 7, all LUNs
Scanning host 4 for  SCSI target IDs  0 1 2 3 4 5 6 7, all LUNs
Scanning host 5 for  SCSI target IDs  0 1 2 3 4 5 6 7, all LUNs
Scanning host 6 for  SCSI target IDs  0 1 2 3 4 5 6 7, all LUNs
Scanning host 7 for  all SCSI target IDs, all LUNs
 Scanning for device 7 0 0 10 ...
OLD: Host: scsi7 Channel: 00 Id: 00 Lun: 10
      Vendor: NETAPP   Model: LUN C-Mode       Rev: 8300
      Type:   Direct-Access                    ANSI SCSI revision: 05
 Scanning for device 7 0 0 11 ...
OLD: Host: scsi7 Channel: 00 Id: 00 Lun: 11
      Vendor: NETAPP   Model: LUN C-Mode       Rev: 8300
      Type:   Direct-Access                    ANSI SCSI revision: 05
 Scanning for device 7 0 0 12 ...
...
OLD: Host: scsi9 Channel: 00 Id: 01 Lun: 18
      Vendor: NETAPP   Model: LUN C-Mode       Rev: 8300
      Type:   Direct-Access                    ANSI SCSI revision: 05
 Scanning for device 9 0 1 19 ...
OLD: Host: scsi9 Channel: 00 Id: 01 Lun: 19
      Vendor: NETAPP   Model: LUN C-Mode       Rev: 8300
      Type:   Direct-Access                    ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.
```

Compruebe si hay dispositivos multivía

El proceso de detección de LUN también activa la recreación de dispositivos multivía, pero se sabe que el controlador multivía de Linux tiene problemas ocasionales. El resultado de `multipath -ll` debe comprobarse para verificar que la salida tiene el aspecto esperado. Por ejemplo, la salida a continuación muestra los dispositivos multivía asociados con a. `NETAPP` cadena de proveedor. Cada dispositivo tiene cuatro rutas, dos con una prioridad de 50 y dos con una prioridad de 10. Aunque la salida exacta puede variar con

diferentes versiones de Linux, esta salida tiene el aspecto esperado.

Consulte la documentación de utilidades de host para la versión de Linux que utiliza para verificar que el `/etc/multipath.conf` los ajustes son correctos.

```
[root@host1 /]# multipath -ll
3600a098038303558735d493762504b36 dm-5 NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 7:0:1:4  sdat 66:208 active ready running
| `- 9:0:1:4  sdbn 68:16  active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 7:0:0:4  sdf  8:80   active ready running
  `- 9:0:0:4  sdz  65:144 active ready running
3600a098038303558735d493762504b2d dm-10 NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 7:0:1:8  sdax 67:16  active ready running
| `- 9:0:1:8  sdbr 68:80  active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 7:0:0:8  sdj  8:144  active ready running
  `- 9:0:0:8  sdad 65:208 active ready running
...
3600a098038303558735d493762504b37 dm-8 NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 7:0:1:5  sdau 66:224 active ready running
| `- 9:0:1:5  sdbo 68:32  active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 7:0:0:5  sdg  8:96   active ready running
  `- 9:0:0:5  sdaa 65:160 active ready running
3600a098038303558735d493762504b4b dm-22 NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 7:0:1:19 sdbi 67:192 active ready running
| `- 9:0:1:19 sdcc 69:0   active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 7:0:0:19 sdu  65:64  active ready running
  `- 9:0:0:19 sdao 66:128 active ready running
```

Reactivar el grupo de volúmenes LVM

Si las LUN LVM se han detectado correctamente, el `vgchange --activate y` el comando debería tener éxito. Este es un buen ejemplo del valor de un gestor de volúmenes lógicos. Un cambio en el WWN de una LUN o incluso un número de serie no es importante, porque los metadatos del grupo de volúmenes se escriben en la propia LUN.

El SO analizó las LUN y detectó una pequeña cantidad de datos escritos en la LUN que la identifica como un volumen físico que pertenece al `sanvg volumegroup`. Luego construyó todos los dispositivos necesarios. Todo lo que se requiere es reactivar el grupo de volúmenes.

```
[root@host1 /]# vgchange --activate y sanvg
  Found duplicate PV fpCzdLTuKfy2xDZjai1NliJh3TjLUBiT: using
/dev/mapper/3600a098038303558735d493762504b46 not /dev/sdp
  Using duplicate PV /dev/mapper/3600a098038303558735d493762504b46 from
subsystem DM, ignoring /dev/sdp
  2 logical volume(s) in volume group "sanvg" now active
```

Vuelva a montar los sistemas de archivos

Una vez que se reactiva el grupo de volúmenes, los sistemas de archivos pueden montarse con todos los datos originales intactos. Como se ha explicado anteriormente, los sistemas de archivos funcionan completamente incluso si la replicación de datos sigue activa en el grupo de back.

```
[root@host1 /]# mount /orabin
[root@host1 /]# mount /backups
[root@host1 /]# df -k
Filesystem                          1K-blocks      Used Available Use%
Mounted on
/dev/mapper/rhel-root                52403200   8837100  43566100  17% /
devtmpfs                             65882776         0  65882776   0% /dev
tmpfs                                 6291456        84   6291372   1%
/dev/shm
tmpfs                                65898668      9884  65888784   1% /run
tmpfs                                65898668         0  65898668   0%
/sys/fs/cgroup
/dev/sda1                              505580    224828    280752  45% /boot
fas8060-nfs-public:/install          199229440 119368256  79861184  60%
/install
fas8040-nfs-routable:/snapomatic       9961472     30528   9930944   1%
/snapomatic
tmpfs                                13179736        16  13179720   1%
/run/user/42
tmpfs                                13179736         0  13179736   0%
/run/user/0
/dev/mapper/sanvg-lvorabin           20961280  12357456   8603824  59%
/orabin
/dev/mapper/sanvg-lvbackups          73364480  62947536  10416944  86%
/backups
```

Repetir escaneo para dispositivos ASM

Los dispositivos ASMLib deberían haber sido redescubiertos cuando los dispositivos SCSI se volvieron a analizar. La redetección se puede verificar en línea reiniciando ASMLib y luego escaneando los discos.

Este paso sólo es relevante para las configuraciones de ASM en las que se utiliza ASMLib.

Precaución: Si no se utiliza ASMLib, el `/dev/mapper` los dispositivos deberían haberse vuelto a crear automáticamente. Sin embargo, es posible que los permisos no sean correctos. Debe definir permisos especiales en los dispositivos subyacentes para ASM en ausencia de ASMLib. Hacer esto generalmente se logra a través de entradas especiales en cualquiera de los `/etc/multipath.conf` o. `udev` reglas, o posiblemente en ambos conjuntos de reglas. Es posible que estos archivos deban actualizarse para reflejar los cambios en el entorno en términos de WWN o números de serie para asegurarse de que los dispositivos ASM siguen teniendo los permisos correctos.

En este ejemplo, al reiniciar ASMLib y buscar discos se muestran las mismas 10 LUN de ASM que el entorno original.

```
[root@host1 /]# oracleasm exit
Unmounting ASMlib driver filesystem: /dev/oracleasm
Unloading module "oracleasm": oracleasm
[root@host1 /]# oracleasm init
Loading module "oracleasm": oracleasm
Configuring "oracleasm" to use device physical block size
Mounting ASMlib driver filesystem: /dev/oracleasm
[root@host1 /]# oracleasm scandisks
Reloading disk partitions: done
Cleaning any stale ASM disks...
Scanning system for ASM disks...
Instantiating disk "ASM0"
Instantiating disk "ASM1"
Instantiating disk "ASM2"
Instantiating disk "ASM3"
Instantiating disk "ASM4"
Instantiating disk "ASM5"
Instantiating disk "ASM6"
Instantiating disk "ASM7"
Instantiating disk "ASM8"
Instantiating disk "ASM9"
```

Reinicie los servicios de grid

Ahora que los dispositivos LVM y ASM están en línea y disponibles, los servicios de grid se pueden reiniciar.

```
[root@host1 /]# cd /orabin/product/12.1.0/grid/bin
[root@host1 bin]# ./crsctl start has
```

Reinicie la base de datos

Una vez reiniciados los servicios de grid, se puede activar la base de datos. Puede que sea necesario esperar unos minutos para que los servicios de ASM estén completamente disponibles antes de intentar iniciar la base de datos.

```
[root@host1 bin]# su - oracle
[oracle@host1 ~]$ . oraenv
ORACLE_SID = [oracle] ? FLIDB
The Oracle base has been set to /orabin
[oracle@host1 ~]$ sqlplus / as sysdba
SQL*Plus: Release 12.1.0.2.0
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to an idle instance.
SQL> startup
ORACLE instance started.
Total System Global Area 3221225472 bytes
Fixed Size                  4502416 bytes
Variable Size            1207962736 bytes
Database Buffers         1996488704 bytes
Redo Buffers               12271616 bytes
Database mounted.
Database opened.
SQL>
```

Finalización

Desde el punto de vista del host, la migración se completa, pero las operaciones de I/O siguen funcionando desde la cabina externa hasta que se eliminan las relaciones de importación.

Antes de eliminar las relaciones, debe confirmar que el proceso de migración se ha completado para todas las LUN.

```
Cluster01::*> lun import show -vserver vserver1 -fields foreign-
disk,path,operational-state
vserver   foreign-disk path              operational-state
--------- ------------ ----------------- -----------------
vserver1 800DT$HuVWB/ /vol/new_asm/LUN4 completed
vserver1 800DT$HuVWBW /vol/new_asm/LUN0 completed
vserver1 800DT$HuVWBX /vol/new_asm/LUN1 completed
vserver1 800DT$HuVWBY /vol/new_asm/LUN2 completed
vserver1 800DT$HuVWBZ /vol/new_asm/LUN3 completed
vserver1 800DT$HuVWBa /vol/new_asm/LUN5 completed
vserver1 800DT$HuVWBb /vol/new_asm/LUN6 completed
vserver1 800DT$HuVWBc /vol/new_asm/LUN7 completed
vserver1 800DT$HuVWBd /vol/new_asm/LUN8 completed
vserver1 800DT$HuVWBe /vol/new_asm/LUN9 completed
vserver1 800DT$HuVWBf /vol/new_lvm/LUN0 completed
vserver1 800DT$HuVWBg /vol/new_lvm/LUN1 completed
vserver1 800DT$HuVWBh /vol/new_lvm/LUN2 completed
vserver1 800DT$HuVWBi /vol/new_lvm/LUN3 completed
vserver1 800DT$HuVWBj /vol/new_lvm/LUN4 completed
vserver1 800DT$HuVWBk /vol/new_lvm/LUN5 completed
vserver1 800DT$HuVWBl /vol/new_lvm/LUN6 completed
vserver1 800DT$HuVWBm /vol/new_lvm/LUN7 completed
vserver1 800DT$HuVWBn /vol/new_lvm/LUN8 completed
vserver1 800DT$HuVWBo /vol/new_lvm/LUN9 completed
20 entries were displayed.
```

Suprimir relaciones de importación

Una vez completado el proceso de migración, elimine la relación de migración. Una vez hecho esto, las operaciones de I/O se proporcionan exclusivamente desde las unidades de ONTAP.

```
Cluster01::*> lun import delete -vserver vserver1 -path /vol/new_asm/LUN0
Cluster01::*> lun import delete -vserver vserver1 -path /vol/new_asm/LUN1
...
Cluster01::*> lun import delete -vserver vserver1 -path /vol/new_lvm/LUN8
Cluster01::*> lun import delete -vserver vserver1 -path /vol/new_lvm/LUN9
```

Anular el registro de LUN externas

Finalmente, modifique el disco para eliminar el `is-foreign` designación.

```
Cluster01::*> storage disk modify {-serial-number 800DT$HuVWBW} -is
-foreign false
Cluster01::*> storage disk modify {-serial-number 800DT$HuVWBX} -is
-foreign false
...
Cluster01::*> storage disk modify {-serial-number 800DT$HuVWBn} -is
-foreign false
Cluster01::*> storage disk modify {-serial-number 800DT$HuVWBo} -is
-foreign false
Cluster01::*>
```

Conversión de protocolos

El cambio del protocolo utilizado para acceder a una LUN es un requisito habitual.

En algunos casos, forma parte de una estrategia global para migrar datos al cloud. TCP/IP es el protocolo de la nube y el cambio de FC a iSCSI permite facilitar la migración a diversos entornos de cloud. En otros casos, iSCSI puede ser conveniente aprovechar los costes reducidos de una SAN IP. En ocasiones, una migración podría utilizar un protocolo diferente como medida temporal. Por ejemplo, si una cabina externa y LUN basadas en ONTAP no pueden coexistir en los mismos HBA, puede utilizar LUN de iSCSI el tiempo suficiente para copiar datos de la cabina anterior. Entonces, puede volver a convertir a FC después de eliminar las LUN antiguas del sistema.

El siguiente procedimiento muestra la conversión de FC a iSCSI, pero los principios generales se aplican a una conversión de iSCSI a FC inversa.

Instale el iniciador de iSCSI

La mayoría de los sistemas operativos incluyen un iniciador iSCSI de software de forma predeterminada, pero si no se incluye uno, se puede instalar fácilmente.

```
[root@host1 /]# yum install -y iscsi-initiator-utils
Loaded plugins: langpacks, product-id, search-disabled-repos,
subscription-
              : manager
Resolving Dependencies
--> Running transaction check
---> Package iscsi-initiator-utils.x86_64 0:6.2.0.873-32.el7 will be
updated
--> Processing Dependency: iscsi-initiator-utils = 6.2.0.873-32.el7 for
package: iscsi-initiator-utils-iscsiuio-6.2.0.873-32.el7.x86_64
---> Package iscsi-initiator-utils.x86_64 0:6.2.0.873-32.0.2.el7 will be
an update
--> Running transaction check
---> Package iscsi-initiator-utils-iscsiuio.x86_64 0:6.2.0.873-32.el7 will
be updated
---> Package iscsi-initiator-utils-iscsiuio.x86_64 0:6.2.0.873-32.0.2.el7
```

```
will be an update
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
===
 Package                         Arch   Version              Repository
Size
================================================================================
===
Updating:
 iscsi-initiator-utils           x86_64 6.2.0.873-32.0.2.el7 ol7_latest 416
k
Updating for dependencies:
 iscsi-initiator-utils-iscsiuio x86_64 6.2.0.873-32.0.2.el7 ol7_latest  84
k
Transaction Summary
================================================================================
===
Upgrade  1 Package (+1 Dependent package)
Total download size: 501 k
Downloading packages:
No Presto metadata available for ol7_latest
(1/2): iscsi-initiator-utils-6.2.0.873-32.0.2.el7.x86_6 | 416 kB   00:00
(2/2): iscsi-initiator-utils-iscsiuio-6.2.0.873-32.0.2. |  84 kB   00:00
--------------------------------------------------------------------------------
---
Total                                           2.8 MB/s | 501 kB
00:00Cluster01
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Updating   : iscsi-initiator-utils-iscsiuio-6.2.0.873-32.0.2.el7.x86
1/4
  Updating   : iscsi-initiator-utils-6.2.0.873-32.0.2.el7.x86_64
2/4
  Cleanup    : iscsi-initiator-utils-iscsiuio-6.2.0.873-32.el7.x86_64
3/4
  Cleanup    : iscsi-initiator-utils-6.2.0.873-32.el7.x86_64
4/4
rhel-7-server-eus-rpms/7Server/x86_64/productid       | 1.7 kB     00:00
rhel-7-server-rpms/7Server/x86_64/productid           | 1.7 kB     00:00
  Verifying  : iscsi-initiator-utils-6.2.0.873-32.0.2.el7.x86_64
1/4
  Verifying  : iscsi-initiator-utils-iscsiuio-6.2.0.873-32.0.2.el7.x86
2/4
```

```
  Verifying  : iscsi-initiator-utils-iscsiuio-6.2.0.873-32.el7.x86_64
3/4
  Verifying  : iscsi-initiator-utils-6.2.0.873-32.el7.x86_64
4/4
Updated:
  iscsi-initiator-utils.x86_64 0:6.2.0.873-32.0.2.el7
Dependency Updated:
  iscsi-initiator-utils-iscsiuio.x86_64 0:6.2.0.873-32.0.2.el7
Complete!
[root@host1 /]#
```

Identificar el nombre del iniciador de iSCSI

Se genera un nombre de iniciador iSCSI único durante el proceso de instalación. En Linux, se encuentra en el `/etc/iscsi/initiatorname.iscsi` archivo. Este nombre se utiliza para identificar el host en la SAN IP.

```
[root@host1 /]# cat /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.1992-05.com.redhat:497bd66ca0
```

Cree un nuevo iGroup

Un igroup forma parte de la arquitectura de enmascaramiento LUN de ONTAP. No es posible acceder a un LUN recién creado a menos que se conceda acceso en primer lugar a un host. Para lograr este paso, debe crear un igroup que enumere los nombres de iniciadores iSCSI o WWN de FC que requieren acceso.

En este ejemplo, se crea un igroup que contiene el iniciador iSCSI del host Linux.

```
Cluster01::*> igroup create -igroup linuxiscsi -protocol iscsi -ostype
linux -initiator iqn.1994-05.com.redhat:497bd66ca0
```

Apague el entorno

Antes de cambiar el protocolo de LUN, las LUN deben estar completamente desactivadas. Cualquier base de datos en uno de los LUN que se van a convertir debe cerrarse, los sistemas de archivos deben desmontarse y los grupos de volúmenes deben desactivarse. Donde se utiliza ASM, asegúrese de que el grupo de discos de ASM está desmontado y cierre todos los servicios de grid.

Desasigne las LUN de la red FC

Una vez que las LUN estén completamente en modo inactivo, quite las asignaciones del iGroup FC original.

```
Cluster01::*> lun unmap -vserver vserver1 -path /vol/new_asm/LUN0 -igroup
linuxhost
Cluster01::*> lun unmap -vserver vserver1 -path /vol/new_asm/LUN1 -igroup
linuxhost
...
Cluster01::*> lun unmap -vserver vserver1 -path /vol/new_lvm/LUN8 -igroup
linuxhost
Cluster01::*> lun unmap -vserver vserver1 -path /vol/new_lvm/LUN9 -igroup
linuxhost
```

Vuelva a asignar los LUN a la red IP

Otorgue acceso a cada LUN al nuevo grupo de iniciadores basado en iSCSI.

```
Cluster01::*> lun map -vserver vserver1 -path /vol/new_asm/LUN0 -igroup
linuxiscsi
Cluster01::*> lun map -vserver vserver1 -path /vol/new_asm/LUN1 -igroup
linuxiscsi
...
Cluster01::*> lun map -vserver vserver1 -path /vol/new_lvm/LUN8 -igroup
linuxiscsi
Cluster01::*> lun map -vserver vserver1 -path /vol/new_lvm/LUN9 -igroup
linuxiscsi
Cluster01::*>
```

Detectar destinos iSCSI

Existen dos fases para la detección iSCSI. El primero es detectar los destinos, que no es lo mismo que detectar una LUN. La `iscsiadm` el comando que se muestra a continuación sondea el grupo de portales especificado por el `-p argument` Y almacena una lista de todas las direcciones IP y puertos que ofrecen servicios iSCSI. En este caso, hay cuatro direcciones IP que tienen servicios iSCSI en el puerto predeterminado 3260.

> Este comando puede tardar varios minutos en completarse si no se puede acceder a alguna de las direcciones IP de destino.

```
[root@host1 ~]# iscsiadm -m discovery -t st -p fas8060-iscsi-public1
10.63.147.197:3260,1033 iqn.1992-
08.com.netapp:sn.807615e9ef6111e5a5ae90e2ba5b9464:vs.3
10.63.147.198:3260,1034 iqn.1992-
08.com.netapp:sn.807615e9ef6111e5a5ae90e2ba5b9464:vs.3
172.20.108.203:3260,1030 iqn.1992-
08.com.netapp:sn.807615e9ef6111e5a5ae90e2ba5b9464:vs.3
172.20.108.202:3260,1029 iqn.1992-
08.com.netapp:sn.807615e9ef6111e5a5ae90e2ba5b9464:vs.3
```

Descubra LUN de iSCSI

Después de detectar los destinos iSCSI, reinicie el servicio iSCSI para detectar los LUN iSCSI disponibles y crear dispositivos asociados, como dispositivos multivía o ASMLib.

```
[root@host1 ~]# service iscsi restart
Redirecting to /bin/systemctl restart  iscsi.service
```

Reinicie el entorno

Reinicie el entorno reactivando los grupos de volúmenes, volviendo a montar sistemas de archivos, reiniciando los servicios de RAC, etc. Como medida de precaución, NetApp recomienda reiniciar el servidor una vez que se haya completado el proceso de conversión para asegurarse de que todos los archivos de configuración sean correctos y de que se eliminen todos los dispositivos obsoletos.

Precaución: Antes de reiniciar un host, asegúrese de que todas las entradas en `/etc/fstab` Que se comentan los recursos SAN migrados de referencia. Si este paso no se realiza y hay problemas con el acceso a la LUN, el resultado puede ser un sistema operativo que no se inicia. Este problema no daña los datos. Sin embargo, puede ser muy incómodo arrancar en modo de rescate o un modo similar y correcto `/etc/fstab` Para que el sistema operativo se pueda iniciar para permitir que se inicien los esfuerzos de solución de problemas.

Scripts de ejemplo

Los scripts presentados se proporcionan como ejemplos de cómo realizar scripts de varias tareas del sistema operativo y de la base de datos. Se suministran tal cual. Si se necesita soporte para un procedimiento concreto, póngase en contacto con NetApp o con un distribuidor de NetApp.

Cierre de la base de datos

El siguiente script Perl toma un argumento único del SID de Oracle y cierra una base de datos. Se puede ejecutar como usuario oracle o como raíz.

```
#! /usr/bin/perl
use strict;
use warnings;
my $oraclesid=$ARGV[0];
my $oracleuser='oracle';
my @out;
my $uid=$<;
if ($uid == 0) {
@out=`su - $oracleuser -c '. oraenv << EOF1
77 Migration of Oracle Databases to NetApp Storage Systems © 2021 NetApp,
Inc. All rights reserved
$oraclesid
EOF1
sqlplus / as sysdba << EOF2
shutdown immediate;
EOF2
'
`;}
else {
@out=`. oraenv << EOF1
$oraclesid
EOF4
sqlplus / as sysdba << EOF2
shutdown immediate;
EOF2
`;};
print @out;
if ("@out" =~ /ORACLE instance shut down/) {
print "$oraclesid shut down\n";
exit 0;}
elsif ("@out" =~ /Connected to an idle instance/) {
print "$oraclesid already shut down\n";
exit 0;}
else {
print "$oraclesid failed to shut down\n";
exit 1;}
```

Inicio de la base de datos

El siguiente script Perl toma un argumento único del SID de Oracle y cierra una base de datos. Se puede ejecutar como usuario oracle o como raíz.

```
#! /usr/bin/perl
use strict;
use warnings;
my $oraclesid=$ARGV[0];
my $oracleuser='oracle';
my @out;
my $uid=$<;
if ($uid == 0) {
@out=`su - $oracleuser -c '. oraenv << EOF1
$oraclesid
EOF1
sqlplus / as sysdba << EOF2
startup;
EOF2
'
`;}
else {
@out=`. oraenv << EOF3
$oraclesid
EOF1
sqlplus / as sysdba << EOF2
startup;
EOF2
`;};
print @out;
if ("@out" =~ /Database opened/) {
print "$oraclesid started\n";
exit 0;}
elsif ("@out" =~ /cannot start already-running ORACLE/) {
print "$oraclesid already started\n";
exit 1;}
else {
78 Migration of Oracle Databases to NetApp Storage Systems © 2021 NetApp,
Inc. All rights reserved
print "$oraclesid failed to start\n";
exit 1;}
```

Convertir el sistema de archivos a sólo lectura

El siguiente script toma un argumento del sistema de archivos e intenta desmontarlo y volver a montarlo como de solo lectura. Esto resulta útil durante los procesos de migración en los que un sistema de ficheros debe estar disponible para replicar los datos y, sin embargo, debe protegerse frente a daños accidentales.

```
#! /usr/bin/perl
use strict;
#use warnings;
my $filesystem=$ARGV[0];
my @out=`umount '$filesystem'`;
if ($? == 0) {
 print "$filesystem unmounted\n";
 @out = `mount -o ro '$filesystem'`;
 if ($? == 0) {
 print "$filesystem mounted read-only\n";
 exit 0;}}
else {
 print "Unable to unmount $filesystem\n";
 exit 1;}
print @out;
```

Sustituya el sistema de archivos

El siguiente ejemplo de script se utiliza para reemplazar un sistema de archivos por otro. Debido a que edita el archivo `/etc/fstab `, debe ejecutarse como root. Acepta un único argumento delimitado por comas de los sistemas de archivos antiguos y nuevos.

1. Para sustituir el sistema de archivos, ejecute el siguiente script:

```
#! /usr/bin/perl
use strict;
#use warnings;
my $oldfs;
my $newfs;
my @oldfstab;
my @newfstab;
my $source;
my $mountpoint;
my $leftover;
my $oldfstabentry='';
my $newfstabentry='';
my $migratedfstabentry='';
($oldfs, $newfs) = split (',',$ARGV[0]);
open(my $filehandle, '<', '/etc/fstab') or die "Could not open
/etc/fstab\n";
while (my $line = <$filehandle>) {
 chomp $line;
 ($source, $mountpoint, $leftover) = split(/[ , ]/,$line, 3);
 if ($mountpoint eq $oldfs) {
 $oldfstabentry = "#Removed by swap script $source $oldfs $leftover";}
```

```
 elsif ($mountpoint eq $newfs) {
 $newfstabentry = "#Removed by swap script $source $newfs $leftover";
 $migratedfstabentry = "$source $oldfs $leftover";}
 else {
 push (@newfstab, "$line\n")}}
79 Migration of Oracle Databases to NetApp Storage Systems © 2021
NetApp, Inc. All rights reserved
push (@newfstab, "$oldfstabentry\n");
push (@newfstab, "$newfstabentry\n");
push (@newfstab, "$migratedfstabentry\n");
close($filehandle);
if ($oldfstabentry eq ''){
 die "Could not find $oldfs in /etc/fstab\n";}
if ($newfstabentry eq ''){
 die "Could not find $newfs in /etc/fstab\n";}
my @out=`umount '$newfs'`;
if ($? == 0) {
 print "$newfs unmounted\n";}
else {
 print "Unable to unmount $newfs\n";
 exit 1;}
@out=`umount '$oldfs'`;
if ($? == 0) {
 print "$oldfs unmounted\n";}
else {
 print "Unable to unmount $oldfs\n";
 exit 1;}
system("cp /etc/fstab /etc/fstab.bak");
open ($filehandle, ">", '/etc/fstab') or die "Could not open /etc/fstab
for writing\n";
for my $line (@newfstab) {
 print $filehandle $line;}
close($filehandle);
@out=`mount '$oldfs'`;
if ($? == 0) {
 print "Mounted updated $oldfs\n";
 exit 0;}
else{
 print "Unable to mount updated $oldfs\n";
 exit 1;}
exit 0;
```

Como ejemplo del uso de este script, supongamos que los datos de `/oradata` se ha migrado a. `/neworadata` y.. `/logs` se ha migrado a. `/newlogs`. Uno de los métodos más simples para realizar esta tarea es mediante una simple operación de copia de archivos para reubicar el nuevo dispositivo en el punto de montaje original.

2. Suponga que los sistemas de archivos antiguos y nuevos están presentes en la `/etc/fstab` el archivo es el siguiente:

```
cluster01:/vol_oradata /oradata nfs rw,bg,vers=3,rsize=65536,wsize=65536
0 0
cluster01:/vol_logs /logs nfs rw,bg,vers=3,rsize=65536,wsize=65536 0 0
cluster01:/vol_neworadata /neworadata nfs
rw,bg,vers=3,rsize=65536,wsize=65536 0 0
cluster01:/vol_newlogs /newlogs nfs rw,bg,vers=3,rsize=65536,wsize=65536
0 0
```

3. Cuando se ejecuta, este script desmonta el sistema de archivos actual y lo reemplaza por el nuevo:

```
[root@jfsc3 scripts]# ./swap.fs.pl /oradata,/neworadata
/neworadata unmounted
/oradata unmounted
Mounted updated /oradata
[root@jfsc3 scripts]# ./swap.fs.pl /logs,/newlogs
/newlogs unmounted
/logs unmounted
Mounted updated /logs
```

4. El script también actualiza el `/etc/fstab` archivar según corresponda. En el ejemplo que se muestra aquí, incluye los siguientes cambios:

```
#Removed by swap script cluster01:/vol_oradata /oradata nfs
rw,bg,vers=3,rsize=65536,wsize=65536 0 0
#Removed by swap script cluster01:/vol_neworadata /neworadata nfs
rw,bg,vers=3,rsize=65536,wsize=65536 0 0
cluster01:/vol_neworadata /oradata nfs
rw,bg,vers=3,rsize=65536,wsize=65536 0 0
#Removed by swap script cluster01:/vol_logs /logs nfs
rw,bg,vers=3,rsize=65536,wsize=65536 0 0
#Removed by swap script cluster01:/vol_newlogs /newlogs nfs
rw,bg,vers=3,rsize=65536,wsize=65536 0 0
cluster01:/vol_newlogs /logs nfs rw,bg,vers=3,rsize=65536,wsize=65536 0
0
```

Migración de bases de datos automatizada

Este ejemplo muestra el uso de scripts de apagado, inicio y reemplazo del sistema de archivos para automatizar completamente una migración.

```
```

```
#! /usr/bin/perl
use strict;
#use warnings;
my $oraclesid=$ARGV[0];
my @oldfs;
my @newfs;
my $x=1;
while ($x < scalar(@ARGV)) {
   ($oldfs[$x-1], $newfs[$x-1]) = split (',',$ARGV[$x]);
   $x+=1;}
my @out=`./dbshut.pl '$oraclesid'`;
print @out;
if ($? ne 0) {
   print "Failed to shut down database\n";
   exit 0;}
$x=0;
while ($x < scalar(@oldfs)) {
   my @out=`./mk.fs.readonly.pl '$oldfs[$x]'`;
   if ($? ne 0) {
      print "Failed to make filesystem $oldfs[$x] readonly\n";
      exit 0;}
   $x+=1;}
$x=0;
while ($x < scalar(@oldfs)) {
   my @out=`rsync -rlpogt --stats --progress --exclude='.snapshot'
'$oldfs[$x]/' '/$newfs[$x]/'`;
   print @out;
   if ($? ne 0) {
      print "Failed to copy filesystem $oldfs[$x] to $newfs[$x]\n";
      exit 0;}
   else {
      print "Succesfully replicated filesystem $oldfs[$x] to
$newfs[$x]\n";}
   $x+=1;}
$x=0;
while ($x < scalar(@oldfs)) {
   print "swap $x $oldfs[$x] $newfs[$x]\n";
   my @out=`./swap.fs.pl '$oldfs[$x],$newfs[$x]'`;
   print @out;
   if ($? ne 0) {
      print "Failed to swap filesystem $oldfs[$x] for $newfs[$x]\n";
      exit 1;}
   else {
      print "Swapped filesystem $oldfs[$x] for $newfs[$x]\n";}
   $x+=1;}
my @out=`./dbstart.pl '$oraclesid'`;
```

```
print @out;
```

Mostrar ubicaciones de archivos

Este script recopila una serie de parámetros críticos de la base de datos e imprime en un formato fácil de leer. Este script puede ser útil al revisar diseños de datos. Además, el script se puede modificar para otros usos.

```
#! /usr/bin/perl
#use strict;
#use warnings;
my $oraclesid=$ARGV[0];
my $oracleuser='oracle';
my @out;
sub dosql{
        my $command = @_[0];
        my @lines;
        my $uid=$<;
        if ($uid == 0) {
        @lines=`su - $oracleuser -c "export ORAENV_ASK=NO;export
ORACLE_SID=$oraclesid;. oraenv -s << EOF1
EOF1
sqlplus -S / as sysdba << EOF2
set heading off
$command
EOF2
"
        `;}
        else {
        $command=~s/\\\\\\/\\/g;
        @lines=`export ORAENV_ASK=NO;export ORACLE_SID=$oraclesid;. oraenv
-s << EOF1
EOF1
sqlplus -S / as sysdba << EOF2
set heading off
$command
EOF2
        `;};
return @lines}
print "\n";
@out=dosql('select name from v\\\\\$datafile;');
print "$oraclesid datafiles:\n";
for $line (@out) {
        chomp($line);
        if (length($line)>0) {print "$line\n";}}
print "\n";
@out=dosql('select member from v\\\\\$logfile;');
```

```
print "$oraclesid redo logs:\n";
for $line (@out) {
        chomp($line);
        if (length($line)>0) {print "$line\n";}}
print "\n";
@out=dosql('select name from v\\\\\$tempfile;');
print "$oraclesid temp datafiles:\n";
for $line (@out) {
        chomp($line);
        if (length($line)>0) {print "$line\n";}}
print "\n";
@out=dosql('show parameter spfile;');
print "$oraclesid spfile\n";
for $line (@out) {
        chomp($line);
        if (length($line)>0) {print "$line\n";}}
print "\n";
@out=dosql('select name||\' \'||value from v\\\\\$parameter where
isdefault=\'FALSE\';');
print "$oraclesid key parameters\n";
for $line (@out) {
        chomp($line);
        if ($line =~ /control_files/) {print "$line\n";}
        if ($line =~ /db_create/) {print "$line\n";}
        if ($line =~ /db_file_name_convert/) {print "$line\n";}
        if ($line =~ /log_archive_dest/) {print "$line\n";}}
        if ($line =~ /log_file_name_convert/) {print "$line\n";}
        if ($line =~ /pdb_file_name_convert/) {print "$line\n";}
        if ($line =~ /spfile/) {print "$line\n";}
print "\n";
```

Limpieza de migración de ASM

```
#! /usr/bin/perl
#use strict;
#use warnings;
my $oraclesid=$ARGV[0];
my $oracleuser='oracle';
my @out;
sub dosql{
        my $command = @_[0];
        my @lines;
        my $uid=$<;
        if ($uid == 0) {
        @lines=`su - $oracleuser -c "export ORAENV_ASK=NO;export
```

```
ORACLE_SID=$oraclesid;. oraenv -s << EOF1
EOF1
sqlplus -S / as sysdba << EOF2
set heading off
$command
EOF2
"
        `;}
        else {
        $command=~s/\\\\\\\/\\/g;
        @lines=`export ORAENV_ASK=NO;export ORACLE_SID=$oraclesid;. oraenv
-s << EOF1
EOF1
sqlplus -S / as sysdba << EOF2
set heading off
$command
EOF2
        `;}
return @lines}
print "\n";
@out=dosql('select name from v\\\\\$datafile;');
print @out;
print "shutdown immediate;\n";
print "startup mount;\n";
print "\n";
for $line (@out) {
        if (length($line) > 1) {
                chomp($line);
                ($first, $second,$third,$fourth)=split('_',$line);
                $fourth =~ s/^TS-//;
                $newname=lc("$fourth.dbf");
                $path2file=$line;
                $path2file=~ /(^.*.\/)/;
                print "host mv $line $1$newname\n";}}
print "\n";
for $line (@out) {
        if (length($line) > 1) {
                chomp($line);
                ($first, $second,$third,$fourth)=split('_',$line);
                $fourth =~ s/^TS-//;
                $newname=lc("$fourth.dbf");
                $path2file=$line;
                $path2file=~ /(^.*.\/)/;
                print "alter database rename file '$line' to
'$1$newname';\n";}}
print "alter database open;\n";
```

```
print "\n";
```

Conversión de ASM al nombre del sistema de archivos

```
set serveroutput on;
set wrap off;
declare
    cursor df is select file#, name from v$datafile;
    cursor tf is select file#, name from v$tempfile;
    cursor lf is select member from v$logfile;
    firstline boolean := true;
begin
    dbms_output.put_line(CHR(13));
    dbms_output.put_line('Parameters for log file conversion:');
    dbms_output.put_line(CHR(13));
    dbms_output.put('*.log_file_name_convert = ');
    for lfrec in lf loop
        if (firstline = true) then
            dbms_output.put('''' || lfrec.member || ''', ');
            dbms_output.put('''/NEW_PATH/' ||
regexp_replace(lfrec.member,'^.*/','') || '''');
        else
            dbms_output.put(',''' || lfrec.member || ''', ');
            dbms_output.put('''/NEW_PATH/' ||
regexp_replace(lfrec.member,'^.*/','') || '''');
        end if;
        firstline:=false;
    end loop;
    dbms_output.put_line(CHR(13));
    dbms_output.put_line(CHR(13));
    dbms_output.put_line('rman duplication script:');
    dbms_output.put_line(CHR(13));
    dbms_output.put_line('run');
    dbms_output.put_line('{');
    for dfrec in df loop
        dbms_output.put_line('set newname for datafile ' ||
            dfrec.file# || ' to ''' || dfrec.name ||''';');
    end loop;
    for tfrec in tf loop
        dbms_output.put_line('set newname for tempfile ' ||
            tfrec.file# || ' to ''' || tfrec.name ||''';');
    end loop;
    dbms_output.put_line('duplicate target database for standby backup
location INSERT_PATH_HERE;');
    dbms_output.put_line('}');
end;
/
```

Reproduzca los logs en la base de datos

Este archivo de comandos acepta un argumento único de un SID de Oracle para una base de datos que está en modo de montaje e intenta reproducir todos los archive logs disponibles actualmente.

```
#! /usr/bin/perl
use strict;
my $oraclesid=$ARGV[0];
my $oracleuser='oracle';
84 Migration of Oracle Databases to NetApp Storage Systems © 2021 NetApp,
Inc. All rights reserved
my $uid = $<;
my @out;
if ($uid == 0) {
@out=`su - $oracleuser -c '. oraenv << EOF1
$oraclesid
EOF1
sqlplus / as sysdba << EOF2
recover database until cancel;
auto
EOF2
'
`;}
else {
@out=`. oraenv << EOF1
$oraclesid
EOF1
sqlplus / as sysdba << EOF2
recover database until cancel;
auto
EOF2
`;
}
print @out;
```

Logs de Reproducción en Base de Datos en Espera

Este script es idéntico al anterior, excepto que está diseñado para una base de datos en espera.

```
#! /usr/bin/perl
use strict;
my $oraclesid=$ARGV[0];
my $oracleuser='oracle';
my $uid = $<;
my @out;
if ($uid == 0) {
@out=`su - $oracleuser -c '. oraenv << EOF1
$oraclesid
EOF1
sqlplus / as sysdba << EOF2
recover standby database until cancel;
auto
EOF2
'
`;}
else {
@out=`. oraenv << EOF1
$oraclesid
EOF1
sqlplus / as sysdba << EOF2
recover standby database until cancel;
auto
EOF2
`;
}
print @out;
```

Notas adicionales

Optimización del rendimiento y evaluación comparativa

Las pruebas precisas del rendimiento del almacenamiento de la base de datos son un tema muy complicado. Requiere una comprensión de los siguientes problemas:

- IOPS y rendimiento
- La diferencia entre las operaciones de I/O en primer plano y en segundo plano
- El efecto de la latencia sobre la base de datos
- Numerosos sistemas operativos y configuraciones de red que también afectan al rendimiento del almacenamiento

Además, hay tareas que no son de almacenamiento que se deben tener en cuenta. Hay un punto en el cual la optimización del rendimiento del almacenamiento no proporciona ventajas útiles, porque el rendimiento del almacenamiento ya no es un factor limitador del rendimiento.

La mayoría de clientes de bases de datos seleccionan ahora las cabinas all-flash, lo que crea algunas consideraciones adicionales. Por ejemplo, piense en las pruebas de rendimiento en un sistema AFF A900 de dos nodos:

- Con una tasa de lectura/escritura de 80/20:1, dos nodos de A900 pueden ofrecer más de 1M 000 IOPS de base de datos aleatorias antes de que la latencia supere incluso la marca 150µs. Esto supera con creces las demandas de rendimiento actuales de la mayoría de las bases de datos, que es difícil predecir la mejora esperada. El almacenamiento se borrará en gran medida como un cuello de botella.
- El ancho de banda de red es una fuente cada vez más común de limitaciones de rendimiento. Por ejemplo, las soluciones de discos giratorios suelen ser cuellos de botella en el rendimiento de las bases de datos porque la latencia de I/O es muy alta. Cuando una cabina all-flash elimina las limitaciones de latencia, la barrera cambia frecuentemente a la red. Esto es especialmente notable en entornos virtualizados y sistemas blade donde la verdadera conectividad de red es difícil de visualizar. Esto puede complicar las pruebas de rendimiento si el sistema de almacenamiento en sí no se puede utilizar completamente debido a las limitaciones de ancho de banda.
- Comparar el rendimiento de una cabina all-flash con una cabina que contiene discos giratorios no es posible debido a la latencia drásticamente mejorada de las cabinas all-flash. Los resultados de las pruebas no suelen ser significativos.
- La comparación del rendimiento máximo de IOPS con una cabina all-flash no suele ser una prueba útil porque las bases de datos no están limitadas por las operaciones de I/O de almacenamiento Por ejemplo, supongamos que una cabina puede admitir 500K 000 IOPS aleatorias, mientras que otra puede admitir 300K. La diferencia no es relevante en el mundo real si la base de datos gasta el 99% de su tiempo en procesamiento de CPU. Las cargas de trabajo nunca utilizan todas las funcionalidades de la cabina de almacenamiento. En cambio, las funcionalidades de IOPS máximo pueden ser cruciales en una plataforma de consolidación en la cual se espera que la cabina de almacenamiento se cargue en sus capacidades máximas.
- Considere siempre la latencia así como IOPS en cualquier prueba de almacenamiento. Muchas cabinas de almacenamiento del mercado afirman niveles extremos de IOPS, pero la latencia hace que dichas IOPS sean inútiles en dichos niveles. El destino típico de las cabinas all-flash es la marca 1ms. Un método mejor de prueba no es medir el máximo de IOPS posibles, sino determinar cuántas IOPS puede admitir una cabina de almacenamiento antes de que la latencia media sea superior a 1ms ms.

Oracle Automatic Workload Repository y benchmarking

El estándar oro para las comparaciones de rendimiento de Oracle es un informe de Oracle Automatic Workload Repository (AWR).

Hay varios tipos de informes de AWR. Desde el punto de vista del almacenamiento, un informe generado por la ejecución del `awrrpt.sql` Command es el más completo y valioso porque se dirige a una instancia de base de datos específica e incluye algunos histogramas detallados que desglosan eventos de I/O de almacenamiento en función de la latencia.

La comparación ideal de dos cabinas de rendimiento implica ejecutar la misma carga de trabajo en cada cabina y producir un informe de AWR que apunte con precisión a la carga de trabajo. En el caso de una carga de trabajo de ejecución muy prolongada, se puede utilizar un único informe de AWR con un tiempo transcurrido que abarque el tiempo de inicio y de finalización, pero es preferible dividir los datos de AWR como varios informes. Por ejemplo, si un trabajo por lotes se ejecutó desde la medianoche hasta las 6 a.m., cree una serie de informes de AWR de una hora de medianoche a las 1 a.m., de 1 a.m. a 2 a.m., etc.

En otros casos, se debe optimizar una consulta muy corta. La mejor opción es un informe de AWR basado en una instantánea de AWR creada cuando se inicia la consulta y una segunda instantánea de AWR creada cuando finaliza la consulta. El servidor de la base de datos debería ser silencioso para minimizar la actividad en segundo plano que oscurecería la actividad de la consulta en análisis.

Cuando los informes de AWR no están disponibles, los informes de Oracle statspack son una buena alternativa. Contienen la mayoría de las mismas estadísticas de E/S que un informe AWR.

Oracle AWR y solución de problemas

Un informe AWR es también la herramienta más importante para analizar un problema de rendimiento.

Al igual que sucede con las pruebas de rendimiento, la solución de problemas de rendimiento requiere medir con precisión una carga de trabajo determinada. Siempre que sea posible, facilite los datos de AWR cuando notifique un problema de rendimiento al centro de soporte de NetApp o cuando trabaje con un NetApp o con un equipo de cuentas de partners sobre una nueva solución.

Al proporcionar datos de AWR, tenga en cuenta los siguientes requisitos:

- Ejecute el `awrrpt.sql` comando para generar el informe. La salida puede ser texto o HTML.
- Si se utiliza Oracle Real Application Clusters (RAC), genere informes de AWR para cada instancia del cluster.
- Indique la hora específica a la que ha existido el problema. El tiempo transcurrido máximo aceptable de un informe de AWR suele ser de una hora. Si un problema persiste durante varias horas o implica una operación de varias horas, como un trabajo por lotes, proporcione varios informes de AWR de una hora que cubran todo el período que se va a analizar.
- Si es posible, ajuste el intervalo de instantáneas de AWR a 15 minutos. Este ajuste permite realizar un análisis más detallado. Esto también requiere ejecuciones adicionales de `awrrpt.sql` para proporcionar un informe para cada intervalo de 15 minutos.
- Si el problema es una consulta de ejecución muy corta, proporcione un informe AWR basado en una instantánea AWR creada al iniciar la operación y una segunda instantánea AWR creada al finalizar la operación. El servidor de base de datos debería ser silencioso para minimizar la actividad en segundo plano que oscurecería la actividad de la operación en análisis.
- Si se informa de un problema de rendimiento en determinados momentos pero no en otros, proporcione datos de AWR adicionales que demuestren un buen rendimiento para la comparación.

calibrar_io

La `calibrate_io` nunca se debe usar el comando para probar, comparar ni hacer pruebas de rendimiento de los sistemas de almacenamiento. Tal y como se indica en la documentación de Oracle, este procedimiento calibra las capacidades de E/S del almacenamiento.

La calibración no es lo mismo que la evaluación comparativa. El objetivo de este comando es emitir E/S para ayudar a calibrar las operaciones de base de datos y mejorar su eficiencia mediante la optimización del nivel de E/S emitidas al host. Debido al tipo de I/O que realiza el `calibrate_io` La operación no representa la E/S real del usuario de la base de datos, los resultados no son predecibles y, con frecuencia, ni siquiera se pueden reproducir.

SLOB2

SLOB2, el Silly Little Oracle Benchmark, se ha convertido en la herramienta preferida para evaluar el rendimiento de la base de datos. Fue desarrollado por Kevin Closson y está disponible en "https://kevinclosson.net/slob/". Se necesitan minutos para instalar y configurar, y utiliza una base de datos Oracle real para generar patrones de E/S en un tablespace definido por el usuario. Es una de las pocas opciones de prueba disponibles que puede saturar una cabina all-flash con I/O. También es útil para generar

niveles mucho más bajos de I/O para simular cargas de trabajo de almacenamiento que son bajas IOPS, pero sensibles a la latencia.

Swingbench

Swingbench puede ser útil para probar el rendimiento de las bases de datos, pero es extremadamente difícil utilizar Swingbench de una manera que pone a prueba el almacenamiento. NetApp no ha observado ninguna prueba de Swingbench que haya producido suficientes I/O como para representar una carga significativa en ninguna cabina AFF. En casos limitados, la prueba de entrada de órdenes (OET) puede utilizarse para evaluar el almacenamiento desde un punto de vista de latencia. Esto podría ser útil en situaciones en las que una base de datos tiene una dependencia de latencia conocida para consultas particulares. Se debe tener precaución para asegurarse de que el host y la red estén correctamente configurados de modo que se puedan aprovechar las posibilidades de latencia de una cabina all-flash.

HammerDB

HammerDB es una herramienta de prueba de bases de datos que simula las pruebas TPC-C y TPC-H. Construir un conjunto de datos lo suficientemente grande puede llevar mucho tiempo para ejecutar correctamente una prueba, pero puede ser una herramienta eficaz para evaluar el rendimiento de las aplicaciones de almacén de datos y OLTP.

Orión

La herramienta Oracle Orion se usaba comúnmente con Oracle 9, pero no se ha mantenido para garantizar la compatibilidad con los cambios en varios sistemas operativos de host. Rara vez se utiliza con Oracle 10 u Oracle 11 debido a incompatibilidades con el sistema operativo y la configuración del almacenamiento.

Oracle reescribió la herramienta y se instala por defecto con Oracle 12c. Aunque este producto se ha mejorado y utiliza muchas de las mismas llamadas que utiliza una base de datos Oracle real, no utiliza exactamente la misma ruta de acceso de código o el comportamiento de E/S utilizado por Oracle. Por ejemplo, la mayoría de las operaciones de I/O de Oracle se realizan de forma síncrona, lo que significa que la base de datos se detiene hasta que la E/S se completa a medida que la operación de E/S se completa en primer plano. Un inundamiento simple de un sistema de almacenamiento con I/O aleatorias no es una reproducción de las operaciones de I/O de Oracle reales y no ofrece un método directo de comparar matrices de almacenamiento o medir el efecto de los cambios de configuración.

Dicho esto, existen algunos casos de uso de Orion, como la medición general del rendimiento máximo posible de una determinada configuración host-red-almacenamiento o para medir el estado de un sistema de almacenamiento. Con una cuidadosa realización de pruebas, podrían concebirse pruebas de Orion útiles para comparar cabinas de almacenamiento o evaluar el efecto de un cambio en la configuración, siempre y cuando los parámetros incluyan considerar la consideración de IOPS, el rendimiento y la latencia, y tratar de replicar fielmente una carga de trabajo realista.

NFSv3 bloqueos obsoletos

Si un servidor de base de datos Oracle se bloquea, es posible que tenga problemas con los bloqueos NFS obsoletos al reiniciar. Este problema se puede evitar prestando especial atención a la configuración de la resolución de nombres en el servidor.

Este problema surge porque la creación de un bloqueo y la eliminación de un bloqueo utilizan dos métodos ligeramente diferentes de resolución de nombres. Existen dos procesos, el Network Lock Manager (NLM) y el cliente NFS. El NLM utiliza `uname n` para determinar el nombre de host, mientras que el `rpc.statd` usos de procesos `gethostbyname()`. Estos nombres de host deben coincidir para que el sistema operativo borre correctamente los bloqueos obsoletos. Por ejemplo, es posible que el host esté buscando bloqueos propiedad

de `dbserver5`, pero las cerraduras fueron registradas por el anfitrión como `dbserver5.mydomain.org`. Si `gethostbyname()` no devuelve el mismo valor que `uname -a`, entonces el proceso de liberación de bloqueo no se ha realizado correctamente.

El siguiente script de ejemplo verifica si la resolución de nombres es totalmente coherente:

```
#! /usr/bin/perl
$uname=`uname -n`;
chomp($uname);
($name, $aliases, $addrtype, $length, @addrs) = gethostbyname $uname;
print "uname -n yields: $uname\n";
print "gethostbyname yields: $name\n";
```

Si `gethostbyname` no coincide `uname`, los bloqueos obsoletos son probables. Por ejemplo, este resultado revela un problema potencial:

```
uname -n yields: dbserver5
gethostbyname yields: dbserver5.mydomain.org
```

La solución se encuentra generalmente cambiando el orden en el que aparecen los hosts en `/etc/hosts`. Por ejemplo, supongamos que el archivo hosts incluye esta entrada:

```
10.156.110.201  dbserver5.mydomain.org dbserver5 loghost
```

Para resolver este problema, cambie el orden en el que aparecen el nombre de dominio completo y el nombre de host corto:

```
10.156.110.201  dbserver5 dbserver5.mydomain.org loghost
```

`gethostbyname()` ahora devuelve el corto `dbserver5` nombre de host, que coincide con la salida de `uname`. Por lo tanto, los bloqueos se borran automáticamente después de un fallo del servidor.

Verificación de la alineación de WAFL

La correcta alineación de WAFL es fundamental para un buen rendimiento. Aunque ONTAP gestiona bloques en 4KB unidades, este hecho no significa que ONTAP realice todas las operaciones en 4KB unidades. De hecho, ONTAP admite operaciones de bloque de diferentes tamaños, pero la contabilidad subyacente es administrada por WAFL en 4KB unidades.

El término “alineación” se refiere a cómo Oracle I/O corresponde a estas 4KB unidades. Para obtener un rendimiento óptimo, el bloque de 8KB KB de Oracle debe residir en dos bloques físicos de 4KB WAFL en una unidad. Si un bloque se equipara con 2KB, este bloque reside en la mitad de un bloque de 4KB KB, un 4KB bloque completo independiente y, a continuación, la mitad de un tercer bloque de 4KB KB. Esta disposición provoca una degradación del rendimiento.

La alineación no es un problema en los sistemas de archivos NAS. Los archivos de datos de Oracle se alinean con el inicio del archivo en función del tamaño del bloque de Oracle. Por lo tanto, los tamaños de bloque de 8KB, 16KB y 32KB se alinean siempre. Todas las operaciones de bloque se desplazan desde el inicio del archivo en unidades de 4 kilobytes.

Por el contrario, los LUN suelen contener algún tipo de encabezado de controlador o metadatos del sistema de archivos en su inicio que crea una desviación. La alineación rara vez es un problema en los sistemas operativos modernos, ya que estos sistemas operativos están diseñados para unidades físicas que podrían utilizar un sector nativo de 4KB, que también requiere que la E/S se alinee con los límites de 4KB para un rendimiento óptimo.

Sin embargo, hay algunas excepciones. Es posible que una base de datos se haya migrado desde un SO antiguo que no estaba optimizado para 4KB E/S, o que se haya producido un error de usuario durante la creación de la partición que podría haber producido un desplazamiento que no está en unidades de 4KB GB de tamaño.

Los siguientes ejemplos son específicos de Linux, pero el procedimiento se puede adaptar para cualquier sistema operativo.

Alineado

El siguiente ejemplo muestra una comprobación de alineación en una sola LUN con una partición única.

En primer lugar, cree la partición que utiliza todas las particiones disponibles en la unidad.

```
[root@host0 iscsi]# fdisk /dev/sdb
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF
disklabel
Building a new DOS disklabel with disk identifier 0xb97f94c1.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.
The device presents a logical sector size that is smaller than
the physical sector size. Aligning to a physical sector (or optimal
I/O) size boundary is recommended, or performance may be impacted.
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-10240, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-10240, default 10240):
Using default value 10240
Command (m for help): w
The partition table has been altered!
Calling ioctl() to re-read partition table.
Syncing disks.
[root@host0 iscsi]#
```

La alineación se puede comprobar matemáticamente con el siguiente comando:

```
[root@host0 iscsi]# fdisk -u -l /dev/sdb
Disk /dev/sdb: 10.7 GB, 10737418240 bytes
64 heads, 32 sectors/track, 10240 cylinders, total 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 65536 bytes
Disk identifier: 0xb97f94c1
   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1              32    20971519    10485744   83  Linux
```

La salida muestra que las unidades son de 512 bytes, y el inicio de la partición es de 32 unidades. Esto es un total de 32 x 512 = 16.834 bytes, que es un múltiplo completo de bloques de 4KB WAFL. Esta partición está correctamente alineada.

Para verificar la alineación correcta, lleve a cabo los siguientes pasos:

1. Identifique el identificador único universal (UUID) de la LUN.

```
FAS8040SAP::> lun show -v /vol/jfs_luns/lun0
              Vserver Name: jfs
                  LUN UUID: ed95d953-1560-4f74-9006-85b352f58fcd
                    Mapped: mapped`                `
```

2. Introduzca el shell del nodo en la controladora ONTAP.

```
FAS8040SAP::> node run -node FAS8040SAP-02
Type 'exit' or 'Ctrl-D' to return to the CLI
FAS8040SAP-02> set advanced
set not found.  Type '?' for a list of commands
FAS8040SAP-02> priv set advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp
         personnel.
```

3. Inicie recopilaciones estadísticas en el UUID de destino identificado en el primer paso.

```
FAS8040SAP-02*> stats start lun:ed95d953-1560-4f74-9006-85b352f58fcd
Stats identifier name is 'Ind0xffffff08b9536188'
FAS8040SAP-02*>
```

4. Realice algunas operaciones de I/O. Es importante utilizar el `iflag` Argumento para asegurarse de que la E/S es síncrona y no se almacena en búfer.

Tenga mucho cuidado con este comando. Inversión del `if` y.. `of` los argumentos destruyen los datos.

```
[root@host0 iscsi]# dd if=/dev/sdb1 of=/dev/null iflag=dsync count=1000
bs=4096
1000+0 records in
1000+0 records out
4096000 bytes (4.1 MB) copied, 0.0186706 s, 219 MB/s
```

5. Detenga las estadísticas y visualice el histograma de alineación. Todas las operaciones de I/O deben estar en la `.0` Bucket, que indica las I/O alineadas con un límite de bloque de 4KB KB.

```
FAS8040SAP-02*> stats stop
StatisticsID: Ind0xffffff08b9536188
lun:ed95d953-1560-4f74-9006-85b352f58fcd:instance_uuid:ed95d953-1560-
4f74-9006-85b352f58fcd
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.0:186%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.1:0%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.2:0%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.3:0%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.4:0%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.5:0%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.6:0%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.7:0%
```

Mal alineado

En el siguiente ejemplo, se muestran operaciones de I/O mal alineadas:

1. Cree una partición que no se alinee con un límite 4KB. Este no es el comportamiento predeterminado en los sistemas operativos modernos.

```
[root@host0 iscsi]# fdisk -u /dev/sdb
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First sector (32-20971519, default 32): 33
Last sector, +sectors or +size{K,M,G} (33-20971519, default 20971519):
Using default value 20971519
Command (m for help): w
The partition table has been altered!
Calling ioctl() to re-read partition table.
Syncing disks.
```

2. La partición se ha creado con un desplazamiento de 33 sectores en lugar del 32 por defecto. Repita el procedimiento descrito en "Alineado". El histograma aparece de la siguiente manera:

```
FAS8040SAP-02*> stats stop
StatisticsID: Ind0xffffff0468242e78
lun:ed95d953-1560-4f74-9006-85b352f58fcd:instance_uuid:ed95d953-1560-
4f74-9006-85b352f58fcd
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.0:0%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.1:136%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.2:4%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.3:0%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.4:0%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.5:0%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.6:0%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_align_histo.7:0%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:read_partial_blocks:31%
```

La desalineación es clara. La E/S cae principalmente en el* *`.1` período, que coincide con el desplazamiento esperado. Cuando se creó la partición, se movió 512 bytes más al dispositivo que el valor predeterminado optimizado, lo que significa que el histograma está compensado en 512 bytes.

Además, el `read_partial_blocks` La estadística es diferente de cero, lo que significa que se han realizado I/O que no han llenado todo un bloque de 4KB KB.

Registro de repetición

Los procedimientos que se explican aquí son aplicables a los archivos de datos. Los redo logs y archive logs de Oracle tienen patrones de E/S diferentes. Por ejemplo, redo log es una sobrescritura circular de un único archivo. Si se utiliza el tamaño predeterminado de bloque de 512 bytes, las estadísticas de escritura se ven algo así:

```
FAS8040SAP-02*> stats stop
StatisticsID: Ind0xffffff0468242e78
lun:ed95d953-1560-4f74-9006-85b352f58fcd:instance_uuid:ed95d953-1560-4f74-
9006-85b352f58fcd
lun:ed95d953-1560-4f74-9006-85b352f58fcd:write_align_histo.0:12%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:write_align_histo.1:8%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:write_align_histo.2:4%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:write_align_histo.3:10%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:write_align_histo.4:13%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:write_align_histo.5:6%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:write_align_histo.6:8%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:write_align_histo.7:10%
lun:ed95d953-1560-4f74-9006-85b352f58fcd:write_partial_blocks:85%
```

La E/S se distribuiría en todos los bloques de histograma, pero esto no supone un problema de rendimiento. Sin embargo, las tasas de redo-log extremadamente altas podrían beneficiarse del uso de un tamaño de bloque de 4KB KB. En este caso, es conveniente asegurarse de que los LUN de redo registro están alineados correctamente. Sin embargo, esto no es tan importante para un buen rendimiento como la alineación de archivos de datos.

PostgreSQL

Descripción general

PostgreSQL viene con variantes que incluyen PostgreSQL, PostgreSQL Plus y EDB Postgres Advanced Server (EPAS). PostgreSQL suele ponerse en marcha como base de datos de back-end para aplicaciones de varios niveles. Es compatible con paquetes de middleware comunes (como PHP, Java, Python, Tcl/Tk, ODBC, etc.). JDBC) y, desde siempre, ha sido una opción popular para los sistemas de gestión de bases de datos de código abierto. ONTAP es una opción excelente para ejecutar bases de datos PostgreSQL en cuanto a su fiabilidad, alto rendimiento y eficacia.

Esta documentación sobre ONTAP y la base de datos PostgreSQL reemplaza a la base de datos *TR-4770: PostgreSQL sobre las mejores prácticas de ONTAP.*

A medida que los datos crecen exponencialmente, la gestión de datos se vuelve más compleja para las empresas. Esta complejidad aumenta los costes de licencias, operaciones, soporte y mantenimiento. Para reducir el coste total de propiedad, considere la posibilidad de cambiar de bases de datos comerciales a bases de datos de código abierto con un almacenamiento de back-end fiable y de alto rendimiento.

ONTAP es una plataforma ideal, ya que ONTAP está literalmente diseñada para bases de datos. Numerosas funciones, como las optimizaciones de latencia de I/O aleatorias, pasando por una calidad de servicio avanzada o una funcionalidad FlexClone básica, se crearon específicamente para cubrir las necesidades de cargas de trabajo de bases de datos.

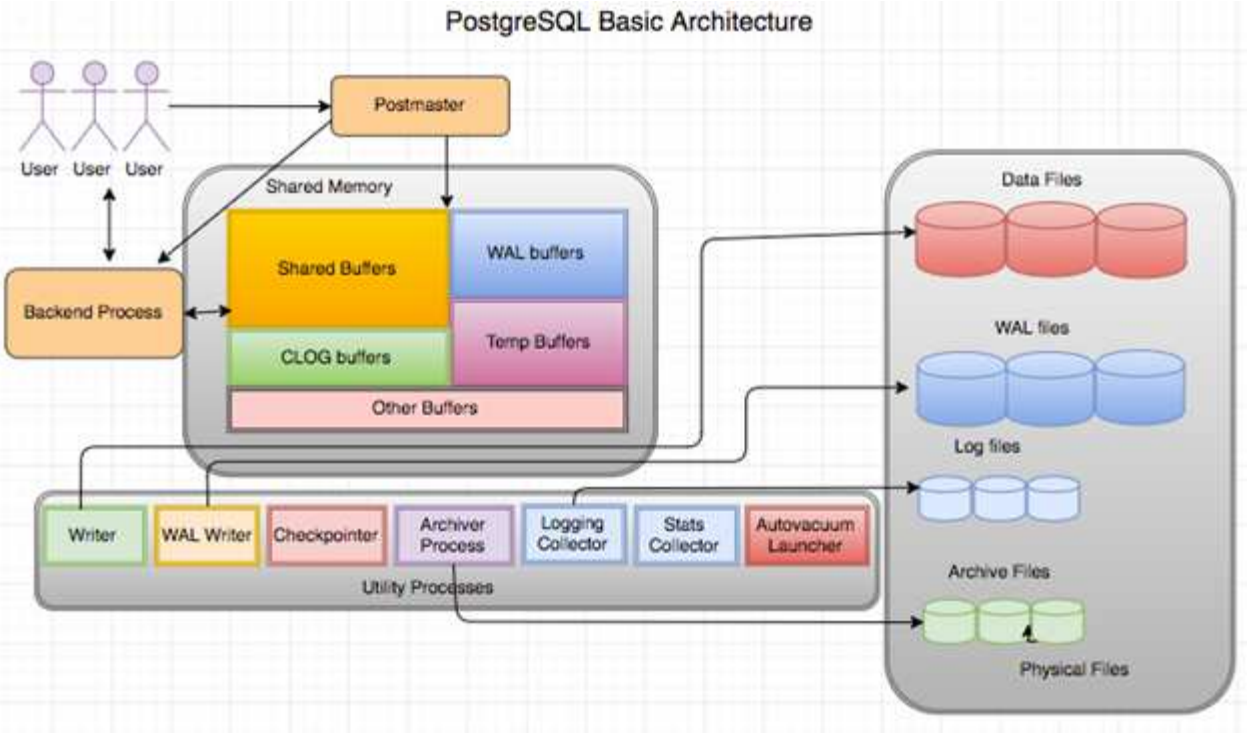
Otras funciones como las actualizaciones no disruptivas (entre ellas la sustitución de almacenamiento) garantizan que sus bases de datos cruciales seguirán estando disponibles. También se puede disponer de recuperación ante desastres instantánea para entornos grandes mediante MetroCluster o seleccionar bases de datos usando SnapMirror active sync.

Y lo que es más importante, ONTAP ofrece un rendimiento sin igual con la capacidad de dimensionar la solución en función de sus necesidades únicas. Nuestros sistemas de gama alta pueden ofrecer más de 1M 000 IOPS con latencias de microsegundos, pero si solo necesita 100K 000 IOPS, puede ajustar el tamaño de su solución de almacenamiento con una controladora más pequeña aún ejecutando exactamente el mismo sistema operativo de almacenamiento.

Configuración de la base de datos

Arquitectura

PostgreSQL es un RDBMS basado en la arquitectura de cliente y servidor. Una instancia PostgreSQL se conoce como un cluster de base de datos, que es una colección de bases de datos en lugar de una colección de servidores.



Hay tres elementos principales en una base de datos PostgreSQL: El postmaster, el front-end (cliente) y el back-end El cliente envía solicitudes al postmaster con información como el protocolo IP y a qué base de datos conectarse. El posmaster autentica la conexión y la pasa al proceso back-end para continuar la comunicación. El proceso back-end ejecuta la consulta y envía los resultados directamente al front-end (cliente).

Una instancia PostgreSQL se basa en un modelo multiproceso en lugar de un modelo multithread. Genera múltiples procesos para diferentes trabajos, y cada proceso tiene su propia funcionalidad. Los procesos principales incluyen el proceso del cliente, el proceso del escritor de WAL, el proceso del escritor en segundo plano y el proceso del puntero de control:

- Cuando un proceso de cliente (primer plano) envía solicitudes de lectura o escritura a la instancia de PostgreSQL, no lee ni escribe datos directamente en el disco. Primero almacena los datos en buffers compartidos y buffers de registro de escritura anticipada (WAL).
- Un proceso de escritor WAL manipula el contenido de los buffers compartidos y los buffers WAL para escribir en los logs WAL. Los registros WAL son normalmente registros de transacciones de PostgreSQL y se escriben secuencialmente. Por lo tanto, para mejorar el tiempo de respuesta de la base de datos, PostgreSQL primero escribe en los registros de transacciones y reconoce al cliente.
- Para poner la base de datos en un estado coherente, el proceso de escritor en segundo plano comprueba periódicamente el buffer compartido para ver si hay páginas sucias. A continuación, vacía los datos en los archivos de datos que se almacenan en volúmenes o LUN de NetApp.
- El proceso de puntero de control también se ejecuta periódicamente (con menos frecuencia que el proceso en segundo plano) e impide cualquier modificación en los buffers. Indica al proceso de escritor WAL que escriba y vacíe el registro de punto de control al final de los registros WAL que están almacenados en el disco NetApp. También indica al proceso de escritura en segundo plano que escriba y vacíe todas las páginas sucias en el disco.

Parámetros de inicialización

Cree un nuevo cluster de base de datos mediante `initdb` programa. An `initdb` script

crea los archivos de datos, las tablas del sistema y las bases de datos de plantilla (template0 y template1) que definen el cluster.

La base de datos de plantillas representa una base de datos de stock. Contiene definiciones para tablas del sistema, vistas estándar, funciones y tipos de dato. `pgdata` actúa como argumento para el `initdb` script que especifica la ubicación del cluster de base de datos.

Todos los objetos de base de datos en PostgreSQL son administrados internamente por los OIDs respectivos. Las tablas y los índices también se gestionan mediante OID individuales. Las relaciones entre los objetos de base de datos y sus respectivos OID se almacenan en las tablas de catálogo del sistema adecuadas, según el tipo de objeto. Por ejemplo, los OIDs de las bases de datos y las tablas de pila se almacenan en `pg_database` y `pg_class, respectivamente. Puede determinar los OID emitiendo consultas en el cliente PostgreSQL.

Cada base de datos tiene sus propias tablas individuales y archivos de índice que están restringidos a 1GB. Cada tabla tiene dos archivos asociados, sufijos respectivamente con `_fsm` y.. `_vm`. Se les conoce como el mapa de espacio libre y el mapa de visibilidad. Estos archivos almacenan la información sobre la capacidad de espacio libre y tienen visibilidad en cada página del archivo de tabla. Los índices solo tienen mapas de espacio libre individuales y no tienen mapas de visibilidad.

La `pg_xlog/pg_wal` el directorio contiene los logs de escritura anticipada. Los registros de escritura anticipada se utilizan para mejorar el rendimiento y la fiabilidad de las bases de datos. Cada vez que actualiza una fila en una tabla, PostgreSQL escribe primero el cambio en el registro de escritura anticipada y, más tarde, escribe las modificaciones en las páginas de datos reales en un disco. La `pg_xlog` el directorio normalmente contiene varios archivos, pero initdb crea solo el primero. Se añaden archivos adicionales según sea necesario. Cada archivo xlog tiene 16MB cm de longitud.

Configuración

Existen varias configuraciones de ajuste PostgreSQL que pueden mejorar el rendimiento.

Los parámetros más utilizados son los siguientes:

- `max_connections = <num>`: El número máximo de conexiones de base de datos que se deben tener al mismo tiempo. Use este parámetro para restringir el intercambio en disco y eliminar el rendimiento. En función de los requisitos de la aplicación, también puede ajustar este parámetro para la configuración del pool de conexiones.
- `shared_buffers = <num>`: El método más simple para mejorar el rendimiento de su servidor de base de datos. El valor por defecto es bajo para la mayoría del hardware moderno. Se establece durante la implementación en aproximadamente el 25% de la RAM disponible en el sistema. Esta configuración de parámetro varía según cómo funciona con instancias de base de datos concretas; es posible que tenga que aumentar y disminuir los valores por prueba y error. Sin embargo, es probable que si lo establece alto, el rendimiento se vea afectado.
- `effective_cache_size = <num>`: Este valor indica al optimizador de PostgreSQL cuánta memoria PostgreSQL tiene disponible para almacenar datos en caché y ayuda a determinar si se debe usar un índice. Un valor mayor aumenta la probabilidad de usar un índice. Este parámetro se debe definir en la cantidad de memoria asignada a. `shared_buffers` Más la cantidad de caché del sistema operativo disponible. A menudo, este valor supera el 50% de la memoria total del sistema.
- `work_mem = <num>`: Este parámetro controla la cantidad de memoria que se utilizará en las operaciones de ordenación y las tablas hash. Si realiza una clasificación intensiva en su aplicación, es posible que necesite aumentar la cantidad de memoria, pero tenga cuidado. No es un parámetro de todo el sistema, sino uno por operación. Si una consulta compleja tiene varias operaciones de ordenación en ella, utiliza

varias unidades de memoria work_mem, y varios back-ends podrían estar haciendo esto simultáneamente. Esta consulta a menudo puede hacer que el servidor de base de datos cambie si el valor es demasiado grande. Esta opción se llamaba anteriormente sort_mem en versiones anteriores de PostgreSQL.

- `fsync = <boolean> (on or off)`: Este parámetro determina si todas sus páginas WAL deben sincronizarse con el disco mediante el uso de fsync() antes de que se confirme una transacción. Desactivarlo puede mejorar el rendimiento de escritura y activarlo aumenta la protección frente al riesgo de daño cuando el sistema se bloquea.
- `checkpoint_timeout`: El proceso de punto de control vacía los datos confirmados en el disco. Esto implica una gran cantidad de operaciones de lectura/escritura en disco. El valor se establece en segundos y los valores más bajos disminuyen el tiempo de recuperación de fallos y el aumento de los valores puede reducir la carga en los recursos del sistema reduciendo las llamadas de punto de control. En función de la criticidad de la aplicación, el uso y la disponibilidad de la base de datos, defina el valor de checkpoint_timeout.
- `commit_delay = <num>` y.. `commit_siblings = <num>`: Estas opciones se utilizan juntas para ayudar a mejorar el rendimiento mediante la escritura de múltiples transacciones que se comprometen a la vez. Si hay varios objetos COMMIT_SIDBINGS activos en el momento en que la transacción se está confirmando, el servidor espera a COMMIT_DELAY microsegundos para intentar confirmar varias transacciones a la vez.
- `max_worker_processes / max_parallel_workers`: Configure el número óptimo de trabajadores para los procesos. Max_parallel_workers corresponde al Núm. De CPU disponibles. Dependiendo del diseño de la aplicación, las consultas pueden requerir un número menor de trabajadores para las operaciones en paralelo. Es mejor mantener el valor de ambos parámetros igual, pero ajustar el valor después de la prueba.
- `random_page_cost = <num>`: Este valor controla la forma en que PostgreSQL visualiza las lecturas de disco no secuenciales. Un valor más alto significa que PostgreSQL es más probable que use una exploración secuencial en lugar de una exploración de índice, lo que indica que su servidor tiene discos rápidos Modificar esta configuración después de evaluar otras opciones como optimización basada en planes, aspirar, indexar para alterar consultas o esquemas.
- `effective_io_concurrency = <num>`: Este parámetro establece el número de operaciones de E/S de disco simultáneas que PostgreSQL intenta ejecutar simultáneamente. Al aumentar este valor, aumenta el número de operaciones de I/O que cualquier sesión de PostgreSQL individual intenta iniciar en paralelo. El rango permitido es de 1 a 1.000, o cero para deshabilitar la emisión de solicitudes de E/S asíncronas. Actualmente, esta configuración sólo afecta a las exploraciones de pila de bitmap. Las unidades de estado sólido (SSD) y otro almacenamiento basado en memoria (NVMe) pueden procesar muchas solicitudes concurrentes, con lo que el mejor valor puede ser entre cientos.

Consulte la documentación de PostgreSQL para obtener una lista completa de los parámetros de configuración de PostgreSQL.

BRINDIS

TOAST es la sigla en inglés de la Técnica de Almacenamiento de Atributos Sobredimensionados. PostgreSQL utiliza un tamaño de página fijo (comúnmente 8KB) y no permite que las tuplas se abarquen varias páginas. Por lo tanto, no es posible almacenar valores de campo grandes directamente. Cuando intenta almacenar una fila que excede este tamaño, TOAST divide los datos de las columnas grandes en “pedazos” más pequeños y los almacena en una tabla de TOSTADAS.

Los grandes valores de atributos tostados se extraen (si se selecciona) solo en el momento en que se envía el conjunto de resultados al cliente. La tabla en sí es mucho más pequeña y puede caber más filas en la caché de buffers compartida de lo que podría sin ningún almacenamiento fuera de línea (TOSTADO).

VACÍO

En el funcionamiento normal de PostgreSQL, las tuplas que se eliminan o quedan obsoletas por una actualización no se eliminan físicamente de su tabla; permanecen presentes hasta que se ejecuta EL VACÍO. Por lo tanto, debe ejecutar EL VACÍO periódicamente, especialmente en tablas actualizadas con frecuencia. A continuación, se debe reclamar el espacio que ocupa para que las nuevas filas lo reutilicen, a fin de evitar la interrupción del espacio en disco. Sin embargo, no devuelve el espacio al sistema operativo.

El espacio libre dentro de una página no está fragmentado. EL VACÍO reescribe todo el bloque, empaquetando eficientemente las filas restantes y dejando un único bloque contiguo de espacio libre en una página.

Por el contrario, EL VACÍO COMPLETO compacta activamente las tablas escribiendo una versión completamente nueva del archivo de tabla sin espacio muerto. Esta acción minimiza el tamaño de la tabla, pero puede tardar mucho tiempo. También requiere espacio adicional en disco para la nueva copia de la tabla hasta que finalice la operación. El objetivo del VACÍO DE rutina es evitar la actividad COMPLETA DEL VACÍO. Este proceso no solo mantiene las tablas en su tamaño mínimo, sino que también mantiene el uso constante del espacio en disco.

Espacios de tabla

Al inicializar el cluster de la base de datos, se crean automáticamente dos tablespaces.

La `pg_global` el tablespace se utiliza para catálogos de sistemas compartidos. La `pg_default` tablespace es el tablespace por defecto de las bases de datos template1 y template0. Si la partición o el volumen en el que se inicializó el cluster se queda sin espacio y no se puede ampliar, se puede crear un tablespace en una partición diferente y utilizarlo hasta que se pueda volver a configurar el sistema.

Un índice muy utilizado se puede colocar en un disco rápido y de alta disponibilidad, como un dispositivo de estado sólido. Además, se puede almacenar una tabla que almacene datos archivados que no se utilizan con poca frecuencia o que no son críticos para el rendimiento en un sistema de disco menos costoso y más lento como las unidades SAS o SATA.

Los tablespaces forman parte del cluster de base de datos y no se pueden tratar como una recopilación autónoma de archivos de datos. Dependen de los metadatos contenidos en el directorio de datos principal y, por lo tanto, no se pueden asociar a otro clúster de base de datos ni realizar copias de seguridad individuales. Del mismo modo, si pierde un tablespace (mediante la supresión de archivos, fallos de disco, etc.), el cluster de base de datos puede volverse ilegible o no se puede iniciar. Colocar un tablespace en un sistema de archivos temporal como un disco RAM pone en riesgo la fiabilidad de todo el cluster.

Una vez creado, se puede utilizar un tablespace desde cualquier base de datos si el usuario solicitante tiene suficientes privilegios. PostgreSQL utiliza enlaces simbólicos para simplificar la implementación de tablespaces. PostgreSQL añade una fila al `pg_tablespace` Tabla (una tabla en todo el clúster) y asigna un nuevo identificador de objeto (OID) a esa fila. Por último, el servidor utiliza el OID para crear un enlace simbólico entre el cluster y el directorio dado. El directorio `$PGDATA/pg_tblspc` contiene enlaces simbólicos que apuntan a cada uno de los tablespaces no incorporados definidos en el cluster.

Configuración del almacenamiento

NFS

Las bases de datos PostgreSQL se pueden alojar en sistemas de archivos NFSv3 o NFSv4. La mejor opción depende de factores fuera de la base de datos.

Por ejemplo, el comportamiento de bloqueo NFSv4 puede ser preferible en ciertos entornos agrupados en clúster. (Consulte "aquí" para obtener más información).

De lo contrario, la funcionalidad de la base de datos debería ser casi idéntica, incluido el rendimiento. El único requisito es el uso del `hard` opción de montaje. Esto es necesario para garantizar que los tiempos de espera de software no produzcan errores de E/S irrecuperables.

Si se elige NFSv4 como protocolo, NetApp recomienda usar NFSv4,1. Existen algunas mejoras funcionales en el protocolo NFSv4 en NFSv4,1 que mejoran la resiliencia con respecto a la versión NFSv4,0.

Utilice las siguientes opciones de montaje para cargas de trabajo generales de bases de datos:

```
rw,hard,nointr,bg,vers=[3|4],proto=tcp,rsize=65536,wsize=65536
```

Si se esperan operaciones de I/O secuenciales pesadas, los tamaños de transferencia NFS pueden aumentar, tal como se describe en la siguiente sección.

Tamaños de transferencia de NFS

De forma predeterminada, ONTAP limita el tamaño de I/O de NFS a 64K.

La I/O aleatoria con la mayoría de aplicaciones y bases de datos utiliza un tamaño de bloque mucho más pequeño, que es muy inferior al máximo de 64K KB. Las operaciones de I/O de grandes bloques suelen estar en paralelo, por lo que el máximo de 64K KB tampoco se limita a obtener el ancho de banda máximo.

Hay algunas cargas de trabajo en las que el máximo de 64K crea una limitación. En particular, las operaciones de subproceso único como la operación de copia de seguridad o recuperación o una exploración de tabla completa de la base de datos se ejecutan de forma más rápida y eficiente si la base de datos puede realizar menos E/S pero más grandes. El tamaño óptimo de gestión de I/O para ONTAP es de 256K KB.

El tamaño de transferencia máximo para una SVM de ONTAP determinada se puede cambiar de la siguiente manera:

```
Cluster01::> set advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
Cluster01::*> nfs server modify -vserver vserver1 -tcp-max-xfer-size
262144
Cluster01::*>
```

> No reduzca nunca el tamaño máximo permitido de transferencia en ONTAP por debajo del valor de rsize/wsize de los sistemas de archivos NFS montados actualmente. Esto puede crear bloqueos o incluso corrupción de datos con algunos sistemas operativos. Por ejemplo, si los clientes NFS se establecen actualmente con un valor de rsize/wsize de 65536 000, el tamaño de transferencia máximo de ONTAP se podría ajustar entre 65536 000 y 1048576 000 sin que ello afecte a porque los propios clientes están limitados. Reducir el tamaño máximo de transferencia por debajo de 65536 puede dañar la disponibilidad o los datos.

Una vez que se aumenta el tamaño de transferencia en el nivel de ONTAP, se utilizarán las siguientes

opciones de montaje:

```
rw,hard,nointr,bg,vers=[3|4],proto=tcp,rsize=262144,wsize=262144
```

NFSv3 Tablas de ranuras TCP

Si NFSv3 se utiliza con Linux, es fundamental configurar correctamente las tablas de ranuras TCP.

Las tablas de ranuras TCP son equivalentes a NFSv3 a la profundidad de la cola del adaptador de bus de host (HBA). En estas tablas se controla el número de operaciones de NFS que pueden extraordinarias a la vez. El valor predeterminado suele ser 16, que es demasiado bajo para un rendimiento óptimo. El problema opuesto ocurre en los kernels más nuevos de Linux, que pueden aumentar automáticamente el límite de la tabla de ranuras TCP a un nivel que sature el servidor NFS con solicitudes.

Para obtener un rendimiento óptimo y evitar problemas de rendimiento, ajuste los parámetros del núcleo que controlan las tablas de ranuras TCP.

Ejecute el `sysctl -a | grep tcp.*.slot_table` command, y observe los siguientes parámetros:

```
# sysctl -a | grep tcp.*.slot_table
sunrpc.tcp_max_slot_table_entries = 128
sunrpc.tcp_slot_table_entries = 128
```

Todos los sistemas Linux deben incluir `sunrpc.tcp_slot_table_entries`, pero solo algunos incluyen `sunrpc.tcp_max_slot_table_entries`. Ambos deben establecerse en 128.

Si no se establecen estos parámetros, puede tener efectos significativos en el rendimiento. En algunos casos, el rendimiento es limitado porque el sistema operativo linux no está emitiendo suficiente I/O. En otros casos, las latencias de I/O aumentan cuando el sistema operativo linux intenta emitir más operaciones de I/O de las que se pueden mantener.

SAN

Las bases de datos PostgreSQL con SAN generalmente se alojan en sistemas de archivos xfs, pero otras se pueden usar si es compatible con el proveedor del sistema operativo

Mientras que una única LUN puede admitir por lo general hasta 100K 000 IOPS, las bases de datos con un gran volumen de I/O normalmente requieren el uso de LVM con segmentación.

Segmentación de LVM

Antes de la era de las unidades flash, se utilizaba la segmentación para ayudar a superar las limitaciones de rendimiento de las unidades giratorias. Por ejemplo, si un sistema operativo necesita realizar una operación de lectura de 1MB KB, para leer que 1MB TB de datos de una sola unidad se requeriría buscar y leer muchos cabezales de unidad ya que 1MB se transfiere lentamente. Si esos 1MB TB de datos se segmentaron en 8 LUN, el sistema operativo podría emitir ocho operaciones de lectura de 128K KB en paralelo y reducir el tiempo necesario para realizar la transferencia de 1MB GB.

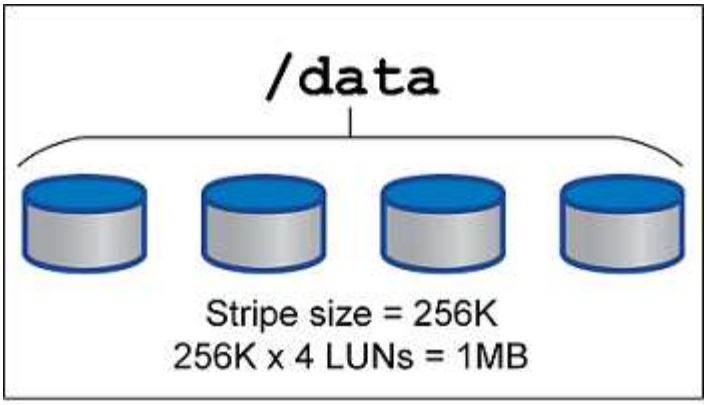
La segmentación con unidades giratorias era más difícil porque se tenía que conocer el patrón de I/O con anterioridad. Si la segmentación no se ajustó correctamente para los patrones de I/O reales, las configuraciones seccionadas podrían dañar el rendimiento. Con las bases de datos de Oracle y, especialmente con las configuraciones all-flash, la segmentación es mucho más fácil de configurar y se ha demostrado que mejora drásticamente el rendimiento.

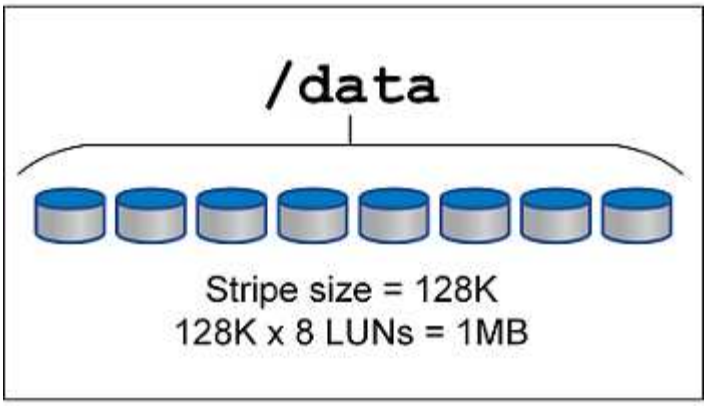
Los gestores de volúmenes lógicos como Oracle ASM segmentan por defecto, pero el LVM del sistema operativo nativo no lo hacen. Algunos de ellos unen varias LUN como un dispositivo concatenado, lo que da como resultado archivos de datos que existen en un único dispositivo LUN. Esto provoca puntos calientes. Otras implementaciones de LVM toman por defecto extensiones distribuidas. Esto es similar a la segmentación, pero es más grueso. Las LUN del grupo de volúmenes se dividen en partes grandes, denominadas extensiones y normalmente se miden en muchos megabytes, y los volúmenes lógicos se distribuyen por esas extensiones. El resultado es que las operaciones de I/O aleatorias en un archivo se deben distribuir bien entre las LUN, pero las operaciones de I/O secuenciales no son tan eficientes como podrían.

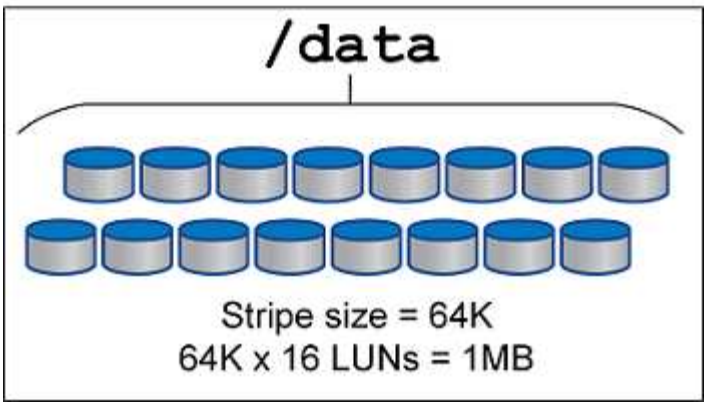
La I/O de aplicaciones con rendimiento intensivo casi siempre es una (a) en unidades del tamaño de bloque básico o (b) un megabyte.

El principal objetivo de una configuración seccionada es garantizar que la I/O de archivo único se pueda realizar como una unidad única y que las I/O de varios bloques, que deben tener un tamaño de 1MB TB, se puedan paralelizar de manera uniforme entre todas las LUN del volumen seccionado. Esto significa que el tamaño de franja no debe ser menor que el tamaño del bloque de la base de datos y el tamaño de franja multiplicado por el número de LUN debe ser 1MB.

En la siguiente figura, se muestran tres opciones posibles para el ajuste del tamaño de la franja y el ancho. Se selecciona el número de LUN para satisfacer los requisitos de rendimiento tal como se han descrito anteriormente, pero en todos los casos los datos totales de una sola franja es 1MB.







Protección de datos

Protección Ddta nativa

Uno de los principales aspectos del diseño del almacenamiento es permitir la protección para volúmenes PostgreSQL. Los clientes pueden proteger sus bases de datos PostgreSQL mediante el método de volcado o mediante copias de seguridad del sistema de archivos. Esta sección explica los diferentes enfoques para realizar una copia de seguridad de bases de datos individuales o de todo el cluster.

Existen tres enfoques para respaldar los datos de PostgreSQL:

- Volcado de SQL Server
- Backup de nivel de sistema de archivos

- Archivado continuo

La idea detrás del método de volcado de SQL Server es generar un archivo con comandos de SQL Server que, cuando se devuelve al servidor, pueda volver a crear la base de datos como estaba en el momento del volcado. PostgreSQL proporciona los programas de utilidad `pg_dump` y.. `pg_dump_all` para crear backup individual y a nivel de clúster. Estos volcados son lógicos y no contienen suficiente información para ser utilizada por WAL Replay.

Una estrategia de backup alternativa consiste en utilizar copias de seguridad a nivel de sistema de archivos, en las que los administradores copian directamente los archivos que PostgreSQL utiliza para almacenar los datos en la base de datos. Este método se realiza en modo offline: La base de datos o el cluster deben cerrarse. Otra alternativa es usar `pg_basebackup` Para ejecutar la copia de seguridad de transmisión en caliente de la base de datos PostgreSQL.

Snapshot

Las copias de seguridad basadas en instantáneas con PostgreSQL requieren la configuración de instantáneas para archivos de datos, archivos WAL y archivos WAL archivados para proporcionar una recuperación completa o puntual.

Para las bases de datos PostgreSQL, el tiempo promedio de backup con snapshots es de unos pocos segundos a unos pocos minutos. Esta velocidad de backup es entre 60 y 100 veces más rápida que `pg_basebackup` y otros enfoques de backup basados en sistemas de archivos.

Las copias Snapshot en el almacenamiento de NetApp pueden ser coherentes con los fallos y con las aplicaciones. Se crea una copia Snapshot coherente con los fallos en el almacenamiento sin desactivar la base de datos, mientras que se crea una copia Snapshot coherente con la aplicación mientras la base de datos está en modo de backup. NetApp también garantiza que las copias Snapshot posteriores sean backups permanentes para ahorrar en almacenamiento y mejorar la eficiencia de la red.

Como las copias Snapshot son rápidas y no afectan al rendimiento del sistema, puede programar varias copias Snapshot diariamente en lugar de crear un único backup diario, como ocurre con otra tecnología de backup en streaming. Cuando es necesaria una operación de restauración y recuperación, el tiempo de inactividad del sistema se reduce gracias a dos funciones clave:

- La tecnología de recuperación de datos de NetApp SnapRestore significa que la operación de restauración se ejecuta en segundos.
- Los objetivos de punto de recuperación agresivos (RPO) significan que es necesario aplicar menos registros de base de datos y que también se acelera la nueva recuperación.

Para realizar el backup de PostgreSQL, debe asegurarse de que los volúmenes de datos estén protegidos simultáneamente con WAL (grupo de consistencia) y los registros archivados. Mientras utiliza la tecnología Snapshot para copiar archivos WAL, asegúrese de ejecutar `pg_stop` Para vaciar todas las entradas de WAL que se deben archivar. Si vacíe las entradas DE WAL durante la restauración, solo tendrá que detener la base de datos, desmontar o eliminar el directorio de datos existente, y realizar una operación de SnapRestore en el almacenamiento. Una vez finalizada la restauración, puede montar el sistema y devolverlo a su estado actual. Para la recuperación point-in-time, también puede restaurar WAL y archive logs; luego PostgreSQL decide el punto más consistente y lo recupera automáticamente.

Los grupos de coherencia son una función en ONTAP y se recomienda cuando hay varios volúmenes montados en una sola instancia o en una base de datos con varios espacios de tabla. Una snapshot de grupo de coherencia garantiza que todos los volúmenes estén agrupados y protegidos. Un grupo de consistencia puede gestionarse de manera eficiente desde ONTAP System Manager, e incluso puede clonarlo para crear

una copia de instancia de una base de datos con fines de prueba o desarrollo.

Software para la protección de datos

El complemento de NetApp SnapCenter para base de datos de PostgreSQL, combinado con las tecnologías de Snapshot y FlexClone de NetApp, le ofrece ventajas como:

- Backup y restauración rápidos.
- Clones con gestión eficiente del espacio.
- La capacidad de crear un sistema de recuperación ante desastres rápido y eficaz.

> Puede que prefiera elegir los partners de backup premium de NetApp, como Veeam Software y Commvault, bajo las siguientes circunstancias:
>
> - Gestionar cargas de trabajo en un entorno heterogéneo
> - Almacenar backups en el cloud o en cinta para su retención a largo plazo
> - Soporte para una amplia gama de versiones y tipos de SO

El plugin de SnapCenter para PostgreSQL es un plugin de soporte comunitario y la configuración y documentación está disponible en la tienda de automatización de NetApp. Con SnapCenter, el usuario puede realizar backups de la base de datos, clonar y restaurar los datos remotamente.

SAP

VMware

VMware vSphere con ONTAP

VMware vSphere con ONTAP

ONTAP ha servido como solución de almacenamiento líder para VMware vSphere y, más recientemente, entornos de Cloud Foundation desde su introducción en el centro de datos moderno en 2002. Sigue introduciendo funciones innovadoras que simplifican la gestión y reducen los costes.

Este documento presenta la solución ONTAP para vSphere, donde se destaca la información de producto más reciente y las prácticas recomendadas para simplificar la puesta en marcha, mitigar los riesgos y simplificar la gestión.

> Esta documentación sustituye a los informes técnicos publicados anteriormente *TR-4597: VMware vSphere para ONTAP*

Las prácticas recomendadas complementan otros documentos, como guías y listas de compatibilidad. Se desarrollan según pruebas de laboratorio y una amplia experiencia de campo por parte de ingenieros y clientes de NetApp. Puede que no sean las únicas prácticas compatibles que funcionan en todos los entornos, pero suelen ser las soluciones más sencillas que satisfacen las necesidades de la mayoría de los clientes.

Este documento se centra en las funcionalidades de los lanzamientos recientes de ONTAP (9.x) ejecutados en vSphere 7,0 o posterior. Consulte la "Herramienta de matriz de interoperabilidad (IMT)" y "Guía de compatibilidad de VMware" para obtener detalles relacionados con versiones específicas.

¿Por qué elegir ONTAP para VMware vSphere?

Los clientes eligen con confianza ONTAP for vSphere para soluciones de almacenamiento SAN y NAS. La nueva arquitectura de almacenamiento desagregado simplificada, que se incluye en las últimas matrices All SAN, ofrece una experiencia simplificada familiar para los administradores de almacenamiento SAN y, al mismo tiempo, conserva la mayoría de las integraciones y el conjunto de características de los sistemas ONTAP tradicionales. Los sistemas ONTAP proporcionan una protección excepcional de instantáneas y herramientas de gestión sólidas. Al descargar funciones al almacenamiento dedicado, ONTAP maximiza los recursos del host, reduce costos y mantiene un rendimiento óptimo. Además, las cargas de trabajo se pueden migrar fácilmente mediante Storage vMotion a través de VMFS, NFS o vVols.

Las ventajas de usar ONTAP para vSphere

Hay muchas razones por las que decenas de miles de clientes han seleccionado ONTAP como solución de almacenamiento para vSphere, como un sistema de almacenamiento unificado que admite los protocolos SAN y NAS, sólidas funcionalidades de protección de datos mediante copias Snapshot con gestión eficiente del espacio y una gran cantidad de herramientas para ayudarle a gestionar los datos de aplicaciones. El uso de un sistema de almacenamiento independiente del hipervisor permite descargar numerosas funciones y maximizar su inversión en sistemas de host vSphere. Este método no solo garantiza que los recursos del host se centren en las cargas de trabajo de las aplicaciones, sino que también evita efectos de rendimiento

aleatorios en las aplicaciones de operaciones de almacenamiento.

El uso de ONTAP junto con vSphere es una excelente combinación que le permite reducir los gastos de hardware del host y software VMware. También puede proteger sus datos a un menor coste y con un alto rendimiento constante. Debido a que las cargas de trabajo virtualizadas son móviles, puede explorar diferentes enfoques usando Storage vMotion para mover máquinas virtuales entre almacenes de datos VMFS, NFS o vVols , todo en el mismo sistema de almacenamiento.

Estos son los factores clave que los clientes valoran hoy en día:

- **Almacenamiento unificado.** Los sistemas que ejecutan ONTAP están unificados de varias maneras importantes. Originalmente, este enfoque se refería a los protocolos NAS y SAN, y ONTAP continúa siendo una plataforma líder para SAN, junto con su fortaleza original en NAS. En el mundo vSphere, este enfoque también podría significar un sistema unificado para la infraestructura de escritorio virtual (VDI) junto con la infraestructura de servidor virtual (VSI). Los sistemas que ejecutan ONTAP suelen ser menos costosos para VSI que las matrices empresariales tradicionales y, además, tienen capacidades avanzadas de eficiencia de almacenamiento para manejar VDI en el mismo sistema. ONTAP también unifica una variedad de medios de almacenamiento, desde SSD hasta SATA, y puede extenderlo fácilmente a la nube. No es necesario comprar un sistema operativo de almacenamiento para el rendimiento, otro para los archivos y otro más para la nube. ONTAP los une a todos.
- **Cabina All SAN (ASA).** Los sistemas de ONTAP ASA más recientes (a partir de A1K, A90, A70, A50, A30 y A20) se basan en una nueva arquitectura de almacenamiento que elimina el paradigma de almacenamiento tradicional de ONTAP relativo a la gestión de agregados y volúmenes. Como no hay recursos compartidos del sistema de archivos, no se necesitan volúmenes. Todo el almacenamiento conectado a un par de alta disponibilidad se trata como una zona de disponibilidad de almacenamiento común (SAZ) dentro de la que los LUN y los espacios de nombres de NVMe se aprovisionan como «unidades de almacenamiento» (SUS). Los últimos sistemas ASA han sido diseñados para ser fáciles de gestionar, gracias a una experiencia familiar para los administradores de almacenamiento SAN. Esta nueva arquitectura es ideal para entornos de vSphere, ya que permite una gestión sencilla de los recursos de almacenamiento y ofrece una experiencia simplificada para los administradores de almacenamiento SAN. La arquitectura de ASA también es compatible con la tecnología NVMe over Fabrics (NVMe-oF) más reciente, que proporciona un rendimiento y una escalabilidad aún mayores para las cargas de trabajo de vSphere.
- **Tecnología Snapshot.** ONTAP fue el primero en ofrecer tecnología Snapshot para la protección de datos y sigue siendo la más avanzada en el sector. Este método de protección de datos con un uso eficiente del espacio se ha ampliado para dar soporte a las API de VMware vSphere para la integración de cabinas (VAAI). Esta integración le permite aprovechar las capacidades Snapshot de ONTAP en las operaciones de backup y restauración, y reducir el impacto en su entorno de producción. Este método también permite utilizar copias Snapshot para una rápida recuperación de equipos virtuales, lo que reduce el tiempo y el esfuerzo necesarios para restaurar datos. Además, la tecnología Snapshot de ONTAP se integra con las soluciones Live Site Recovery (VLSR, anteriormente Site Recovery Manager [SRM]) de VMware, por lo que proporciona una estrategia de protección de datos completa para su entorno virtualizado.
- **Volúmenes virtuales y gestión de almacenamiento basada en políticas.** NetApp fue uno de los primeros socios de diseño de VMware en el desarrollo de vSphere Virtual Volumes (vVols), aportando información arquitectónica y soporte temprano para vVols y VMware vSphere API for Storage Awareness (VASA). Este enfoque no solo aportó una gestión granular del almacenamiento de máquinas virtuales a VMFS, sino que también respaldó la automatización del aprovisionamiento de almacenamiento a través de una gestión de almacenamiento basada en políticas. Este enfoque permite a los arquitectos de almacenamiento diseñar grupos de almacenamiento con diferentes capacidades que los administradores de máquinas virtuales pueden utilizar fácilmente. ONTAP lidera la industria del almacenamiento en escala vVol, y admite cientos de miles de vVols en un solo clúster, mientras que los proveedores de matrices empresariales y matrices flash más pequeñas admiten tan solo varios miles de vVols por matriz. NetApp también está impulsando la evolución de la gestión granular de máquinas virtuales con sus próximas

capacidades.

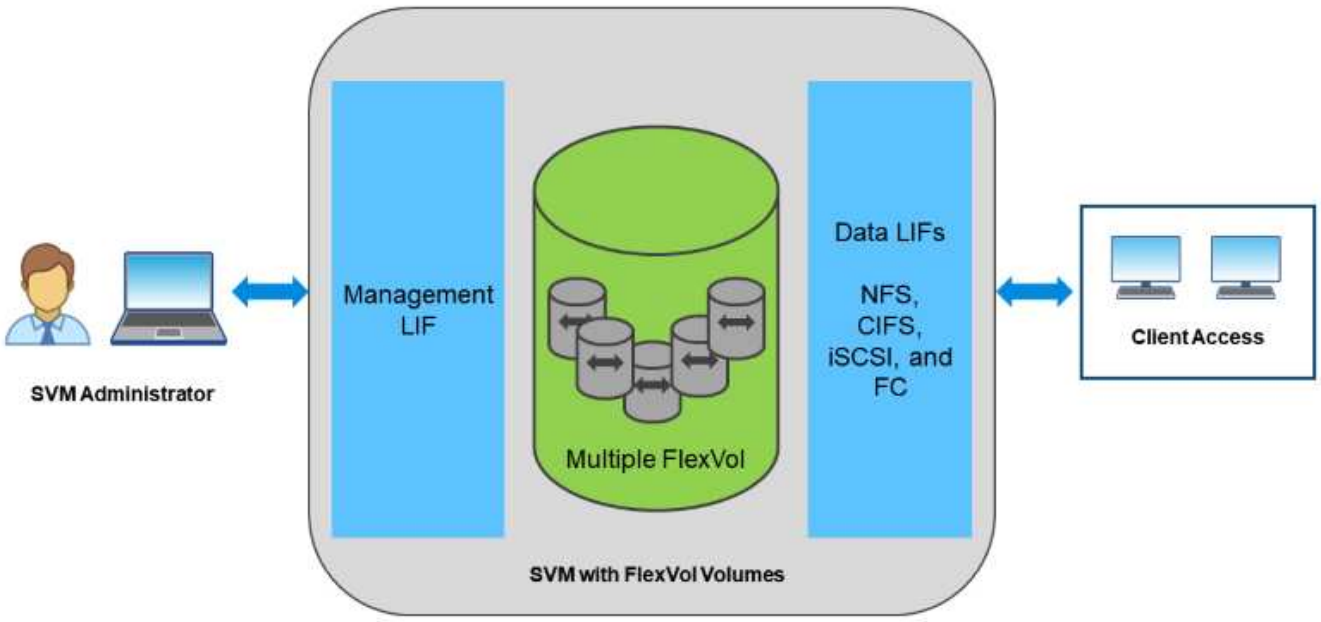
- **Eficiencia de almacenamiento.** Si bien NetApp fue el primero en ofrecer deduplicación para cargas de trabajo de producción, esta innovación no fue la primera ni la última en esta área. Todo comenzó con instantáneas, un mecanismo de protección de datos que ahorra espacio y no afecta el rendimiento, junto con la tecnología FlexClone para hacer instantáneamente copias de lectura y escritura de máquinas virtuales para uso en producción y respaldo. NetApp continuó ofreciendo capacidades en línea, incluidas deduplicación, compresión y deduplicación de bloque cero, para aprovechar al máximo el almacenamiento de los costosos SSD. ONTAP también agregó la capacidad de empaquetar operaciones de E/S y archivos más pequeños en un bloque de disco usando compactación. La combinación de estas capacidades ha permitido que los clientes experimenten comúnmente ahorros de hasta 5:1 para VSI y hasta 30:1 para VDI. La última generación de sistemas ONTAP también incluye compresión y deduplicación aceleradas por hardware, lo que puede mejorar aún más la eficiencia del almacenamiento y reducir los costos. Este enfoque permite almacenar más datos en menos espacio, lo que reduce el costo general de almacenamiento y mejora el rendimiento. NetApp confía tanto en sus capacidades de eficiencia de almacenamiento que ofrece un enlace: https://www.netapp.com/pdf.html?item=/media/79014-ng-937-Efficiency-Guarantee-Customer-Flyer.pdf [Garantía de eficiencia^].
- **Multitenencia.** ONTAP ha sido durante mucho tiempo líder en multitenencia, lo que le permite crear múltiples máquinas virtuales de almacenamiento (SVM) en un solo clúster. Este enfoque le permite aislar cargas de trabajo y brindar diferentes niveles de servicio a diferentes inquilinos, lo que lo hace ideal para proveedores de servicios y grandes empresas. La última generación de sistemas ONTAP también incluye soporte para la gestión de la capacidad de los inquilinos. Esta función le permite establecer límites de capacidad para cada inquilino, garantizando que ningún inquilino pueda consumir todos los recursos disponibles. Este enfoque ayuda a garantizar que todos los inquilinos reciban el nivel de servicio que esperan, al tiempo que proporciona un alto nivel de seguridad y aislamiento entre ellos. Además, las capacidades multitenencia de ONTAP están integradas con la plataforma vSphere de VMware, lo que le permite administrar y monitorear fácilmente su entorno virtualizado a través de "Herramientas de ONTAP para VMware vSphere" y "Información sobre la infraestructura de datos" .
- **Nube híbrida.** Ya sea que se utilicen para una nube privada local, una infraestructura de nube pública o una nube híbrida que combina lo mejor de ambas, las soluciones ONTAP lo ayudan a construir su estructura de datos para agilizar y optimizar la administración de datos. Comience con sistemas all-flash de alto rendimiento y luego combínelos con sistemas de almacenamiento en disco o en la nube para la protección de datos y la computación en la nube. Elija entre Azure, AWS, IBM o Google Cloud para optimizar costos y evitar la dependencia. Aproveche el soporte avanzado para OpenStack y tecnologías de contenedores según sea necesario. NetApp también ofrece copias de seguridad basadas en la nube (SnapMirror Cloud, Cloud Backup Service y Cloud Sync) y herramientas de archivado y niveles de almacenamiento (FabricPool) para ONTAP para ayudar a reducir los gastos operativos y aprovechar el amplio alcance de la nube.
- **Y mucho más.** saque partido del rendimiento extremo de las cabinas AFF A-Series de NetApp para acelerar su infraestructura virtualizada a la vez que gestiona los costes. Disfrute de operaciones no disruptivas, desde el mantenimiento hasta las actualizaciones, pasando por la sustitución completa de su sistema de almacenamiento, mediante clústeres ONTAP de escalado horizontal. Proteja los datos en reposo con funcionalidades de cifrado de NetApp sin coste adicional. Asegúrese de que el rendimiento cumple los niveles de servicio empresarial a través de funcionalidades de calidad de servicio de gran precisión. Todos ellos forman parte de la amplia gama de funcionalidades que incluyen ONTAP, el software para la gestión de datos empresariales líder del sector.

Almacenamiento unificado

ONTAP unifica el almacenamiento mediante un enfoque simplificado definido por software para una gestión segura y eficiente, un rendimiento mejorado y una escalabilidad fluida. Este enfoque mejora la protección de datos y permite usar eficazmente los recursos cloud.

En un principio, este método unificado hacía referencia a la compatibilidad de los protocolos NAS y SAN en un solo sistema de almacenamiento, y ONTAP sigue siendo una plataforma líder para SAN junto con su solidez original en NAS. ONTAP ahora también ofrece compatibilidad con el protocolo de objetos S3. Aunque S3 no se utiliza para almacenes de datos, puede usarlo para aplicaciones «in-guest». Puede obtener más información sobre la compatibilidad con el protocolo S3 en ONTAP en el "Información general de la configuración de S3". El término almacenamiento unificado ha evolucionado para suponer un método unificado de la gestión del almacenamiento que incluye la capacidad de gestionar todos tus recursos de almacenamiento desde una única interfaz. Esto incluye la capacidad de gestionar recursos de almacenamiento en cloud y en las instalaciones, los sistemas de cabinas All SAN (ASA) más recientes y la capacidad de gestionar varios sistemas de almacenamiento desde una única interfaz.

Una máquina virtual de almacenamiento (SVM) es la unidad de multi-tenancy seguro en ONTAP. Es una construcción lógica que permite al cliente acceder a los sistemas que ejecutan ONTAP. Las SVM pueden servir datos de forma simultánea mediante varios protocolos de acceso a los datos a través de interfaces lógicas (LIF). Los SVM proporcionan acceso a los datos de nivel de archivo mediante protocolos NAS, como CIFS y NFS, y acceso a datos de nivel de bloque mediante protocolos SAN, como iSCSI, FC/FCoE y NVMe. Los SVM pueden servir datos a clientes SAN y NAS de forma independiente a la vez, así como con S3.



En el mundo de vSphere, este enfoque también podría significar un sistema unificado para una infraestructura de puestos de trabajo virtuales (VDI) junto con una infraestructura de servidores virtuales (VSI). Los sistemas que ejecutan ONTAP suelen ser más económicos para VSI que las cabinas empresariales tradicionales y, al mismo tiempo, cuentan con funcionalidades de eficiencia del almacenamiento avanzadas para gestionar VDI en el mismo sistema. ONTAP también unifica varios medios de almacenamiento, desde SSD a SATA, y puede ampliarlos fácilmente al cloud. No es necesario comprar una cabina flash para el rendimiento, una cabina SATA para archivos y sistemas independientes para la nube. ONTAP los une a todos.

NOTA: Para obtener más información sobre SVM, almacenamiento unificado y acceso de clientes, consulte "Virtualización del almacenamiento" En el centro de documentación de ONTAP 9.

Herramientas de virtualización para ONTAP

NetApp proporciona varias herramientas de software independientes compatibles con sistemas ONTAP y ASA tradicionales, integrando vSphere para administrar de forma eficaz su entorno virtualizado.

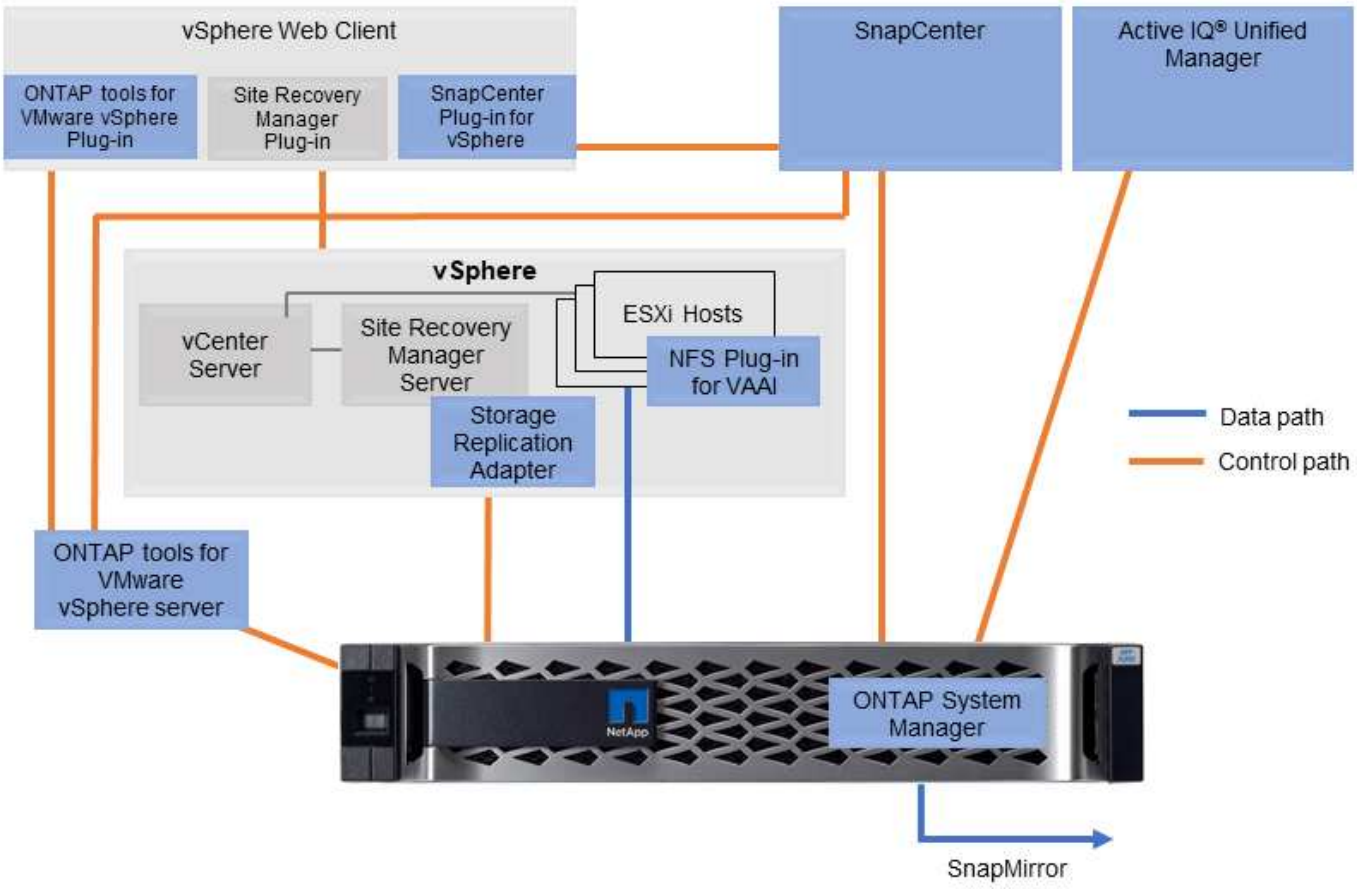
Las siguientes herramientas están incluidas con la licencia ONTAP One sin coste adicional. Consulte la figura 1 para obtener una descripción de cómo funcionan estas herramientas juntas en su entorno vSphere.

Herramientas de ONTAP para VMware vSphere

"Herramientas de ONTAP para VMware vSphere" Es un conjunto de herramientas para usar el almacenamiento de ONTAP junto con vSphere. El complemento de vCenter, anteriormente conocido como Virtual Storage Console (VSC), simplifica las funciones de gestión y eficiencia del almacenamiento, mejora la disponibilidad y reduce los costes de almacenamiento y la sobrecarga operativa, tanto si usa SAN como NAS. Utiliza prácticas recomendadas para aprovisionar almacenes de datos y optimiza la configuración de host ESXi para entornos de almacenamiento en bloques y NFS. Para obtener todos estos beneficios, NetApp recomienda el uso de estas herramientas de ONTAP como mejor práctica al utilizar vSphere con sistemas que ejecuten ONTAP. Incluye un dispositivo de servidor, extensiones de interfaz de usuario para vCenter, VASA Provider y Storage Replication Adapter. Casi todo lo que incluye las herramientas de ONTAP se puede automatizar mediante API de REST sencillas, consumibles gracias a las herramientas de automatización más modernas.

- **Extensiones de la interfaz de usuario de vCenter.** Las extensiones de interfaz de usuario de las herramientas de ONTAP simplifican el trabajo de los equipos de operaciones y los administradores de vCenter al integrar menús contextuales fáciles de usar para gestionar hosts y almacenamiento, portlets informativos y funcionalidades de alertas nativas directamente en la interfaz de usuario de vCenter para flujos de trabajo optimizados.
- **Proveedor VASA para ONTAP.** el Proveedor VASA para ONTAP es compatible con el marco de trabajo VMware vStorage APIs for Storage Awareness (VASA). Se suministra como parte de las herramientas de ONTAP para VMware vSphere como un dispositivo virtual único para facilitar la puesta en marcha. EL proveedor DE VASA conecta vCenter Server con ONTAP para ayudar en el aprovisionamiento y la supervisión del almacenamiento de máquinas virtuales. Permite el soporte de VMware Virtual Volumes (vVols), la gestión de los perfiles de las funcionalidades del almacenamiento y el rendimiento vVols individual, y las alarmas para supervisar la capacidad y el cumplimiento de los perfiles.
- **Adaptador de Replicación de Almacenamiento.** El SRA se utiliza junto con Live Site Recovery (VLSR)/Site Recovery Manager (SRM) de VMware para gestionar la replicación de datos entre sitios de producción y de recuperación ante desastres mediante SnapMirror para la replicación basada en cabinas. Puede automatizar la tarea de conmutación al nodo de respaldo en caso de desastre y ayudar a probar las réplicas de recuperación ante desastres sin interrupciones para garantizar la confianza en su solución de recuperación ante desastres.

La figura siguiente muestra las herramientas de ONTAP para vSphere.



Complemento de SnapCenter para VMware vSphere

El "Complemento de SnapCenter para VMware vSphere" es un plugin para vCenter Server que permite gestionar backups y restauraciones de máquinas virtuales (VM) y almacenes de datos. Proporciona una única interfaz para gestionar backups, restauraciones y clones de equipos virtuales y almacenes de datos en varios sistemas de ONTAP. SnapCenter admite la replicación y la recuperación desde sitios secundarios mediante SnapMirror. Las últimas versiones también admiten SnapMirror a la nube (S3), copias Snapshot a prueba de manipulaciones, SnapLock y sincronización activa de SnapMirror. El Plugin de SnapCenter para VMware vSphere puede integrarse con complementos de aplicaciones SnapCenter con el fin de proporcionar backups consistentes con las aplicaciones.

Plugin NFS para VAAI de VMware

El "Plugin NFS de NetApp para VAAI de VMware" es un plugin para hosts ESXi que permite utilizar funciones VAAI con almacenes de datos NFS en ONTAP. Es compatible con copias de descarga para operaciones de clonado, reserva de espacio para archivos de disco virtual gruesos y descarga de copias Snapshot. La descarga de operaciones de copia en el almacenamiento no es necesariamente más rápida de completarse, pero reduce los requisitos de ancho de banda de red y libera a recursos del host, como ciclos de CPU, búferes y colas. Puede usar las herramientas de ONTAP para VMware vSphere para instalar el plugin en hosts ESXi o, si es compatible, vSphere Lifecycle Manager (VLCM).

Opciones de software premium

Los siguientes productos de software premium están disponibles en NetApp. No se incluyen con la licencia de ONTAP One y deben adquirirse por separado. * "Recuperación tras siniestros (DR) de BlueXP " Para VMware vSphere. Este es un servicio basado en la nube que proporciona recuperación ante desastres y backup para entornos de VMware. Puede utilizarse con o sin SnapCenter y admite la recuperación ante desastres de las

instalaciones a las instalaciones usando SAN o NAS, y on-premises hacia/desde la nube utilizando NFS donde es compatible. * "Información sobre la infraestructura de datos (DII)". Es un servicio basado en la nube que proporciona supervisión y análisis para entornos de VMware. Admite otros proveedores de almacenamiento en entornos de almacenamiento heterogéneos, así como varios proveedores de switches y otros hipervisores. DII proporciona información completa e integral sobre el rendimiento, la capacidad y el estado de su entorno VMware.

Volúmenes virtuales (vVols) y gestión basada en políticas de almacenamiento (SPBM)

Anunciada por primera vez en 2012, NetApp fue un partner de diseño temprano con VMware en el desarrollo de VMware vSphere APIs for Storage Awareness (VASA), la base de la gestión basada en políticas de almacenamiento (SPBM) con cabinas de almacenamiento empresarial. Este enfoque trajo una gestión granular del almacenamiento de las máquinas virtuales limitada al almacenamiento de VMFS y NFS.

Como partner de diseño tecnológico, NetApp proporcionó información sobre la arquitectura y en 2015 anunció la compatibilidad con vVols. Esta nueva tecnología ahora permitió la automatización del aprovisionamiento de almacenamiento granular de equipos virtuales y realmente nativo de la cabina a través de SPBM.

Volúmenes virtuales (vVols)

Los vVols son una revolucionaria arquitectura de almacenamiento que permite gestionar el almacenamiento de forma granular de las máquinas virtuales y no solo por equipo virtual (incluidos los metadatos de las máquinas virtuales), sino incluso por VMDK. Los vVols son un componente clave de la estrategia de centro de datos definido por software (SDDC) que forma la base de VMware Cloud Foundation (VCF), lo que proporciona una arquitectura de almacenamiento más eficiente y escalable para entornos virtualizados.

VVols permite que las máquinas virtuales consuman almacenamiento por equipo virtual, ya que cada objeto de almacenamiento de equipo virtual es una entidad única en NetApp ONTAP. En los sistemas ASA R2 que ya no requieren gestión de volúmenes, esto significa que cada objeto de almacenamiento de VM es una única unidad de almacenamiento (SU) en la matriz que se puede controlar de forma independiente. De este modo, se pueden crear normativas de almacenamiento que se pueden aplicar a VMDK o máquinas virtuales individuales (y, por lo tanto, SUS indivudual), lo que proporciona un control granular sobre los servicios de almacenamiento como el rendimiento, la disponibilidad y la protección de datos.

Gestión basada en la política de almacenamiento (SPBM)

La SPBM proporciona un marco que funciona como capa de abstracción entre los servicios de almacenamiento disponibles para su entorno de virtualización y los elementos de almacenamiento aprovisionados mediante políticas. Este método permite a los arquitectos de almacenamiento diseñar pools de almacenamiento con diferentes funcionalidades. Los administradores de equipos virtuales pueden consumir fácilmente estos pools. De este modo, los administradores pueden ajustar los requisitos de las cargas de trabajo de las máquinas virtuales con los pools de almacenamiento aprovisionados. Este enfoque simplifica la gestión del almacenamiento y permite usar los recursos de almacenamiento de forma más eficiente.

El SPBM es un componente clave de vVols, que ofrece un marco basado en normativas para gestionar los servicios de almacenamiento. Los administradores de vSphere crean políticas usando reglas y funcionalidades expuestas por el proveedor de VASA (VP) del proveedor. Es posible crear políticas para diferentes servicios de almacenamiento, tales como rendimiento, disponibilidad y protección de datos. Las políticas se pueden asignar a máquinas virtuales o VMDK individuales, lo que proporciona control granular sobre los servicios de almacenamiento.

NetApp ONTAP y vVols

NetApp ONTAP lidera la industria del almacenamiento en vVols Scale, que admite cientos de miles de vVols en un único clúster*. Por el contrario, las cabinas empresariales y los proveedores de cabinas Flash más pequeños admiten hasta varios miles de vVols por cabina. ONTAP proporciona una solución de almacenamiento escalable y eficiente para entornos VMware vSphere que admite vVols con un amplio conjunto de servicios de almacenamiento, que incluye deduplicación de datos, compresión, thin provisioning y protección de datos. SPBM permite una integración perfecta con entornos VMware vSphere.

Anteriormente ya hemos mencionado que los administradores de equipos virtuales pueden consumir capacidad como pools de almacenamiento. Esto se realiza mediante el uso de contenedores de almacenamiento que se representan en vSphere como almacenes de datos lógicos.

Los contenedores de almacenamiento los crean los administradores de almacenamiento y se utilizan para agrupar los recursos de almacenamiento que pueden consumir los administradores de las máquinas virtuales. Los contenedores de almacenamiento se pueden crear de forma diferente en función del tipo de sistema ONTAP que use. Con los clústeres tradicionales de ONTAP 9, se asignan a los contenedores uno o varios volúmenes FlexVol de respaldo que, juntos, forman el pool de almacenamiento. Con los sistemas R2 de ASA, el clúster entero es el pool de almacenamiento.

Para obtener más información sobre VMware vSphere Virtual Volumes, SPBM y ONTAP, consulte "TR-4400: VMware vSphere Virtual Volumes con ONTAP".

*Dependiendo de la plataforma y el protocolo

Almacenes de datos y protocolos

Información general sobre las funciones de protocolo y almacenes de datos de vSphere

Se utilizan seis protocolos para conectar VMware vSphere a almacenes de datos en un sistema que ejecuta ONTAP:

- FCP
- NVMe/FC
- NVMe/TCP
- ISCSI
- NFS v3
- NFS v4,1

FCP, NVMe/FC, NVMe/TCP e iSCSI son protocolos de bloque que utilizan el sistema de archivos de máquina virtual de vSphere (VMFS) para almacenar máquinas virtuales dentro de LUN de ONTAP o espacios de nombres de NVMe que se encuentran en un ONTAP FlexVol volume. NFS es un protocolo de archivos que coloca equipos virtuales en almacenes de datos (que son simplemente volúmenes de ONTAP) sin necesidad de VMFS. SMB (CIFS), iSCSI, NVMe/TCP o NFS también se puede utilizar directamente de un sistema operativo invitado a ONTAP.

Las siguientes tablas presentan funciones de almacén de datos tradicionales compatibles con vSphere con ONTAP. Esta información no se aplica a almacenes de datos vVols, pero, generalmente, se aplica a vSphere 6.x y versiones posteriores mediante versiones ONTAP compatibles. También se puede consultar el "Herramienta VMware Configuration Maximums" para conocer versiones de vSphere específicas para confirmar límites específicos.

Característica/función	FC	ISCSI	NVMe-of	NFS
Formato	Asignación de dispositivo sin formato (RDM) o VMFS	VMFS o RDM	VMFS	n.a.
Número máximo de almacenes de datos o LUN	1024 LUN por host	1024 LUN por servidor	256 nombres por servidor	256 conexiones NFS por host (afectadas por nconnect y trunking de sesiones) NFS predeterminado. MaxVolumes tiene 8 años. Utilice las herramientas de ONTAP para VMware vSphere para aumentar a 256.
Tamaño máximo de almacén de datos	64 TB	64 TB	64 TB	300 TB de volumen FlexVol o superior con volumen FlexGroup
Tamaño máximo de archivo del almacén de datos	62 TB	62 TB	62 TB	62TB con ONTAP 9.12.1P2 y posterior
Profundidad de cola óptima por LUN o sistema de archivos	64-256	64-256	Autonegociar	Consulte NFS.MaxQueueDepth en "Host ESXi recomendado y otra configuración de ONTAP".

En la siguiente tabla se enumeran las funcionalidades relacionadas con el almacenamiento de VMware admitidas.

Capacidad/función	FC	ISCSI	NVMe-of	NFS
VMotion	Sí	Sí	Sí	Sí
VMotion de almacenamiento	Sí	Sí	Sí	Sí
Ha de VMware	Sí	Sí	Sí	Sí
Planificador de recursos distribuidos de almacenamiento (SDRS)	Sí	Sí	Sí	Sí

Capacidad/función	FC	ISCSI	NVMe-of	NFS
Software de backup habilitado para VMware vStorage APIs for Data Protection (VADP)	Sí	Sí	Sí	Sí
Microsoft Cluster Service (MSCS) o clustering de recuperación tras fallos en un equipo virtual	Sí	Sí [1]	Sí [1]	No admitido
Tolerancia a fallos	Sí	Sí	Sí	Sí
Recuperación de sitios activos/Gestor de recuperación de sitios	Sí	Sí	No [2]	v3 Solo [2]
Equipos virtuales con thin provisioning (discos virtuales)	Sí	Sí	Sí	Sí Esta configuración es la predeterminada para todas las máquinas virtuales de NFS cuando no se utiliza VAAI.
Accesos múltiples nativos de VMware	Sí	Sí	Sí	La conexión de enlaces de sesión NFS v4,1 requiere ONTAP 9.14.1 y posterior

En la siguiente tabla se enumeran las funciones de gestión de almacenamiento de ONTAP admitidas.

Característica/función	FC	ISCSI	NVMe-of	NFS
Deduplicación de datos	Ahorro en la cabina	Ahorro en la cabina	Ahorro en la cabina	De ahorro en el almacén de datos
Aprovisionamiento ligero	Almacén de datos o RDM	Almacén de datos o RDM	Almacén de datos	Almacén de datos
Redimensión de almacén de datos	Crezca solo	Crezca solo	Crezca solo	Crecer, crecimiento automático y reducción
Complementos de SnapCenter para aplicaciones Windows y Linux (en invitado)	Sí	Sí	Sí	Sí

Característica/función	FC	ISCSI	NVMe-of	NFS
Supervisión y configuración del host mediante herramientas de ONTAP para VMware vSphere	Sí	Sí	Sí	Sí
Aprovisionar mediante las herramientas de ONTAP para VMware vSphere	Sí	Sí	Sí	Sí

En la siguiente tabla se enumeran las funciones de backup admitidas.

Característica/función	FC	ISCSI	NVMe-of	NFS
Snapshots de ONTAP	Sí	Sí	Sí	Sí
SRM compatible con backups replicados	Sí	Sí	No [2]	v3 Solo [2]
SnapMirror para volúmenes	Sí	Sí	Sí	Sí
Acceso a imagen VMDK	Software de backup habilitado para SnapCenter y VADP	Software de backup habilitado para SnapCenter y VADP	Software de backup habilitado para SnapCenter y VADP	El software de backup habilitado para SnapCenter y VADP, vSphere Client y el explorador de almacén de datos de vSphere Web Client
Acceso de nivel de ficheros VMDK	Software de backup habilitado para SnapCenter y VADP, solamente Windows	Software de backup habilitado para SnapCenter y VADP, solamente Windows	Software de backup habilitado para SnapCenter y VADP, solamente Windows	Software de backup y aplicaciones de terceros habilitados para SnapCenter y VADP
Granularidad de NDMP	Almacén de datos	Almacén de datos	Almacén de datos	Almacén de datos o máquina virtual

[1] **NetApp recomienda** usar iSCSI en invitado para clústeres de Microsoft en lugar de VMDK con capacidad para múltiples escritores en un almacén de datos VMFS. Este enfoque es totalmente compatible con Microsoft y VMware, ofrece una gran flexibilidad con ONTAP (SnapMirror para sistemas ONTAP en las instalaciones o en el cloud), es fácil de configurar y automatizar y se puede proteger con SnapCenter. VSphere 7 añade una nueva opción de VMDK en clúster. Es diferente de los VMDK habilitados para el multiescritor, que requieren un almacén de datos VMFS 6 que tenga habilitada la compatibilidad con VMDK en clúster. Se aplican otras restricciones. Consulte la documentación de VMware "Configuración de clústeres de conmutación por error de Windows Server"para conocer las directrices de configuración.

[2] Los almacenes de datos que utilizan NVMe-oF y NFS v4,1 requieren replicación de vSphere. Actualmente, SRM no admite la replicación basada en cabinas para NFS v4,1. Actualmente, las herramientas de ONTAP para vSphere Storage Replication Adapter (SRA) de VMware no admiten la replicación basada en cabinas con NVMe-oF.

Seleccionar un protocolo de almacenamiento

Los sistemas que se ejecutan en ONTAP son compatibles con los principales protocolos de almacenamiento, de modo que los clientes pueden elegir el que mejor se adapte a su entorno, en función de la infraestructura de red existente y las aptitudes previstas para el personal. Históricamente, las pruebas de NetApp generalmente han mostrado poca diferencia entre los protocolos que se ejecutan a velocidades de línea similares y el número de conexiones. Sin embargo, NVMe-oF (NVMe/TCP y NVMe/FC) muestra aumentos notables en IOPS, reducción de la latencia y hasta un 50 % o más de reducción en el consumo de CPU del host según la I/O de almacenamiento. En el otro extremo, NFS ofrece la mayor flexibilidad y facilidad de gestión, especialmente para un gran número de máquinas virtuales. Todos estos protocolos pueden usarse y gestionarse con las herramientas de ONTAP para VMware vSphere, lo que ofrece una interfaz sencilla para crear y gestionar almacenes de datos.

Los siguientes factores pueden ser útiles a la hora de considerar una opción de protocolo:

- **Entorno operativo actual.** Aunque los EQUIPOS DE TI suelen especializarse en la gestión de la infraestructura IP de Ethernet, no todos tienen experiencia a la hora de gestionar una estructura SAN FC. Sin embargo, es posible que el uso de una red IP de uso general que no está diseñada para el tráfico de almacenamiento no funcione bien. Considere la infraestructura de red de que dispone, las mejoras planificadas y las capacidades y la disponibilidad del personal para gestionarlos.
- **Facilidad de configuración.** más allá de la configuración inicial de la estructura FC (conmutadores y cableado adicionales, zonificación y verificación de interoperabilidad de HBA y firmware), los protocolos de bloque también requieren la creación y asignación de LUN y descubrimiento y formato por parte del SO invitado. Una vez creados y exportados los volúmenes de NFS, el host ESXi los monta y está listo para usarse. NFS no tiene ninguna cualificación de hardware o firmware especial que gestionar.
- **Facilidad de gestión.** Con los protocolos SAN, si se necesita más espacio, son necesarios varios pasos: Ampliar una LUN, volver a analizar para descubrir el nuevo tamaño y, posteriormente, aumentar el sistema de archivos). Aunque sea posible aumentar una LUN, reducir el tamaño de una LUN no lo es. NFS permite ajustar fácilmente el tamaño, y el sistema de almacenamiento puede automatizar este ajuste de tamaño. SAN ofrece recuperación de espacio mediante comandos de DESASIGNAR/TRIM/UNMAP del sistema operativo invitado, para que se pueda devolver espacio de los archivos eliminados a la cabina. Este tipo de recuperación de espacio no es difícil con los almacenes de datos NFS.
- **Transparencia del espacio de almacenamiento.** la utilización del almacenamiento suele ser más fácil de ver en entornos NFS, ya que Thin Provisioning devuelve ahorros inmediatamente. Del mismo modo, los ahorros en deduplicación y clonado están disponibles inmediatamente para otras máquinas virtuales en el mismo almacén de datos o para otros volúmenes del sistema de almacenamiento. La densidad de las máquinas virtuales también es superior en un almacén de datos NFS, que puede mejorar el ahorro de la deduplicación y reducir los costes de gestión al tener menos almacenes de datos que gestionar.

Distribución de almacenes de datos

Los sistemas de almacenamiento ONTAP ofrecen una gran flexibilidad a la hora de crear almacenes de datos para equipos virtuales y discos virtuales. Aunque muchas prácticas recomendadas de ONTAP se aplican al usar las herramientas de ONTAP para aprovisionar almacenes de datos para vSphere (se muestran en la sección "Host ESXi recomendado y otra configuración de ONTAP"), estas son algunas directrices adicionales a tener en cuenta:

- La puesta en marcha de vSphere con almacenes de datos NFS de ONTAP da como resultado una implementación de alto rendimiento y fácil de gestionar que proporciona ratios de máquina virtual a

almacén de datos que no pueden obtenerse con protocolos de almacenamiento basados en bloques. Esta arquitectura puede provocar un aumento diez veces en la densidad de los almacenes de datos con una reducción correlacionada en el número de almacenes de datos. Aunque un almacén de datos de mayor tamaño puede beneficiar a la eficiencia del almacenamiento y proporcionar ventajas operativas, considere la posibilidad de utilizar al menos cuatro almacenes de datos (volúmenes FlexVol) por nodo para almacenar sus máquinas virtuales en una sola controladora ONTAP para obtener el máximo rendimiento de los recursos de hardware. Este enfoque también permite establecer almacenes de datos con diferentes políticas de recuperación. Algunas se pueden hacer backups o replicarse con una frecuencia mayor que otras en función de las necesidades de las empresas. No se necesitan varios almacenes de datos en los volúmenes de FlexGroup para mejorar el rendimiento, ya que se escalan por diseño.

- **NetApp recomienda** el uso de volúmenes FlexVol para la mayoría de los almacenes de datos NFS. A partir de la versión ONTAP 9,8, se admiten los volúmenes FlexGroup también para su uso como almacenes de datos y, por lo general, se recomienda en determinados casos de uso. No se recomiendan normalmente otros contenedores de almacenamiento de ONTAP, como qtrees, porque actualmente no son compatibles con las herramientas de ONTAP para VMware vSphere o con el complemento de NetApp SnapCenter para VMware vSphere.
- Un buen tamaño para un almacén de datos con volúmenes FlexVol es de entre 4 y 8 TB. Este tamaño es un buen punto de equilibrio entre rendimiento, facilidad de gestión y protección de datos. Empiece con poco (digamos, 4 TB) y crezca el almacén de datos según sea necesario (hasta el máximo de 300 TB). Los almacenes de datos más pequeños son más rápidos de recuperar desde un backup o después de un desastre y se pueden mover rápidamente en el clúster. Considere la posibilidad de utilizar el ajuste de tamaño automático de ONTAP para aumentar y reducir automáticamente el volumen a medida que se modifique el espacio utilizado. De forma predeterminada, las herramientas de ONTAP para el asistente de aprovisionamiento de almacenes de datos de VMware vSphere utilizan el tamaño automático para nuevos almacenes de datos. System Manager o la línea de comandos pueden personalizarse los umbrales de crecimiento y reducción, y el tamaño máximo y mínimo.
- Como alternativa, los almacenes de datos VMFS se pueden configurar con espacios de nombres NVMe o LUN (denominados unidades de almacenamiento en nuevos sistemas ASA) a los que se accede mediante FC, iSCSI, NVMe/FC o NVMe/TCP. VMFS permite a los almacenes de datos acceder de forma simultánea a cada servidor ESX de un clúster. Los almacenes de datos VMFS pueden tener un tamaño de hasta 64 TB y constan de hasta 32 LUN de 2 TB (VMFS 3) o una única LUN de 64 TB (VMFS 5). El tamaño máximo de LUN de ONTAP es de 128TB TB en los sistemas AFF, ASA y FAS. NetApp siempre recomienda utilizar un único LUN grande para cada almacén de datos en vez de intentar utilizar extensiones. Al igual que sucede con NFS, considere la posibilidad de utilizar varios almacenes de datos (volúmenes o unidades de almacenamiento) para maximizar el rendimiento en una única controladora de ONTAP.
- Los sistemas operativos invitados (SO) antiguos necesitaban alineación con el sistema de almacenamiento para obtener el mejor rendimiento y eficiencia del almacenamiento. Sin embargo, los sistemas operativos modernos admitidos por el proveedor de distribuidores de Microsoft y Linux como Red Hat ya no requieren ajustes para alinear la partición del sistema de archivos con los bloques del sistema de almacenamiento subyacente en un entorno virtual. Si utiliza un antiguo sistema operativo que pueda requerir la alineación, busque en la base de conocimientos de soporte de NetApp los artículos mediante «alineación de VM» o solicite una copia de TR-3747 a partir de un contacto de ventas o partner de NetApp.
- Evite el uso de utilidades de desfragmentación en el sistema operativo invitado, ya que no ofrece beneficios de rendimiento y afecta a la eficiencia del almacenamiento y al uso del espacio de instantáneas. Considere también desactivar la indización de búsquedas en el sistema operativo invitado para escritorios virtuales.
- ONTAP ha dirigido el sector mediante funciones innovadoras de eficiencia del almacenamiento, que le permiten sacar el máximo partido a su espacio en disco utilizable. Los sistemas AFF llevan esta eficiencia aún más allá gracias a la compresión y la deduplicación inline predeterminadas. Los datos se deduplican en todos los volúmenes de un agregado, por lo que ya no necesita agrupar sistemas operativos similares y aplicaciones similares en un único almacén de datos para optimizar el ahorro.

- En algunos casos, es posible que ni siquiera se necesite un almacén de datos. Piense en sistemas de archivos propiedad del invitado como NFS, SMB, NVMe/TCP o iSCSI gestionados por el invitado. Para obtener orientación específica sobre las aplicaciones, consulte los informes técnicos de NetApp para su aplicación. Por ejemplo, "Bases de datos de Oracle en ONTAP" tiene una sección sobre la virtualización con detalles útiles.
- Los discos de primera clase (o discos virtuales mejorados) permiten discos gestionados por vCenter independientemente de una máquina virtual con vSphere 6.5 y versiones posteriores. Aunque son gestionados principalmente por la API, pueden ser útiles con vVols, sobre todo cuando las herramientas de OpenStack o Kubernetes las gestionan. Son compatibles tanto con ONTAP como con herramientas de ONTAP para VMware vSphere.

Migración de almacenes de datos y máquinas virtuales

Al migrar las máquinas virtuales desde un almacén de datos existente en otro sistema de almacenamiento a ONTAP, estas son algunas prácticas que deben tenerse en cuenta:

- Use Storage vMotion para mover la mayoría de los equipos virtuales a ONTAP. Este método no solo no es disruptivo para la ejecución de equipos virtuales, sino que también permite funciones de eficiencia del almacenamiento de ONTAP como deduplicación y compresión inline para procesar los datos a medida que migran. Considere usar funcionalidades de vCenter para seleccionar varias máquinas virtuales de la lista de inventario y programar la migración (utilice la tecla Ctrl mientras hace clic en acciones) en un momento adecuado.
- Aunque podría planificar con cuidado la migración a los almacenes de datos de destino adecuados, a menudo es más sencillo migrar de forma masiva y luego organizarse más tarde, según sea necesario. Puede que desee utilizar este enfoque para guiar la migración a diferentes almacenes de datos si tiene necesidades específicas de protección de datos, como distintas programaciones de Snapshot. Asimismo, una vez que los equipos virtuales se encuentran en el clúster de NetApp, Storage vMotion puede utilizar descargas de VAAI para mover equipos virtuales entre los almacenes de datos del clúster sin necesidad de realizar una copia basada en host. Tenga en cuenta que NFS no descarga vMotion de almacenamiento de equipos virtuales encendidos, pero VMFS sí lo hace.
- Los equipos virtuales que necesitan una migración más cuidadosa incluyen las bases de datos y las aplicaciones que utilizan almacenamiento conectado. En general, considere el uso de las herramientas de la aplicación para gestionar la migración. Para Oracle, considere la posibilidad de utilizar herramientas de Oracle como RMAN o ASM para migrar los archivos de base de datos. Consulte "Migración de bases de datos de Oracle a sistemas de almacenamiento de ONTAP" para obtener más información. Del mismo modo, para SQL Server, plantéese utilizar SQL Server Management Studio o herramientas de NetApp, como SnapManager para SQL Server o SnapCenter.

Herramientas de ONTAP para VMware vSphere

La mejor práctica más importante cuando se usa vSphere con sistemas que ejecutan ONTAP es instalar y utilizar las herramientas de ONTAP para el complemento VMware vSphere (anteriormente conocido como Virtual Storage Console). Este complemento de vCenter simplifica la gestión del almacenamiento, mejora la disponibilidad y reduce los costes de almacenamiento y la sobrecarga operativa, tanto si se utiliza SAN o NAS, en ASA, AFF, FAS o incluso en ONTAP Select (una versión definida por software de ONTAP que se ejecuta en una máquina virtual VMware o KVM). Utiliza prácticas recomendadas para el aprovisionamiento de almacenes de datos y optimiza la configuración del host ESXi para los tiempos de espera de multivía y HBA (que se describen en el apéndice B). Dado que es un complemento de vCenter, está disponible para todos los clientes web de vSphere que se conectan al servidor vCenter.

El plugin también le ayuda a utilizar otras herramientas ONTAP en entornos de vSphere. Le permite instalar el complemento de NFS para VMware VAAI, que permite realizar copias de datos descargados en ONTAP para las operaciones de clonado de equipos virtuales, reservar espacio para archivos de disco virtual gruesos y

descargar la copia Snapshot de ONTAP.

> En los clústeres de vSphere basados en imágenes, seguirá queriendo añadir el plugin NFS a su imagen para que no cumplan las normativas al instalarlo con las herramientas de ONTAP.

Las herramientas de ONTAP también son la interfaz de gestión para numerosas funciones de VASA Provider para ONTAP, compatible con la gestión basada en políticas de almacenamiento con vVols.

En general, **NetApp recomienda** el uso de las herramientas de ONTAP para la interfaz de VMware vSphere en vCenter para aprovisionar almacenes de datos tradicionales y vVols a fin de garantizar que se siguen las mejores prácticas.

Redes generales

La configuración de los ajustes de red cuando se utiliza vSphere con sistemas que ejecutan ONTAP es sencilla y similar a otra configuración de red. Estas son algunas cosas a tener en cuenta:

- Hay que separar el tráfico de la red de almacenamiento de otras redes. Se puede lograr una red independiente a través de una VLAN dedicada o switches independientes para el almacenamiento. Si la red de almacenamiento comparte rutas físicas como los enlaces ascendentes, puede que necesite calidad de servicio o puertos adicionales para garantizar el ancho de banda suficiente. No conecte los hosts directamente al almacenamiento; utilice switches para que tengan rutas redundantes y permita que VMware HA funcione sin intervención alguna. Consulte "Conexión de red directa" para obtener más información.
- Las tramas gigantes se pueden utilizar si se desean y admiten en la red, especialmente si se utiliza iSCSI. Si se usan, asegúrese de que estén configurados de la misma forma en todos los dispositivos de red, VLAN, etc., en la ruta entre el almacenamiento y el host ESXi. De lo contrario, puede que observe problemas de rendimiento o conexión. La MTU también debe establecerse de forma idéntica en el switch virtual ESXi, el puerto de VMkernel y, además, en los puertos físicos o los grupos de interfaces de cada nodo ONTAP.
- NetApp solo recomienda deshabilitar el control de flujo de red en los puertos de interconexión de clúster de un clúster de ONTAP. NetApp no ofrece otras recomendaciones para seguir las prácticas recomendadas para los puertos de red restantes que se usan para el tráfico de datos. Debe activar o desactivar según sea necesario. Consulte "CONSULTE TR-4182" para obtener más información sobre el control de flujo.
- Cuando las cabinas de almacenamiento ESXi y ONTAP están conectadas a redes de almacenamiento Ethernet, **NetApp recomienda** configurar los puertos Ethernet a los que se conectan estos sistemas como puertos periféricos del protocolo de árbol de expansión rápido (RSTP) o mediante la función PortFast de Cisco. **NetApp recomienda** habilitar la función de troncal PortFast de árbol de expansión en entornos que utilizan la característica PortFast de Cisco y que tienen habilitado el troncalización de VLAN 802,1Q para el servidor ESXi o las cabinas de almacenamiento ONTAP.
- **NetApp recomienda** las siguientes mejores prácticas para la agregación de enlaces:
  - Utilice switches que admitan la agregación de enlaces de puertos en dos chasis de switch separados mediante un enfoque de grupo de agregación de enlaces de varios chasis, como Virtual PortChannel (VPC) de Cisco.
  - Deshabilite LACP para los puertos del switch conectados a ESXi a menos que utilice dvSwitch 5.1 o una versión posterior con LACP configurado.
  - Utilice LACP para crear agregados de enlaces para sistemas de almacenamiento de ONTAP con grupos de interfaces dinámicas multimodo con puerto o hash IP. Consulte "Gestión de redes" para obtener más orientación.

- Utilice una política de agrupación de hash IP en ESXi cuando utilice la agregación de enlaces estáticos (por ejemplo, EtherChannel) y vSwitch estándar, o la agregación de enlaces basada en LACP con switches distribuidos de vSphere. Si no se utiliza la agregación de enlaces, utilice en su lugar «Ruta basada en el identificador de puerto virtual de origen».

SAN (FC, FCoE, NVMe/FC, iSCSI), RDM

En vSphere, hay cuatro formas de utilizar dispositivos de almacenamiento de bloques:

- Con almacenes de datos VMFS
- Con asignación de dispositivos sin formato (RDM)
- Como LUN conectado a iSCSI o espacio de nombres conectado a NVMe/TCP, al que accede y controla un iniciador de software desde un sistema operativo invitado de máquina virtual
- Como almacén de datos vVols

VMFS es un sistema de archivos en clúster de alto rendimiento que proporciona almacenes de datos que son pools de almacenamiento compartido. Los almacenes de datos VMFS se pueden configurar con LUN a los que se accede mediante espacios de nombres FC, iSCSI, FCoE o NVMe a los que se accede mediante los protocolos NVMe/FC o NVMe/TCP. VMFS permite a cada servidor ESX de un clúster acceder al almacenamiento de forma simultánea. El tamaño máximo de LUN suele ser de 128TB TB a partir de ONTAP 9.12.1P2 (y versiones anteriores con los sistemas ASA). Por lo tanto, es posible crear un almacén de datos VMFS 5 o 6 de tamaño máximo de 64TB TB utilizando una única LUN.

Las extensiones son un concepto de almacenamiento de vSphere por el que puede unir varios LUN para crear un único almacén de datos de mayor tamaño. Nunca se deben utilizar extensiones para alcanzar el tamaño deseado del almacén de datos. Una única LUN es la mejor práctica para un almacén de datos VMFS.

VSphere incluye soporte incorporado para varias rutas hacia los dispositivos de almacenamiento. VSphere puede detectar el tipo de dispositivo de almacenamiento en los sistemas de almacenamiento compatibles y configurar automáticamente la pila multivía para admitir las capacidades del sistema de almacenamiento que se esté utilizando, el uso del protocolo utilizado o si se utiliza ASA, AFF, FAS o ONTAP definido por software.

Tanto vSphere como ONTAP admiten el acceso asimétrico de unidad lógica (ALUA) para establecer rutas activo/optimizado y activo/no optimizado para Fibre Channel e iSCSI, y Acceso asimétrico a espacios de nombres (ANA) para espacios de nombres NVMe mediante NVMe/FC y NVMe/TCP. En ONTAP, una ruta optimizada para ALUA o ANA sigue una ruta de datos directa, mediante un puerto de destino en el nodo que aloja el LUN o el espacio de nombres al que se está accediendo. ALUA/ANA está activado de manera predeterminada en vSphere y ONTAP. El software multivía de vSphere reconoce el clúster de ONTAP como ALUA o ANA y utiliza el complemento nativo adecuado con la política de equilibrio de carga round robin.

Con los sistemas ASA de NetApp, las LUN y los espacios de nombres se presentan a los hosts ESXi con rutas simétricas. Lo que significa que todas las rutas están activas y optimizadas. El software multivía en vSphere reconoce el sistema ASA como simétrico y utiliza el plugin nativo adecuado con la política de equilibrio de carga round robin.

Consulte "Host ESXi recomendado y otra configuración de ONTAP"para obtener información sobre los ajustes de acceso múltiple optimizados.

ESXi no ve ninguna LUN, espacios de nombres o rutas más allá de sus límites. En un clúster de ONTAP mayor, es posible alcanzar el límite de ruta antes del límite de LUN. Para solucionar esta limitación, ONTAP admite una asignación de LUN selectiva (SLM) en la versión 8.3 y posteriores.

Consulte el "Herramienta VMware Configuration Maximums" para obtener los límites admitidos más actualizados en ESXi.

SLM limita los nodos que anuncian rutas a un LUN determinado. Una mejor práctica de NetApp es tener al menos dos LIF por nodo y utilizar SLM para limitar las rutas anunciadas al nodo que aloja el LUN y su partner de alta disponibilidad. Aunque existen otras rutas, no se anuncian por defecto. Es posible modificar las rutas anunciadas con los argumentos de nodo de informes Agregar y quitar dentro de SLM. Tenga en cuenta que las LUN creadas en versiones anteriores a la 8,3 anuncian todas las rutas y deben modificarse únicamente para anunciar las rutas al par de alta disponibilidad que aloja. Para obtener más información sobre SLM, consulte la sección 5,9 de "CONSULTE TR-4080". El método anterior de conjuntos de puertos también puede utilizarse para reducir aún más las rutas disponibles para una LUN. Los conjuntos de puertos ayudan a reducir el número de rutas visibles a través de las cuales los iniciadores de un igroup pueden ver LUN.

- SLM está habilitado de forma predeterminada. A menos que utilice conjuntos de puertos, no se requiere ninguna configuración adicional.
- Para las LUN creadas antes de Data ONTAP 8,3, aplique manualmente SLM ejecutando `lun mapping remove-reporting-nodes` el comando para quitar los nodos de informe de LUN y restringir el acceso de las LUN al nodo propietario del LUN y su partner de alta disponibilidad.

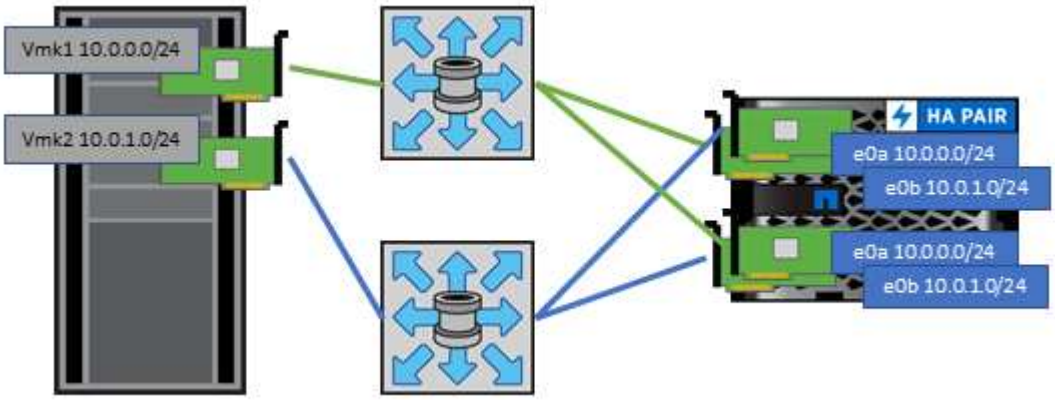
Los protocolos de bloque basados en SCSI (iSCSI, FC y FCoE) acceden a los LUN usando ID de LUN y números de serie, junto con nombres únicos. FC y FCoE utilizan nombres a nivel mundial (WWN y WWPN), e iSCSI utiliza nombres completos de iSCSI (IQN) para establecer rutas en función de las asignaciones de LUN a igroup filtradas por conjuntos de puertos y SLM. Los protocolos de bloques basados en NVMe se gestionan asignando el espacio de nombres con un ID de espacio de nombres generado automáticamente a un subsistema NVMe y asignando dicho subsistema al nombre completo de NVMe (NQN) de los hosts. Independientemente de FC o TCP, los espacios de nombres de NVMe se asignan mediante el NQN y no el puerto WWPN o WWNN. A continuación, el host crea una controladora definida por software para que el subsistema asignado acceda a sus espacios de nombres. La ruta a las LUN y los espacios de nombres dentro de ONTAP no tiene sentido para los protocolos de bloques y no se presenta en ninguna parte del protocolo. Por lo tanto, no es necesario montar de forma interna un volumen que solo contiene LUN; por lo tanto, no es necesaria una ruta de unión para los volúmenes que contengan LUN usadas en los almacenes de datos.

Otras prácticas recomendadas a tener en cuenta:

- Compruebe "Host ESXi recomendado y otra configuración de ONTAP"los ajustes recomendados por NetApp en colaboración con VMware.
- Asegúrese de que se crea una interfaz lógica (LIF) para cada SVM en cada nodo del clúster de ONTAP para garantizar la máxima disponibilidad y movilidad. La práctica recomendada para SAN de ONTAP es usar dos puertos físicos y LIF por nodo, uno para cada estructura. ALUA se utiliza para analizar las rutas e identificar las rutas activas optimizadas (directas) en comparación con las rutas activas no optimizadas. ALUA se utiliza para FC, FCoE e iSCSI.
- En el caso de las redes iSCSI, utilice varias interfaces de red de VMkernel en distintas subredes de la red con la agrupación de NIC cuando haya varios switches virtuales. También puede utilizar varias NIC físicas conectadas a varios switches físicos para proporcionar alta disponibilidad y mayor rendimiento. En la figura siguiente se proporciona un ejemplo de conectividad multivía. En ONTAP, configure un grupo de interfaces de un único modo para realizar la conmutación al nodo de respaldo con dos o más enlaces conectados a dos o más switches, o bien utilice LACP u otra tecnología de agregación de enlaces con grupos de interfaces multimodo para proporcionar alta disponibilidad y las ventajas de la agregación de enlaces.
- Si el protocolo de autenticación por desafío mutuo (CHAP) se utiliza en ESXi para la autenticación de destino, también debe configurarse en ONTAP mediante la CLI (`vserver iscsi security create`) O con System Manager (edite Initiator Security en almacenamiento > SVM > SVM Settings > Protocols >

iSCSI).

- Utilice las herramientas de ONTAP para VMware vSphere para crear y gestionar LUN y iGroups. El plugin determina automáticamente los WWPN de los servidores y crea iGroups adecuados. También configura las LUN de acuerdo con las prácticas recomendadas y las asigna a los iGroups correctos.
- Use los DMR con cuidado porque pueden ser más difíciles de manejar, y también usan rutas, que son limitadas como se describió anteriormente. Las LUN de ONTAP son compatibles con ambos "modo de compatibilidad físico y virtual" RDM.
- Para obtener más información sobre cómo usar NVMe/FC con vSphere 7.0, consulte este tema "Guía de configuración de hosts ONTAP NVMe/FC" y.. "CONSULTE TR-4684".En la siguiente figura, se muestra la conectividad multivía de un host de vSphere a un LUN de ONTAP.



NFS

ONTAP representa, entre otras cosas, una cabina NAS de escalado horizontal para empresas. ONTAP proporciona acceso concurrente a los almacenes de datos conectados a NFS desde muchos hosts ESXi, lo que supera con creces los límites impuestos en los sistemas de archivos VMFS. El uso de NFS con vSphere proporciona cierta facilidad de uso y ventajas de visibilidad de la eficiencia del almacenamiento, como se menciona en "almacenes de datos"la sección.

Las siguientes prácticas recomendadas se recomiendan al usar NFS de ONTAP con vSphere:

- Use las herramientas de ONTAP para VMware vSphere (las mejores prácticas más importantes):
  - Utilizar herramientas de ONTAP para VMware vSphere para aprovisionar almacenes de datos, ya que simplifica la gestión automática de políticas de exportación.
  - Cuando se crean almacenes de datos para clústeres de VMware con el plugin, seleccione el clúster en lugar de un único servidor ESX. Esta opción la activa para montar automáticamente el almacén de datos en todos los hosts del clúster.
  - Use la función de montaje del plugin para aplicar almacenes de datos existentes a servidores nuevos.
  - Si no se utilizan las herramientas de ONTAP para VMware vSphere, utilice una única política de exportación para todos los servidores o para cada cluster de servidores donde se necesite un control de acceso adicional.
- Utilice una sola interfaz lógica (LIF) para cada SVM en cada nodo del clúster de ONTAP. Ya no son necesarias las recomendaciones anteriores de una LIF por almacén de datos. Aunque el acceso directo (LIF y almacén de datos en el mismo nodo) es el mejor, no se preocupe por el acceso indirecto, ya que el efecto sobre el rendimiento suele ser mínimo (microsegundos).

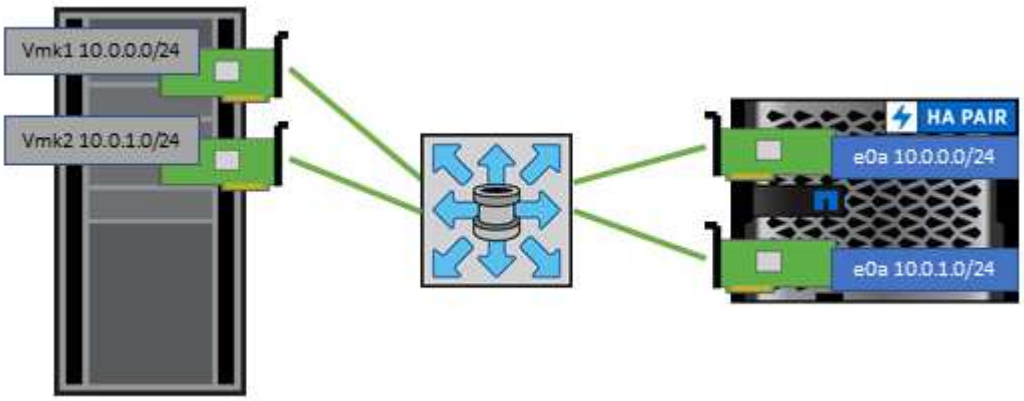
- Si usa fpolicy, asegúrese de excluir los archivos .lck, ya que los utiliza vSphere para bloquear cada vez que se enciende una máquina virtual.
- Todas las versiones de VMware vSphere compatibles en la actualidad pueden usar NFS v3 y v4,1. La compatibilidad oficial con nconnect se agregó a la actualización 2 de vSphere 8,0 para NFS v3 y a la actualización 3 para NFS v4,1. Para NFS v4,1, vSphere sigue admitiendo el truncado de sesión, la autenticación Kerberos y la autenticación Kerberos con integridad. Es importante tener en cuenta que el trunking de sesión requiere ONTAP 9.14.1 o una versión posterior. Puede obtener más información sobre la función nconnect y cómo mejora el rendimiento en "La función de NFSv3 nconnect con NetApp y VMware".

  - El valor máximo para nconnect en vSphere 8 es 4 y el valor predeterminado es 1. El límite de valor máximo en vSphere se puede aumentar por host a través de una configuración avanzada, sin embargo, por lo general no es necesario.
  - Se recomienda un valor de 4 para los entornos que requieren más rendimiento del que puede proporcionar una única conexión TCP.
  - Tenga en cuenta que ESXi tiene un límite de 256 conexiones NFS y cada conexión nconnect cuenta para ese total. Por ejemplo, dos almacenes de datos con nconnect=4 contarían como ocho conexiones totales.
  - Es importante probar el impacto de nconnect en el rendimiento en su entorno antes de implementar cambios a gran escala en los entornos de producción.

- Vale la pena señalar que NFSv3 y NFSv4,1 utilizan diferentes mecanismos de bloqueo. NFSv3 utiliza bloqueo del lado del cliente, mientras que NFSv4,1 utiliza bloqueo del lado del servidor. Aunque un volumen ONTAP se puede exportar mediante ambos protocolos, ESXi solo puede montar un almacén de datos a través de un protocolo. Sin embargo, esto no significa que otros hosts ESXi no puedan montar el mismo almacén de datos mediante una versión diferente. Para evitar cualquier problema, es esencial especificar la versión del protocolo que se debe utilizar al montar, asegurándose de que todos los hosts utilicen la misma versión y, por lo tanto, el mismo estilo de bloqueo. Es crucial evitar mezclar versiones de NFS entre hosts. Si es posible, utilice perfiles de host para comprobar el cumplimiento.
  - Dado que no existe ninguna conversión automática de almacenes de datos entre NFSv3 y NFSv4.1, cree un nuevo almacén de datos NFSv4.1 y utilice Storage vMotion para migrar las máquinas virtuales al nuevo almacén de datos.
  - Consulte las notas de la tabla de interoperabilidad de NFS v4,1 en la "Herramienta de matriz de interoperabilidad de NetApp" para ver los niveles de parches de ESXi específicos necesarios para el soporte.
- Tal como se ha mencionado en "configuración", si no utiliza el CSI de vSphere para Kubernetes, debe establecer newSyncInterval por "VMware KB 386364"
- Las reglas de políticas de exportación de NFS se usan para controlar el acceso de los hosts vSphere. Puede usar una política con varios volúmenes (almacenes de datos). Con NFS, ESXi utiliza el estilo de seguridad sys (UNIX) y requiere la opción de montaje root para ejecutar equipos virtuales. En ONTAP, esta opción se denomina superusuario y cuando se utiliza la opción superusuario, no es necesario especificar el ID de usuario anónimo. Tenga en cuenta que reglas de políticas de exportación con diferentes valores para `-anon` y `-allow-suid` pueden causar problemas de detección de SVM con las herramientas de ONTAP. Las direcciones IP deben ser una lista separada por comas sin espacios de las direcciones de puertos de vmkernel que montan los almacenes de datos. He aquí una regla de política de ejemplo:
  - Protocolo de acceso: nfs (que incluye nfs3 y nfs4)
  - Lista de nombres de host, direcciones IP, grupos de red o dominios de coincidencia de cliente: 192.168.42.21,192.168.42.22

- Regla de acceso de RO: Cualquiera
- Regla de acceso RW: Cualquiera
- ID de usuario al que se asignan los usuarios anónimos: 65534
- Tipos de seguridad de superusuario: Cualquiera
- Honor setuid Bits en SETATTR: True
- Permitir la creación de dispositivos: True

- Si se utiliza el plugin de NFS de NetApp para VMware VAAI, el protocolo se debe establecer `nfs` como cuando se crea o se modifica la regla de política de exportación. El protocolo NFSv4 se requiere para que la copia de VAAI descargue el trabajo y especificando el protocolo como `nfs` automáticamente incluye las versiones NFSv3 y NFSv4. Esto es necesario incluso si el tipo de almacén de datos se crea como NFS v3.
- Los volúmenes de almacenes de datos NFS se unen desde el volumen raíz de la SVM; por lo tanto, ESXi también debe tener acceso al volumen raíz para navegar y montar volúmenes de almacenes de datos. La política de exportación del volumen raíz y para cualquier otro volumen en el que esté anidada la unión del volumen de almacenes de datos, debe incluir una regla o reglas para los servidores ESXi que les otorgan acceso de solo lectura. A continuación, se muestra una política de ejemplo para el volumen raíz, que también utiliza el complemento VAAI:
  - Protocolo de acceso: nfs
  - Client Match Spec: 192.168.42.21,192.168.42.22
  - Regla DE ACCESO DE RO: Sys
  - Regla de acceso RW: Nunca (mejor seguridad para el volumen raíz)
  - UID anónimo
  - Superusuario: Sys (también necesario para el volumen raíz con VAAI)
- Aunque ONTAP ofrece una estructura de espacio de nombres de volúmenes flexibles para organizar los volúmenes en un árbol mediante uniones, este enfoque no tiene valor para vSphere. Crea un directorio para cada equipo virtual en la raíz del almacén de datos, independientemente de la jerarquía de espacio de nombres del almacenamiento. Por lo tanto, la práctica recomendada es simplemente montar la ruta de unión para volúmenes para vSphere en el volumen raíz de la SVM, que es la forma en que las herramientas de ONTAP para VMware vSphere aprovisiona almacenes de datos. No tener rutas de unión anidadas también significa que ningún volumen depende de ningún otro volumen que no sea el volumen raíz y que el hecho de desconectar un volumen o destruirlo, incluso intencionalmente, no afecta la ruta a otros volúmenes.
- El tamaño de bloque de 4K se ajusta a las particiones NTFS en almacenes de datos NFS. En la siguiente figura, se muestra la conectividad de un host vSphere a un almacén de datos NFS de ONTAP.



En la siguiente tabla, se enumeran las versiones de NFS y las funciones compatibles.

Funciones de vSphere	NFSv3	NFSv4,1
VMotion y Storage vMotion	Sí	Sí
Alta disponibilidad	Sí	Sí
Tolerancia a fallos	Sí	Sí
DRS	Sí	Sí
Perfiles de host	Sí	Sí
DRS de almacenamiento	Sí	No
Control de la actividad de I/o de almacenamiento	Sí	No
SRM	Sí	No
Volúmenes virtuales	Sí	No
Aceleración de hardware (VAAI)	Sí	Sí
Autenticación Kerberos	No	Sí (mejorada con vSphere 6.5 y versiones posteriores para ser compatible con AES, krb5i)
Compatibilidad con accesos múltiples	No	Sí (ONTAP 9.14.1)

Volúmenes de FlexGroup

Utilice ONTAP y FlexGroup Volumes con VMware vSphere para obtener almacenes de datos sencillos y escalables que aprovechan toda la potencia de todo un clúster de ONTAP.

ONTAP 9,8, junto con las herramientas de ONTAP para VMware vSphere 9,8-9,13 y el complemento SnapCenter para VMware 4,4, y otras versiones más recientes, añadieron compatibilidad con almacenes de datos respaldados por volúmenes de FlexGroup en vSphere. Los volúmenes FlexGroup simplifican la creación de grandes almacenes de datos y crean automáticamente los volúmenes constituyentes distribuidos necesarios en el clúster ONTAP para obtener el rendimiento máximo de un sistema ONTAP.

Utilice FlexGroup Volumes con vSphere si necesita un único almacén de datos de vSphere escalable con la potencia de un clúster ONTAP completo, o si cuenta con cargas de trabajo de clonado muy grandes que pueden beneficiarse del mecanismo de clonado de FlexGroup manteniendo constantemente la memoria caché de clonado caliente.

Descarga de copias

Además de las amplias pruebas del sistema con cargas de trabajo de vSphere, ONTAP 9,8 añadió un nuevo mecanismo de descarga de copia para los almacenes de datos de FlexGroup. Este nuevo sistema emplea un motor de copia mejorado para replicar archivos entre componentes en segundo plano a la vez que permite el acceso al origen y al destino. A continuación, esta caché local de componente se utiliza para crear rápidamente instancias de clones de equipos virtuales bajo demanda.

Para habilitar la descarga de copias optimizada para FlexGroup, consulte "Cómo configurar volúmenes de ONTAP FlexGroup para permitir la descarga de la copia de VAAI"

Puede ocurrir que si utiliza la clonación de VAAI, pero no clona lo suficiente para mantener la caché caliente, es posible que los clones no sean más rápidos que una copia basada en host. Si ese es el caso, puede ajustar el tiempo de espera de la caché para adaptarse mejor a sus necesidades.

Considere el siguiente escenario:

- Ha creado un nuevo FlexGroup con 8 componentes
- El tiempo de espera de caché para el nuevo FlexGroup se establece en 160 minutos

En esta situación, los primeros 8 clones que se realizarán serán copias completas, no clones de archivos locales. Cualquier clonación adicional de ese equipo virtual antes de que caduque el tiempo de espera de 160 segundos utilizará el motor de clonado de archivos dentro de cada componente en turno rotatorio para crear copias casi inmediatas distribuidas uniformemente en los volúmenes constituyentes.

Cada trabajo de clon nuevo que recibe un volumen restablece el tiempo de espera. Si un volumen constituyente de FlexGroup de ejemplo no recibe una solicitud de clonado antes del tiempo de espera, se borrará la caché de esa máquina virtual en particular y el volumen se deberá volver a completar. Además, si el origen del clon original cambia (por ejemplo, ha actualizado la plantilla), la caché local de cada componente se invalidará para evitar cualquier conflicto. Como se ha indicado anteriormente, la caché se puede ajustar y se puede configurar para satisfacer las necesidades del entorno.

Para obtener más información sobre el uso de FlexGroup Volumes con VAAI, consulte este artículo de la base de conocimientos: "VAAI: ¿Cómo funciona el almacenamiento en caché con volúmenes FlexGroup?"

En entornos donde no es posible aprovechar al máximo la caché FlexGroup, pero aún así requerir un clonado rápido entre volúmenes, considere el uso de vVols. La clonación entre volúmenes con vVols es mucho más rápida que el uso de almacenes de datos tradicionales y no utiliza una caché.

Configuración de calidad de servicio

Se admite la configuración de la calidad de servicio en el nivel de FlexGroup mediante ONTAP System Manager o el shell del clúster; sin embargo, no se proporciona para la máquina virtual ni la integración con vCenter.

La calidad de servicio (IOPS máx./mín.) se puede establecer en máquinas virtuales individuales o en todas las máquinas virtuales de un almacén de datos en ese momento en la interfaz de usuario de vCenter o mediante las API de REST con las herramientas de ONTAP. La configuración de la calidad de servicio en todas las máquinas virtuales sustituye cualquier configuración independiente por cada máquina virtual. Los ajustes no amplían en el futuro a máquinas virtuales nuevas o migradas; establezca la calidad de servicio en las nuevas máquinas virtuales o vuelva a aplicar la calidad de servicio a todas las máquinas virtuales del almacén de datos.

Tenga en cuenta que VMware vSphere trata todas las I/O de un almacén de datos NFS como una única cola por host, y la limitación de la calidad de servicio de un equipo virtual puede afectar al rendimiento de otras máquinas virtuales del mismo almacén de datos en ese host. Esto contrasta con vVols, que puede mantener su configuración de política de calidad de servicio si migran a otro almacén de datos y no afecta la I/O de otras máquinas virtuales cuando se acelera.

Métricas

ONTAP 9,8 también agregó nuevas métricas de rendimiento basadas en archivos (IOPS, rendimiento y latencia) para archivos FlexGroup. Estas métricas pueden visualizarse en la consola de herramientas de ONTAP para la consola de VMware vSphere e informes de VM. Las herramientas de ONTAP para el complemento VMware vSphere también le permiten establecer reglas de calidad de servicio (QoS) con una combinación de IOPS máximo o mínimo. Estos conjuntos se pueden establecer en todas las máquinas

virtuales de un almacén de datos o individualmente para máquinas virtuales específicas.

Mejores prácticas

- Utilice las herramientas de ONTAP para crear almacenes de datos de FlexGroup a fin de garantizar que el FlexGroup se cree de forma óptima y que las políticas de exportación se configuren en consonancia con su entorno vSphere. Sin embargo, después de crear el volumen FlexGroup con herramientas de ONTAP, se dará cuenta de que todos los nodos del clúster de vSphere utilizan una sola dirección IP para montar el almacén de datos. Esto podría provocar un cuello de botella en el puerto de red. Para evitar este problema, desmonte el almacén de datos y vuelva a montarlo mediante el asistente para almacenes de datos estándar de vSphere mediante un nombre DNS round-robin que equilibre la carga entre las LIF en la máquina virtual de almacenamiento. Tras el montaje, las herramientas de ONTAP podrán volver a gestionar el almacén de datos. Si no hay herramientas de ONTAP disponibles, use los valores predeterminados de FlexGroup y cree la política de exportación siguiendo las directrices de "Almacenes de datos y protocolos: NFS".
- Al ajustar el tamaño a un almacén de datos FlexGroup, tenga en cuenta que FlexGroup consta de varios volúmenes FlexVol más pequeños que crean un espacio de nombres mayor. De este modo, configure el tamaño del almacén de datos para que sea al menos 8x (asumiendo los 8 componentes predeterminados) el tamaño del archivo VMDK más grande y un margen no utilizado del 10 al 20% para permitir flexibilidad en el reequilibrio. Por ejemplo, si tiene un VMDK de 6TB GB en el entorno, ajuste el tamaño del almacén de datos FlexGroup como mínimo 52,8TB (6x8+10 %).
- VMware y NetApp admiten el trunking de sesiones NFSv4,1 a partir de ONTAP 9.14.1. Consulte las notas de la herramienta de matriz de interoperabilidad (IMT) de NFS 4,1 de NetApp para ver detalles específicos de la versión. NFSv3 no admite varias rutas físicas de un volumen, pero admite nconnect a partir de vSphere 8.0U2. Puede encontrar más información sobre nconnect en el "NFSv3 Función nConnect con NetApp y VMware".
- Use el plugin de NFS para VAAI de VMware para la descarga de copias. Tenga en cuenta que, aunque el clonado se mejora dentro de un almacén de datos de FlexGroup, como se ha mencionado anteriormente, ONTAP no ofrece importantes ventajas de rendimiento con respecto a la copia del host ESXi al copiar máquinas virtuales entre FlexVol y/o volúmenes de FlexGroup. Por tanto, tenga en cuenta las cargas de trabajo de clonado cuando decida usar volúmenes de VAAI o FlexGroup. La modificación del número de volúmenes constituyentes es una forma de optimizar para la clonación basada en FlexGroup. Al igual que el ajuste del timeout de caché mencionado anteriormente.
- Utilice herramientas de ONTAP para VMware vSphere 9,8-9,13 para supervisar el rendimiento de las VM de FlexGroup mediante métricas de ONTAP (informes de la consola y de VM), y para gestionar la calidad de servicio en máquinas virtuales individuales. Estas métricas no están disponibles a través de los comandos o las API de ONTAP.
- El plugin de SnapCenter para VMware vSphere versión 4,4 y versiones posteriores admite el backup y la recuperación de máquinas virtuales en un almacén de datos FlexGroup en el sistema de almacenamiento principal. SCV 4,6 añade compatibilidad con SnapMirror para almacenes de datos basados en FlexGroup. La forma más eficiente de proteger los datos es usar copias Snapshot y replicación basadas en cabinas.

Configuración de red

La configuración de los ajustes de red cuando se utiliza vSphere con sistemas que ejecutan ONTAP es sencilla y similar a otra configuración de red.

Estas son algunas cosas a tener en cuenta:

- Hay que separar el tráfico de la red de almacenamiento de otras redes. Se puede lograr una red independiente a través de una VLAN dedicada o switches independientes para el almacenamiento. Si la red de almacenamiento comparte rutas físicas como los enlaces ascendentes, puede que necesite calidad

de servicio o puertos adicionales para garantizar el ancho de banda suficiente. No conecte los hosts directamente al sistema de almacenamiento a menos que la guía de la solución lo indique específicamente; utilice switches para tener rutas redundantes y permita que VMware HA funcione sin intervención alguna.

- Se deben utilizar tramas gigantes si la red es compatible. Si se usan, asegúrese de que estén configurados de la misma forma en todos los dispositivos de red, VLAN, etc., en la ruta entre el almacenamiento y el host ESXi. De lo contrario, puede que observe problemas de rendimiento o conexión. La MTU también debe establecerse de forma idéntica en el switch virtual ESXi, el puerto de VMkernel y, además, en los puertos físicos o los grupos de interfaces de cada nodo ONTAP.
- NetApp solo recomienda deshabilitar el control de flujo de red en los puertos de interconexión del clúster de un clúster de ONTAP. NetApp no hace ninguna otra recomendación en cuanto a las mejores prácticas relativas al control de flujo para los puertos de red restantes que se usan para el tráfico de datos. Debe habilitarla o deshabilitarla según sea necesario. Consulte "CONSULTE TR-4182" para obtener más información sobre el control de flujo.
- Cuando las cabinas de almacenamiento ESXi y ONTAP están conectadas a redes de almacenamiento Ethernet, NetApp recomienda configurar los puertos Ethernet a los que se conectan estos sistemas como puertos periféricos del protocolo de árbol de expansión rápido (RSTP) o mediante la función PortFast de Cisco. NetApp recomienda habilitar la función de enlace troncal Spanning-Tree PortFast en entornos que utilizan la función Cisco PortFast y que tienen la conexión de enlaces VLAN 802.1Q habilitada tanto para el servidor ESXi como para las cabinas de almacenamiento ONTAP.
- NetApp recomienda las siguientes prácticas recomendadas para la agregación de enlaces:
  - Utilice switches que admitan la agregación de enlaces de puertos en dos chasis de switch separados mediante un enfoque de grupo de agregación de enlaces de varios chasis, como Virtual PortChannel (VPC) de Cisco.
  - Deshabilite LACP para los puertos del switch conectados a ESXi a menos que utilice dvSwitch 5.1 o una versión posterior con LACP configurado.
  - LACP se utiliza para crear agregados de enlaces para sistemas de almacenamiento ONTAP con grupos de interfaces dinámicas multimodo con hash IP.
  - Use una política de agrupación de hash IP en ESXi.

En la siguiente tabla se ofrece un resumen de los elementos de configuración de red e indica dónde se aplican los ajustes.

Elemento	ESXi	Conmutador	Nodo	SVM
Dirección IP	VMkernel	No**	No**	Sí
Agregación de enlaces	Switch virtual	Sí	Sí	No*
VLAN	VMkernel y grupos de puertos de máquina virtual	Sí	Sí	No*
Control de flujo	NIC	Sí	Sí	No*
Árbol expansivo	No	Sí	No	No
MTU (para tramas gigantes)	Conmutador virtual y puerto de VMkernel (9000)	Sí (configurado como máx.)	Sí (9000)	No*

Elemento	ESXi	Conmutador	Nodo	SVM
Grupos de conmutación por error	No	No	Sí (crear)	Sí (seleccione)

*Las LIF de SVM se conectan a puertos, grupos de interfaces o interfaces VLAN que tienen VLAN, MTU y otras configuraciones. Sin embargo, la configuración no se gestiona a nivel de SVM.

**Estos dispositivos tienen direcciones IP propias para la administración, pero estas direcciones no se utilizan en el contexto de las redes de almacenamiento ESXi.

SAN (FC, NVMe/FC, iSCSI, NVMe/TCP), RDM

ONTAP ofrece almacenamiento basado en bloques para VMware vSphere utilizando el protocolo iSCSI tradicional y Fibre Channel (FCP) así como el protocolo de bloque de nueva generación altamente eficiente y eficiente, NVMe over Fabrics (NVMe-oF), con soporte para NVMe/FC y NVMe/TCP.

Para obtener las mejores prácticas detalladas para implementar protocolos de bloque para almacenamiento de máquinas virtuales con vSphere y ONTAP, consulte "Almacenes de datos y protocolos: SAN"

NFS

VSphere permite a los clientes utilizar cabinas NFS de nivel empresarial para proporcionar acceso simultáneo a los almacenes de datos en todos los nodos de un clúster ESXi. Como se ha mencionado en la "almacenes de datos" sección, existen algunas ventajas de facilidad de uso y visibilidad de la eficiencia del almacenamiento cuando se usa NFS con vSphere.

Para conocer las prácticas recomendadas, consulte "Almacenes de datos y protocolos: NFS"

Conexión de red directa

A veces, los administradores de almacenamiento prefieren simplificar sus infraestructuras eliminando los switches de red de la configuración. Esto puede ser soportado en algunos escenarios. Sin embargo, hay algunas limitaciones y advertencias a tener en cuenta.

ISCSI y NVMe/TCP

Un host que utilice iSCSI o NVMe/TCP se puede conectar directamente a un sistema de almacenamiento y funcionar normalmente. El motivo son las rutas. Las conexiones directas a dos controladoras de almacenamiento diferentes dan como resultado dos rutas independientes para el flujo de datos. La pérdida de una ruta, un puerto o una controladora no impide que se utilice la otra ruta.

NFS

Se puede utilizar el almacenamiento NFS conectado directamente, pero con una limitación considerable: El fallo no funcionará si no se realiza una ejecución significativa de secuencias de comandos, que sería responsabilidad del cliente.

El motivo por el que la recuperación tras fallos sin interrupciones se complica gracias al almacenamiento NFS de conexión directa es el enrutamiento que se produce en el sistema operativo local. Por ejemplo, supongamos que un host tiene una dirección IP de 192.168.1.1/24 y está directamente conectado a una controladora ONTAP con la dirección IP 192.168.1.50/24. Durante la conmutación al nodo de respaldo, esa dirección 192.168.1.50 puede conmutar al nodo de respaldo a la otra controladora y estará disponible para el host, pero ¿cómo detecta el host su presencia? La dirección 192.168.1.1 original todavía existe en la NIC host

que ya no se conecta a un sistema operativo. El tráfico destinado a 192.168.1.50 seguiría enviándose a un puerto de red inoperable.

La segunda NIC del SO podría configurarse como 19 2.168.1.2 y sería capaz de comunicarse con la dirección fallida en 192.168.1.50, pero las tablas de enrutamiento locales tendrían un valor predeterminado de usar una dirección **y solo una** para comunicarse con la subred 192.168.1.0/24. Un administrador de sistema podría crear un marco de scripting que detectara una conexión de red fallida y alterara las tablas de enrutamiento locales o activara o desactivara las interfaces. El procedimiento exacto dependerá del sistema operativo en uso.

En la práctica, los clientes de NetApp disponen de NFS conectado directamente, pero normalmente solo para cargas de trabajo en las que se pueden pausar I/O durante las recuperaciones tras fallos. Cuando se utilizan montajes duros, no debe haber ningún error de E/S durante dichas pausas. El E/S se debe congelar hasta que se restauren los servicios, ya sea mediante una conmutación por recuperación o mediante intervención manual para mover las direcciones IP entre las NIC del host.

Conexión directa FC

No es posible conectar directamente un host a un sistema de almacenamiento ONTAP mediante el protocolo FC. La razón es el uso de NPIV. El WWN que identifica un puerto ONTAP FC con la red de FC utiliza un tipo de virtualización denominado NPIV. Cualquier dispositivo conectado a un sistema ONTAP debe poder reconocer un WWN de NPIV. No hay proveedores de HBA actuales que ofrezcan un HBA que se pueda instalar en un host que admita un destino NPIV.

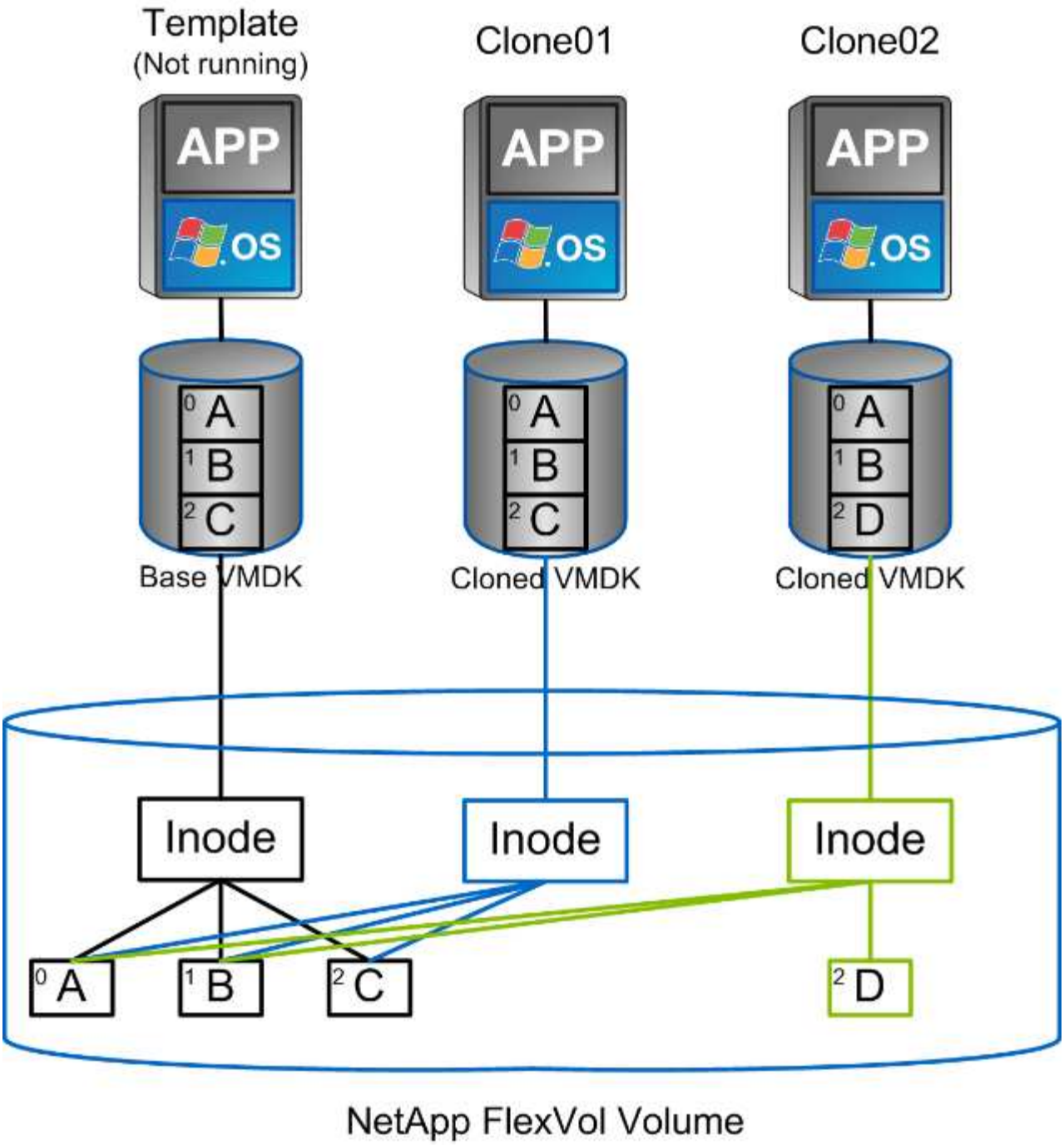
Clonado de máquinas virtuales y almacenes de datos

El clonado de un objeto de almacenamiento le permite crear rápidamente copias para un uso adicional, como el aprovisionamiento de equipos virtuales adicionales, operaciones de backup/recuperación de datos, etc.

En vSphere, es posible clonar una máquina virtual, un disco virtual, VVol o un almacén de datos. Después de que se clona, el objeto se puede personalizar aún más, a menudo mediante un proceso automatizado. VSphere es compatible con ambos clones de copias completas, así como clones enlazados, donde sigue los cambios de forma independiente del objeto original.

Los clones enlazados son excelentes para ahorrar espacio, pero aumentan la cantidad de I/o que vSphere gestiona para el equipo virtual, lo que afecta al rendimiento de ese equipo virtual y, quizás, al host en general. Por eso los clientes de NetApp suelen usar clones basados en sistemas de almacenamiento para obtener lo mejor de ambos mundos: Un uso eficiente del almacenamiento y un mayor rendimiento.

La siguiente figura muestra la clonación de ONTAP.



La clonado puede descargarse en sistemas que ejecutan ONTAP a través de varios mecanismos, normalmente a nivel de máquina virtual, VVol o almacén de datos. Entre ellos se incluyen los siguientes:

- VVols utiliza el proveedor de API de vSphere para el reconocimiento del almacenamiento (VASA) de NetApp. Los clones de ONTAP se utilizan para admitir copias Snapshot VVOL gestionadas por vCenter, que gestionan el espacio de forma eficiente y tienen un efecto de I/O mínimo para crearlas y eliminarlas. Las máquinas virtuales también pueden clonarse mediante vCenter y también se descargan en ONTAP, ya sea en un único almacén de datos/volumen o entre almacenes de datos/volúmenes.
- Clonado y migración de vSphere mediante API de vSphere: Integración de cabina (VAAI). Las operaciones de clonado de máquinas virtuales se pueden descargar en ONTAP tanto en entornos SAN como NAS (NetApp proporciona un complemento ESXi para habilitar VAAI para NFS). VSphere solo libera las operaciones en máquinas virtuales frías (apagadas) de un almacén de datos NAS, mientras que las operaciones en máquinas virtuales activas (clonado y vMotion de almacenamiento) también se descargan

para SAN. ONTAP utiliza el método más eficaz basado en el origen y el destino. Esta capacidad también es utilizada por "Omnissa Horizon View".

- SRA (utilizado con Live Site Recovery/Site Recovery Manager de VMware). Aquí, se utilizan clones para probar la recuperación de la réplica de recuperación ante desastres de forma no disruptiva.
- Backup y recuperación de datos con herramientas de NetApp como SnapCenter. Los clones de máquinas virtuales se utilizan para verificar las operaciones de backup, así como para montar un backup de equipo virtual para poder restaurar los archivos individuales.

El clonado descargado de ONTAP puede invocarse con VMware, NetApp y herramientas de terceros. Los clones que se descargan en ONTAP tienen varias ventajas. Ofrecen una gestión eficiente del espacio en la mayoría de los casos, y necesitan almacenamiento solo para los cambios en el objeto; no hay ningún efecto adicional en el rendimiento para leerlos y escribirlos; en algunos casos, el rendimiento mejora si se comparten los bloques en las cachés de alta velocidad. También descargan los ciclos de CPU y las operaciones de I/o de red del servidor ESXi. La copia de datos descargados dentro de un almacén de datos tradicional utilizando un FlexVol volume puede ser rápida y eficiente con licencia de FlexClone (incluida en la licencia ONTAP One), pero las copias entre volúmenes FlexVol pueden ser más lentas. Si mantiene las plantillas de equipos virtuales como origen de los clones, considere colocarlas en el volumen del almacén de datos (utilice carpetas o bibliotecas de contenido para organizarlas) para lograr clones rápidos con un uso eficiente del espacio.

También es posible clonar un volumen o LUN directamente en ONTAP para clonar un almacén de datos. Con almacenes de datos NFS, la tecnología FlexClone puede clonar un volumen completo, y el clon se puede exportar desde ONTAP y montar en ESXi como otro almacén de datos. En almacenes de datos VMFS, ONTAP puede clonar una LUN dentro de un volumen o un volumen entero, incluida una o varias LUN dentro de él. Una LUN que contiene un VMFS debe asignarse a un iGroup de ESXi y, a continuación, volver a firmar la bandeja de ESXi para que se monte y utilice como almacén de datos normal. Para algunos casos de uso temporales, se puede montar un VMFS clonado sin renuncias. Una vez que se ha clonado un almacén de datos, los equipos virtuales del interior se pueden registrar, volver a configurar y personalizar como si se clonaran individualmente.

En algunos casos, se pueden utilizar otras funciones con licencia para mejorar la clonación, como SnapRestore para backup o FlexClone. Estas licencias se incluyen a menudo en los paquetes de licencias sin coste adicional. Se necesita una licencia de FlexClone para las operaciones de clonado de VVol, así como para admitir Snapshot gestionadas de un VVol (que se descargan del hipervisor a ONTAP). Una licencia de FlexClone también puede mejorar ciertos clones basados en VAAI cuando se usan en un almacén de datos/volumen (crea copias instantáneas con gestión eficiente del espacio en lugar de copias de bloques). El SRA también usa para probar la recuperación de una réplica de DR, y el SnapCenter para las operaciones de clonado y para buscar copias de backup para restaurar archivos individuales.

Protección de datos

El backup y la recuperación rápida de sus máquinas virtuales son ventajas clave de usar ONTAP para vSphere. Esta funcionalidad se puede gestionar fácilmente dentro de vCenter mediante el complemento SnapCenter para VMware vSphere. Muchos clientes mejoran sus soluciones de backup de terceros con SnapCenter para aprovechar la tecnología Snapshot de ONTAP, ya que ofrece la forma más rápida y sencilla de recuperar una máquina virtual con ONTAP. SnapCenter está disponible de forma gratuita para los clientes que tengan la licencia ONTAP One, mientras que otros paquetes de licencia también pueden estar disponibles.

Además, el complemento SnapCenter para VMware puede integrarse con "BlueXP para backup y recuperación de datos de equipos virtuales", lo que posibilita soluciones de backup 3-2-1 efectivas para la mayoría de los sistemas ONTAP. Tenga en cuenta que se pueden aplicar algunas tarifas si se utiliza backup y

recuperación de BlueXP para máquinas virtuales con servicios premium, como almacenes de objetos para almacenamiento de backup adicional. En esta sección se describen las diversas opciones disponibles para proteger las máquinas virtuales y los almacenes de datos.

Snapshots de volumen de NetApp ONTAP

Use copias Snapshot para realizar copias rápidas de sus máquinas virtuales o almacenes de datos sin afectar al rendimiento y, a continuación, envíelas a un sistema secundario usando SnapMirror para la protección de datos fuera del sitio a largo plazo. Este método minimiza el espacio de almacenamiento y el ancho de banda de red porque solo almacena la información modificada.

Las copias Snapshot son una función clave de ONTAP, que le permite crear copias de un momento específico de sus datos. Permiten una gestión eficiente del espacio y se pueden crear rápidamente, por lo que son ideales para proteger equipos virtuales y almacenes de datos. Las copias Snapshot pueden utilizarse para distintos fines, como backup, recuperación de datos y pruebas. Estas copias Snapshot son diferentes de las copias snapshot de VMware (coherencia) y son adecuadas para la protección a largo plazo. Las copias Snapshot gestionadas con vCenter de VMware solo se recomiendan para su uso a corto plazo debido al rendimiento y otros efectos. Consulte "Limitaciones de Snapshot"si desea obtener más información.

Las snapshots se crean a nivel de volumen, y se pueden usar para proteger todas las máquinas virtuales y los almacenes de datos que hay en ese volumen. Esto significa que puede crear una copia de Snapshot de todo un almacén de datos, lo que incluye todas las máquinas virtuales que contiene.

En almacenes de datos NFS, puede ver fácilmente archivos de máquinas virtuales en snapshots navegando por el directorio .snapshots. De este modo, puede acceder rápidamente a ficheros y restaurarlos desde una instantánea sin necesidad de utilizar una solución de backup específica.

Para los almacenes de datos VMFS, se puede crear un FlexClone del almacén de datos a partir de la snapshot que desee. Esto permite crear un nuevo almacén de datos que esté basado en la snapshot, que se puede usar con fines de prueba o desarrollo. La FlexClone solo consumirá espacio para los cambios realizados después de realizar la snapshot, por lo que constituye una forma con gestión eficiente del espacio de crear una copia del almacén de datos. Una vez creada la FlexClone, puede asignar el LUN o el espacio de nombres a un host ESXi, como un almacén de datos normal. Esto no solo permite restaurar archivos específicos de equipos virtuales, sino que también le permite crear rápidamente entornos de prueba o desarrollo basados en datos de producción sin que el rendimiento del entorno de producción se vea afectado.

Para obtener más información sobre las Snapshot, consulte la documentación de ONTAP. Los siguientes enlaces proporcionan información adicional: "Copias Snapshot locales de ONTAP" "Replicación de ONTAP SnapMirror"

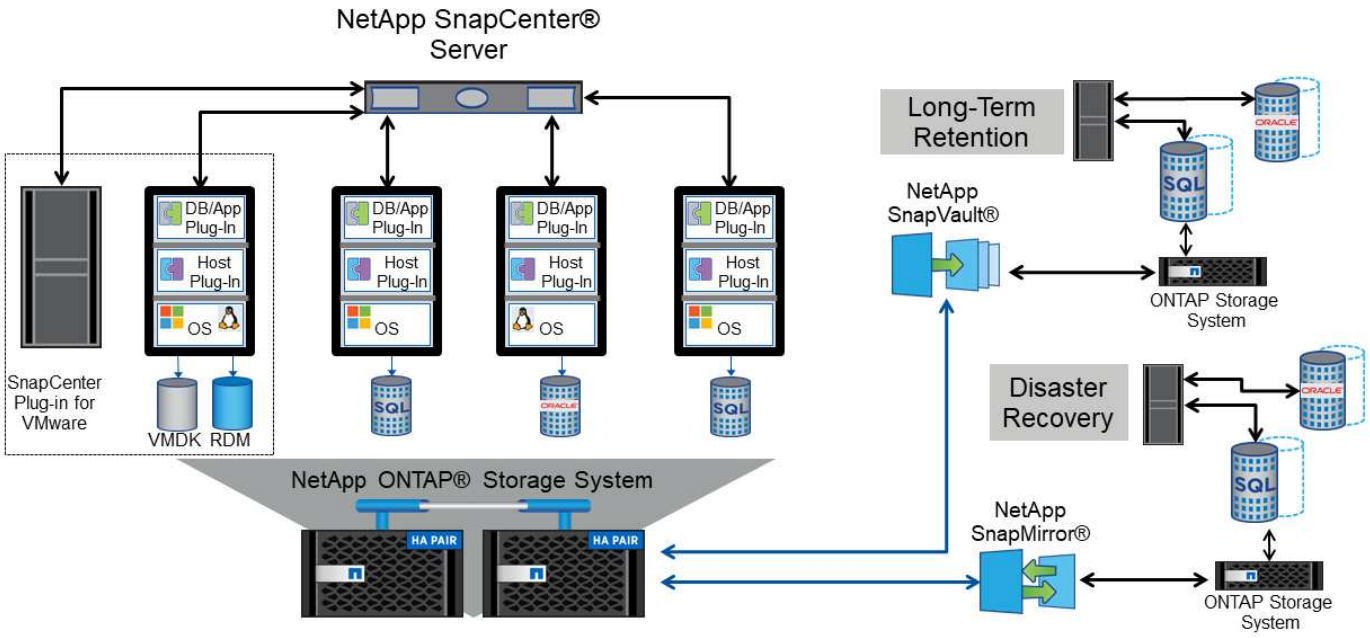
Complemento de SnapCenter para VMware vSphere

SnapCenter permite crear políticas de backup que se pueden aplicar a varias tareas. Estas políticas pueden definir programaciones, retención, replicación y otras funcionalidades. Continúan permitiendo una selección opcional de snapshots consistentes con las máquinas virtuales, lo que aprovecha la capacidad del hipervisor para poner en modo inactivo las operaciones de I/O antes de tomar una snapshot de VMware. Sin embargo, debido al efecto sobre el rendimiento de las snapshots de VMware, generalmente no se recomiendan a menos que necesite que el sistema de archivos invitados se coloque en modo inactivo. En su lugar, utilice los snapshots para protección general y use herramientas de aplicaciones como los complementos de aplicaciones de SnapCenter para proteger los datos transaccionales, como SQL Server u Oracle.

Estos complementos ofrecen funcionalidades ampliadas para proteger las bases de datos tanto en entornos físicos como virtuales. Con vSphere, puede utilizarlos para proteger bases de datos de SQL Server u Oracle donde los datos se almacenan en LUN de RDM, vVols o espacios de nombres NVMe/TCP y LUN iSCSI directamente conectados al sistema operativo invitado o archivos VMDK en almacenes de datos VMFS o

NFS. Estos plugins permiten especificar distintos tipos de backups de bases de datos, ya sea compatible con backups en línea o sin conexión, y proteger archivos de base de datos junto con archivos de registro. Además de backup y recuperación de datos, los plugins también admiten la clonado de bases de datos para fines de prueba o desarrollo.

En la siguiente figura se muestra un ejemplo de la instalación de SnapCenter.



Para obtener información sobre el tamaño, consulte la "Guía de configuración del complemento de SnapCenter para VMware vSphere"

Herramientas de ONTAP para VMware vSphere con VMware Live Site Recovery

Las herramientas de ONTAP para VMware vSphere (OT4VS) son un complemento gratuito que proporciona una integración sin problemas entre VMware vSphere y NetApp ONTAP. Le permite gestionar el almacenamiento de ONTAP directamente desde vSphere Web Client, lo que facilita la realización de tareas como el aprovisionamiento del almacenamiento, la gestión de la replicación y la supervisión del rendimiento.

Para funcionalidades mejoradas de recuperación ante desastres, considere el uso del SRA de NetApp para ONTAP, que forma parte de las herramientas de ONTAP para VMware vSphere, junto con Live Site Recovery de VMware (antes conocido como Site Recovery Manager). Esta herramienta no solo admite la replicación de almacenes de datos a un sitio de recuperación ante desastres mediante SnapMirror, sino que también permite realizar pruebas no disruptivas en el entorno de recuperación ante desastres mediante el clonado de los almacenes de datos replicados. Además, la recuperación tras un desastre y la reprotección de la producción después de resolver una interrupción del servicio se optimiza gracias a las funciones de automatización integradas.

Recuperación ante desastres de BlueXP

Recuperación ante desastres de BlueXP (DR) es un servicio basado en cloud que proporciona una solución completa para proteger sus datos y aplicaciones en caso de desastre. Ofrece una gama de funciones, como conmutación al respaldo y conmutación tras recuperación automatizadas, puntos de recuperación de múltiples puntos de tiempo, recuperación ante desastres consistente con las aplicaciones y soporte para sistemas de ONTAP tanto en las instalaciones como en el cloud. La recuperación ante desastres de BlueXP está diseñada para funcionar perfectamente con ONTAP y su entorno de VMware vSphere, lo que proporciona una solución

unificada para la recuperación ante desastres.

VSphere Metro Storage Cluster (VMSC) con sincronización activa NetApp MetroCluster y SnapMirror

Por último, para obtener el nivel más elevado de protección de datos, considere la configuración de clúster de almacenamiento Metro (VMSC) vSphere de VMware con NetApp MetroCluster. VMSC es una solución compatible con NetApp certificada por VMware que utiliza replicación síncrona, lo que le ofrece las mismas ventajas de un clúster de alta disponibilidad pero distribuido en diferentes ubicaciones para protegerse frente a desastres en el sitio. NetApp SnapMirror Active Sync, con ASA y AFF y MetroCluster con AFF, ofrece configuraciones rentables para replicación síncrona con recuperación transparente desde cualquier fallo de componente de almacenamiento individual así como recuperación transparente en el caso de sincronización activa de SnapMirror o recuperación con un único comando en caso de desastre en el centro con MetroCluster. "CONSULTE TR-4128"

Calidad de servicio (QoS)

Los límites de rendimiento son útiles para controlar los niveles de servicio, gestionar cargas de trabajo desconocidas o probar las aplicaciones antes de la puesta en marcha para asegurarse de que no afecten a otras cargas de trabajo en la producción. También se pueden utilizar para limitar una carga de trabajo abusivas una vez que se identifica.

Compatibilidad con las políticas de calidad de servicio de ONTAP

Los sistemas que ejecutan ONTAP pueden utilizar la función de calidad de servicio del almacenamiento para limitar el rendimiento en MB/s y/o I/O por segundo (IOPS) para diferentes objetos de almacenamiento, como archivos, LUN, volúmenes o SVM completas.

También admite niveles mínimos de servicio basados en IOPS para proporcionar un rendimiento constante para los objetos SAN en ONTAP 9.2 y para los objetos NAS en ONTAP 9.3.

El límite máximo de rendimiento de calidad de servicio en un objeto se puede establecer en Mbps o IOPS. Si se utilizan ambos, ONTAP aplica el primer límite alcanzado. Una carga de trabajo puede contener varios objetos y una política de calidad de servicio se puede aplicar a una o más cargas de trabajo. Cuando se aplica una política a varias cargas de trabajo, las cargas de trabajo comparten el límite total de la política. No se admiten los objetos anidados (por ejemplo, los archivos de un volumen no pueden tener cada uno su propia política). Los valores mínimos de calidad de servicio solo se pueden establecer en IOPS.

Las siguientes herramientas están disponibles en este momento para gestionar las políticas de calidad de servicio de ONTAP y aplicarlas a los objetos:

- CLI de ONTAP
- System Manager de ONTAP
- OnCommand Workflow Automation
- Active IQ Unified Manager
- Kit de herramientas NetApp PowerShell para ONTAP
- Herramientas de ONTAP para VASA Provider de VMware vSphere

Para asignar una normativa de calidad de servicio a un LUN, incluidos VMFS y RDM, la SVM de ONTAP (mostrada como Vserver), la ruta de LUN y el número de serie pueden obtenerse en el menú sistemas de almacenamiento de la página de inicio de ONTAP Tools para VMware vSphere. Seleccione el sistema de almacenamiento (SVM) y, a continuación, Related Objects > SAN. Use este enfoque cuando especifique la

calidad de servicio mediante una de las herramientas de ONTAP.

Consulte "Información general sobre la gestión y el control del rendimiento" si quiere más información.

Almacenes de datos NFS sin vVols

Una política de calidad de servicio de ONTAP puede aplicarse a todo el almacén de datos o archivos VMDK individuales que contiene. Sin embargo, es importante entender que todas las máquinas virtuales de un almacén de datos NFS tradicional (sin vVols) comparten una cola de I/O común desde un host determinado. Si alguna máquina virtual está regulada por una política de calidad de servicio de ONTAP, esta opción, en la práctica, provoca que todas las operaciones de I/O de ese almacén de datos parezcan aceleradas para ese host.

Ejemplo:
* Se configura un límite de QoS en vm1.vmdk para un volumen que se monta como almacén de datos NFS tradicional mediante el host esxi-01.
* El mismo host (esxi-01) está usando vm2.vmdk y está en el mismo volumen.
* Si vm1.vmdk se acelera, entonces vm2.vmdk también parecerá estar estrangulado ya que comparte la misma cola de IO con vm1.vmdk.

Esto no se aplica a vVols.

A partir de vSphere 6,5, puede gestionar los límites granulares de archivos en almacenes de datos que no son vVols aprovechando la gestión basada en políticas de almacenamiento (SPBM) con Storage I/O Control (SIOC) v2.

Consulte los siguientes enlaces para obtener más información sobre la gestión del rendimiento con las políticas de SIOC y SPBM.

"Reglas basadas en host de SPBM: SIOC v2"
"Gestione los recursos de I/O de almacenamiento con vSphere"

Para asignar una política de calidad de servicio a un VMDK en NFS, tenga en cuenta las siguientes directrices:

- La política debe aplicarse a la `vmname-flat.vmdk` que contiene la imagen del disco virtual real, no la `vmname.vmdk` (archivo de descriptor de disco virtual) o. `vmname.vmx` (Archivo descriptor de máquina virtual).
- No aplique políticas a otros archivos del equipo virtual, como archivos de intercambio virtual (`vmname.vswp`).
- Cuando utilice el cliente web de vSphere para buscar rutas de archivos (Datastore > Files), tenga en cuenta que combina la información del `- flat.vmdk` y.. `. vmdk` y simplemente muestra un archivo con el nombre del `. vmdk` pero el tamaño del `- flat.vmdk`. Agregar `-flat` en el nombre del archivo para obtener la ruta correcta.

Los almacenes de datos de FlexGroup ofrecen funcionalidades de calidad de servicio mejoradas al usar las herramientas de ONTAP para VMware vSphere 9.8 y versiones posteriores. Puede establecer fácilmente la calidad de servicio en todas las máquinas virtuales de un almacén de datos o en máquinas virtuales específicas. Consulte la sección FlexGroup de este informe para obtener más información. Tenga en cuenta que se siguen aplicando las limitaciones de la calidad de servicio mencionadas anteriormente con almacenes de datos NFS tradicionales.

Almacenes de datos de VMFS

Al usar los LUN de ONTAP, las políticas de calidad de servicio se pueden aplicar al volumen de FlexVol que contiene los LUN o los LUN individuales, pero no archivos VMDK individuales, ya que ONTAP no es consciente del sistema de archivos VMFS.

Almacenes de datos de vVols

La calidad de servicio mínima o máxima se puede establecer fácilmente en máquinas virtuales o VMDK individuales sin que ello afecte a ningún otro equipo virtual o VMDK gracias a la gestión basada en políticas de almacenamiento y vVols.

Al crear el perfil de funcionalidad de almacenamiento para el contenedor de VVol, especifique un valor de IOPS máximo y/o mínimo con la funcionalidad de rendimiento y, a continuación, haga referencia a este SCP con la política de almacenamiento de la máquina virtual. Use esta política cuando cree la máquina virtual o aplique la política a una máquina virtual existente.

> VVols requiere el uso de herramientas de ONTAP para VMware vSphere, que funciona como proveedor VASA para ONTAP. Consulte "VMware vSphere Virtual Volumes (vVols) con ONTAP"para ver las prácticas recomendadas de vVols.

ONTAP QoS y VMware SIOC

La calidad de servicio de ONTAP y el control de I/O de almacenamiento de VMware vSphere (SIOC) son tecnologías complementarias que los administradores de vSphere y de almacenamiento pueden utilizar conjuntamente para gestionar el rendimiento de las máquinas virtuales de vSphere alojadas en sistemas que ejecutan ONTAP. Cada herramienta tiene sus propias fuerzas, como se muestra en la siguiente tabla. Debido a los distintos ámbitos de VMware vCenter y ONTAP, algunos objetos pueden verse y gestionarse mediante un sistema, no el otro.

Propiedad	Calidad de servicio de ONTAP	VMware SIOC
Cuando está activo	La directiva está siempre activa	Activo cuando existe una contención (latencia por encima del umbral de los almacenes de datos)
Tipo de unidades	IOPS, Mbps	IOPS, recursos compartidos
Alcance de vCenter o aplicaciones	Varios entornos de vCenter, otros hipervisores y aplicaciones	Un único servidor vCenter
¿Establecer QoS en la máquina virtual?	VMDK solo en NFS	VMDK en NFS o VMFS
¿Establecer QoS en el LUN (RDM)?	Sí	No
¿Configurar QoS en LUN (VMFS)?	Sí	Sí (el almacén de datos puede acelerarse)
¿Configurar calidad de servicio en el volumen (almacén de datos NFS)?	Sí	Sí (el almacén de datos puede acelerarse)
¿Configurar la calidad de servicio en SVM (inquilino)?	Sí	No

Propiedad	Calidad de servicio de ONTAP	VMware SIOC
¿Enfoque basado en políticas?	Sí, pueden compartirse todas las cargas de trabajo de la política o aplicarse por completo a cada carga de trabajo de la política.	Sí, con vSphere 6.5 y posterior.
Se requiere licencia	Incluido con ONTAP	Enterprise Plus

Planificador de recursos distribuidos de almacenamiento de VMware

El planificador de recursos distribuidos de almacenamiento (SDRS) de VMware es una función de vSphere que coloca los equipos virtuales en el almacenamiento en función de la latencia de I/o actual y el uso del espacio. A continuación, mueve la máquina virtual o los VMDK de forma no disruptiva entre los almacenes de datos de un clúster de almacenes de datos (también conocido como "pod"), seleccionando el mejor almacén de datos en el que colocar la máquina virtual o los VMDK en el clúster de almacenes de datos. Un clúster de almacenes de datos es una colección de almacenes de datos similares que se agregan en una única unidad de consumo desde la perspectiva del administrador de vSphere.

Cuando se usan SDRS con herramientas de ONTAP para VMware vSphere, primero debe crear un almacén de datos con el plugin, utilizar vCenter para crear el clúster de almacén de datos y, a continuación, añadir el almacén de datos. Una vez creado el clúster de almacenes de datos, es posible añadir almacenes de datos adicionales al clúster de almacenes de datos directamente desde el asistente de aprovisionamiento de la página Details.

Otras prácticas recomendadas de ONTAP para SDRS incluyen lo siguiente:

- Todos los almacenes de datos del clúster deben usar el mismo tipo de almacenamiento (como SAS, SATA o SSD), ser todos los almacenes de datos VMFS o NFS y tener la misma configuración de replicación y protección.
- Considere el uso de SDR en modo predeterminado (manual). Este enfoque permite revisar las recomendaciones y decidir si se aplican o no. Tenga en cuenta los siguientes efectos de las migraciones de VMDK:
  - Cuando SDRS mueve VMDK entre almacenes de datos, se pierde cualquier ahorro de espacio con la clonado o deduplicación de ONTAP. Puede volver a ejecutar la deduplicación para recuperar este ahorro.
  - Después de que SDRS mueva los VMDK, NetApp recomienda volver a crear las snapshots en el almacén de datos de origen porque el espacio se bloqueará por la máquina virtual que se movió.
  - Mover VMDK entre almacenes de datos en el mismo agregado tiene pocas ventajas y LOS SDRS no tienen visibilidad en otras cargas de trabajo que puedan compartir el agregado.

Gestión basada en políticas de almacenamiento y vVols

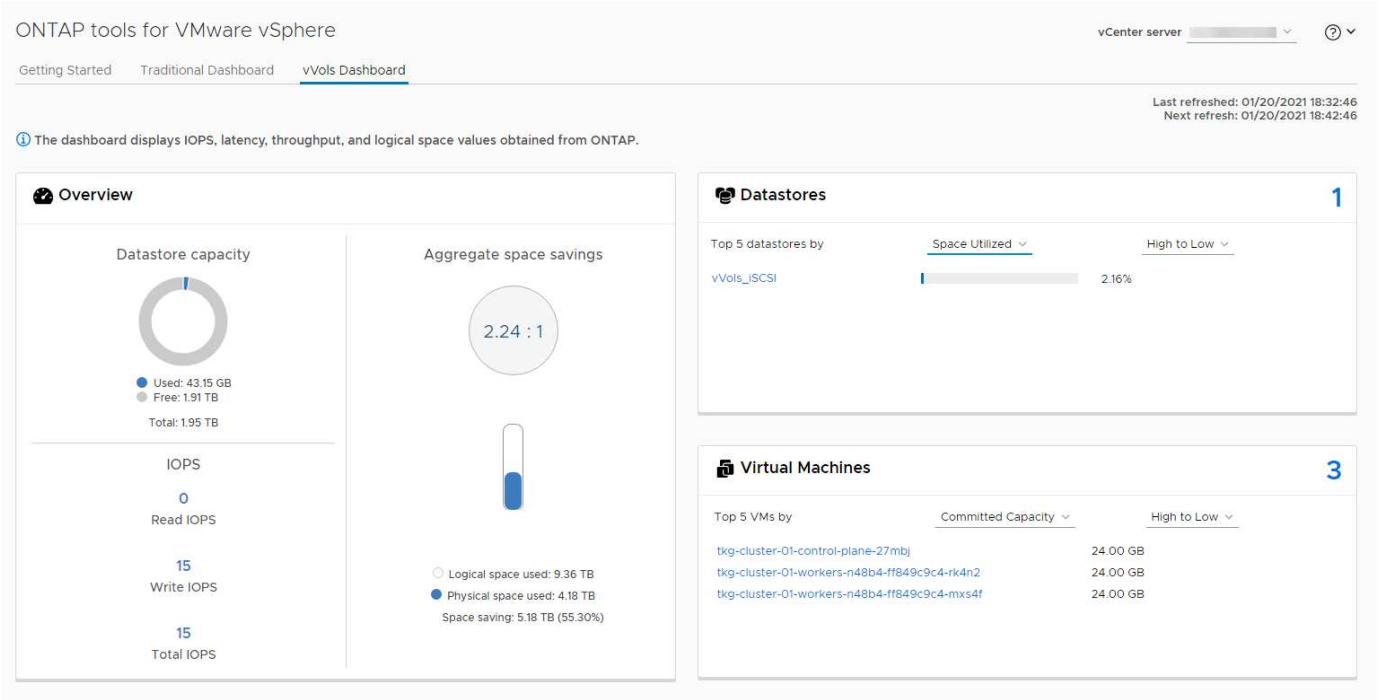
Las API de VMware vSphere para el reconocimiento del almacenamiento (VASA) facilitan que un administrador de almacenamiento configure almacenes de datos con funcionalidades bien definidas y permiten que el administrador de equipos virtuales los utilice siempre que sea necesario para aprovisionar máquinas virtuales sin tener que interactuar entre sí. Merece la pena echar un vistazo a este enfoque para ver cómo puede optimizar sus operaciones de almacenamiento de virtualización y evitar un gran trabajo trivial.

Antes de VASA, los administradores de máquinas virtuales podían definir políticas de almacenamiento de máquinas virtuales, pero tenían que trabajar con el administrador de almacenamiento para identificar los almacenes de datos adecuados, a menudo usando documentación o convenciones de nomenclatura. Con VASA, el administrador de almacenamiento puede definir una serie de capacidades de almacenamiento, como

el rendimiento, la clasificación por niveles, el cifrado y la replicación. Un conjunto de funcionalidades para un volumen o un conjunto de volúmenes se denomina perfil de capacidad de almacenamiento (SCP).

El SCP admite QoS mínimo y/o máximo para los vVols de datos de una VM. La calidad de servicio mínima solo se admite en los sistemas AFF. Las herramientas de ONTAP para VMware vSphere incluyen una consola donde se muestra el rendimiento granular de máquinas virtuales y la capacidad lógica para vVols en sistemas ONTAP.

La siguiente figura muestra las herramientas de ONTAP para el panel de vVols de VMware vSphere 9.8.



Una vez definido el perfil de funcionalidad de almacenamiento, puede utilizarse para aprovisionar equipos virtuales mediante la normativa de almacenamiento que identifique sus requisitos. La asignación entre la política de almacenamiento de máquinas virtuales y el perfil de capacidad de almacenamiento de almacenes de datos permite que vCenter muestre una lista de almacenes de datos compatibles que podrá seleccionar. Este enfoque se conoce como gestión basada en políticas de almacenamiento.

VASA proporciona la tecnología para consultar el almacenamiento y devolver un conjunto de funcionalidades de almacenamiento a vCenter. Los proveedores de VASA proporcionan la traducción entre las API y construcciones del sistema de almacenamiento y las API de VMware que comprende vCenter. VASA Provider de NetApp para ONTAP se ofrece como parte de las herramientas de ONTAP para VM del dispositivo VMware vSphere. El complemento de vCenter proporciona la interfaz para aprovisionar y gestionar almacenes de datos VVOL, así como la capacidad para definir perfiles de capacidades de almacenamiento (SCPs).

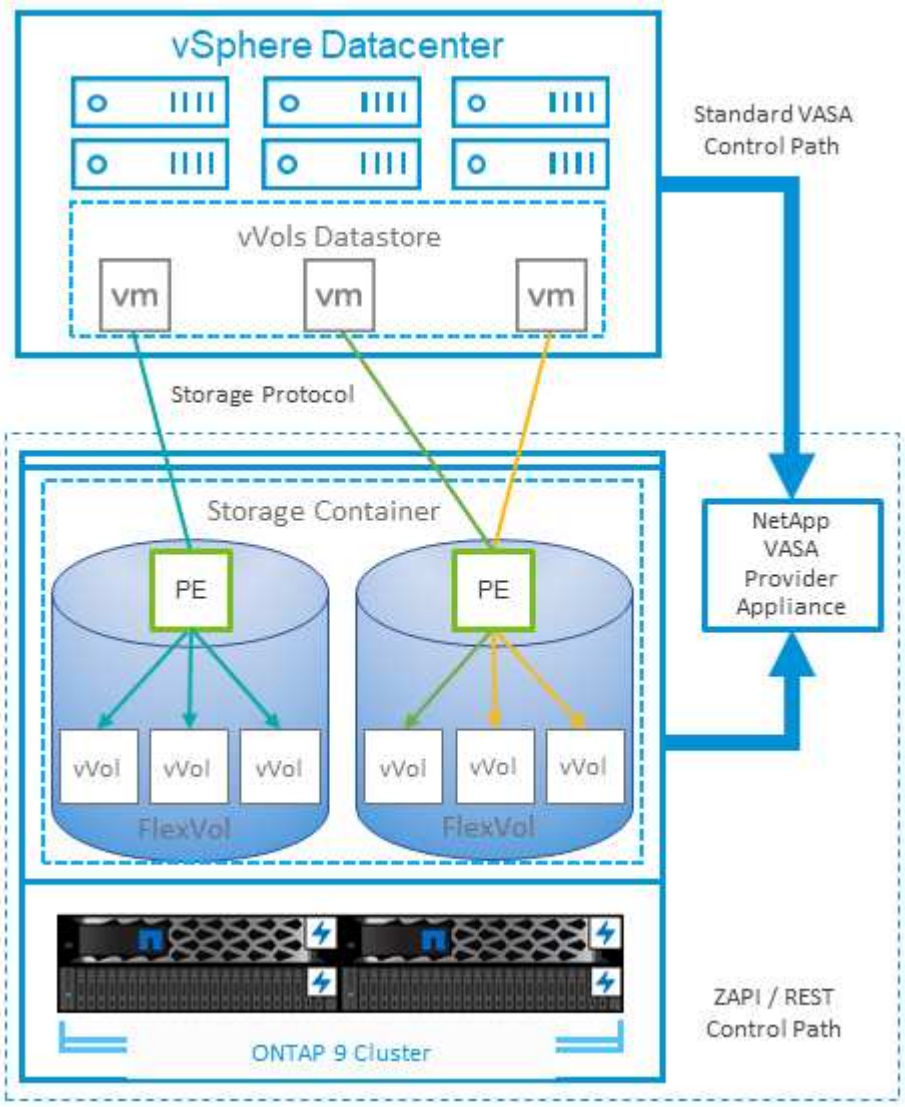
ONTAP admite almacenes de datos de VVol tanto VMFS como NFS. El uso de vVols con almacenes DE datos SAN aporta algunas de las ventajas de NFS, como la granularidad a nivel de equipo virtual. Aquí encontrará algunas prácticas recomendadas para tener en cuenta y información adicional en "CONSULTE TR-4400":

- Un almacén de datos de VVol puede consistir en varios volúmenes de FlexVol en varios nodos de clúster. El método más sencillo es un único almacén de datos, incluso cuando los volúmenes tienen diferentes funcionalidades. SPBM garantiza que se utiliza un volumen compatible para la máquina virtual. Sin embargo, todos los volúmenes deben formar parte de una única SVM de ONTAP y se debe acceder a ellos mediante un único protocolo. Un LIF por nodo para cada protocolo es suficiente. Evite el uso de varias versiones de ONTAP en un único almacén de datos de VVol, ya que las funcionalidades de

almacenamiento pueden variar entre las versiones.

- Utilice las herramientas de ONTAP para el plugin de VMware vSphere para crear y gestionar almacenes de datos de VVol. Además de gestionar el almacén de datos y su perfil, crea automáticamente un extremo de protocolo para acceder a vVols, si es necesario. Si se utilizan LUN, tenga en cuenta que los extremos de protocolo de LUN se asignan mediante los ID de LUN 300 y posteriores. Compruebe que la opción de configuración del sistema avanzado del host ESXi `Disk.MaxLUN` Permite un número de ID de LUN que sea mayor que 300 (el valor predeterminado es 1,024). Para realizar este paso, seleccione el host ESXi en vCenter, después la pestaña Configure y busque `Disk.MaxLUN` En la lista Advanced System Settings.
- No instale ni migre VASA Provider, vCenter Server (basado en dispositivos o Windows) ni las herramientas de ONTAP para VMware vSphere en un almacén de datos vVols, ya que estos dependen mutuamente, lo cual limita la capacidad de gestionarlos en caso de una interrupción del suministro eléctrico u otra interrupción del centro de datos.
- Realice un backup regular de la máquina virtual del proveedor de VASA. Como mínimo, cree copias Snapshot por hora del almacén de datos tradicional que contenga VASA Provider. Para obtener más información sobre la protección y recuperación del proveedor de VASA, consulte este tema "Artículo de base de conocimientos".

La siguiente figura muestra los componentes de vVols.



Migración al cloud y backup

Otra ventaja de ONTAP es la amplia compatibilidad con el cloud híbrido, al fusionar sistemas en el cloud privado local con funcionalidades de cloud público. Estas son algunas de las soluciones cloud de NetApp que se pueden usar junto con vSphere:

- **Ofertas de primera parte.** Amazon FSx para NetApp ONTAP, Google Cloud NetApp Volumes y Azure NetApp Files proporcionan servicios de almacenamiento gestionados multiprotocolo y de alto rendimiento en los principales entornos de nube pública. Pueden ser utilizados directamente por VMware Cloud en AWS (VMC en AWS), Azure VMware Solution (AVS) y Google Cloud VMware Engine (GCVE) como almacenes de datos o almacenamiento para sistemas operativos invitados (GOS) e instancias de computación.
- **Cloud Volumes ONTAP.** el software para la gestión de datos Cloud Volumes ONTAP de NetApp proporciona control, protección, flexibilidad y eficiencia para sus datos en el cloud que elija. Cloud Volumes ONTAP es un software para la gestión de datos nativo en el cloud e integrado en el almacenamiento de ONTAP. Utilícelo con Cloud Manager para poner en marcha y gestionar instancias de Cloud Volumes ONTAP junto con sus sistemas ONTAP locales. Aproveche las funcionalidades avanzadas de NAS e iSCSI SAN junto con la gestión de datos unificada, incluidas copias Snapshot y replicación de SnapMirror.
- **Servicios en la nube.** Utilice el backup y recuperación de datos de BlueXP o SnapMirror Cloud para proteger los datos de los sistemas locales mediante almacenamiento de cloud público. Cloud Sync ayuda a migrar y mantener sincronizados sus datos en NAS, almacenes de objetos y almacenamiento de Cloud Volumes Service. La recuperación ante desastres de BlueXP ofrece una solución rentable y eficiente para aprovechar las tecnologías de NetApp como base para una solución de recuperación ante desastres robusta y capaz para la recuperación de desastres en el cloud, de recuperación de desastres en las instalaciones y de on-premises a on-premises.
- **FabricPool.** FabricPool ofrece una organización en niveles rápida y fácil para los datos de ONTAP. Los bloques inactivos se pueden migrar a un almacén de objetos en clouds públicos o en un almacén de objetos de StorageGRID privado y se recuerdan automáticamente cuando se vuelve a acceder a los datos de ONTAP. También puede usar el nivel de objeto como un tercer nivel de protección para los datos que ya está gestionado por SnapVault. Este enfoque le permite "Almacenar más snapshots de sus máquinas virtuales" En sistemas de almacenamiento ONTAP principales o secundarios
- **ONTAP Select.** Utilice el almacenamiento definido por software de NetApp para ampliar su cloud privado a través de Internet a instalaciones y oficinas remotas, donde puede utilizar ONTAP Select para ofrecer compatibilidad con servicios de bloques y archivos, así como las mismas funcionalidades de gestión de datos vSphere que tiene en su centro de datos empresarial.

A la hora de diseñar sus aplicaciones basadas en máquinas virtuales, tenga en cuenta la movilidad del cloud futura. Por ejemplo, en lugar de colocar los archivos de datos y aplicaciones en conjunto, utilizan una exportación de NFS o LUN independiente para los datos. Esto permite migrar la máquina virtual y los datos por separado a los servicios de cloud.

Para obtener una visión más detallada de más temas de seguridad, consulte los siguientes recursos.

- "Documentación de Cloud Volumes ONTAP"
- "Documentación de ONTAP Select"
- "Documentación de backup y recuperación de BlueXP"
- "Documentación de la recuperación ante desastres de BlueXP"
- "Amazon FSX para ONTAP de NetApp"
- "VMware Cloud en AWS"

- "¿Qué es Azure NetApp Files?
  "
- "Solución Azure VMware"
- "Motor de Google Cloud VMware"
- "¿Qué es Google Cloud NetApp Volumes?"

Cifrado para datos de vSphere

Hoy en día, hay cada vez más demandas de protección de los datos en reposo mediante el cifrado. Aunque el foco inicial era la información financiera y de atención sanitaria, existe un creciente interés en proteger toda la información, ya sea en archivos, bases de datos u otros tipos de datos.

Los sistemas que ejecutan ONTAP facilitan la protección de cualquier dato con cifrado en reposo. El cifrado de almacenamiento de NetApp (NSE) utiliza unidades de autocifrado (SED) con ONTAP para proteger los datos SAN y NAS. NetApp también ofrece el cifrado de volúmenes de NetApp y el cifrado de agregados de NetApp como un método sencillo basado en software para cifrar volúmenes en cualquier unidad de disco. Este cifrado de software no requiere unidades de disco especiales ni gestores de claves externos y está disponible para los clientes de ONTAP sin coste adicional. Puede actualizarla y empezar a utilizarla sin interrumpir la actividad de sus clientes o aplicaciones, y están validados según el estándar FIPS 140-2 de nivel 1, incluido el gestor de claves incorporado.

Existen varios métodos para proteger los datos de las aplicaciones virtualizadas que se ejecutan en VMware vSphere. Uno de los métodos consiste en proteger los datos con software dentro de los equipos virtuales a nivel de SO «guest». Los hipervisores más recientes, como vSphere 6.5, ahora admiten el cifrado a nivel de equipo virtual como otra alternativa. Sin embargo, el cifrado del software de NetApp es simple y fácil y tiene estas ventajas:

- **Sin efecto sobre la CPU del servidor virtual.** algunos entornos de servidor virtual necesitan todos los ciclos de CPU disponibles para sus aplicaciones, aunque las pruebas han demostrado que se necesitan hasta 5 veces los recursos de CPU con cifrado a nivel de hipervisor. Incluso si el software de cifrado admite el conjunto de instrucciones AES-NI de Intel para descargar la carga de trabajo de cifrado (como lo hace el cifrado de software NetApp), este enfoque podría no ser factible debido a la necesidad de nuevas CPU que no son compatibles con servidores antiguos.
- **Onboard Key Manager incluido.** El cifrado de software de NetApp incluye un gestor de claves incorporado sin coste adicional, lo que facilita empezar sin servidores de gestión de claves de alta disponibilidad complejos de adquirir y utilizar.
- **No afecta a la eficiencia del almacenamiento.** las técnicas de eficiencia del almacenamiento como la deduplicación y la compresión se utilizan ampliamente hoy en día y son clave para utilizar medios de disco flash de forma rentable. Sin embargo, por lo general, los datos cifrados no se pueden deduplicar o comprimir. El cifrado de almacenamiento y hardware de NetApp funciona a un nivel inferior y permite el uso completo de funciones de eficiencia del almacenamiento de NetApp, líderes del sector, a diferencia de otros métodos.
- **Cifrado granular sencillo del almacén de datos.** con el cifrado de volúmenes de NetApp, cada volumen obtiene su propia clave AES de 256 bits. Si necesita cambiarlo, puede hacerlo con un solo comando. Este método es genial si tiene varios clientes o necesita probar el cifrado independiente para diferentes departamentos o aplicaciones. Este cifrado se gestiona a nivel de almacén de datos, lo cual es mucho más fácil que gestionar equipos virtuales individuales.

Es fácil empezar a utilizar el cifrado de software. Una vez instalada la licencia, solo tiene que configurar el administrador de claves incorporado especificando una clave de acceso y, a continuación, crear un volumen

nuevo o mover un volumen del lado del almacenamiento para habilitar el cifrado. NetApp está trabajando para añadir compatibilidad más integrada con funcionalidades de cifrado en futuros lanzamientos de sus herramientas de VMware.

Para obtener una visión más detallada de más temas de seguridad, consulte los siguientes recursos.

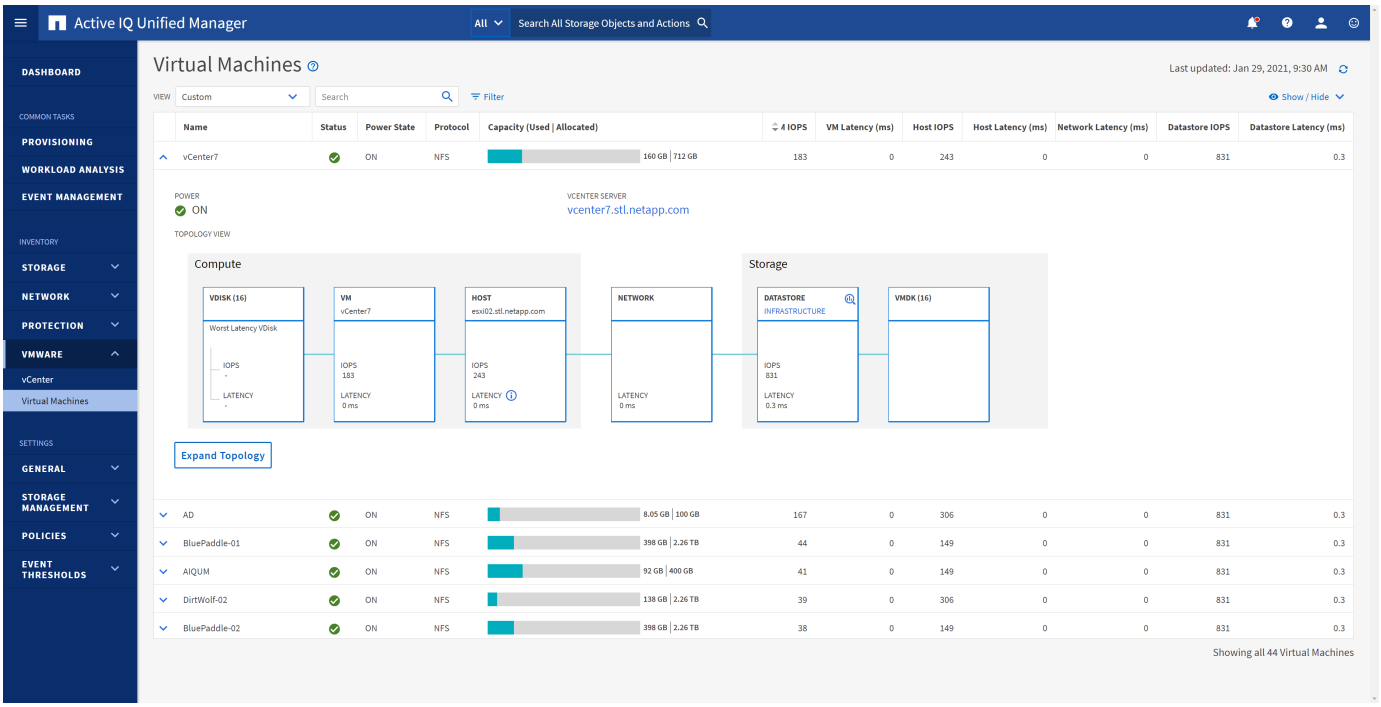
- "Informes técnicos de seguridad"
- "Guías de refuerzo de seguridad"
- "Documentación de productos de seguridad y cifrado de datos de ONTAP"

Active IQ Unified Manager

Active IQ Unified Manager proporciona visibilidad de los VM en su infraestructura virtual y permite supervisar y solucionar los problemas de almacenamiento y rendimiento en su entorno virtual.

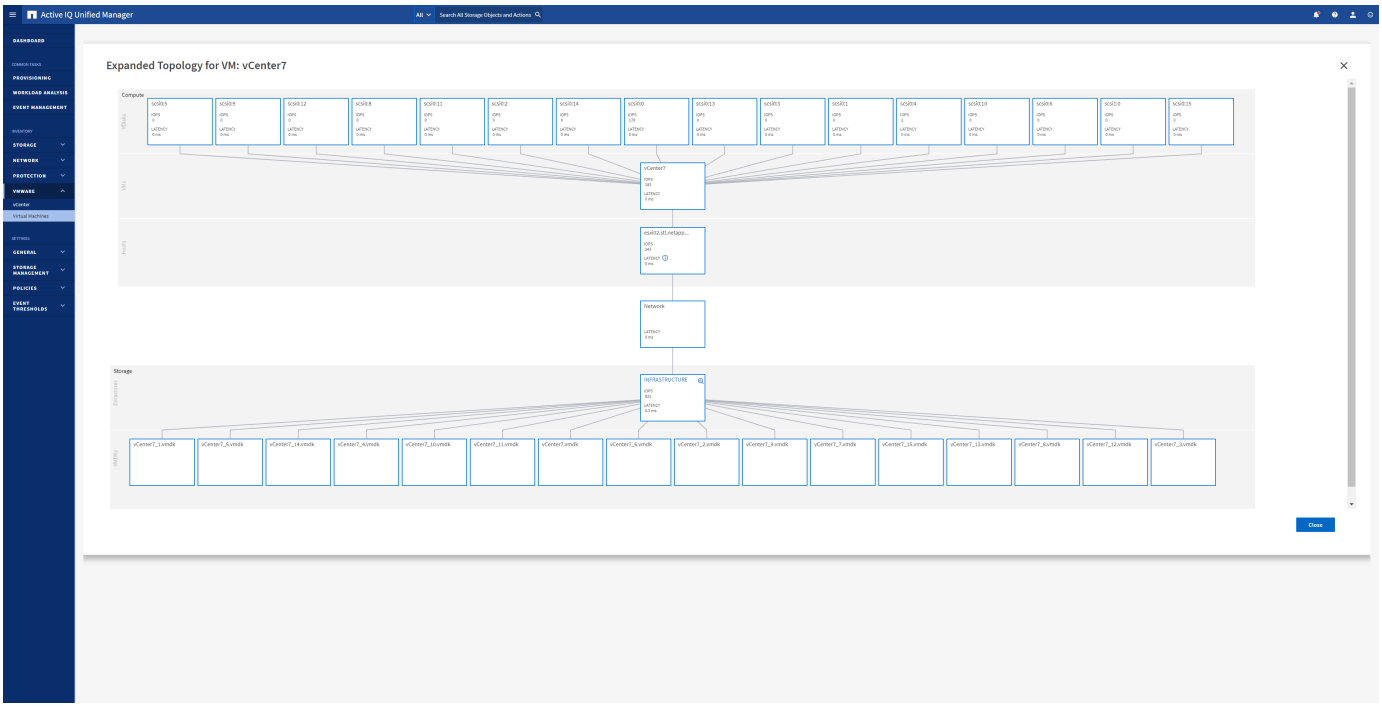
Una infraestructura virtual típica puesta en marcha en ONTAP tiene diversos componentes que se distribuyen en las capas informática, de red y de almacenamiento. Cualquier retraso en el rendimiento de una aplicación de equipo virtual puede producirse debido a una combinación de latencias que deben afrontar los distintos componentes de las capas respectivas.

La siguiente captura de pantalla muestra la vista Máquinas virtuales de Active IQ Unified Manager.



Unified Manager presenta el subsistema subyacente de un entorno virtual en una vista topológica para determinar si se ha producido un problema de latencia en el nodo de computación, la red o el almacenamiento. La vista también destaca el objeto específico que provoca el desfase en el rendimiento a la hora de dar pasos correctivas y solucionar el problema subyacente.

La siguiente captura de pantalla muestra la topología ampliada de AIUM.



Gestión basada en políticas de almacenamiento y vVols

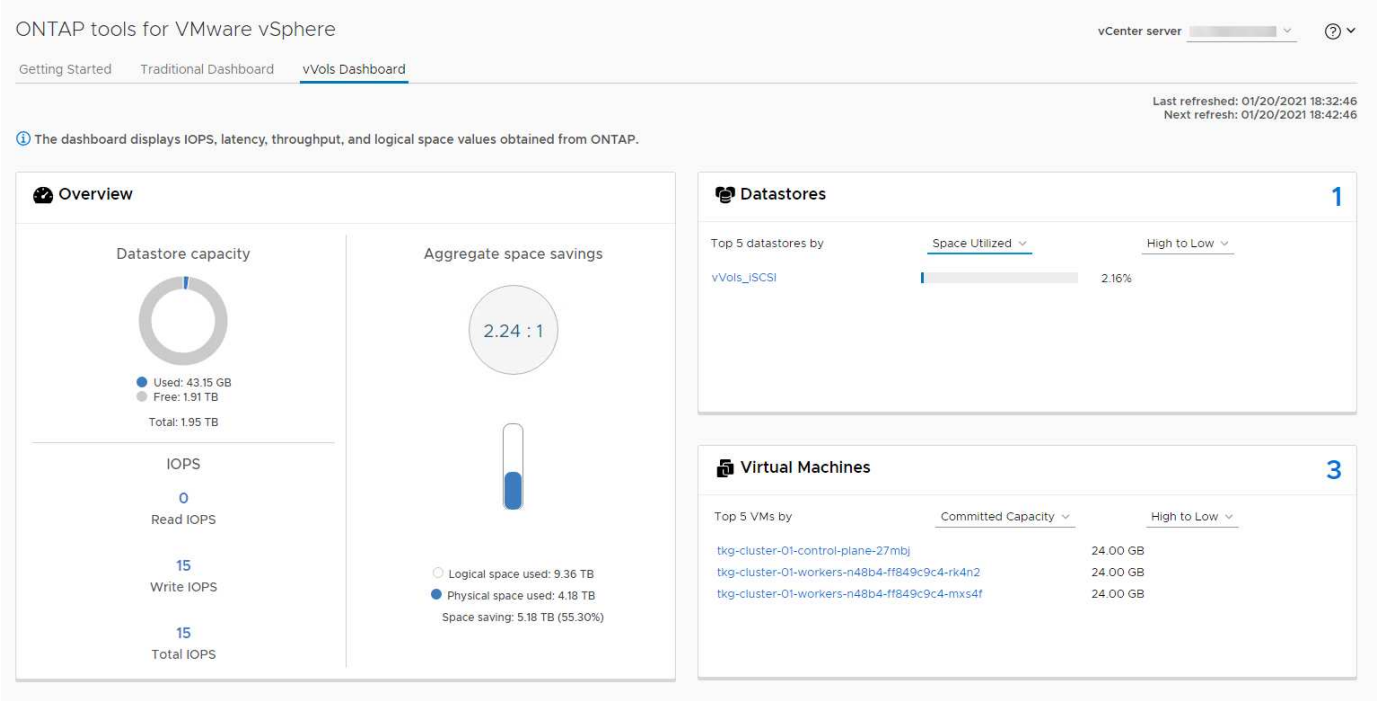
Las API de VMware vSphere para el reconocimiento del almacenamiento (VASA) facilitan que un administrador de almacenamiento configure almacenes de datos con funcionalidades bien definidas y permiten que el administrador de equipos virtuales los utilice siempre que sea necesario para aprovisionar máquinas virtuales sin tener que interactuar entre sí.

Merece la pena echar un vistazo a este enfoque para ver cómo puede optimizar sus operaciones de almacenamiento de virtualización y evitar un gran trabajo trivial.

Antes de VASA, los administradores de máquinas virtuales podían definir políticas de almacenamiento de máquinas virtuales, pero tenían que trabajar con el administrador de almacenamiento para identificar los almacenes de datos adecuados, a menudo usando documentación o convenciones de nomenclatura. Con VASA, el administrador de almacenamiento puede definir una serie de capacidades de almacenamiento, como el rendimiento, la clasificación por niveles, el cifrado y la replicación. Un conjunto de funcionalidades para un volumen o un conjunto de volúmenes se denomina perfil de capacidad de almacenamiento (SCP).

El SCP admite QoS mínimo y/o máximo para los vVols de datos de una VM. La calidad de servicio mínima solo se admite en los sistemas AFF. Las herramientas de ONTAP para VMware vSphere incluyen una consola donde se muestra el rendimiento granular de máquinas virtuales y la capacidad lógica para vVols en sistemas ONTAP.

La siguiente figura muestra las herramientas de ONTAP para el panel de vVols de VMware vSphere 9.8.



Una vez definido el perfil de funcionalidad de almacenamiento, puede utilizarse para aprovisionar equipos virtuales mediante la normativa de almacenamiento que identifique sus requisitos. La asignación entre la política de almacenamiento de máquinas virtuales y el perfil de capacidad de almacenamiento de almacenes de datos permite que vCenter muestre una lista de almacenes de datos compatibles que podrá seleccionar. Este enfoque se conoce como gestión basada en políticas de almacenamiento.

VASA proporciona la tecnología para consultar el almacenamiento y devolver un conjunto de funcionalidades de almacenamiento a vCenter. Los proveedores de VASA proporcionan la traducción entre las API y construcciones del sistema de almacenamiento y las API de VMware que comprende vCenter. VASA Provider de NetApp para ONTAP se ofrece como parte de las herramientas de ONTAP para VM del dispositivo VMware vSphere. El complemento de vCenter proporciona la interfaz para aprovisionar y gestionar almacenes de datos VVOL, así como la capacidad para definir perfiles de capacidades de almacenamiento (SCPs).

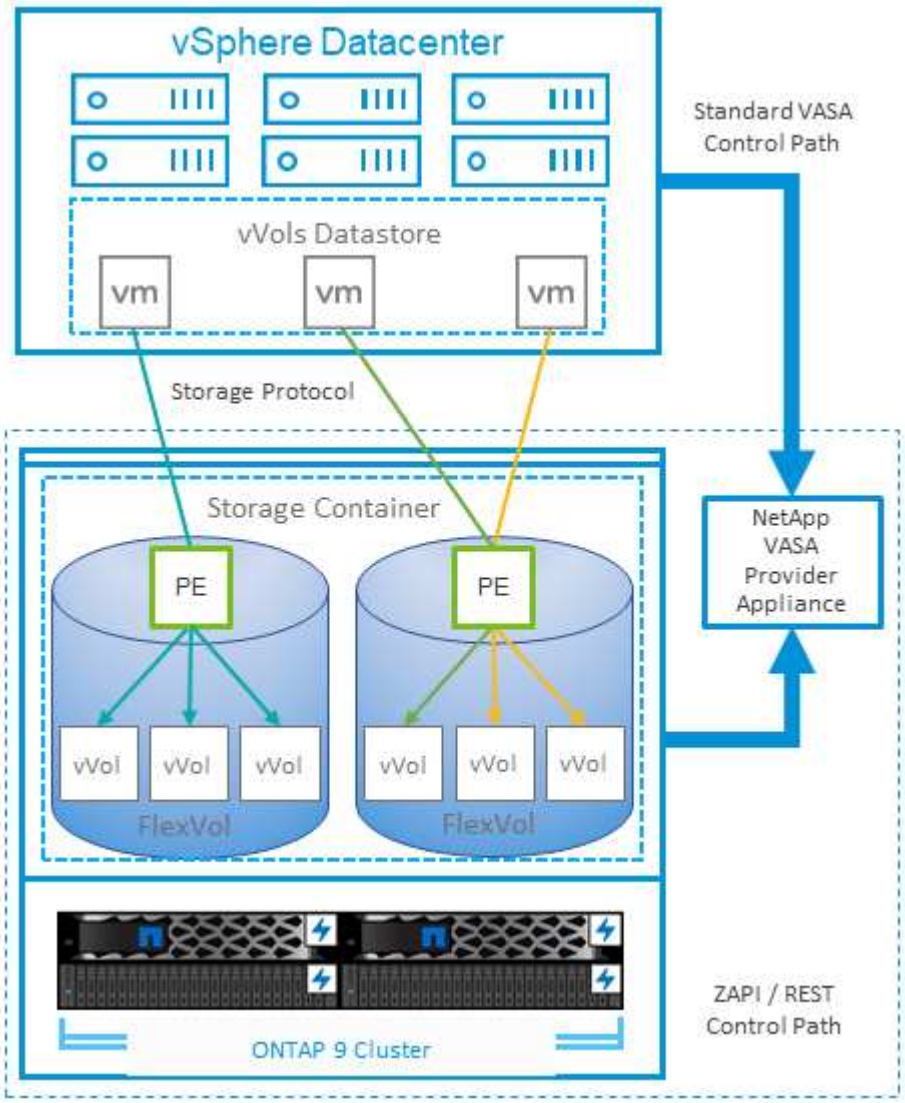
ONTAP admite almacenes de datos de VVol tanto VMFS como NFS. El uso de vVols con almacenes DE datos SAN aporta algunas de las ventajas de NFS, como la granularidad a nivel de equipo virtual. Aquí encontrará algunas prácticas recomendadas para tener en cuenta y información adicional en "CONSULTE TR-4400":

- Un almacén de datos de VVol puede consistir en varios volúmenes de FlexVol en varios nodos de clúster. El método más sencillo es un único almacén de datos, incluso cuando los volúmenes tienen diferentes funcionalidades. SPBM garantiza que se utiliza un volumen compatible para la máquina virtual. Sin embargo, todos los volúmenes deben formar parte de una única SVM de ONTAP y se debe acceder a ellos mediante un único protocolo. Un LIF por nodo para cada protocolo es suficiente. Evite el uso de varias versiones de ONTAP en un único almacén de datos de VVol, ya que las funcionalidades de almacenamiento pueden variar entre las versiones.
- Utilice las herramientas de ONTAP para el plugin de VMware vSphere para crear y gestionar almacenes de datos de VVol. Además de gestionar el almacén de datos y su perfil, crea automáticamente un extremo de protocolo para acceder a vVols, si es necesario. Si se utilizan LUN, tenga en cuenta que los extremos de protocolo de LUN se asignan mediante los ID de LUN 300 y posteriores. Compruebe que la opción de configuración del sistema avanzado del host ESXi `Disk.MaxLUN` Permite un número de ID de LUN que sea mayor que 300 (el valor predeterminado es 1,024). Para realizar este paso, seleccione el host ESXi en vCenter, después la pestaña Configure y busque `Disk.MaxLUN` En la lista Advanced System Settings.
- No instale ni migre VASA Provider, vCenter Server (basado en dispositivos o Windows) ni las herramientas

de ONTAP para VMware vSphere en un almacén de datos vVols, ya que estos dependen mutuamente, lo cual limita la capacidad de gestionarlos en caso de una interrupción del suministro eléctrico u otra interrupción del centro de datos.

- Realice un backup regular de la máquina virtual del proveedor de VASA. Como mínimo, cree copias Snapshot por hora del almacén de datos tradicional que contenga VASA Provider. Para obtener más información sobre la protección y recuperación del proveedor de VASA, consulte este tema "Artículo de base de conocimientos".

La siguiente figura muestra los componentes de vVols.



Planificador de recursos distribuidos de almacenamiento de VMware

El planificador de recursos distribuidos (SDRS) de VMware Storage es una función de vSphere que coloca automáticamente los equipos virtuales en un clúster de almacenes de datos en función de la latencia de I/O y el uso del espacio actuales.

A continuación, mueve la máquina virtual o los VMDK de forma no disruptiva entre los almacenes de datos de un clúster de almacenes de datos (también conocido como "pod"), seleccionando el mejor almacén de datos en el que colocar la máquina virtual o los VMDK en el clúster de almacenes de datos. Un clúster de almacenes de datos es una colección de almacenes de datos similares que se agregan en una única unidad

de consumo desde la perspectiva del administrador de vSphere.

Cuando se usan SDRS con herramientas de ONTAP para VMware vSphere, primero debe crear un almacén de datos con el plugin, utilizar vCenter para crear el clúster de almacén de datos y, a continuación, añadir el almacén de datos. Una vez creado el clúster de almacenes de datos, es posible añadir almacenes de datos adicionales al clúster de almacenes de datos directamente desde el asistente de aprovisionamiento de la página Details.

Otras prácticas recomendadas de ONTAP para SDRS incluyen lo siguiente:

- No utilice SDR a menos que tenga un requisito específico para hacerlo.
  - SDRS no es necesario cuando se utiliza ONTAP. LOS SDRS no son conscientes de las funciones de eficiencia del almacenamiento de ONTAP como la deduplicación y la compresión, por lo que puede tomar decisiones que no sean óptimas para su entorno.
  - LOS SDRS no son conscientes de las políticas de calidad de servicio de ONTAP, por lo que puede tomar decisiones que no sean óptimas para el rendimiento.
  - LOS SDRS no conocen las copias snapshot de ONTAP, por lo que se pueden tomar decisiones que hagan que las snapshots crezcan exponencialmente. Por ejemplo, al mover una máquina virtual a otro almacén de datos, se crean archivos nuevos en el nuevo almacén de datos, lo que hace que la copia Snapshot crezca. Esto se aplica sobre todo en el caso de equipos virtuales con discos de gran tamaño o gran cantidad de snapshots. En caso de que la máquina virtual vuelva a moverse al almacén de datos original, la copia Snapshot del almacén de datos original aumentará aún más.

Si utiliza SDR, tenga en cuenta las siguientes mejores prácticas:

- Todos los almacenes de datos del clúster deben usar el mismo tipo de almacenamiento (como SAS, SATA o SSD), ser todos los almacenes de datos VMFS o NFS y tener la misma configuración de replicación y protección.
- Considere el uso de SDR en modo predeterminado (manual). Este enfoque permite revisar las recomendaciones y decidir si se aplican o no. Tenga en cuenta los siguientes efectos de las migraciones de VMDK:
  - Cuando SDRS mueve VMDK entre almacenes de datos, se puede reducir el ahorro de espacio obtenido con el clonado o la deduplicación de ONTAP, en función de cómo se deduplique o comprima en el destino.
  - Después de que SDRS mueva los VMDK, NetApp recomienda volver a crear las snapshots en el almacén de datos de origen porque el espacio se bloqueará por la máquina virtual que se movió.
  - Mover VMDK entre almacenes de datos en el mismo agregado tiene pocas ventajas y LOS SDRS no tienen visibilidad en otras cargas de trabajo que puedan compartir el agregado.

Puede encontrar más información sobre LOS SDR en la documentación de VMware en "Preguntas frecuentes sobre el DRS de almacenamiento".

Host ESXi recomendado y otra configuración de ONTAP

NetApp ha desarrollado un conjunto de configuraciones óptimas de hosts ESXi tanto para los protocolos NFS como para los protocolos de bloques. También se proporciona orientación específica para configurar el tiempo de espera del adaptador de bus de host y la función multivía para que funcione correctamente con ONTAP basado en pruebas internas de NetApp y VMware.

Estos valores se establecen fácilmente mediante las herramientas de ONTAP para VMware vSphere: En la página de descripción general de herramientas de ONTAP, desplácese hasta la parte inferior y haga clic en Apply Recommended Settings en el portlet de cumplimiento de normativas de host ESXi.

Esta es la configuración de host recomendada para todas las versiones de ONTAP compatibles actualmente.

Configuración del host	Valor recomendado por NetApp	Se requiere reinicio
Configuración avanzada de ESXi		
VMFS3.HardwareAccelerated Locking	Mantener predeterminado (1)	No
VMFS3.EnableBlockDelete	Mantener el valor predeterminado (0), pero se puede cambiar si es necesario. Para obtener más información, consulte "Recuperación de espacio para VMFS5 equipos virtuales"	No
VMFS3.EnableVMFS6Unmap	Mantener valor predeterminado (1) Para obtener más información, consulte "API de VMware vSphere: Integración de cabinas (VAAI)"	No
Ajustes NFS		
NewSyncInterval	Si no utiliza vSphere CSI para Kubernetes, establezca Por "VMware KB 386364"	No
NET.TcpipHeapSize	VSphere 6.0 o posterior; establezca esta opción en 32. El resto de configuraciones de NFS se establecen en 30	Sí
NET.TcpipHeapMax	Configure 512 MB para la mayoría de las versiones de vSphere 6.X. Establezca el valor predeterminado (1024MB) para 6.5U3, 6.7U3 y 7,0 o posterior.	Sí
NFS.MaxVolumes	VSphere 6,0 o posterior, configurado en 256 Todas las demás configuraciones NFS están establecidas en 64.	No
NFS41.MaxVolumes	VSphere 6,0 o posterior, configurado en 256.	No
NFS.MaxQueueDepth	VSphere 6.0 o posterior; establezca esta opción en 128	Sí
NFS.HeartbeatMaxFailures	Establezca en 10 para todas las configuraciones NFS	No
NFS.HeartbeatFrequency	Establezca en 12 para todas las configuraciones NFS	No

Configuración del host	Valor recomendado por NetApp	Se requiere reinicio
NFS.HeartbeatTimeout	Establezca en 5 para todas las configuraciones NFS.	No
SunRPC.MaxConnPerIP	vSphere 7.0 a 8.0, establecido en 128. Esta configuración se ignora en las versiones de ESXi posteriores a 8.0.	No
Configuración de FC/FCoE		
Política de selección de rutas	Establezca el valor RR (round robin) cuando se utilicen rutas FC con ALUA. Establezca COMO FIJO para todas las demás configuraciones. Al establecer este valor en RR, se ayuda a proporcionar un equilibrio de carga en todas las rutas activas/optimizadas. El valor FIJO es para configuraciones antiguas que no pertenecen a ALUA y ayuda a evitar las operaciones de I/o del proxy En otras palabras, ayuda a evitar que las operaciones de I/o vayan al otro nodo de una pareja de alta disponibilidad (ha) en un entorno con Data ONTAP en 7-Mode	No
Disk.QFullSampleSize	Establezca en 32 para todas las configuraciones. Si configura este valor, se evitan los errores de I/O.	No
Disk.QFullThreshold	Establecer en 8 para todas las configuraciones. Si configura este valor, se evitan los errores de I/O.	No
Tiempos de espera de FC HBA de Emulex	Se utiliza el valor predeterminado.	No
Tiempos de espera de HBA FC de QLogic	Se utiliza el valor predeterminado.	No
Configuración iSCSI		
Política de selección de rutas	Establezca el valor RR (round robin) para todas las rutas iSCSI. Al establecer este valor en RR, se ayuda a proporcionar un equilibrio de carga en todas las rutas activas/optimizadas.	No

Configuración del host	Valor recomendado por NetApp	Se requiere reinicio
Disk.QFullSampleSize	Establezca en 32 para todas las configuraciones. Si configura este valor, se evitan los errores de I/O.	No
Disk.QFullThreshold	Establecer en 8 para todas las configuraciones. Si configura este valor, se evitan los errores de I/O.	No

La opción de configuración avanzada de NFS MaxQueueDepth puede no funcionar según lo previsto si se utiliza VMware vSphere ESXi 7.0.1 y VMware vSphere ESXi 7,0.2. Referencia "86331 de la base de conocimientos de VMware" para más información.

Las herramientas de ONTAP también especifican determinada configuración predeterminada al crear volúmenes de ONTAP FlexVol y LUN:

Herramienta ONTAP	Ajuste predeterminado
Reserva de Snapshot (-Porcentaje-espacio de instantáneas)	0
Reserva fraccionaria (-reserva fraccionaria)	0
Actualización del tiempo de acceso (-atime-update)	Falso
Lectura mínima (lectura mínima)	Falso
Snapshots programadas	Ninguno
Eficiencia del almacenamiento	Activado
Garantía de volumen	Ninguno (con thin provisioning)
Tamaño automático del volumen	aumentar_reducción
Reserva de espacio de LUN	Deshabilitado
Asignación de espacio de LUN	Activado

Configuración de multivía para el rendimiento

Aunque no está configurado actualmente por las herramientas de ONTAP disponibles, NetApp sugiere estas opciones de configuración:

- Al utilizar sistemas que no sean ASA en entornos de alto rendimiento o al probar el rendimiento con un único almacén de datos LUN, considere cambiar la configuración de equilibrio de carga de la política de selección de ruta (PSP) round-robin (VMW_PSP_RR) de la configuración de IOPS predeterminada de 1000 a un valor de 1. Ver"VMware KB 2069356" Para más información.
- En vSphere 6.7 Update 1, VMware introdujo un nuevo mecanismo de equilibrio de carga de latencia para Round Robin PSP. La opción de latencia ahora también está disponible cuando se utiliza HPP (complemento de alto rendimiento) con espacios de nombres NVMe y con vSphere 8.0u2 y versiones posteriores, LUN conectados iSCSI y FCP. La nueva opción considera el ancho de banda de E/S y la latencia de la ruta al seleccionar la ruta óptima para E/S. NetApp recomienda utilizar la opción de latencia en entornos con conectividad de ruta no equivalente, como casos con más saltos de red en una ruta que

en otra, o cuando se utiliza un sistema NetApp ASA . Ver "Cambie los parámetros predeterminados para la rotación de redondeo de latencia" Para más información.

Documentación adicional

Para FCP e iSCSI con vSphere 7, puede encontrar más información en "Utilice VMware vSphere 7.x con ONTAP" para FCP e iSCSI con vSphere 8, puede encontrar más información en "Utilice VMware vSphere 8.x con ONTAP" para NVMe-oF con vSphere 7. Para NVMe-oF con vSphere 8, puede encontrar más información en "Para NVMe-oF, puede encontrar más información en NVMe-oF Configuración del host para ESXi 7.x con ONTAP""Para NVMe-oF, puede encontrar más información en NVMe-oF Configuración del host para ESXi 8.x con ONTAP"

Virtual Volumes (vVols) con herramientas de ONTAP 10

Descripción general

ONTAP ha sido una solución de almacenamiento líder para entornos VMware vSphere durante más de dos décadas y continúa añadiendo funcionalidades innovadoras para simplificar la gestión al tiempo que reduce los costes.

Este documento trata las funcionalidades de ONTAP para VMware vSphere Virtual Volumes (vVols), incluida la información más reciente sobre el producto y los casos de uso, junto con las prácticas recomendadas y otra información para optimizar la puesta en marcha y reducir los errores.

> Esta documentación sustituye a los informes técnicos *TR-4400 publicados previamente: VMware vSphere Virtual Volumes (vVols) con ONTAP*

Las prácticas recomendadas complementan otros documentos, como guías y listas de compatibilidad. Se desarrollan según pruebas de laboratorio y una amplia experiencia de campo por parte de ingenieros y clientes de NetApp. Puede que no sean las únicas prácticas que funcionan o son compatibles, pero generalmente son las soluciones más simples que satisfacen las necesidades de la mayoría de los clientes.

> Este documento se ha actualizado para incluir las nuevas funciones de vVols que se encuentran en vSphere 8,0 update 3, el lanzamiento de ONTAP tools 10,4 y los nuevos sistemas NetApp ASA.

Información general sobre Virtual Volumes (vVols)

NetApp comenzó trabajando con VMware para dar soporte a las API vSphere de Storage Awareness (VASA) para vSphere 5 en 2012. Este primer proveedor de VASA permitía definir las capacidades de almacenamiento en un perfil que podía utilizarse para filtrar almacenes de datos al aprovisionar y comprobar después el cumplimiento de la política. Con el tiempo, esta evolución evolucionó y se añadieron nuevas funcionalidades que permitían una mayor automatización en el aprovisionamiento, y nuevos volúmenes virtuales o vVols, donde se utilizan objetos de almacenamiento individuales para archivos de máquinas virtuales y discos virtuales. Estos objetos podrían ser LUN, archivos y ahora con espacios de nombres vSphere 8 - NVMe (se utiliza con las herramientas de ONTAP 9.13P2). NetApp colaboró estrechamente con VMware como partner de referencia para vVols lanzado con vSphere 6 en 2015 y de nuevo como partner de diseño para vVols utilizando NVMe over Fabrics en vSphere 8. NetApp sigue mejorando vVols para aprovechar las últimas funcionalidades de ONTAP.

Hay varios componentes a tener en cuenta:

Proveedor de VASA

Este es el componente de software que gestiona la comunicación entre VMware vSphere y el sistema de almacenamiento. Para ONTAP, VASA Provider se ejecuta en un dispositivo conocido como herramientas de ONTAP para VMware vSphere (herramientas de ONTAP para abreviar). Las herramientas de ONTAP también incluyen un complemento para vCenter, un adaptador de replicación de almacenamiento (SRA) para el administrador de recuperación de sitio de VMware y un servidor API de REST para crear su propia automatización. Una vez que las herramientas de ONTAP se han configurado y registrado con vCenter, ya no es necesario interactuar directamente con el sistema ONTAP, ya que casi todas sus necesidades de almacenamiento pueden gestionarse desde la interfaz de usuario de vCenter o mediante la automatización de la API de REST.

Extremo de protocolo (PE)

El extremo de protocolo es un proxy para I/O entre los hosts ESXi y el almacén de datos vVols. El proveedor VASA de ONTAP crea estos automáticamente, ya sea un LUN de extremo de protocolo (4MB TB de tamaño) por volumen FlexVol del almacén de datos vVols, o un punto de montaje de NFS por interfaz NFS (LIF) en el nodo de almacenamiento que aloja un volumen FlexVol en el almacén de datos. El host ESXi monta estos extremos de protocolo de forma directa en lugar de LUN VVol individuales y archivos de disco virtual. No es necesario gestionar los extremos de protocolo, ya que el proveedor VASA los crea, monta, desmonta y elimina automáticamente, junto con los grupos de interfaces necesarios o las políticas de exportación.

Extremo de protocolo virtual (VPE)

Como novedad en vSphere 8, cuando se usa NVMe over Fabrics (NVMe-oF) con vVols, el concepto de extremo de protocolo ya no es relevante en ONTAP. En su lugar, el host ESXi crea una instancia de PE virtual automáticamente para cada grupo ANA en cuanto se enciende la primera máquina virtual. ONTAP crea automáticamente grupos ANA para cada volumen de FlexVol que usa el almacén de datos.

Otra ventaja de usar NVMe-oF para vVols es que no hay solicitudes de enlace requeridas del proveedor VASA. En su lugar, el host ESXi gestiona la funcionalidad de vinculación de VVol internamente según VPE. Esto reduce la posibilidad de que un enlace masivo de VVOL afecte al servicio.

Para obtener más información, consulte "NVMe y Virtual Volumes" encendido "vmware.com"

Almacén de datos de volúmenes virtuales

| El almacén de datos de volumen virtual es una representación lógica de un contenedor de vVols que crea y mantiene un proveedor de VASA. El contenedor representa un pool de capacidad de almacenamiento aprovisionado a partir de los sistemas de almacenamiento gestionados por el proveedor VASA. Las herramientas de ONTAP admiten la asignación de varios volúmenes de FlexVol (conocidos como volúmenes de backup) a un único almacén de datos vVols, y estos almacenes de datos de vVols pueden abarcar varios nodos de un clúster de ONTAP, que combina sistemas flash e híbridos con distintas funcionalidades. El administrador puede crear nuevos volúmenes de FlexVol con el asistente de aprovisionamiento o la API DE REST, o bien seleccionar volúmenes de FlexVol creados previamente para respaldar el almacenamiento si están disponibles.

Volúmenes virtuales (vVols)

VVols son los archivos y discos de máquina virtual reales almacenados en el almacén de datos vVols. El uso del término VVol (singular) está haciendo referencia a un archivo, LUN o espacio de nombres específico. ONTAP crea espacios de nombres, LUN o archivos de NVMe según el protocolo que utiliza el almacén de datos. Hay varios tipos distintos de vVols; los más comunes son Config (el único con VMFS en él, contiene archivos de metadatos como el archivo VMX de la VM), Data (disco virtual o VMDK) y Swap (creado cuando la VM está encendida). VVols protegido por el cifrado de VM de VMware será de tipo Otro. El cifrado de equipos

virtuales de VMware no se debe confundir con el cifrado de volúmenes de ONTAP o agregados.

Gestión basada en políticas

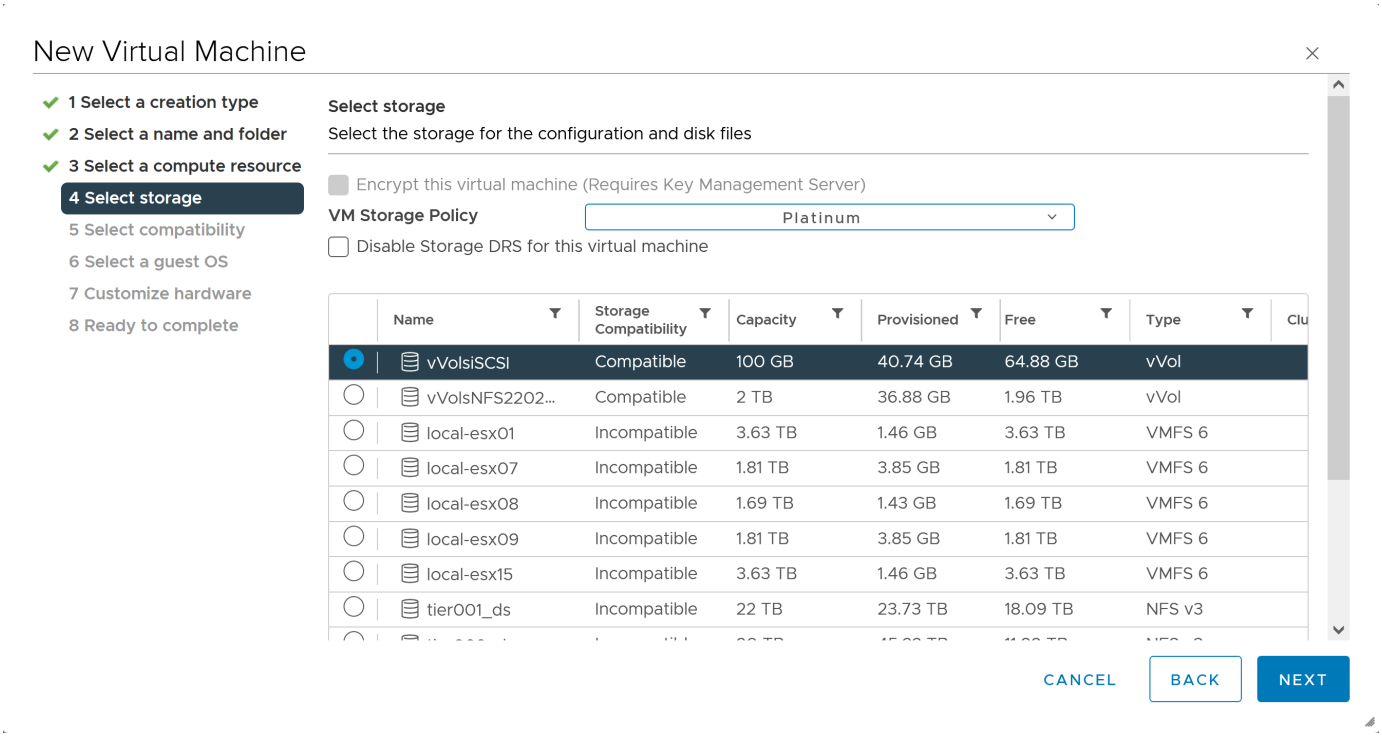
Las API de VMware vSphere para Storage Awareness (VASA) facilitan que un administrador de VM utilice cualquier capacidad de almacenamiento necesaria para aprovisionar máquinas virtuales sin tener que interactuar con su equipo de almacenamiento. Antes de VASA, los administradores de máquinas virtuales podían definir políticas de almacenamiento de máquinas virtuales, pero tenían que trabajar con sus administradores de almacenamiento para identificar los almacenes de datos adecuados, a menudo usando documentación o convenciones de nomenclatura. Con VASA, los administradores de vCenter con los permisos adecuados pueden definir una serie de funcionalidades de almacenamiento que los usuarios de vCenter pueden usar luego para aprovisionar máquinas virtuales. La asignación entre la política de almacenamiento de las máquinas virtuales y las capacidades de almacenes de datos permite a vCenter mostrar una lista de almacenes de datos compatibles para su selección, además de permitir que otras tecnologías como Aria (antes conocida como vRealize) Automation o Tanzu Kubernetes Grid seleccionen automáticamente el almacenamiento de una política asignada. Este enfoque se conoce como gestión basada en políticas de almacenamiento. Si bien las reglas del proveedor VASA y las políticas de almacenamiento de máquinas virtuales también pueden usarse con almacenes de datos tradicionales, nuestro enfoque se centra en los almacenes de datos vVols.

Políticas de almacenamiento de máquinas virtuales

Las políticas de almacenamiento de máquinas virtuales se crean en vCenter en Políticas y perfiles. Para vVols, cree un conjunto de reglas mediante reglas del proveedor de tipo de almacenamiento de NetApp vVols. Las herramientas de ONTAP 10.X ofrecen ahora un método más sencillo que las herramientas de ONTAP 9.X, ya que le permiten especificar directamente los atributos de almacenamiento en la normativa de almacenamiento de las máquinas virtuales misma.

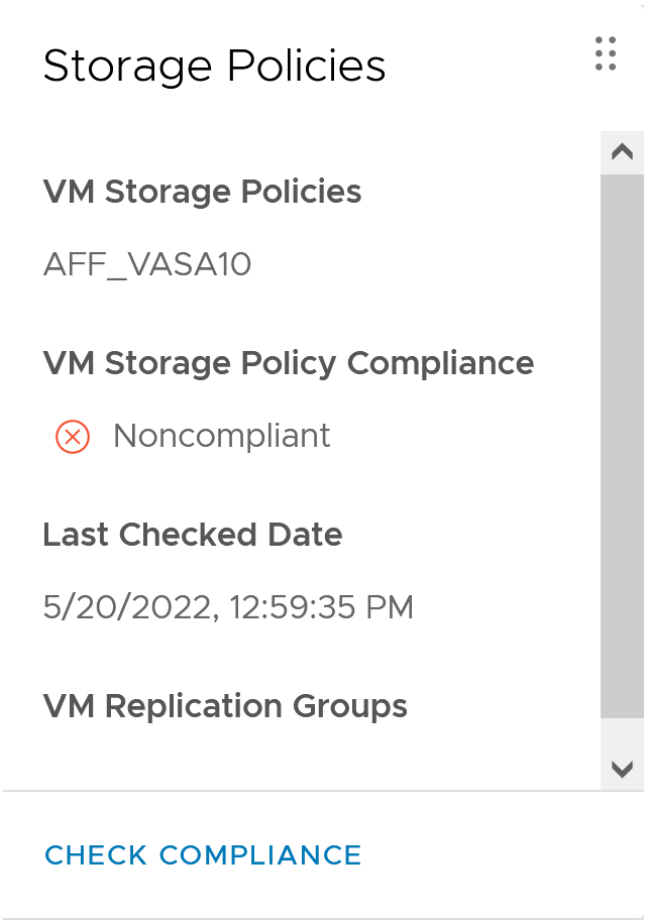
Como se ha mencionado anteriormente, el uso de políticas puede ayudar a simplificar la tarea de aprovisionar un equipo virtual o VMDK. Solo tiene que seleccionar una política adecuada y VASA Provider mostrará los almacenes de datos de vVols compatibles con esa política y colocará el VVOL en una FlexVol volume individual que cumpla las normativas.

Puesta en marcha de equipos virtuales mediante políticas de almacenamiento



Una vez que se aprovisiona una máquina virtual, el proveedor VASA seguirá comprobando el cumplimiento de normativas y alertará al administrador de máquinas virtuales con una alarma en vCenter cuando el volumen de respaldo ya no cumpla con la política.

Cumplimiento de políticas de almacenamiento de máquinas virtuales



Compatibilidad con NetApp vVols

ONTAP ha admitido la especificación VASA desde su versión inicial en 2012. Aunque otros sistemas de almacenamiento de NetApp son compatibles con VASA, este documento se centra en las versiones compatibles actualmente de ONTAP 9.

ONTAP

Además de ONTAP 9 en los sistemas AFF, ASA y FAS, NetApp admite cargas de trabajo de VMware en ONTAP Select, Amazon FSx para NetApp con VMware Cloud en AWS, Azure NetApp Files con la solución de VMware Azure, Cloud Volumes Service con Google Cloud VMware Engine y el almacenamiento privado de NetApp en Equinix sin embargo, la funcionalidad específica puede variar según el proveedor de servicios y la conectividad de red disponible. También está disponible el acceso desde invitados de vSphere a los datos almacenados en dichas configuraciones, así como en Cloud Volumes ONTAP.

En el momento de la publicación, los entornos de los proveedores a hiperescala se limitan solo a los almacenes de datos NFS v3 tradicionales, por lo tanto, los vVols solo están disponibles con sistemas ONTAP en las instalaciones o sistemas conectados al cloud que ofrecen la funcionalidad completa de sistemas en las instalaciones como los alojados por partners de NetApp y proveedores de servicios de todo el mundo.

Para obtener más información sobre ONTAP, consulte "Documentación de productos de ONTAP"

Para obtener más información acerca de las prácticas recomendadas para ONTAP y VMware vSphere, consulte "CONSULTE TR-4597"

Ventajas del uso de vVols con ONTAP

Cuando VMware introdujo la compatibilidad de vVols con VASA 2,0 en 2015, lo describió como «un marco de integración y gestión que ofrece un nuevo modelo operativo para almacenamiento externo (SAN/NAS)». Este modelo operativo ofrece varios beneficios junto con el almacenamiento de ONTAP.

Gestión basada en políticas

Tal como se explica en la sección 1,2, la gestión basada en políticas permite aprovisionar máquinas virtuales y gestionarse posteriormente usando políticas predefinidas. Esto puede ayudar a las operaciones DE TI DE varias maneras:

- * Aumentar velocidad.* Las herramientas ONTAP eliminan la necesidad de que el administrador de vCenter abra tickets con el equipo de almacenamiento para las actividades de aprovisionamiento de almacenamiento. Sin embargo, las funciones de RBAC de las herramientas de ONTAP en vCenter y en el sistema de ONTAP aún permiten equipos independientes (como equipos de almacenamiento) o actividades independientes del mismo equipo restringiendo el acceso a funciones específicas si se desea.
- * Provisionamiento más inteligente. * Las capacidades del sistema de almacenamiento se pueden exponer a través de las API de VASA, lo que permite que los flujos de trabajo de aprovisionamiento aprovechen las capacidades avanzadas sin que el administrador de VM tenga que entender cómo administrar el sistema de almacenamiento.
- * Provisionamiento más rápido.* Se pueden admitir diferentes capacidades de almacenamiento en un único almacén de datos y seleccionarlas automáticamente según sea apropiado para una VM basada en la política de VM.
- **Evite errores.** Las políticas de almacenamiento y VM se desarrollan con anticipación y se aplican según sea necesario sin tener que personalizar el almacenamiento cada vez que se aprovisiona una VM. Las alarmas de cumplimiento de normativas se generan cuando las funcionalidades de almacenamiento van más allá de las políticas definidas. Como se ha mencionado anteriormente, los SCPs hacen que el aprovisionamiento inicial sea predecible y repetible, mientras que basar las políticas de almacenamiento

de los equipos virtuales en los SCPs garantiza una ubicación precisa.

- * Mejor gestión de la capacidad.* Las herramientas VASA y ONTAP permiten ver la capacidad de almacenamiento hasta el nivel de agregado individual si es necesario y proporcionar varias capas de alerta en caso de que la capacidad empiece a ser baja.

Gestión granular de máquinas virtuales en el SAN moderno

Los sistemas de ALMACENAMIENTO SAN que utilizan Fibre Channel e iSCSI fueron los primeros en admitir VMware para ESX, pero no han podido gestionar archivos y discos de máquina virtual individuales desde el sistema de almacenamiento. En su lugar, se aprovisionan los LUN y VMFS gestiona los archivos individuales. Esto hace que sea difícil para el sistema de almacenamiento gestionar directamente el rendimiento, clonación y protección del almacenamiento de equipos virtuales individuales. VVols ofrece la granularidad del almacenamiento de la que los clientes que utilizan almacenamiento NFS ya disfrutan con las funciones SAN sólidas y de alto rendimiento de ONTAP.

Ahora, con las herramientas vSphere 8 y ONTAP para VMware vSphere 9,12 y versiones posteriores, esos mismos controles granulares que utilizan vVols para los protocolos heredados basados en SCSI están ahora disponibles en la SAN Fibre Channel moderna que utiliza NVMe over Fabrics para obtener un rendimiento aún mayor a escala. Con la actualización 1 de vSphere 8,0, ahora es posible implementar una solución NVMe integral completa usando vVols sin ninguna traducción de I/O en la pila de almacenamiento del hipervisor.

Mayor capacidad de descarga de soluciones de almacenamiento

Si bien VAAI ofrece varias operaciones que se descargan en el almacenamiento, existen algunas lagunas que se solucionan por el proveedor VASA. VAAI de SAN no puede descargar las snapshots gestionadas de VMware en el sistema de almacenamiento. VAAI de NFS puede descargar las copias Snapshot gestionadas por máquinas virtuales, pero existen limitaciones para colocar una máquina virtual con copias Snapshot de almacenamiento nativas. Dado que los vVols utilizan LUN, espacios de nombres o archivos individuales para discos de máquinas virtuales, ONTAP puede clonar de forma rápida y eficiente los archivos o LUN para crear copias Snapshot granulares de máquina virtual que ya no requieren archivos delta. VAAI de NFS tampoco admite operaciones de descarga de copias para migraciones activas de Storage vMotion (activadas). La máquina virtual debe apagarse para permitir la descarga de la migración cuando utilice VAAI con almacenes de datos NFS tradicionales. El proveedor VASA en las herramientas de ONTAP permite clones casi instantáneos con un uso eficiente del almacenamiento para migraciones activas e inactivas, y también admite copias casi instantáneas para migraciones entre volúmenes de vVols. Gracias a estas importantes ventajas en términos de eficiencia del almacenamiento, puede que pueda aprovechar al máximo las cargas de trabajo vVols de la "Garantía de eficiencia" programa. De la misma manera, si los clones entre volúmenes que utilizan VAAI no cumplen sus requisitos, probablemente podrá solucionar su reto empresarial gracias a las mejoras en la experiencia de copia con vVols.

Casos de uso comunes para vVols

Además de estos beneficios, también se observan estos casos de uso comunes para el almacenamiento de VVOL:

- **Provisionamiento bajo demanda de VMs**
  - Cloud privado o IaaS de proveedor de servicios.
  - Aproveche la automatización y la orquestación a través del paquete Aria (anteriormente vRealize), OpenStack, etc.
- **Discos de primera clase (FCDs)**
  - Volúmenes persistentes de VMware Tanzu Kubernetes Grid [TKG].
  - Proporcione servicios similares a los de Amazon EBS mediante la gestión independiente del ciclo de

vida de VMDK.

- **Provisionamiento bajo demanda de VMs temporales**
  - Laboratorios de prueba/desarrollo
  - Entornos de formación

Beneficios comunes con vVols

Cuando se utiliza a su máximo beneficio, como en los casos de uso anteriores, vVols proporciona las siguientes mejoras específicas:

- Los clones se crean rápidamente en un solo volumen, o entre varios volúmenes de un clúster de ONTAP, lo cual es una ventaja en comparación con los clones tradicionales con VAAI habilitada. Además, hacen un almacenamiento eficiente. Los clones dentro de un volumen utilizan el clon de archivos de ONTAP, que es como volúmenes FlexClone y solo almacenan cambios del archivo VVol/LUN/espacio de nombres de origen. Con el fin de que los equipos virtuales a largo plazo para la producción u otras aplicaciones se creen con rapidez, ocupan un espacio mínimo y pueden beneficiarse de la protección a nivel de equipo virtual (con el complemento SnapCenter de NetApp para VMware vSphere, copias Snapshot gestionadas de VMware o backup VADP) y gestión del rendimiento (con la calidad de servicio de ONTAP). Los clones entre volúmenes son mucho más rápidos con vVols que con VAAI becuase con VASA, podemos crear el clon y permitir el acceso a él en el destino antes de que se complete la copia. Los bloques de datos se copian como un proceso en segundo plano para completar los VVol de destino. Esto es similar a la forma en que el movimiento de LUN sin interrupciones de ONTAP funciona en los LUN tradicionales.
- Los vVols son la tecnología de almacenamiento ideal cuando se utiliza TKG con vSphere CSI, lo que proporciona capacidades y clases de almacenamiento discretas gestionadas por el administrador de vCenter.
- Los servicios similares a Amazon EBS se pueden entregar a través de FCDs porque un VMDK FCD, como su nombre indica, es un ciudadano de primera clase en vSphere y tiene un ciclo de vida que se puede administrar de forma independiente, independientemente de las VM a las que pueda estar conectado.

Lista de comprobación

Utilice esta lista de comprobación para la instalación para garantizar una puesta en marcha correcta (actualizada para 10,3 y versiones posteriores).

Planificación inicial

- Antes de comenzar la instalación, debe comprobar el "Herramienta de matriz de interoperabilidad (IMT)" para asegurarse de que la implementación ha sido certificada.
- Determine el tamaño y el tipo de configuración de las herramientas de ONTAP que necesita su entorno. Consulte el documento "Límites de configuración para poner en marcha herramientas de ONTAP para VMware vSphere" si desea obtener más información.
- Determine si utilizará SVM multitenant o permitir el acceso completo al clúster. Si utiliza SVM multitenant, deberá tener un LIF de gestión de SVM en cada SVM para usar. Las herramientas de ONTAP deben poder acceder a este LIF a través del puerto 443.
- Determine si utilizará Fibre Channel (FC) para la conectividad de almacenamiento. Si es así, "configurar la división en zonas" debe en sus switches FC para habilitar la conectividad entre los hosts ESXi y los LIF FC de la SVM.
- Determinar si va a usar el adaptador de replicación de almacenamiento (SRA) de herramientas de ONTAP para el administrador de recuperación de sitio (SRM) de VMware o la recuperación de sitios activos

(VLSR). Si es así, necesitará acceder a la interfaz de gestión del servidor SRM/VLSR para instalar el SRA.

- Si va a utilizar la replicación de SnapMirror gestionada por las herramientas de ONTAP (incluidas, entre otras, la sincronización activa de SnapMirror), el administrador de ONTAP debe "Cree una relación de paridad entre clústeres en ONTAP" y "Cree una relación entre iguales de SVM entre clústeres en ONTAP" antes de poder utilizar las herramientas de ONTAP con SnapMirror.
- "Descargue" Las herramientas de ONTAP OVA y, si es necesario, el archivo SRA tar.gz.

Provisión de direcciones IP y registros DNS

- Solicite la siguiente información IP a su equipo de red. Se requieren las primeras tres direcciones IP, y los nodos dos y tres se utilizan para puestas en marcha de escalado horizontal de alta disponibilidad. Los registros de host DNS son necesarios y todos los nombres de nodo y todas las direcciones deben estar en la misma VLAN y subred.
- Dirección de la aplicación de herramientas de ONTAP ___ . ___ . ____ . _____
- Dirección de Servicios Internos ___ . ___ . ____ . _____
- Nombre de host DNS del nodo uno _____
- Dirección IP del nodo uno ___. _ . \ . __
- Máscara de subred ___ . ___ . ____ . _____
- Puerta de enlace predeterminada ___ . ___ . ____ . _____
- Servidor DNS 1 ___ . ___ . ____ . _____
- Servidor DNS 2 ___ . ___ . ____ . _____
- Dominio de búsqueda DNS _____
- Nombre de host DNS del nodo dos (opcional) ____
- Dirección IP del nodo dos (opcional) ___. _ . \ . __
- Nombre de host DNS del nodo tres (opcional) ____
- Dirección IP del nodo tres (opcional) ___. _ . \ . __
- Cree registros DNS para todas las direcciones IP anteriores.

Configuración del firewall de red

- Abra los puertos necesarios para las direcciones IP anteriores en el firewall de red. Consulte la "Requisitos de puertos" para obtener la última actualización.

Reducida

- Se requiere un almacén de datos en un dispositivo de almacenamiento compartido. Opcionalmente, puede utilizar una biblioteca de contenidos en el mismo almacén de datos que el nodo uno para facilitar la clonación rápida de la plantilla con VAAI.
- Biblioteca de contenido (solo necesaria para HA) ____
- Nodo 1 almacén de datos ___
- Almacén de datos de nodo dos (opcional, pero recomendado para HA) _____
- Almacén de datos de nodo tres (opcional, pero recomendado para HA) ____

5 **Implemente el OVA**

- Tenga en cuenta que este paso puede tardar hasta 45 minutos en completarse
- "Implemente el OVA" Con el cliente vSphere.
- En el paso 3 de la implementación de OVA, seleccione la opción para personalizar el hardware de esta máquina virtual y configure lo siguiente en el paso 10:
- Activación de Hot Add de CPU
- Conexión en caliente de memoria

6 **Agregar vCenters a herramientas de ONTAP**

- "Añada instancias de vCenter Server" En el gestor de herramientas de ONTAP.

7 **Añadir back-ends de almacenamiento a herramientas de ONTAP**

- "Configure los roles y privilegios de usuario de ONTAP" Usando el archivo JSON incluido si no utiliza admin.
- Si se utiliza Si se usa multi-tenancy de almacenamiento con SVM
- "clústeres incorporados" En el administrador de herramientas de ONTAP y asócielo con vCenter.
- "SVM integradas" En ONTAP tools vCenter UI.
- Si **NO** usa SVM multitenant
- "clústeres incorporados" Directamente en la interfaz de usuario de ONTAP Tools vCenter. Como alternativa, en esta situación, es posible añadir SVM directamente cuando no se utilizan vVols.

8 **Configurar servicios de dispositivos (opcional)**

- Para utilizar vVols, primero debe "Edite la configuración del dispositivo y habilite el servicio VASA" . Al mismo tiempo, revise los dos elementos siguientes.
- Si tiene pensado utilizar vVols en producción, "alta disponibilidad" con las dos direcciones IP opcionales anteriores.
- Si tiene pensado utilizar las herramientas de ONTAP Storage Replication Adapter (SRA) para el administrador de recuperación de sitio de VMware o la recuperación de sitios activos, "Habilite los servicios de SRA".

9 **Certificados (opcional)**

- Según VMware, se requieren certificados firmados por CA si se utilizan vVols con varios vCenter.
- Servicios VASA ____
- Servicios ADMINISTRATIVOS ____

10 **Otras tareas posteriores al despliegue**

- Cree reglas de antiafinidad para equipos virtuales en una puesta en marcha de alta disponibilidad.

- Si se utiliza alta disponibilidad, los nodos de vMotion de almacenamiento dos y tres para separar almacenes de datos (opcional, pero recomendado).
- "usar administrar certificados" En el administrador de herramientas de ONTAP, para instalar los certificados requeridos firmados por CA.
- Si habilitó SRA para SRM/VLSR para proteger almacenes de datos tradicionales, "Configurar el SRA en el dispositivo VMware Live Site Recovery".
- Configurar Copias de Seguridad Nativas para "RPO casi cero".
- Configurar copias de seguridad regulares en otros medios de almacenamiento.

Usar vVols con ONTAP

La clave para usar vVols con NetApp es las herramientas de ONTAP para VMware vSphere, que son servidores como la interfaz VASA (vSphere API for Storage Awareness) Provider para sistemas ONTAP 9 de NetApp.

Las herramientas de ONTAP también incluyen extensiones de interfaz de usuario de vCenter, servicios API de REST, adaptadores de replicación de almacenamiento para VMware Site Recovery Manager / Live Site Recovery, herramientas de supervisión y configuración de host, y una serie de informes que le ayudan a gestionar mejor su entorno de VMware.

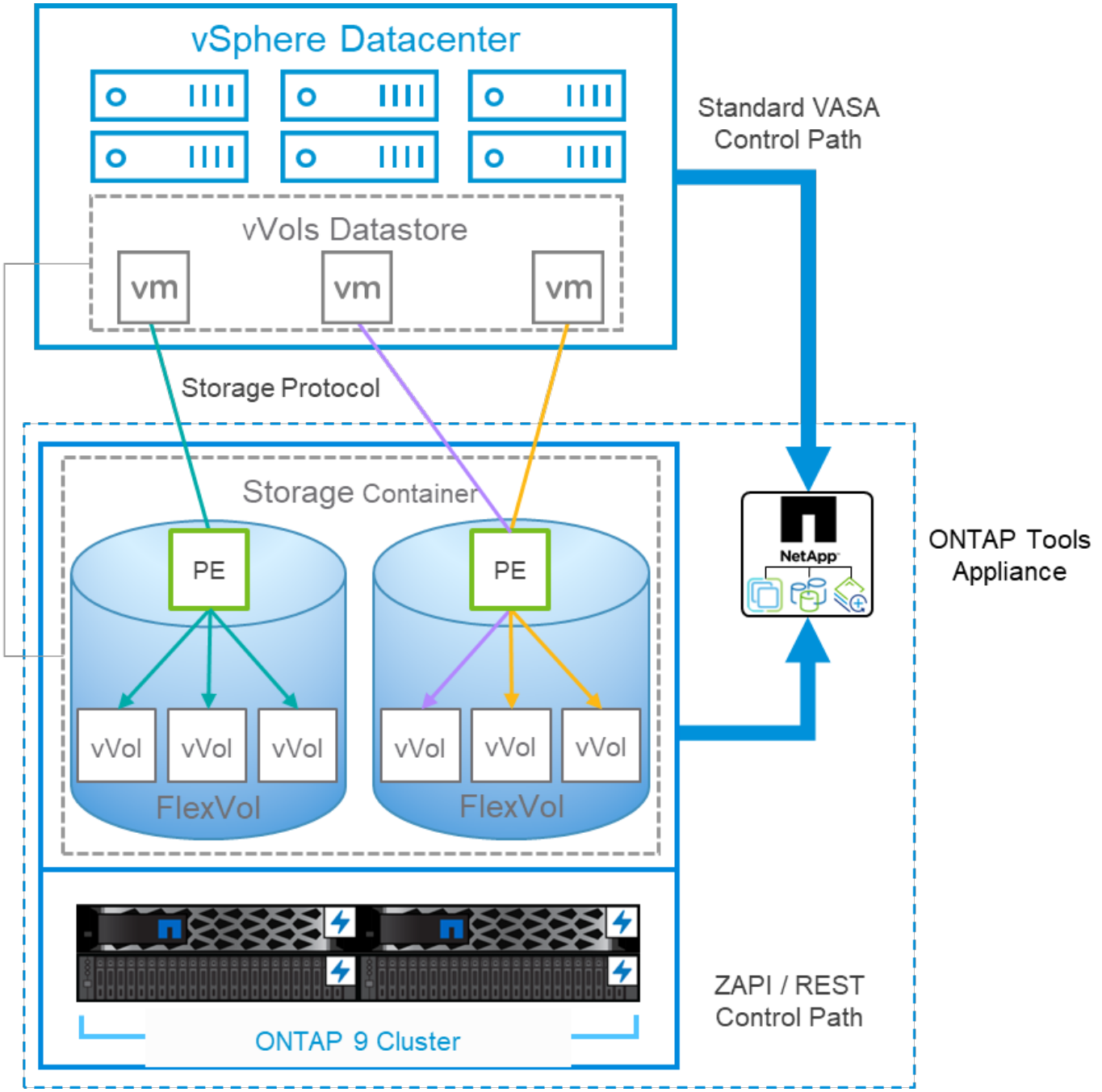
Productos y Documentación

La licencia ONTAP One incluye todas las licencias necesarias para utilizar vVols con sistemas ONTAP. El único requisito adicional es el OVA gratuito con herramientas de ONTAP, que actúa como proveedor VASA. En un entorno vVols, el software VASA Provider traduce las funcionalidades de cabinas en atributos basados en políticas que se pueden aprovechar a través de las API VASA sin que el administrador de vSphere tenga que saber cómo se gestionan las funcionalidades en segundo plano. Esto permite un consumo dinámico de la capacidad de almacenamiento asignada según políticas, lo que elimina la necesidad de crear manualmente almacenes de datos tradicionales y gestionar sus tasas de consumo de almacenamiento individuales. En resumen, vVols elimina toda la complejidad de la gestión del almacenamiento empresarial y la abstrae del administrador de vSphere para que puedan centrarse en la capa de virtualización.

Para los clientes que usan VMware Cloud Foundation con vSAN, vVols se puede agregar a cualquier dominio de gestión o carga de trabajo como almacenamiento complementario. VVols se integra perfectamente con vSAN a través de un marco de administración común basado en políticas de almacenamiento.

La familia de herramientas 10 de ONTAP de última generación moderniza las funcionalidades anteriores con una arquitectura escalable, en contenedores y basada en microservicio que se puede poner en marcha mediante un sencillo dispositivo de formato OVA en ESXi. ONTAP TOOLS 10 combina todas las funcionalidades de tres antiguos dispositivos y productos en una única implementación. Para la gestión de vVols, usará las intuitivas extensiones de interfaz de usuario de vCenter o las API de REST para las herramientas de ONTAP VASA Provider. Tenga en cuenta que el componente SRA es para almacenes de datos tradicionales; Site Recovery Manager de VMware no utiliza SRA para vVols.

ONTAP herramientas de la arquitectura VASA Provider cuando se utiliza iSCSI o FCP con sistemas unificados



Instalación del producto

En el caso de nuevas instalaciones, implemente el dispositivo virtual en el entorno de vSphere. Una vez puesta en marcha, puede iniciar sesión en la interfaz de usuario de administrador o utilizar las API REST para escalar vertical o horizontalmente la puesta en marcha, vCenters (esto registra el complemento con vCenter), sistemas de almacenamiento incorporados y asociar los sistemas de almacenamiento con sus vCenters. Solo es necesario incorporar sistemas de almacenamiento en la interfaz de usuario del administrador de herramientas de ONTAP y asociar clústeres con vCenters si planea utilizar multi-tenancy seguro con SVM dedicadas; de lo contrario, solo puede incorporar los clústeres de almacenamiento deseados en las extensiones de interfaz de usuario de ONTAP tools vCenter o mediante las API de REST.

Consulte "Despliegue de vVols Storage"en este documento, o "Documentación de las herramientas de ONTAP para VMware vSphere".

La práctica recomendada es almacenar las herramientas de ONTAP y los dispositivos vCenter en almacenes de datos NFS o VMFS tradicionales para evitar cualquier conflicto de interdependencia. Puesto que tanto las herramientas vCenter como ONTAP deben comunicarse entre sí durante las operaciones de vVols, no instale ni mueva los dispositivos de herramientas ONTAP ni los dispositivos vCenter Server (VCSA) al almacenamiento vVols que gestionen. Si esto sucede, reiniciar los dispositivos de las herramientas vCenter o ONTAP puede provocar la interrupción del acceso al plano de control y la imposibilidad de arrancar el dispositivo.

Las actualizaciones in situ de las herramientas de ONTAP son compatibles con el archivo ISO de actualización disponible para descargar en "Herramientas de ONTAP para VMware vSphere 10: Descargas" el sitio de soporte de NetApp (se requiere iniciar sesión). Siga "Actualice desde ONTAP tools para VMware vSphere 10.x a 10,3" las instrucciones de la guía para actualizar el aparato. También es posible realizar una actualización en paralelo de las herramientas de ONTAP 9,13 a 10,3. Consulte el "Migre desde ONTAP Tools para VMware vSphere 9.x a 10,3" para obtener información más detallada sobre ese tema.

Para obtener información sobre el ajuste de tamaño del dispositivo virtual y cuáles son los límites de configuración, consulte "Límites de configuración para poner en marcha herramientas de ONTAP para VMware vSphere"

Documentación de producto

La siguiente documentación puede ayudarle a poner en marcha las herramientas de ONTAP.

"Documentación de las herramientas de ONTAP para VMware vSphere"

Manos a la obra

- "Notas de la versión"
- "Información general de las herramientas de ONTAP para VMware vSphere"
- "Ponga en funcionamiento las herramientas de ONTAP"
- "Actualice las herramientas de ONTAP"

Utilice las herramientas de ONTAP

- "Aprovisione los almacenes de datos"
- "Configure el control de acceso basado en roles"
- "Configuración de la alta disponibilidad"
- "Modifique la configuración del host ESXi"

Proteja y gestione almacenes de datos

- "Configure vSphere Metro Storage Cluster (VMSC) con las herramientas ONTAP y la sincronización activa de SnapMirror"
- "Proteja las máquinas virtuales" Con SRM
- "Supervisar clústeres, almacenes de datos y máquinas virtuales"

Consola del proveedor de VASA

VASA Provider incluye una consola con información de rendimiento y capacidad para máquinas virtuales de vVols individuales. Esta información proviene directamente de ONTAP para los archivos y LUN VVOL,

incluidos la latencia, IOPS, rendimiento y más. Está habilitada de forma predeterminada cuando se utilizan todas las versiones compatibles actualmente de ONTAP 9. Tenga en cuenta que, tras la configuración inicial, los datos pueden tardar hasta 30 minutos en rellenar el panel de control.

Otras prácticas recomendadas

El uso de vVols de ONTAP con vSphere es sencillo y sigue los métodos de vSphere publicados (consulte Trabajar con volúmenes virtuales en la documentación de vSphere Storage en VMware para su versión de ESXi). A continuación, se muestran algunas prácticas adicionales que se deben tener en cuenta junto con ONTAP.

Límites

En general, ONTAP admite los límites de vVols definidos por VMware (ver Publicado "Valores máximos de configuración"). Compruebe siempre los "Hardware Universe de NetApp" límites actualizados sobre números y tamaños de LUN, espacios de nombres y archivos.

Utilice las herramientas de ONTAP para las extensiones de interfaz de usuario de VMware vSphere o API REST para aprovisionar almacenes de datos vVols y puntos finales de protocolo.

Aunque es posible crear almacenes de datos vVols con la interfaz general de vSphere, mediante las herramientas de ONTAP se crearán automáticamente extremos de protocolo según sea necesario y se crearán volúmenes de FlexVol (no es necesario con ASA R2) mediante las prácticas recomendadas de ONTAP. Solo tiene que hacer clic con el botón derecho en el host/clúster/centro de datos y, a continuación, seleccionar *ONTAP TOOLS* y *PROVISION datastore*. A partir de ahí, simplemente elija las opciones de vVols deseadas en el asistente.

Nunca almacene el dispositivo de herramientas ONTAP o el dispositivo vCenter Server (VCSA) en un almacén de datos vVols que estén administrando.

Esto puede resultar en una “situación de pollo y huevo” si necesita reiniciar los aparatos porque no serán capaces de volver a ensamblar sus propios vVols mientras se reinician. Puede almacenarlos en un almacén de datos de vVols que se gestiona con otras herramientas de ONTAP y en una puesta en marcha de vCenter.

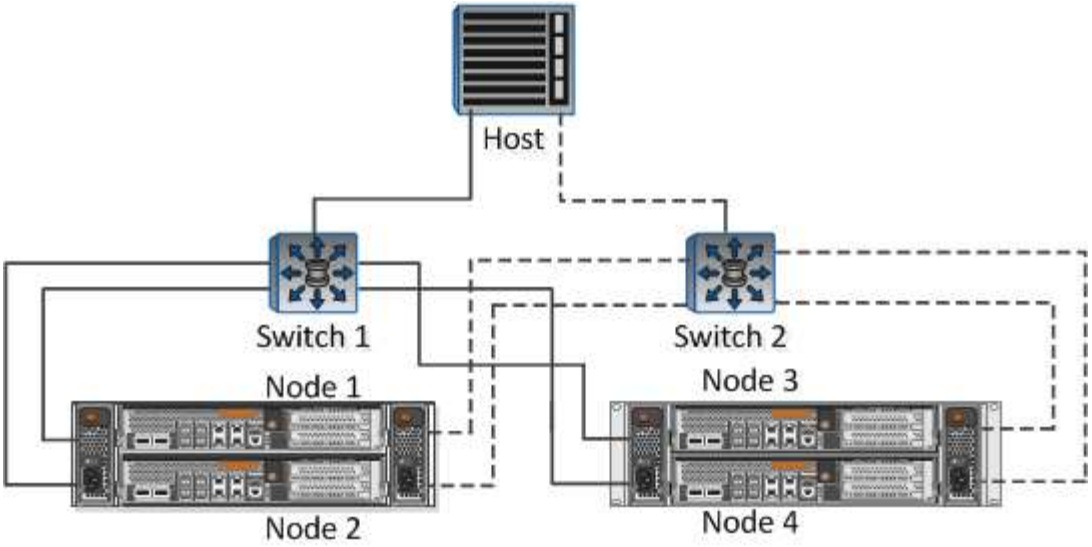
Evite las operaciones vVols a través de diferentes versiones de ONTAP.

Las funcionalidades de almacenamiento compatibles como calidad de servicio, personalidad y otras han cambiado en varias versiones del proveedor VASA; algunas dependen de la versión de ONTAP. El uso de diferentes versiones de un clúster de ONTAP o el movimiento de vVols entre clústeres con diferentes versiones puede provocar un comportamiento inesperado o alarmas de cumplimiento de normativas.

Zone su estructura Fibre Channel antes de usar FCP para vVols.

El proveedor de VASA de herramientas de ONTAP se encarga de gestionar iGroups FCP e iSCSI, así como subsistemas NVMe en ONTAP basado en iniciadores detectados de hosts ESXi gestionados. Sin embargo, no se integra con switches Fibre Channel para gestionar la división en zonas. La división en zonas debe realizarse siguiendo las mejores prácticas antes de realizar ningún aprovisionamiento. A continuación se muestra un ejemplo de división en zonas de un solo iniciador en cuatro sistemas ONTAP:

División en zonas de un solo iniciador:



Consulte los siguientes documentos para obtener más prácticas recomendadas:

"*TR-4080 Mejores prácticas para ONTAP SAN moderno 9*"

"*TR-4684 Implementación y configuración de SAN modernas con NVMe-oF*"

Planifica tus volúmenes de respaldo de FlexVol de acuerdo a tus necesidades.

En el caso de los sistemas R2 que no sean de ASA, puede ser conveniente añadir diversos volúmenes de backup al almacén de datos vVols para distribuir la carga de trabajo por el clúster de ONTAP, admitir distintas opciones de normativas o aumentar el número de LUN o archivos permitidos. Sin embargo, si se requiere una eficiencia del almacenamiento máxima, coloque todos los volúmenes de backup en un único agregado. O, si es necesario un rendimiento de clonación máximo, considere la posibilidad de usar un único volumen de FlexVol y mantener sus plantillas o biblioteca de contenido en el mismo volumen. El proveedor VASA libera muchas operaciones de almacenamiento de vVols en ONTAP, incluidas la migración, el clonado y las copias Snapshot. Cuando esta operación se realiza en un único volumen FlexVol, se usan clones de archivos con gestión eficiente del espacio y están disponibles casi al instante. Cuando esto se realiza en volúmenes de FlexVol, las copias se encuentran disponibles rápidamente y utilizan deduplicación y compresión en línea, pero es posible que no se recupere la máxima eficiencia del almacenamiento hasta que se ejecuten trabajos en segundo plano en volúmenes con deduplicación y compresión en segundo plano. En función del origen y el destino, se puede degradar cierta eficiencia.

Con los sistemas R2 de ASA, esta complejidad se elimina cuando el concepto de un volumen o agregado es abstraído del usuario. La ubicación dinámica se gestiona automáticamente y los extremos de protocolo se crean según sea necesario. Si se requiere un escalado adicional, se pueden crear automáticamente extremos de protocolo adicionales sobre la marcha.

Considera usar Max IOPS para controlar VMs desconocidas o de prueba.

Por primera vez, disponible en VASA Provider 7,1, Max IOPS puede usarse para limitar las IOPS a un VVol específico para una carga de trabajo desconocida y así evitar el impacto en otras cargas de trabajo más críticas. Consulte la Tabla 4 para obtener más información sobre gestión del rendimiento.

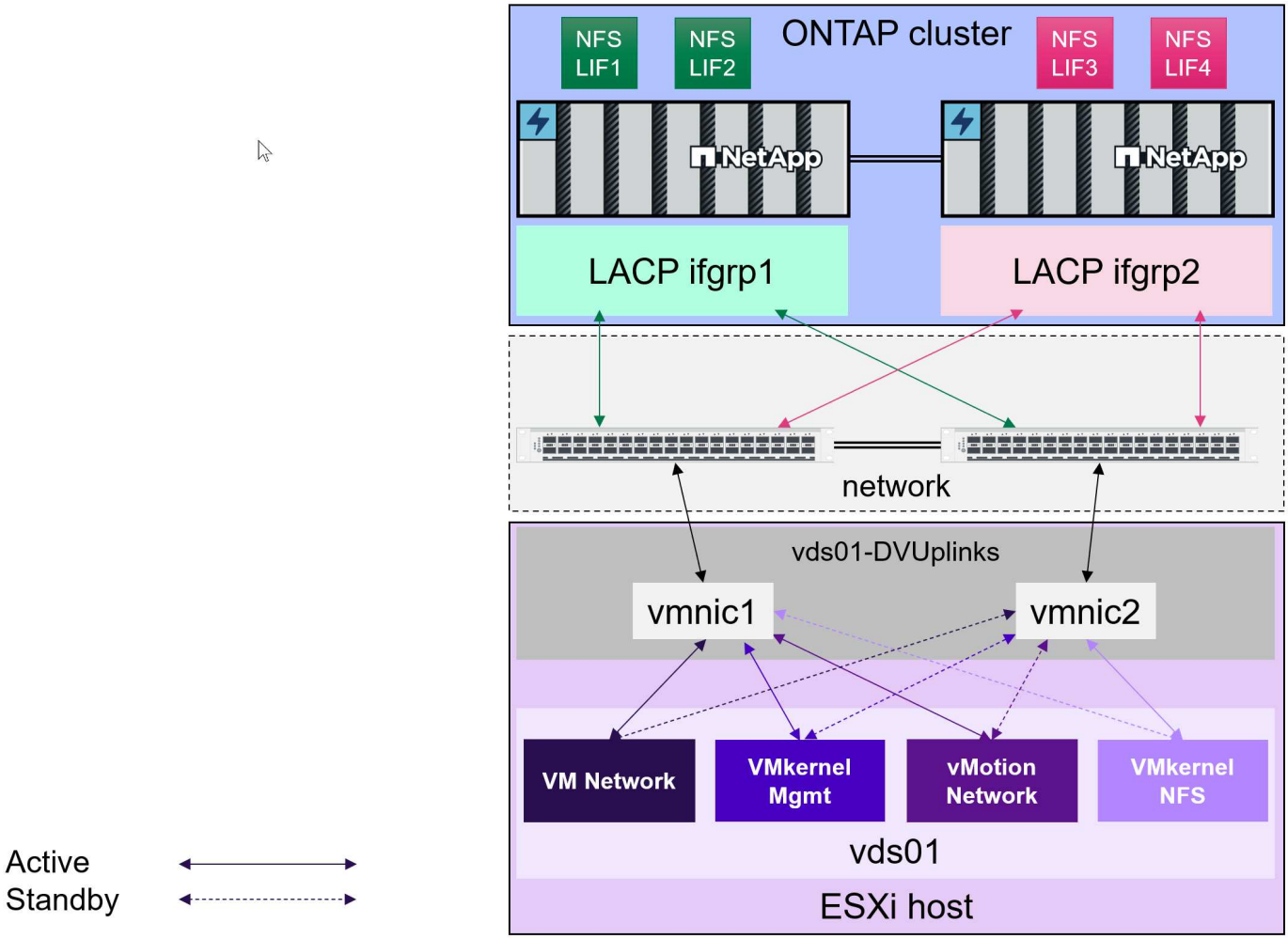
Asegúrese de tener suficientes LIF de datos. Consulte "Despliegue de vVols Storage".

Siga todas las mejores prácticas del protocolo.

Consulte las otras guías de prácticas recomendadas de NetApp y VMware específicas del protocolo que ha

seleccionado. En general, no hay ningún cambio aparte de los ya mencionados.

Ejemplo de configuración de red usando vVols sobre NFS v3



Puesta en marcha de vVols en sistemas AFF, ASA, ASA R2 y FAS

Siga estas mejores prácticas para crear almacenamiento de vVols para los equipos virtuales.

El aprovisionamiento de almacenes de datos vVols implica varios pasos. Los sistemas ASA R2 de NetApp están diseñados para cargas de trabajo de VMware y proporcionan una experiencia de usuario diferente a la de los sistemas ONTAP tradicionales. Al utilizar los sistemas ASA R2, las versiones 10,3 o posteriores de las herramientas de ONTAP requieren menos pasos para configurar e incluir extensiones de interfaz de usuario y soporte de API DE REST optimizado para la nueva arquitectura de almacenamiento.

Preparar la creación de vVols datastores con herramientas ONTAP

Puede omitir los dos primeros pasos del proceso de puesta en marcha si ya utiliza las herramientas de ONTAP para gestionar, automatizar e informar sobre el almacenamiento existente VMFS o el tradicional basado en NFS. También puede consultar este completo "lista de comprobación" para implementar y configurar las herramientas de ONTAP.

1. Cree la Storage Virtual Machine (SVM) y su configuración de protocolos. Tenga en cuenta que puede no ser necesario con los sistemas ASA R2, ya que normalmente ya tendrán una sola máquina virtual de

almacenamiento para servicios de datos. Seleccionará NVMe/FC (solo herramientas ONTAP 9,13), NFSv3, NFSv4,1, iSCSI, FCP o una combinación de estas opciones. NVMe/TCP y NVMe/FC también pueden utilizarse para almacenes de datos VMFS tradicionales con herramientas ONTAP 10,3 y posteriores. Puede usar los asistentes de ONTAP System Manager o la línea de comandos de shell de clúster.

- "Asigne niveles locales (agregados) a SVM" Para todos los sistemas R2 que no son de ASA.
- Al menos un LIF por nodo para cada conexión de switch/estructura. Como práctica recomendada, cree dos o más por nodo para los protocolos basados en FCP, iSCSI o NVMe. Un LIF por nodo es suficiente para vVols basados en NFS, pero este LIF debería estar protegido por un ifgroup de LACP. Consulte "Descripción general de la configuración de LIF" y "Combine puertos físicos para crear grupos de interfaces" para obtener más información.
- Al menos una LIF de gestión por SVM si pretende usar credenciales en el ámbito de SVM para las vCenter de inquilino.
- Si planea usar SnapMirror, asegúrese de que su origen y destino "Los clústeres de ONTAP y las SVM tienen una relación entre iguales".
- Para sistemas R2 que no son de ASA, se pueden crear volúmenes en este momento, pero es recomendable permitir que el asistente *Provision Datastore* de las herramientas de ONTAP los cree. La única excepción a esta regla es si planea utilizar la replicación de vVols con VMware Site Recovery Manager y las herramientas de ONTAP 9,13. Esta configuración es más fácil con volúmenes FlexVol preexistentes con relaciones de SnapMirror existentes. Tenga en cuenta que no habilita la calidad de servicio en ningún volumen para que lo usen vVols, ya que esta se pretende que la gestionen las herramientas de SPBM y ONTAP.

2. "Ponga en marcha herramientas de ONTAP para VMware vSphere" Utilice el OVA descargado del sitio de soporte de NetApp.
   - Las herramientas de ONTAP 10,0 y versiones posteriores admiten varios servidores vCenter por dispositivo, ya no es necesario poner en marcha un dispositivo de herramientas de ONTAP por vCenter.
     - Si tiene pensado conectar varios vCenter a una única instancia de herramientas de ONTAP, debe crear e instalar certificados firmados por CA. Consulte "Gestionar certificados" para ver los pasos.
   - A partir de 10,3, las herramientas de ONTAP ahora se ponen en marcha como un dispositivo de tipo pequeño de nodo único apto para la mayoría de cargas de trabajo que no sean vVols.

- La práctica recomendada es "Herramientas de ONTAP de escalado horizontal" la versión 10,3 y versiones posteriores a la configuración de alta disponibilidad de 3 nodos para todas las cargas de trabajo de producción. Para fines de laboratorios o pruebas, es posible usar la puesta en marcha de un solo nodo.
- La mejor práctica recomendada para el uso de vVols en producción es eliminar cualquier punto único de fallo. Cree reglas anti-afinidad para evitar que las VM de ONTAP Tools se ejecuten juntas en el mismo host. Después de la implementación inicial, también se recomienda usar vMotion de almacenamiento para colocar las máquinas virtuales con las herramientas de ONTAP en diferentes almacenes de datos. Lea más sobre "Uso de reglas de afinidad sin vSphere DRS" o. "Cree una regla de afinidad de VM-VM" También debe programar backups frecuentes, y/o "utilice la utilidad de copia de seguridad de configuración incorporada".

1. Configure las herramientas de ONTAP 10,3 para su entorno.
   - "Añada instancias de vCenter Server" En la IU del administrador de herramientas de ONTAP.
   - ONTAP tools 10,3 admite multi-tenancy seguro. Si no necesita multi-tenancy seguro, puede

simplemente "Añada los clústeres de ONTAP" ir al menú de herramientas de ONTAP en vCenter, hacer clic en *Storage backends* y hacer clic en el botón *add*.

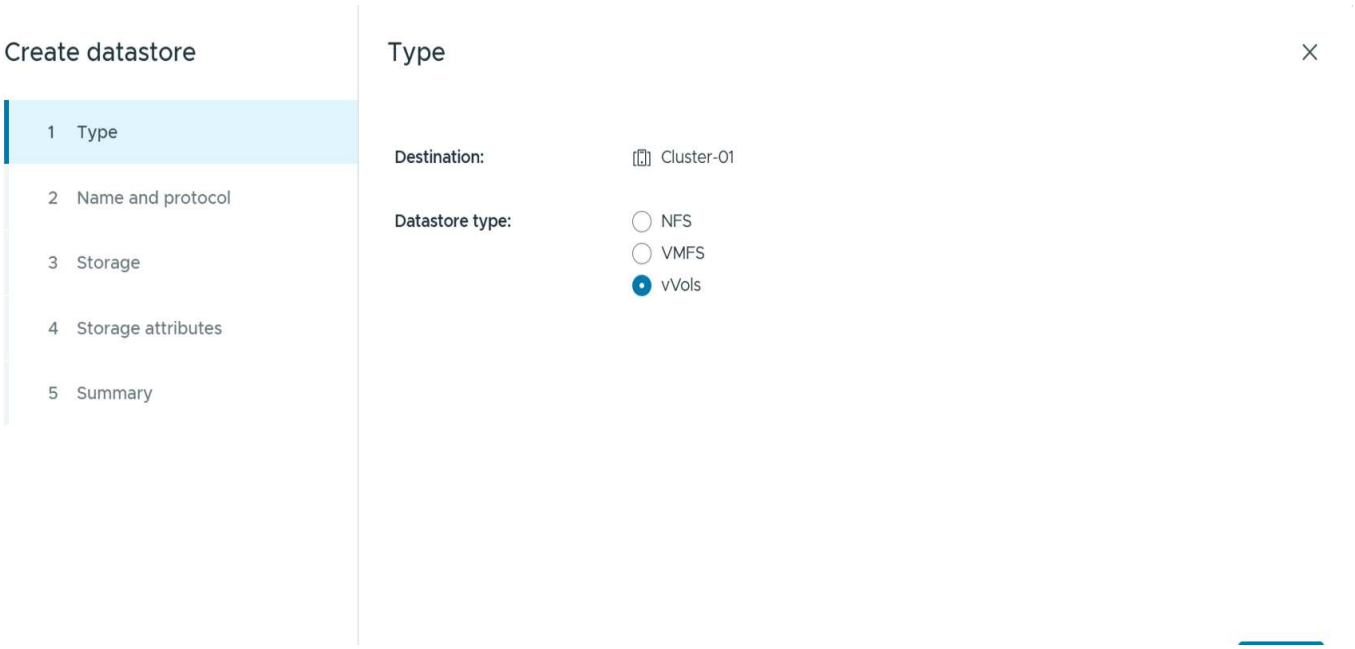
- En un entorno multi-tenant seguro en el que desee delegar máquinas virtuales de almacenamiento (SVM) específicas en vCenter específicos, debe hacer lo siguiente.
  - Inicie sesión en la IU del administrador de herramientas de ONTAP
  - "Cree el clúster de almacenamiento"
  - "Asocie un back-end de almacenamiento a una instancia de vCenter Server"
  - Proporcione las credenciales de SVM específicas al administrador de vCenter que añadirá posteriormente la SVM como back-end de almacenamiento en el menú back-ends de almacenamiento de herramientas de ONTAP de vCenter.

- Crear roles de RBAC para sus cuentas de almacenamiento es una práctica recomendada.
- Las herramientas de ONTAP incluyen un archivo JSON que contiene los permisos de roles necesarios que necesitan las cuentas de acceso de almacenamiento de herramientas de ONTAP. Puede cargar el archivo JSON en ONTAP System Manager para simplificar la creación de roles y usuarios de RBAC.
- Puede obtener más información acerca de los roles de RBAC de ONTAP en "Configure los roles y privilegios de usuario de ONTAP".

El motivo por el que todo el clúster se debe incorporar en la interfaz de usuario del administrador de herramientas de ONTAP es que muchas de las API utilizadas para vVols solo están disponibles en el nivel de clúster.

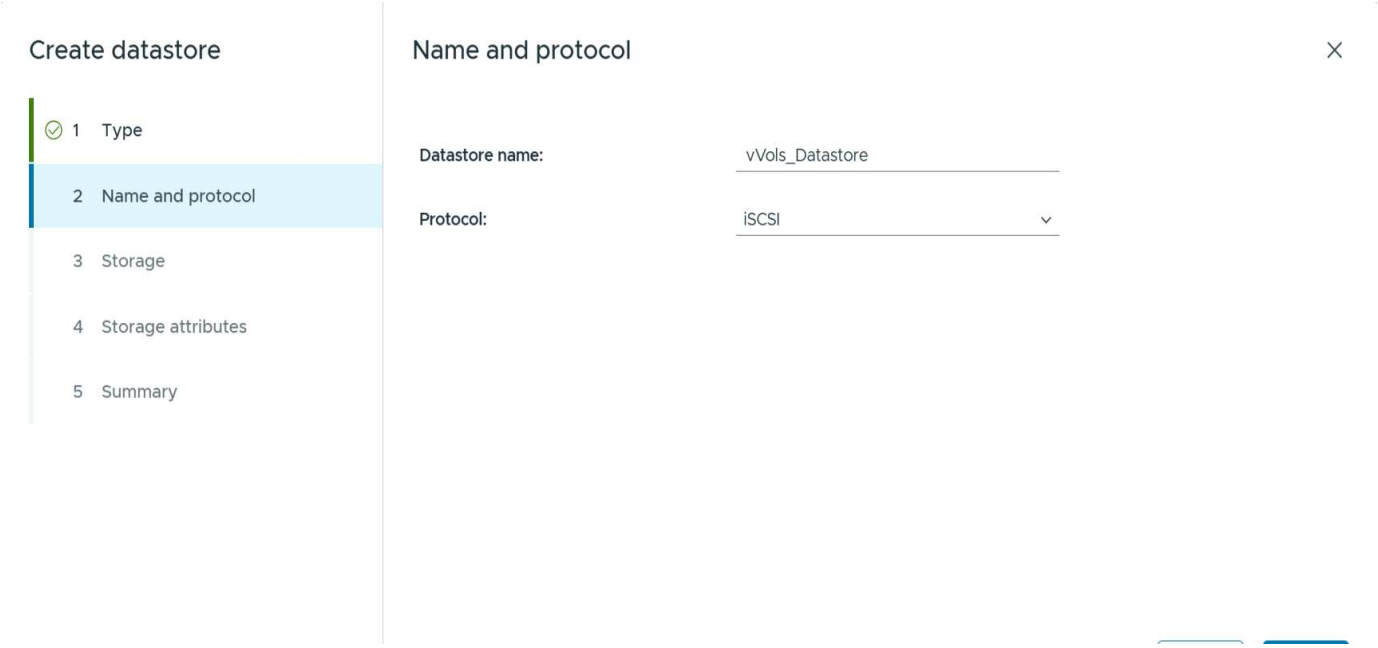
Crear almacenes de datos vVols con herramientas de ONTAP

Haga clic con el botón derecho en el host, clúster o centro de datos en el que desea crear el almacén de datos vVols y, a continuación, seleccione *ONTAP tools* > *Provision Datastore*.

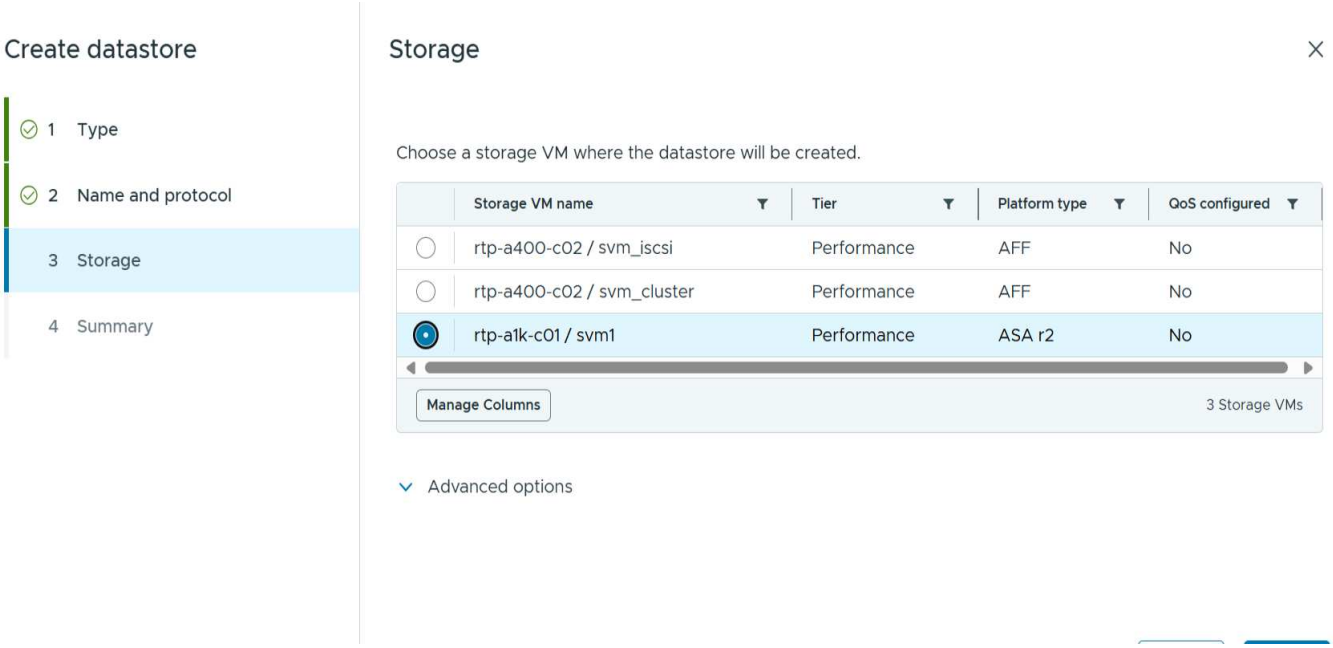


- Elija vVols y proporcione un nombre significativo y seleccione el protocolo deseado. También puede proporcionar una descripción del almacén de datos.

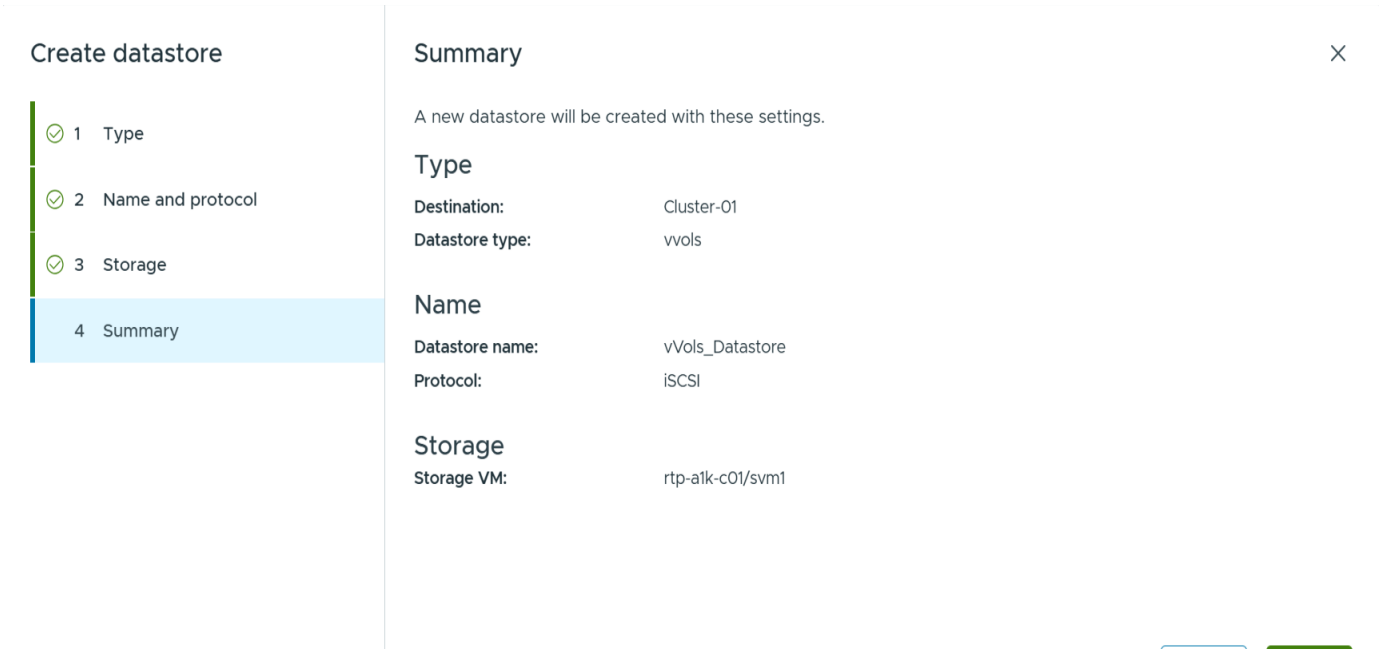
◦ ONTAP tools 10,3 con ASA R2.



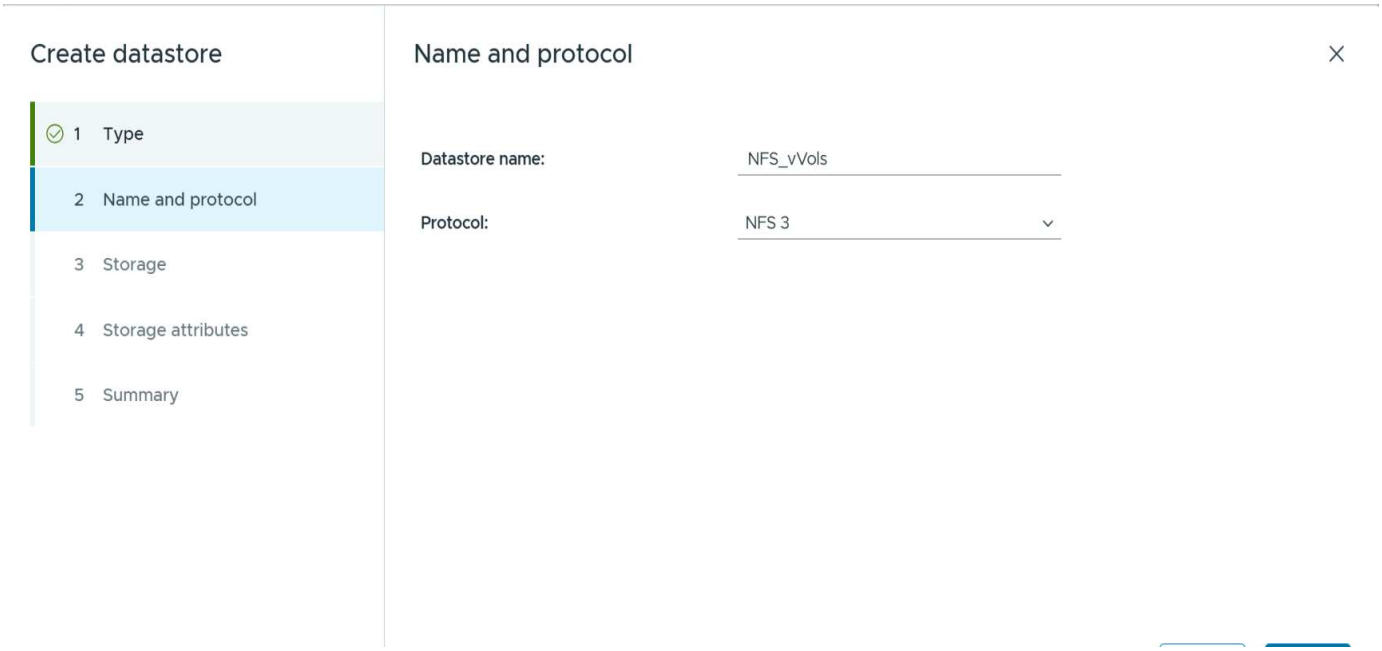
- Seleccione la SVM del sistema ASA R2 y haga clic en *next*.



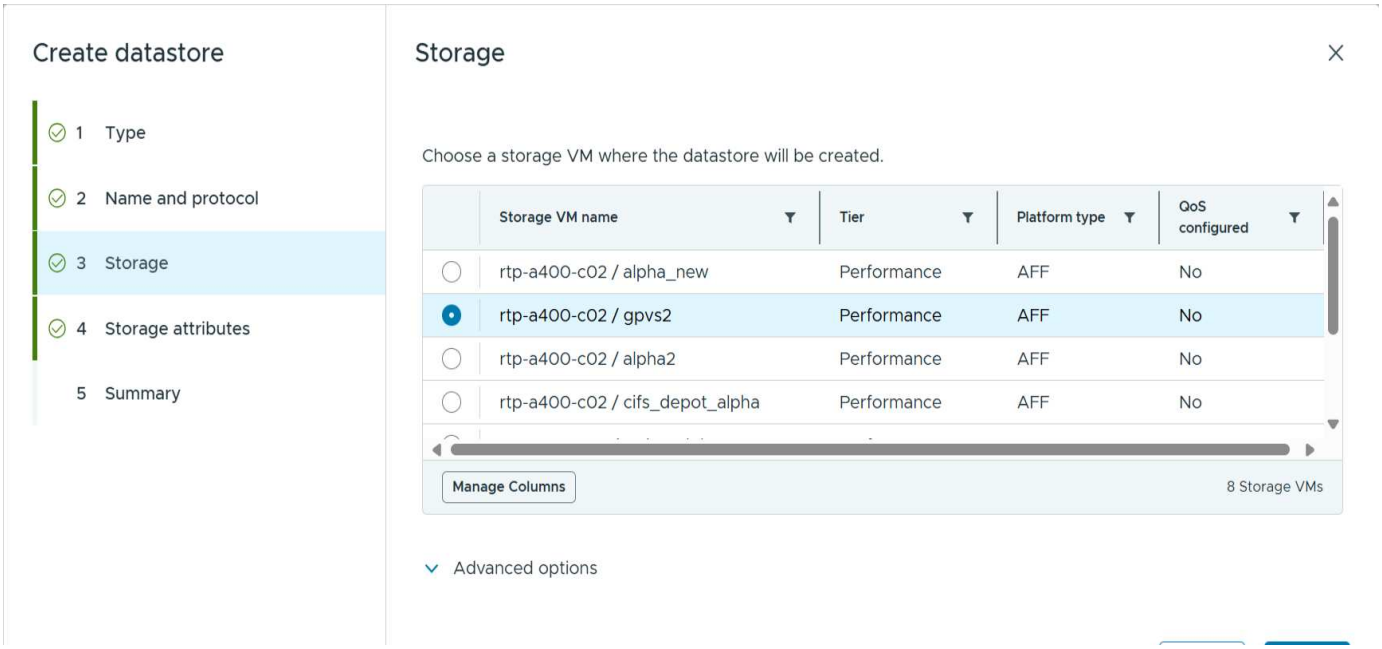
- Haga clic en *FINALIZAR*



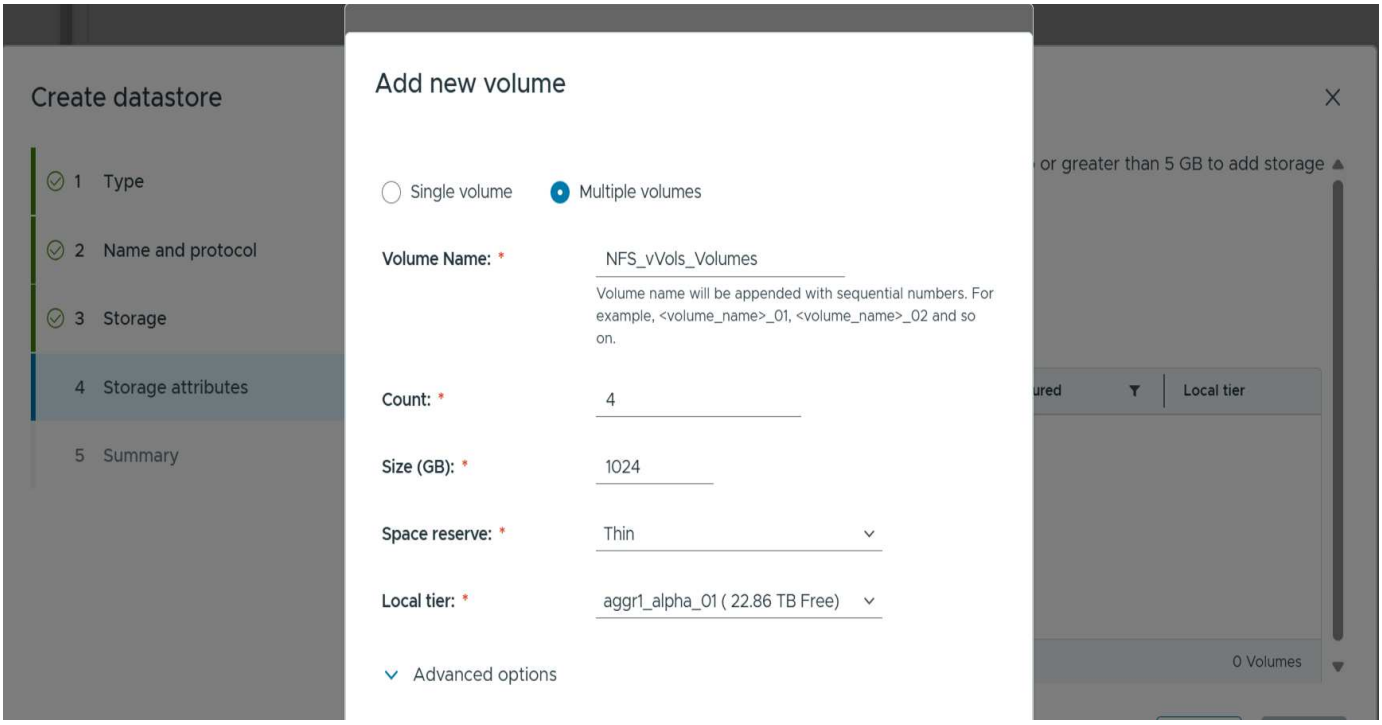
- ¡Así de fácil!
  - ONTAP tools 10,3 con ONTAP FAS, AFF y ASA Previous ASA R2.
- Seleccione el protocolo

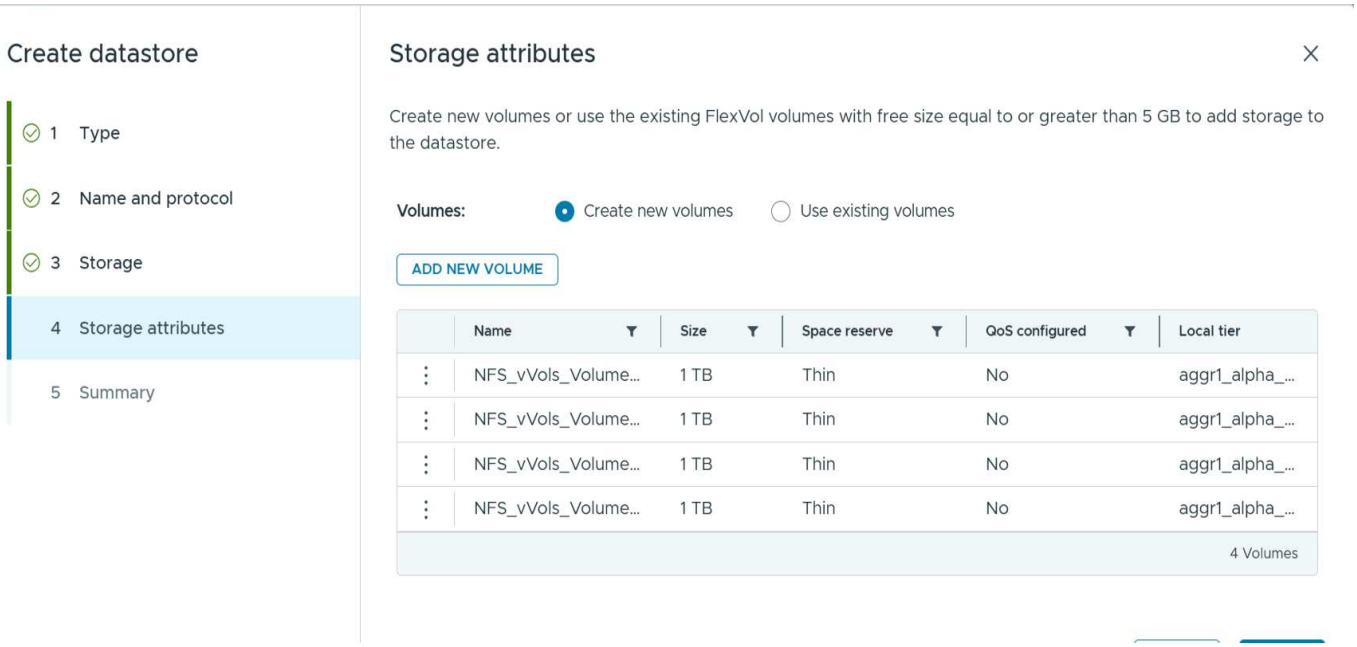


- Seleccione la SVM y haga clic en *next*.

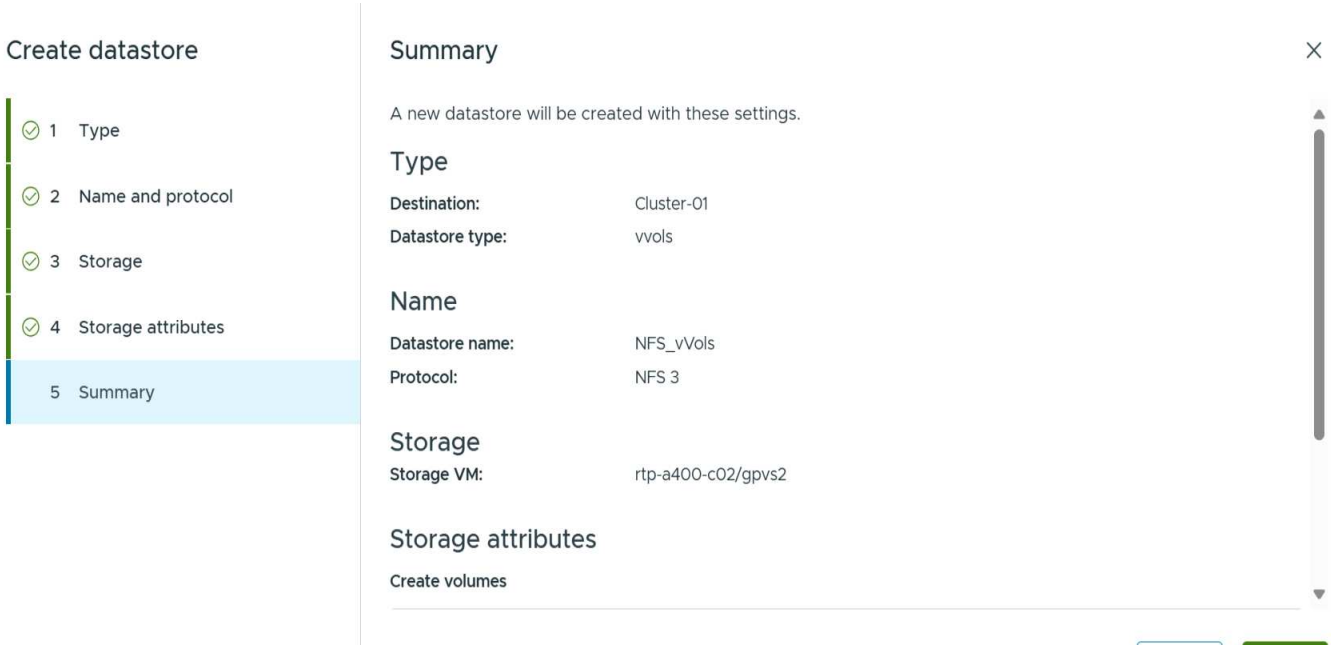


- Haga clic en *add new volumes* o en *Use existing volume* y, a continuación, especifique los atributos. Tenga en cuenta que en ONTAP tools 10,3, puede solicitar la creación de varios volúmenes al mismo tiempo. También es posible añadir varios volúmenes manualmente para equilibrarlos en el clúster de ONTAP. Haga clic en *SIGUIENTE*

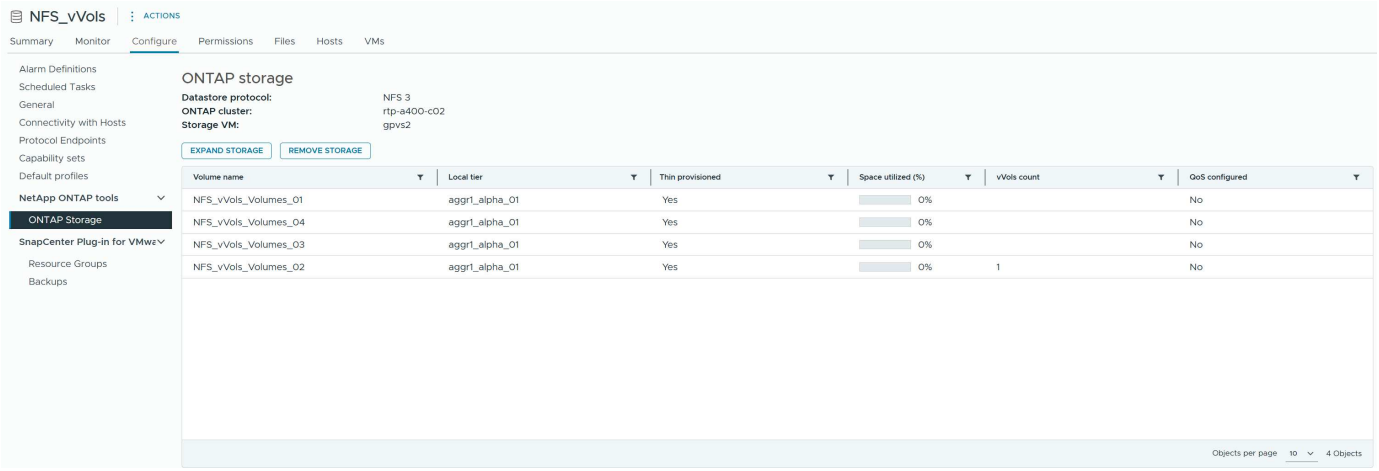




- Haga clic en *FINALIZAR*



- Es posible ver los volúmenes asignados en el menú de herramientas ONTAP de la pestaña de configuración del almacén de datos.



- Ahora puede crear políticas de almacenamiento de máquinas virtuales desde el menú *Policies and Profiles* en la interfaz de usuario de vCenter.

Migración de máquinas virtuales desde almacenes de datos tradicionales a vVols

La migración de máquinas virtuales de almacenes de datos tradicionales a un almacén de datos vVols es tan sencilla como mover máquinas virtuales entre almacenes de datos tradicionales. Solo tiene que seleccionar las máquinas virtuales y, a continuación, seleccionar Migrate en la lista Actions y seleccionar un tipo de migración *change storage only*. Cuando se le solicite, seleccione una política de almacenamiento de máquinas virtuales que coincida con su almacén de datos de vVols. Las operaciones de copia de migración se pueden descargar con vSphere 6,0 y versiones posteriores para las migraciones de SAN VMFS a vVols, pero no de VMDK de NAS a vVols.

Gestionar máquinas virtuales con políticas

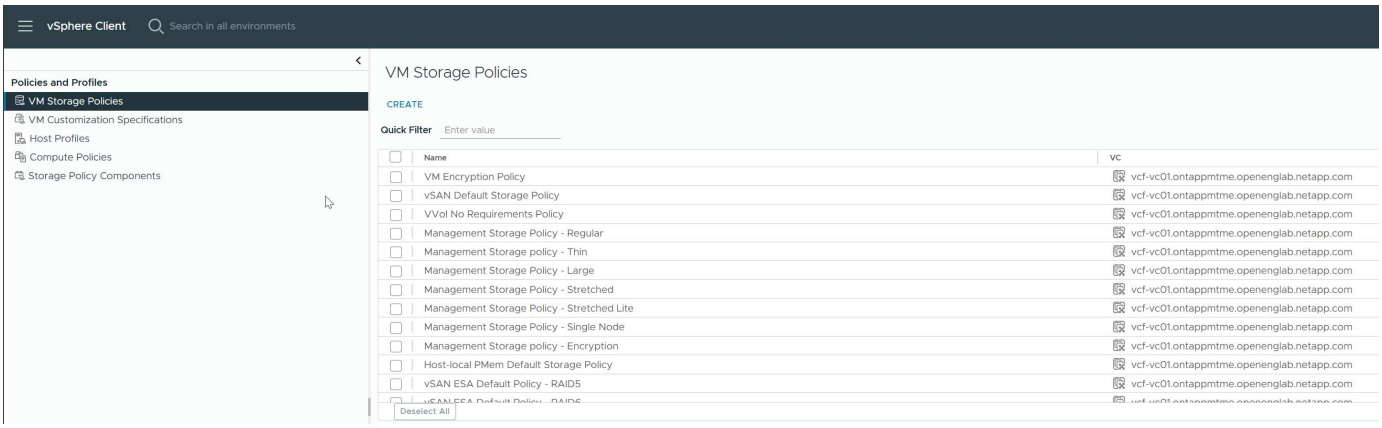
Para automatizar el aprovisionamiento de almacenamiento con gestión basada en políticas, debe crear políticas de almacenamiento de equipos virtuales que se asignen a las capacidades de almacenamiento deseadas.

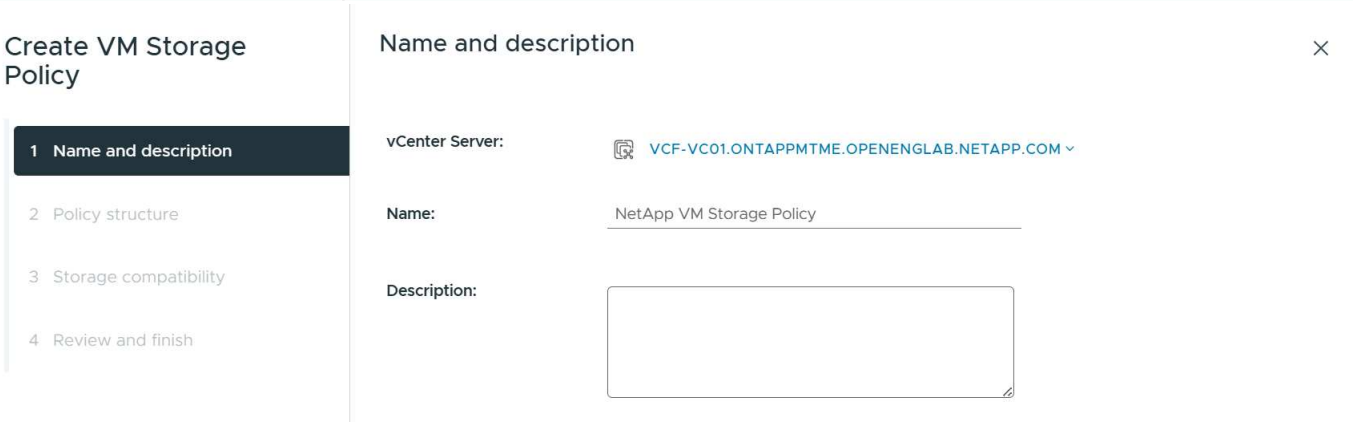
> Las herramientas de ONTAP 10,0 y versiones posteriores ya no utilizan los perfiles de capacidades de almacenamiento como las versiones anteriores. Las capacidades de almacenamiento se definen directamente en la propia política de almacenamiento de máquinas virtuales.

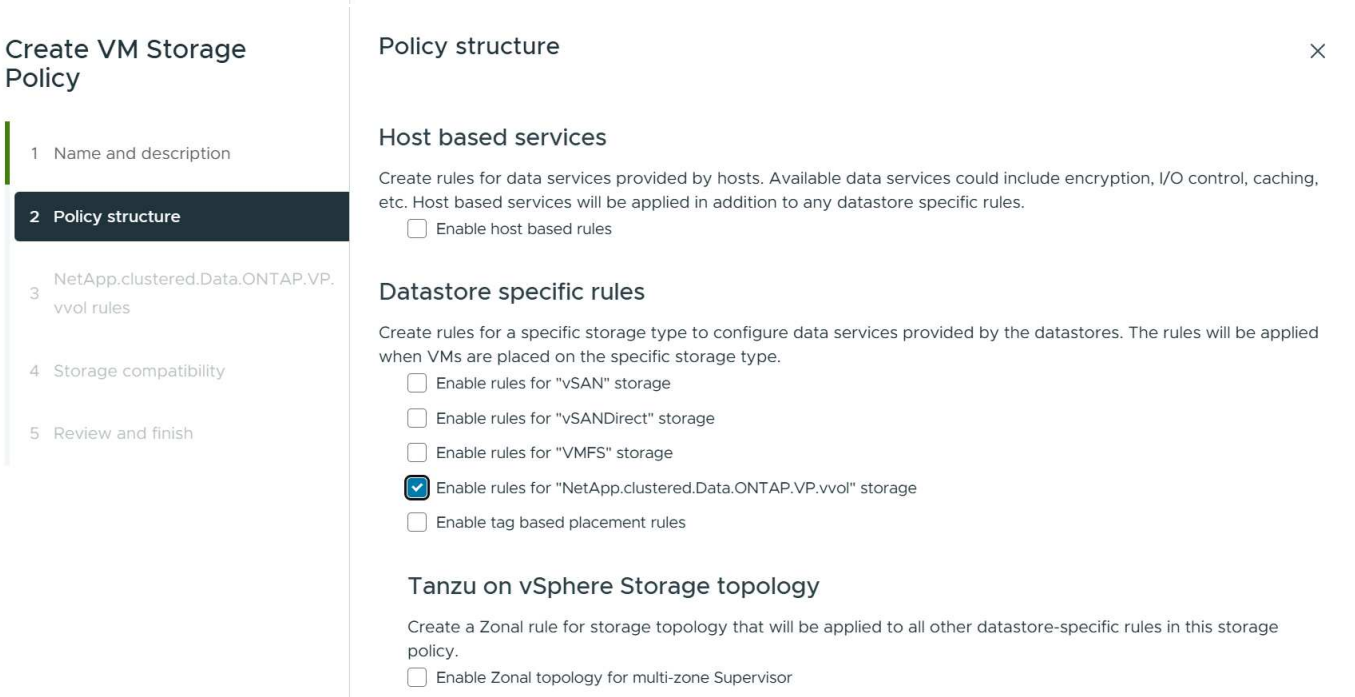
Creación de políticas de almacenamiento de equipos virtuales

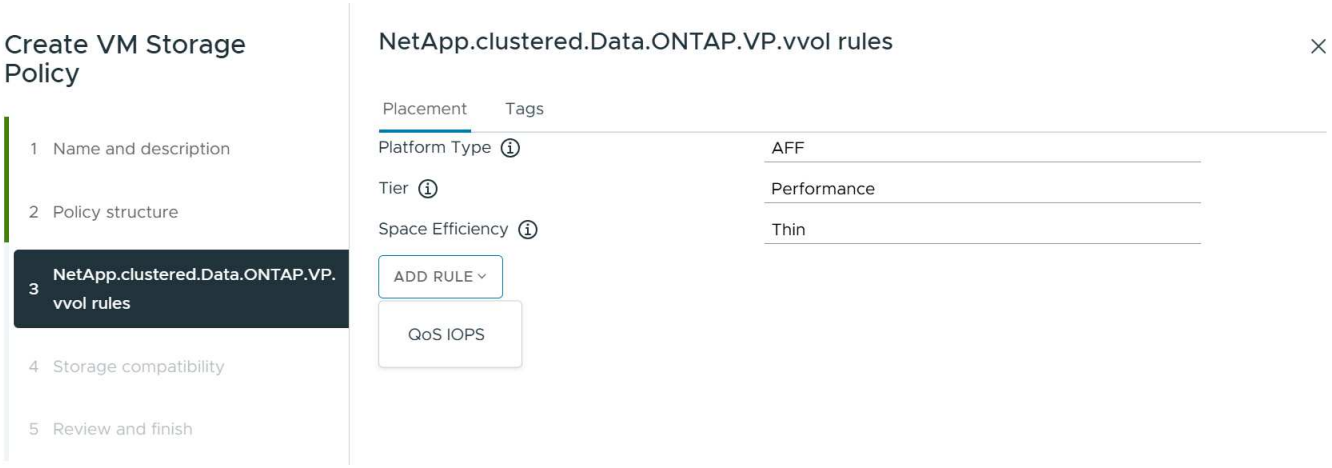
Las políticas de almacenamiento de máquinas virtuales se utilizan en vSphere para gestionar funciones opcionales como Storage I/O Control o vSphere Encryption. También se utilizan con vVols para aplicar funcionalidades de almacenamiento específicas a la máquina virtual. Utilice el tipo de almacenamiento «NetApp.clustered.Data.ONTAP.VP.vvol». Consulte el enlace:vmware-vvols-ontap.html#Best Practices[Ejemplo de configuración de red mediante vVols en NFS v3] para obtener un ejemplo de esto con el proveedor VASA de herramientas de ONTAP. Las reglas para el almacenamiento «NetApp.clustered.Data.ONTAP.VP.VASA10» deben utilizarse con almacenes de datos que no sean vVols.

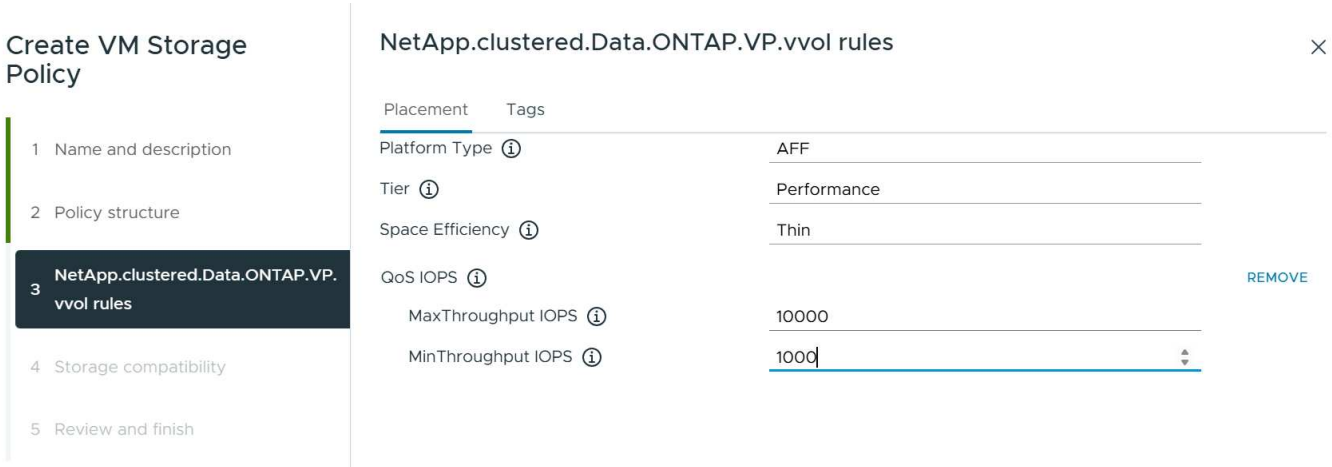
Una vez creada la política de almacenamiento, esta se puede utilizar para aprovisionar nuevos equipos virtuales.

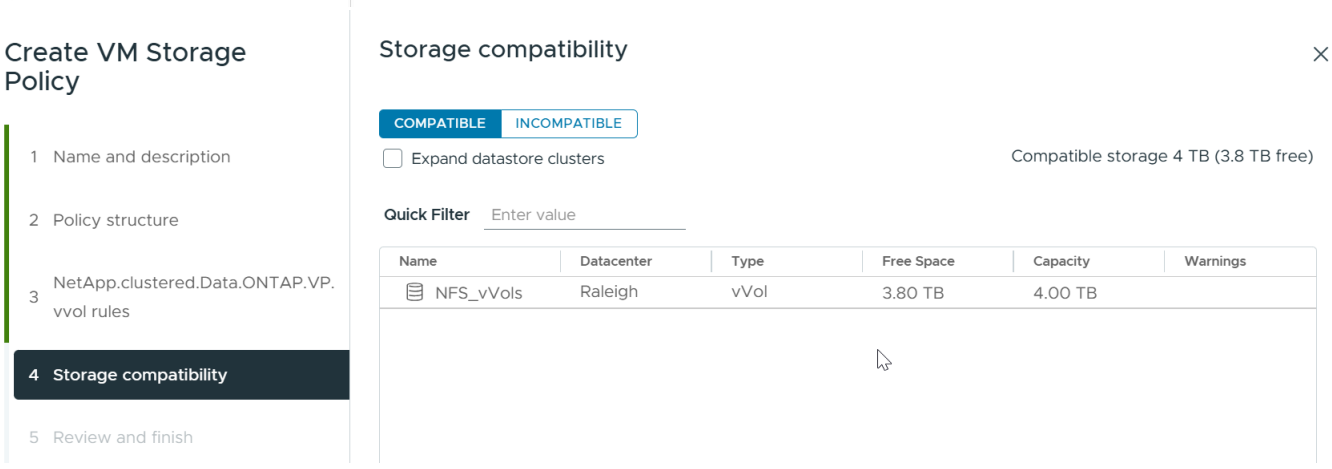

vSphere Client
Search in all environments
Policies and Profiles
VM Storage Policies
VM Customization Specifications
Host Profiles
Compute Policies
Storage Policy Components
VM Storage Policies
CREATE
Quick Filter
Enter value
Name
VC
VM Encryption Policy
vSAN Default Storage Policy
VVol No Requirements Policy
Management Storage Policy - Regular
Management Storage policy - Thin
Management Storage Policy - Large
Management Storage Policy - Stretched
Management Storage Policy - Stretched Lite
Management Storage Policy - Single Node
Management Storage policy - Encryption
Host-local PMem Default Storage Policy
vSAN ESA Default Policy - RAID5
vcf-vc01.ontappmtme.openenglab.netapp.com
Deselect All

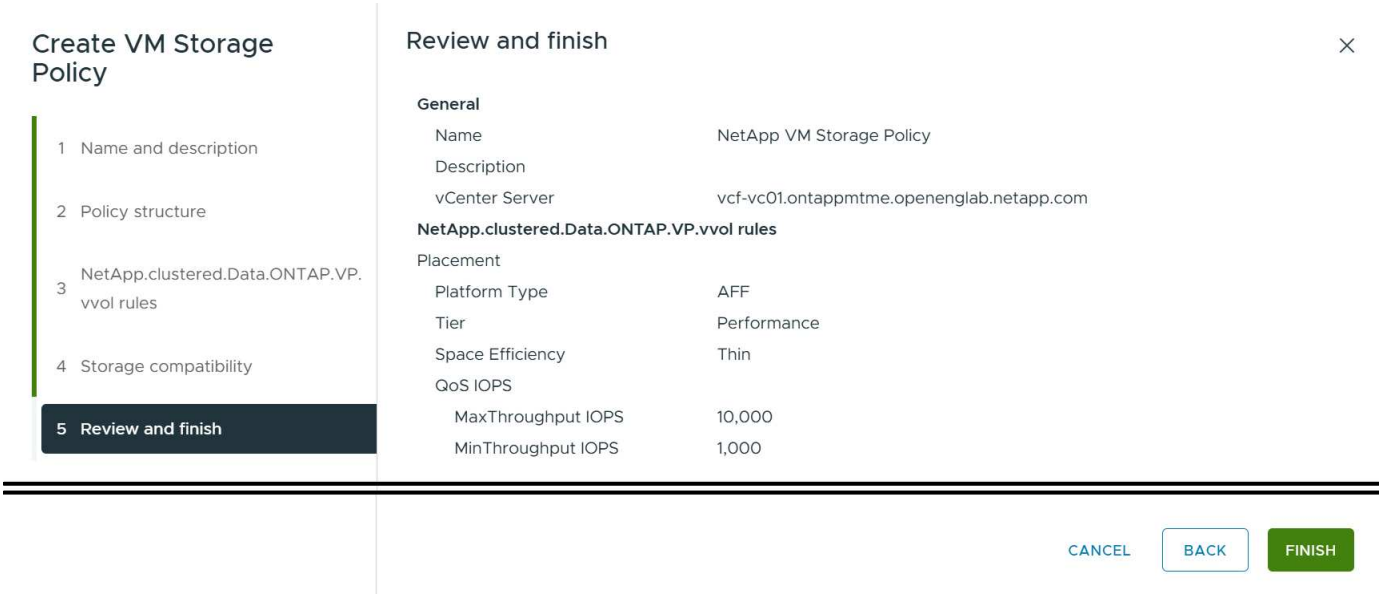

Create VM Storage Policy
1 Name and description
2 Policy structure
3 Storage compatibility
4 Review and finish
Name and description
vCenter Server:
VCF-VC01.ONTAPPMTME.OPENENGLAB.NETAPP.COM
Name:
NetApp VM Storage Policy
Description:


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
Policy structure
Host based services
Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.
Enable host based rules
Datastore specific rules
Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.
Enable rules for "vSAN" storage
Enable rules for "vSANDirect" storage
Enable rules for "VMFS" storage
Enable rules for "NetApp.clustered.Data.ONTAP.VP.vvol" storage
Enable tag based placement rules
Tanzu on vSphere Storage topology
Create a Zonal rule for storage topology that will be applied to all other datastore-specific rules in this storage policy.
Enable Zonal topology for multi-zone Supervisor


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
NetApp.clustered.Data.ONTAP.VP.vvol rules
Placement
Tags
Platform Type
AFF
Tier
Performance
Space Efficiency
Thin
ADD RULE
QoS IOPS


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
NetApp.clustered.Data.ONTAP.VP.vvol rules
Placement
Tags
Platform Type
AFF
Tier
Performance
Space Efficiency
Thin
QoS IOPS
REMOVE
MaxThroughput IOPS
10000
MinThroughput IOPS
1000


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
Storage compatibility
COMPATIBLE
INCOMPATIBLE
Expand datastore clusters
Compatible storage 4 TB (3.8 TB free)
Quick Filter
Enter value
Name
Datacenter
Type
Free Space
Capacity
Warnings
NFS_vVols
Raleigh
vVol
3.80 TB
4.00 TB



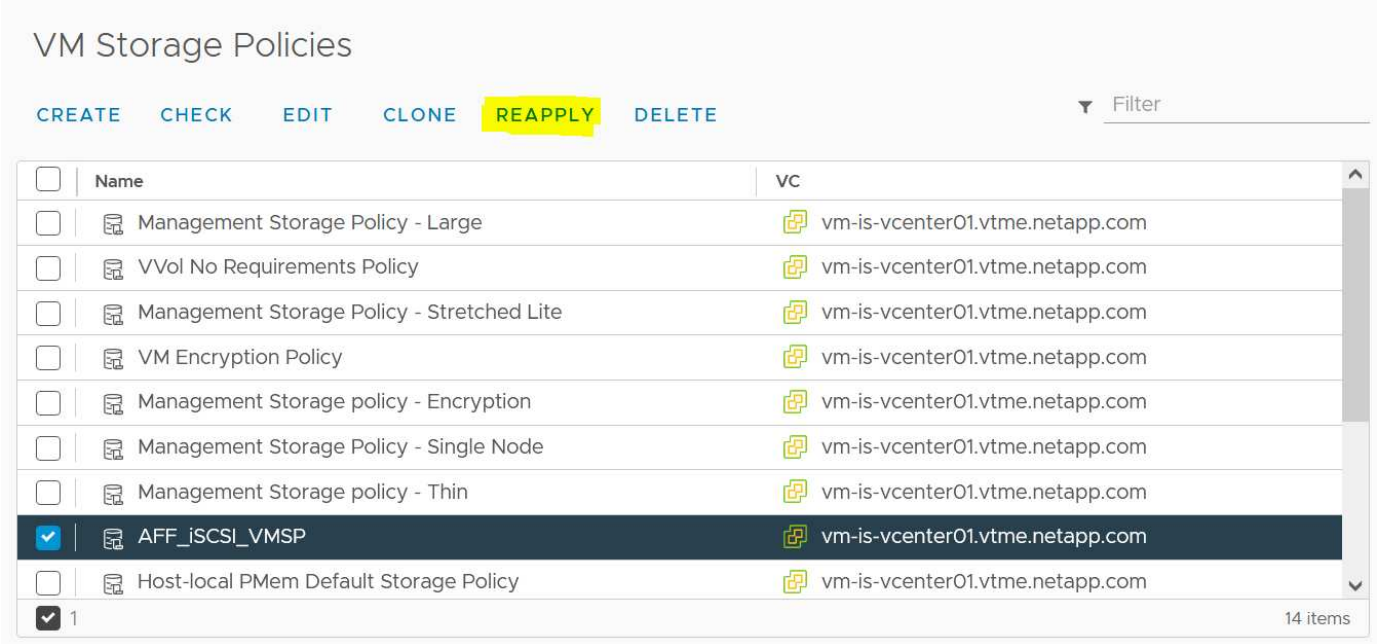
Gestión del rendimiento con herramientas de ONTAP

Las herramientas de ONTAP utilizan su propio algoritmo de colocación equilibrada para colocar un nuevo VVOL en el mejor FlexVol volume con sistemas ASA unificados o clásicos, o zona de disponibilidad de almacenamiento (SAZ) con sistemas ASA R2, dentro de un almacén de datos vVols. La colocación se basa en asociar el almacenamiento de respaldo con la normativa de almacenamiento de las máquinas virtuales. Esto garantiza que el almacén de datos y el almacenamiento de respaldo puedan cumplir con los requisitos de rendimiento especificados.

Cambiar las funcionalidades de rendimiento como IOPS mín. Y máx. Requiere cierta atención a la configuración específica.

- **IOPS mín. Y máx.** se pueden especificar en una Política de VM.
  - Si se cambia la IOPS en la política, no se cambiará la QoS en vVols hasta que se vuelva a aplicar la política de VM a las VM que la usan. También puede crear una nueva política con las IOPS deseadas y aplicarla a las máquinas virtuales de destino. Normalmente, se recomienda simplemente definir políticas de almacenamiento de máquinas virtuales independientes para diferentes niveles de servicio y simplemente cambiar la política de almacenamiento de máquinas virtuales en la máquina virtual.
  - Las personalidades de ASA, ASA R2, AFF y FAS tienen diferentes configuraciones de IOPS. Tanto Min como Max están disponibles en sistemas all-flash; sin embargo, los sistemas que no sean de AFF solo pueden usar ajustes de Max IOPS.
- Las herramientas de ONTAP crean políticas de calidad de servicio individuales no compartidas con las versiones actuales compatibles de ONTAP. Por lo tanto, cada VMDK individual recibirá su propia asignación de IOPS.

Nueva aplicación de la normativa de almacenamiento de equipos virtuales



Protección de vVols

Las siguientes secciones describen los procedimientos y las mejores prácticas para usar vVols de VMware con almacenamiento de ONTAP.

Alta disponibilidad del proveedor de VASA

El proveedor VASA de NetApp se ejecuta como parte del dispositivo virtual junto con el complemento para vCenter y el servidor de la API de REST (anteriormente conocido como Virtual Storage Console [VSC]) y Storage Replication Adapter. Si el proveedor VASA no está disponible, se seguirán ejecutando las máquinas virtuales que utilizan vVols. Sin embargo, no se pueden crear nuevos almacenes de datos vVols y no se puede crear ni enlazar vVols mediante vSphere. Esto significa que las máquinas virtuales que usan vVols no se pueden encender ya que vCenter no podrá solicitar la creación del VVol de intercambio. Y las máquinas virtuales en ejecución no pueden usar vMotion para migrar a otro host porque vVols no puede vincularse al nuevo host.

VASA Provider 7,1 y versiones posteriores admiten nuevas funcionalidades para garantizar que los servicios estén disponibles cuando se necesiten. Incluye nuevos procesos de vigilancia que supervisan el proveedor VASA y los servicios integrados de base de datos. Si detecta un fallo, actualiza los archivos de registro y, a continuación, reinicia los servicios automáticamente.

El administrador de vSphere debe configurar una mayor protección con las mismas funciones de disponibilidad utilizadas para proteger otras máquinas virtuales críticas para el negocio de fallos en software, hardware de host y red. No se requiere configuración adicional en el dispositivo virtual para utilizar estas funciones; simplemente configúrelas mediante enfoques de vSphere estándar. Han sido probados y cuentan con soporte de NetApp.

VSphere High Availability se puede configurar fácilmente para reiniciar un equipo virtual en otro host del clúster de hosts en caso de fallo. La tolerancia a fallos de vSphere proporciona una mayor disponibilidad al crear un equipo virtual secundario que se replica continuamente y que puede asumir el control en cualquier punto. La información adicional sobre estas funciones está disponible en la "Documentación de las herramientas de ONTAP para VMware vSphere (Configurar alta disponibilidad para herramientas de ONTAP)", Además de la documentación de VMware vSphere (busque vSphere Availability en ESXi y vCenter Server).

Las herramientas de ONTAP VASA Provider realiza automáticamente backups de la configuración de vVols en tiempo real en sistemas ONTAP gestionados donde la información de vVols se almacena en metadatos de volumen de FlexVol. En el caso de que el dispositivo de herramientas de ONTAP deje de estar disponible por cualquier motivo, puede implementar uno nuevo de forma fácil y rápida e importar la configuración. Consulte este artículo de la base de conocimientos para obtener más información sobre los pasos de recuperación del proveedor VASA:

"Cómo realizar una recuperación de desastres de un proveedor VASA: Guía de resolución"

Replicación de vVols

Muchos clientes de ONTAP replican sus almacenes de datos tradicionales en sistemas de almacenamiento secundario mediante SnapMirror de NetApp y, a continuación, utilizan el sistema secundario para recuperar máquinas virtuales individuales o todo un sitio en caso de desastre. En la mayoría de los casos, los clientes utilizan una herramienta de software para gestionarlo, por ejemplo, un producto de software de backup como el complemento de NetApp SnapCenter para VMware vSphere o una solución de recuperación ante desastres como Site Recovery Manager de VMware (junto con el adaptador de replicación de almacenamiento en herramientas de ONTAP).

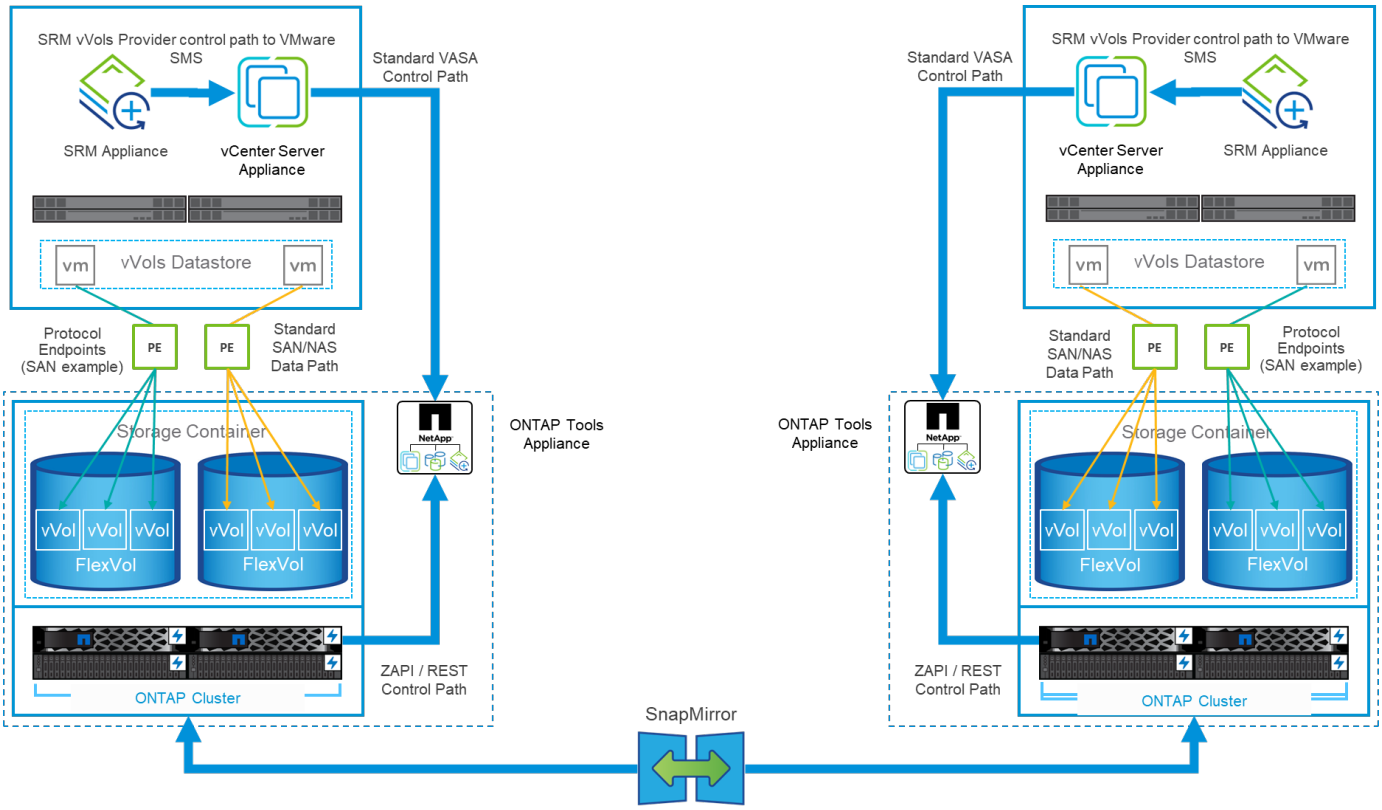
Este requisito de una herramienta de software es aún más importante para gestionar la replicación vVols. A pesar de que algunos aspectos pueden gestionarse mediante funcionalidades nativas (por ejemplo, las copias Snapshot de vVols gestionadas por VMware se descargan a ONTAP, que utiliza clones de archivos o LUN rápidos y eficientes), se necesita una orquestación general para gestionar la replicación y la recuperación. Los metadatos acerca de vVols están protegidos tanto por ONTAP como por el proveedor VASA, pero es necesario procesar más para usarlos en un sitio secundario.

Las herramientas de ONTAP 9.7.1, junto con la versión VMware Site Recovery Manager (SRM) 8,3, añadieron compatibilidad para la recuperación ante desastres y la orquestación del flujo de trabajo de migración aprovechando la tecnología SnapMirror de NetApp.

En la versión inicial de la compatibilidad de SRM con las herramientas de ONTAP 9.7.1, era necesario crear previamente volúmenes de FlexVol y habilitar la protección SnapMirror antes de usarlos como backups de volúmenes para un almacén de datos vVols. A partir de ONTAP TOOLS 9,10, ese proceso ya no es necesario. Ahora puede añadir protección de SnapMirror a los volúmenes de respaldo existentes y actualizar sus políticas de almacenamiento de máquinas virtuales para aprovechar la gestión basada en políticas con recuperación ante desastres y orquestación de migración, y automatización integrada con SRM.

Actualmente, VMware SRM es la única solución de recuperación ante desastres y automatización de la migración para vVols compatible con NetApp, y las herramientas de ONTAP comprobarán la existencia de un servidor SRM 8,3 o posterior registrado en su vCenter antes de permitir habilitar la replicación de vVols. Aunque es posible aprovechar las API de REST DE herramientas de ONTAP para crear sus propios servicios.

Replicación de vVols con SRM



Soporte de MetroCluster

Aunque las herramientas de ONTAP no pueden activar una conmutación por error de MetroCluster, sí son compatibles con los sistemas MetroCluster de NetApp para vVols que realizan el backup de volúmenes en una configuración uniforme de vSphere Metro Storage Cluster (VMSC). La conmutación de un sistema MetroCluster se efectúa de la forma normal.

Aunque SnapMirror Business Continuity (SM-BC) de NetApp también puede utilizarse como base para una configuración VMSC, actualmente no es compatible con vVols.

Consulte estas guías para obtener más información sobre MetroCluster de NetApp:

"*TR-4689 Arquitectura y diseño de la solución MetroCluster IP*"

"*TR-4705 Arquitectura y diseño de la solución MetroCluster de NetApp*"

"*VMware KB 2031038 Soporte de VMware vSphere con NetApp MetroCluster*"

Descripción general de vVols Backup

Existen varios enfoques para proteger las máquinas virtuales, como el uso de agentes de backup internos, la asociación de archivos de datos de máquinas virtuales a un proxy de backup o el uso de API definidas como VMware VADP. Es posible que vVols esté protegido usando los mismos mecanismos, y muchos partners de NetApp admiten backups de VM, incluidos vVols.

Como se ha mencionado anteriormente, las snapshots gestionadas por VMware vCenter se descargan en clones rápidos de archivos o LUN de ONTAP con gestión eficiente del espacio. Se pueden utilizar para realizar backups manuales rápidos, pero el vCenter limita a un máximo de 32 copias Snapshot. Puede utilizar vCenter para tomar Snapshot y revertir según sea necesario.

Comenzando con el complemento SnapCenter para VMware vSphere (SCV) 4,6 cuando se usa junto con

ONTAP Tools 9,10 y versiones posteriores añade soporte para el backup y la recuperación consistentes con los fallos de máquinas virtuales basadas en vVols aprovechando snapshots de volúmenes de ONTAP FlexVol con compatibilidad con replicación de SnapMirror y SnapVault. Se admiten hasta 1023 copias Snapshot por volumen. SCV también puede almacenar más copias Snapshot con una retención más prolongada en volúmenes secundarios mediante SnapMirror con una política de reflejo de almacén.

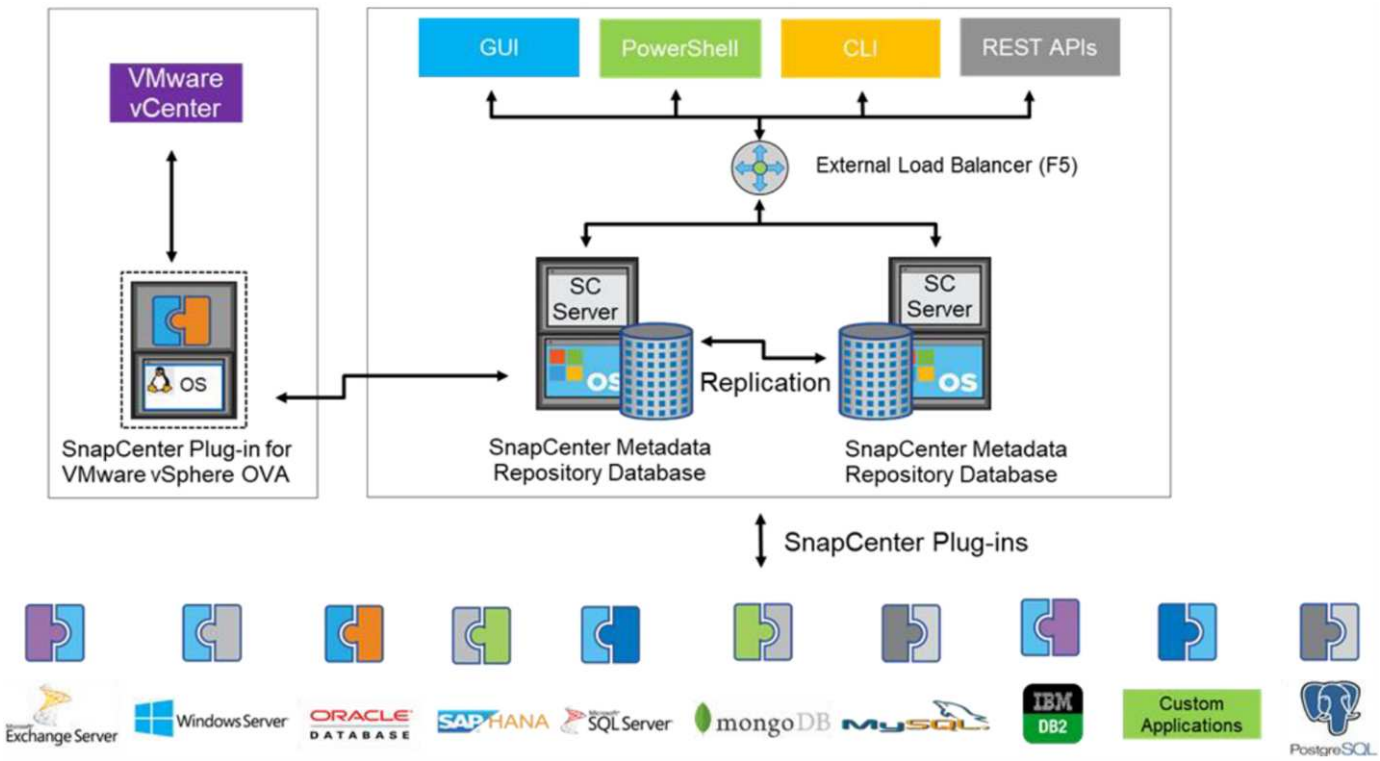
Se introdujo la compatibilidad con vSphere 8,0 con SCV 4,7, que utilizó una arquitectura de complemento local aislada. Se agregó compatibilidad con vSphere 8.0U1 a SCV 4,8, que realizó la transición completa a la nueva arquitectura de complementos remotos.

VVols Backup con el complemento de SnapCenter para VMware vSphere

Con NetApp SnapCenter, ahora puede crear grupos de recursos para vVols basados en etiquetas y/o carpetas para aprovechar automáticamente las snapshots basadas en FlexVol de ONTAP para máquinas virtuales basadas en vVols. De este modo, podrá definir servicios de backup y recuperación de datos que protegerán automáticamente las máquinas virtuales cuando se aprovisionen dinámicamente en su entorno.

El complemento de SnapCenter para VMware vSphere se pone en marcha como dispositivo independiente registrado como extensión de vCenter, gestionado a través de la interfaz de usuario de vCenter o a través de API de REST para la automatización de servicios de backup y recuperación de datos.

Arquitectura SnapCenter



Como los otros complementos de SnapCenter aún no admiten vVols en el momento de escribir este documento, nos centraremos en el modelo de implementación independiente de este documento.

Como SnapCenter utiliza copias Snapshot de ONTAP FlexVol, no se genera ninguna sobrecarga en vSphere ni el rendimiento se ve afectado por las máquinas virtuales tradicionales utilizando copias Snapshot gestionadas de vCenter. Además, dado que la funcionalidad de SCV se expone a través de las API DE REST, es más fácil crear flujos de trabajo automatizados mediante herramientas como Aria Automation de VMware, Ansible, Terraform y prácticamente cualquier otra herramienta de automatización capaz de usar API DE REST estándar.

Para obtener más información sobre las API de REST de SnapCenter, consulte "Información general de las API de REST"

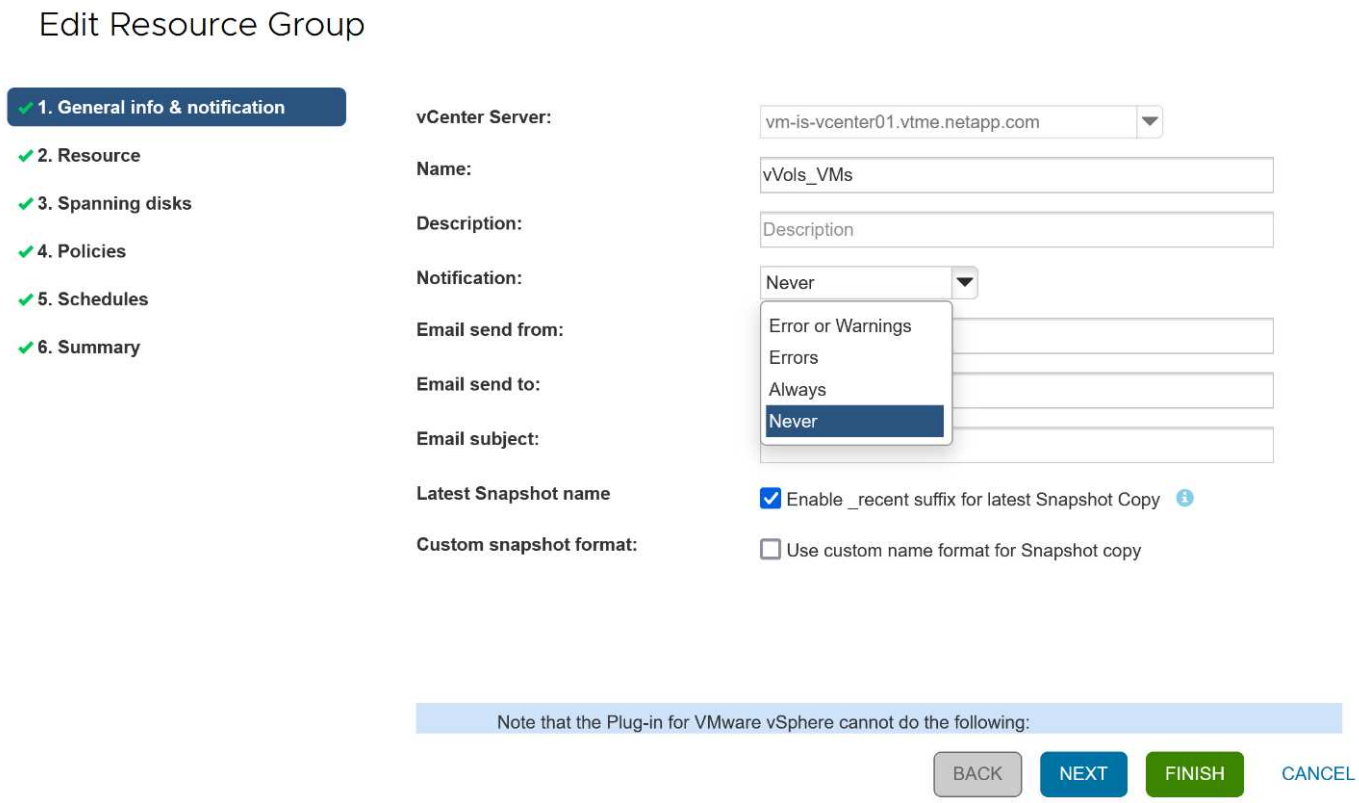
Para obtener información sobre las API de REST del plugin de SnapCenter para VMware vSphere, consulte "API de REST del plugin de SnapCenter para VMware vSphere"

Mejores prácticas

Las siguientes mejores prácticas pueden ayudarle a sacar el máximo partido de la puesta en marcha de SnapCenter.

- SCV es compatible con el control de acceso basado en roles de vCenter Server y de ONTAP, e incluye roles predefinidos de vCenter que se crean automáticamente para usted cuando se registra el plugin. Es posible obtener más información sobre los tipos de RBAC admitidos "aquí."
  - Use la interfaz de usuario de vCenter para asignar acceso a cuentas con menos privilegios mediante los roles predefinidos descritos "aquí".
  - Si utiliza SCV con SnapCenter Server, debe asignar el rol *SnapCenterAdmin*.
  - El control de acceso basado en roles de ONTAP hace referencia a la cuenta de usuario que se utiliza para añadir y gestionar los sistemas de almacenamiento que utiliza SCV. El control de acceso basado en roles de ONTAP no se aplica a los backups basados en vVols. Obtenga más información sobre el control de acceso basado en roles de ONTAP y SCV "aquí".
- Replique sus conjuntos de datos de backups en un segundo sistema mediante SnapMirror para obtener réplicas completas de volúmenes de origen. Como ya se ha mencionado anteriormente, también puede utilizar políticas de mirror-vault para la retención a largo plazo de los datos de backup con independencia de la configuración de retención de copias Snapshot del volumen de origen. Ambos mecanismos son compatibles con vVols.
- Dado que SCV también requiere las herramientas de ONTAP para la funcionalidad de VMware vSphere para vVols, compruebe siempre la compatibilidad de versiones específica de la Herramienta de Matriz de Interoperabilidad (IMT) de NetApp
- Si usa la replicación de vVols con VMware SRM, tenga en cuenta el objetivo de punto de recuperación y la programación de backups de su política
- Diseñe sus políticas de backup con ajustes de retención que cumplan los objetivos de punto de recuperación (RPO) definidos de su organización
- Configure los ajustes de notificación en los grupos de recursos para que se notifique el estado cuando se ejecuten los backups (consulte la figura 10 a continuación).

Opciones de notificación para el grupo de recursos



Comience a usar SCV usando estos documentos

"Obtenga información sobre el plugin de SnapCenter para VMware vSphere"

"Ponga en marcha el plugin de SnapCenter para VMware vSphere"

Resolución de problemas

Existen varios recursos de solución de problemas disponibles con información adicional.

Sitio de soporte de NetApp

Además de una variedad de artículos de la base de conocimientos para los productos de virtualización de NetApp, el sitio de soporte de NetApp también ofrece una página de inicio práctica para el "Herramientas de ONTAP para VMware vSphere" producto. Este portal proporciona enlaces a artículos, descargas, informes técnicos y debates sobre soluciones de VMware sobre la comunidad de NetApp. Está disponible en:

"*Sitio de soporte de NetApp*"

Aquí se encuentra disponible documentación adicional sobre la solución:

"*Soluciones de NetApp para la virtualización con VMware de Broadcom*"

Solución de problemas del producto

Los distintos componentes de las herramientas de ONTAP, como el complemento vCenter, el proveedor VASA y el adaptador de replicación de almacenamiento, se documentan juntos en el repositorio de documentos de NetApp. Sin embargo, cada uno tiene una subsección independiente de la base de conocimientos y puede tener procedimientos específicos de solución de problemas. Estos solucionan los problemas más comunes

que se pueden encontrar con el proveedor VASA.

Problemas de interfaz de usuario del proveedor de VASA

Ocasionalmente, vCenter vSphere Web Client encuentra problemas con los componentes de Serenity, lo que hace que no se muestren los elementos de menú VASA Provider for ONTAP. Consulte Resolver problemas de registro del proveedor VASA en la guía de puesta en marcha o esta base de conocimientos "artículo".

Error de aprovisionamiento del almacén de datos de vVols

En ocasiones, es posible que se agote el tiempo de espera de los servicios de vCenter al crear el almacén de datos vVols. Para corregirlo, reinicie el servicio vmware-sps y vuelva a montar el almacén de datos vVols mediante los menús de vCenter (Storage > New Datastore). Esto se trata en el error del aprovisionamiento de almacenes de datos de vVols con vCenter Server 6,5 en la guía de administración.

La actualización de Unified Appliance no puede montar ISO

Debido a un error en vCenter, es posible que el ISO utilizado para actualizar Unified Appliance de una versión a la siguiente no se pueda montar. Si la ISO se puede conectar al dispositivo en vCenter, siga el proceso en esta base de conocimientos "artículo" para solucionar.

VMware Site Recovery Manager con ONTAP

Recuperación de sitios en vivo de VMware con ONTAP

ONTAP ha sido una solución de almacenamiento líder para VMware vSphere y, más recientemente, Cloud Foundation, desde que ESX se introdujo en los centros de datos modernos hace más de dos décadas. NetApp continúa introduciendo sistemas innovadores, como la última generación de la serie ASA A, junto con funciones como la sincronización activa SnapMirror . Estos avances simplifican la gestión, mejoran la resiliencia y reducen el costo total de propiedad (TCO) de su infraestructura de TI.

Este documento presenta la solución ONTAP para VMware Live Site Recovery (VLSR), anteriormente conocido como Site Recovery Manager (SRM), el software de recuperación ante desastres (DR) líder en la industria de VMware, que incluye la información más reciente del producto y las mejores prácticas para optimizar la implementación, reducir el riesgo y simplificar la gestión continua.

> Esta documentación reemplaza el informe técnico publicado anteriormente *TR-4900: VMware Site Recovery Manager con ONTAP*

Las prácticas recomendadas complementan otros documentos como guías y herramientas de compatibilidad. Se desarrollan según pruebas de laboratorio y una amplia experiencia de campo por parte de ingenieros y clientes de NetApp. En algunos casos, las prácticas recomendadas pueden no ser la opción adecuada para su entorno; sin embargo, generalmente son las soluciones más sencillas que satisfacen las necesidades del mayor número de clientes.

Este documento se centra en las funcionalidades de los últimos lanzamientos de ONTAP 9 cuando se utiliza junto con las herramientas de ONTAP para VMware vSphere 10,4 (que incluye el adaptador de replicación del almacenamiento de NetApp [SRA] y el proveedor VASA [VP]), así como la recuperación de sitio en activo de VMware 9.

¿Por qué usar ONTAP con VLSR o SRM?

Las plataformas de gestión de datos de NetApp impulsadas por ONTAP son algunas de las soluciones de almacenamiento más adoptadas para VLSR. Las razones son abundantes: una plataforma de gestión de datos segura, de alto rendimiento y con protocolo unificado (NAS y SAN juntos) que proporciona eficiencia de almacenamiento que define la industria, multitenencia, controles de calidad de servicio, protección de datos con instantáneas que ahorran espacio y replicación con SnapMirror. Todo ello aprovechando la integración nativa de múltiples nubes híbridas para la protección de las cargas de trabajo de VMware y una gran cantidad de herramientas de automatización y orquestación a su alcance.

Cuando utiliza SnapMirror para la replicación basada en matrices, aprovecha una de las tecnologías más probadas y maduras de ONTAP. SnapMirror le ofrece la ventaja de realizar transferencias de datos seguras y altamente eficientes, copiando únicamente bloques del sistema de archivos modificados, no máquinas virtuales o almacenes de datos completos. Incluso esos bloques aprovechan los ahorros de espacio, como la deduplicación, la compresión y la compactación. Los sistemas ONTAP modernos ahora utilizan SnapMirror independiente de la versión, lo que le permite flexibilidad al seleccionar sus clústeres de origen y destino. SnapMirror se ha convertido verdaderamente en una de las herramientas más poderosas disponibles para la recuperación ante desastres.

Ya sea que utilice almacenes de datos tradicionales conectados a NFS, iSCSI o Fibre Channel (ahora con soporte para almacenes de datos vVols), VLSR proporciona una oferta sólida de primera mano que aprovecha lo mejor de las capacidades de ONTAP para la recuperación ante desastres o la planificación y orquestación de la migración del centro de datos.

Aprovechamiento de VLSR ONTAP 9

VLSR aprovecha las tecnologías avanzadas de gestión de datos de los sistemas de ONTAP al integrarse con herramientas de ONTAP para VMware vSphere, un dispositivo virtual que incluye tres componentes principales:

- El complemento de herramientas de ONTAP para vCenter, anteriormente conocido como consola de almacenamiento virtual (VSC), simplifica las funciones de eficiencia y gestión del almacenamiento, mejora la disponibilidad y reduce los costes de almacenamiento y la sobrecarga operativa, tanto si utiliza SAN como NAS. Utiliza prácticas recomendadas para aprovisionar almacenes de datos y optimiza la configuración de host ESXi para entornos de almacenamiento en bloques y NFS. Para obtener todos estos beneficios, NetApp recomienda este plugin cuando se utiliza vSphere con sistemas que ejecutan ONTAP.
- Las herramientas de ONTAP VASA Provider admiten las API de VMware vStorage para el marco de conocimiento del almacenamiento (VASA). EL proveedor DE VASA conecta vCenter Server con ONTAP para ayudar en el aprovisionamiento y la supervisión del almacenamiento de máquinas virtuales. Esto ha permitido el soporte de VMware Virtual Volumes (vVols) y la gestión de políticas de almacenamiento de VM y el rendimiento de vVols individuales de VM. También proporciona alarmas para controlar la capacidad y el cumplimiento de los perfiles.
- El SRA se usa junto con el VLSR para gestionar la replicación de datos de máquinas virtuales entre sitios de producción y recuperación ante desastres para almacenes de datos VMFS tradicionales y NFS, y también para las pruebas no disruptivas de réplicas de recuperación ante desastres. Ayuda a automatizar las tareas de identificación, recuperación y protección. Incluye tanto un dispositivo de servidor SRA como adaptadores SRA para el servidor SRM de Windows y el dispositivo VLSR.

Después de haber instalado y configurado los adaptadores SRA en el servidor VLSR para proteger almacenes de datos que no sean vVols, puede comenzar la tarea de configurar su entorno vSphere para la recuperación ante desastres.

El SRA proporciona una interfaz de comando y control para que el servidor VLSR gestione los volúmenes de

ONTAP FlexVol que contienen las máquinas virtuales de VMware (VM), además de la replicación de SnapMirror que las protege.

VLSR puede probar su plan de recuperación ante desastres de forma no disruptiva utilizando la tecnología FlexClone , propiedad de NetApp, para realizar clones casi instantáneos de sus almacenes de datos protegidos en su sitio de recuperación ante desastres. VLSR crea un entorno sandbox para realizar pruebas de forma segura para que su organización y sus clientes estén protegidos en caso de un verdadero desastre, lo que le brinda confianza en la capacidad de su organización para ejecutar una conmutación por error durante un desastre.

En caso de verdadero desastre o incluso de una migración planificada, VLSR permite enviar cualquier cambio de última hora al conjunto de datos mediante una actualización final de SnapMirror (si lo decide). A continuación, interrumpe el reflejo y monta el almacén de datos en los hosts de recuperación ante desastres. En ese momento, las máquinas virtuales pueden encenderse automáticamente en cualquier orden de acuerdo con la estrategia planificada previamente.

> Aunque los sistemas ONTAP le permitirán emparejar SVM en el mismo clúster para la replicación de SnapMirror, ese escenario no se ha probado ni certificado con VLSR. Por lo tanto, se recomienda usar solo SVM de diferentes clústeres cuando se utilice VLSR.

VLSR con ONTAP y otros casos de uso: Cloud híbrido y migración

La integración de su implementación de VLSR con las capacidades de gestión de datos avanzadas de ONTAP permite una escala y un rendimiento enormemente mejorados en comparación con las opciones de almacenamiento local. Pero más que eso, aporta la flexibilidad de la nube híbrida. La nube híbrida le permite ahorrar dinero al organizar en niveles los bloques de datos no utilizados desde su matriz de alto rendimiento hasta su hiperescalador preferido usando FabricPool, que podría ser un almacén S3 local como NetApp StorageGRID. También puede usar SnapMirror para sistemas basados en el borde con ONTAP Select definido por software o DR basado en la nube usando Cloud Volumes ONTAP (CVO) o "Almacenamiento NetApp en Equinix Metal®" , u otros servicios alojados en ONTAP .

Podría entonces hacer una conmutación por error de prueba dentro del centro de datos de un proveedor de servicios en cloud con un espacio de almacenamiento prácticamente nulo gracias a FlexClone. La protección de su empresa ahora puede costar menos que nunca.

VLSR también puede utilizarse para ejecutar migraciones planificadas aprovechando SnapMirror para transferir de forma eficiente sus máquinas virtuales desde un centro de datos a otro o incluso dentro del mismo centro de datos, ya sea el suyo o mediante cualquier otro proveedor de servicios para partners de NetApp.

Mejores prácticas de puesta en marcha

Las siguientes secciones describen las mejores prácticas para la puesta en marcha con ONTAP y VMware SRM.

Utilice la versión más reciente de las herramientas de ONTAP 10

ONTAP TOOLS 10 proporciona mejoras significativas con respecto a versiones anteriores, como las siguientes:

- conmutación por error de prueba 8x veces más rápida*
- limpieza y reprotección 2x veces más rápidas*

- 32% más rápido de failover*
- Mayor escala
- Compatibilidad nativa para diseños de sitios compartidos

*Estas mejoras se basan en pruebas internas y pueden variar en función de su entorno.

Distribución y segmentación de SVM para SMT

Con ONTAP, el concepto de las máquinas virtuales de almacenamiento (SVM) proporciona una segmentación estricta en entornos multi-tenant seguros. Los usuarios de SVM en una SVM no pueden acceder a los recursos ni gestionarlos desde otra. De este modo, puede aprovechar la tecnología ONTAP creando SVM independientes para diferentes unidades de negocio que gestionan sus propios flujos de trabajo de SRM en el mismo clúster para mejorar la eficiencia general del almacenamiento.

Considere la posibilidad de gestionar ONTAP mediante cuentas de ámbito SVM y LIF de administración de SVM para no solo mejorar los controles de seguridad, sino también mejorar el rendimiento. El rendimiento es inherentemente mayor cuando se usan conexiones de ámbito SVM porque el SRA no es necesario para procesar todos los recursos de todo un clúster, incluidos los recursos físicos. En su lugar, solo debe comprender los activos lógicos que se abstraen a una SVM en particular.

Prácticas recomendadas para gestionar sistemas ONTAP 9

Como se ha mencionado anteriormente, puede gestionar clústeres de ONTAP utilizando credenciales de ámbito de clúster o de SVM y LIF de gestión. Para obtener un rendimiento óptimo, es posible que desee considerar el uso de las credenciales del ámbito SVM siempre que no utilice vVols. Sin embargo, al hacerlo, debe conocer algunos requisitos y perder algunas funciones.

- La cuenta de SVM predeterminada de vsadmin no tiene el nivel de acceso requerido para realizar tareas de las herramientas de ONTAP. Por lo tanto, debe crear una cuenta de SVM nueva. "Configure los roles y privilegios de usuario de ONTAP" Usando el archivo JSON incluido. Puede utilizarse para cuentas de SVM o de ámbito de clúster.
- Dado que el complemento de interfaz de usuario de vCenter, VASA Provider y el servidor SRA son microservicios totalmente integrados, debe añadir almacenamiento al adaptador de SRA en SRM de la misma manera que añade almacenamiento en la interfaz de usuario de vCenter para las herramientas de ONTAP. De lo contrario, es posible que el servidor SRA no reconozca las solicitudes que se envían desde el SRM a través del adaptador SRA.
- La comprobación de rutas de NFS no se realiza con credenciales de ámbito SVM, a menos que primero "clústeres incorporados" en el administrador de herramientas de ONTAP y las asocie a vCenter. Esto se debe a que la ubicación física se abstrae de forma lógica de la SVM. Sin embargo, este no es un motivo de preocupación, ya que los sistemas ONTAP modernos ya no sufren una disminución notable del rendimiento cuando se utilizan rutas indirectas.
- Es posible que no se informe del ahorro de espacio agregado debido a la eficiencia del almacenamiento.
- Si es compatible, los duplicados de uso compartido de carga no se pueden actualizar.
- Es posible que no se realicen registros de EMS en sistemas ONTAP gestionados con credenciales de ámbito de SVM.

Mejores prácticas operativas

Las siguientes secciones describen las mejores prácticas operativas para el almacenamiento de VMware SRM y ONTAP.

Almacenes de datos y protocolos

- Si es posible, utilice siempre herramientas ONTAP para aprovisionar almacenes de datos y volúmenes. De este modo se garantiza que los volúmenes, rutas de unión, LUN, iGroups, políticas de exportación, y otros ajustes se configuran de forma compatible.
- El SRM admite iSCSI, Fibre Channel y NFS versión 3 con ONTAP 9 al usar la replicación basada en cabinas a través de SRA. SRM no admite la replicación basada en cabinas para NFS versión 4.1 con almacenes de datos tradicionales o vVols.
- Para confirmar la conectividad, siempre compruebe que puede montar y desmontar un almacén de datos de prueba nuevo en el sitio de recuperación ante desastres del clúster de ONTAP de destino. Pruebe cada protocolo que pretenda utilizar para la conectividad de almacenes de datos. Una práctica recomendada es usar las herramientas de ONTAP para crear su almacén de datos de prueba, ya que está haciendo toda la automatización del almacén de datos según las indicaciones del SRM.
- Los protocolos SAN deben ser homogéneos para cada sitio. Puede mezclar NFS y SAN, pero los protocolos SAN no deben mezclarse dentro de un sitio. Por ejemplo, puede utilizar FCP en el sitio A e iSCSI en el sitio B. No debería utilizar FCP e iSCSI en el sitio A.
- Las guías anteriores aconsejan crear LIF para la localidad de datos. Es decir, monte siempre un almacén de datos con una LIF ubicada en el nodo que posee físicamente el volumen. Aunque sigue siendo la mejor práctica, ya no es un requisito en las versiones modernas de ONTAP 9. Siempre que sea posible y si se dan credenciales de ámbito de clúster determinadas, las herramientas de ONTAP seguirán optando por equilibrar la carga entre las LIF locales de los datos, pero no es un requisito de alta disponibilidad ni rendimiento.
- ONTAP 9 se puede configurar para eliminar automáticamente instantáneas para mantener el tiempo de actividad en caso de una condición de falta de espacio cuando autosize no puede suministrar suficiente capacidad de emergencia. La configuración predeterminada para esta funcionalidad no elimina automáticamente las copias Snapshot que crea SnapMirror. Si se eliminan las snapshots de SnapMirror, el SRA de NetApp no puede revertir ni resincronizar la replicación del volumen afectado. Para evitar que ONTAP elimine snapshots de SnapMirror, configure la funcionalidad de eliminación automática de snapshots como 'Probar'.

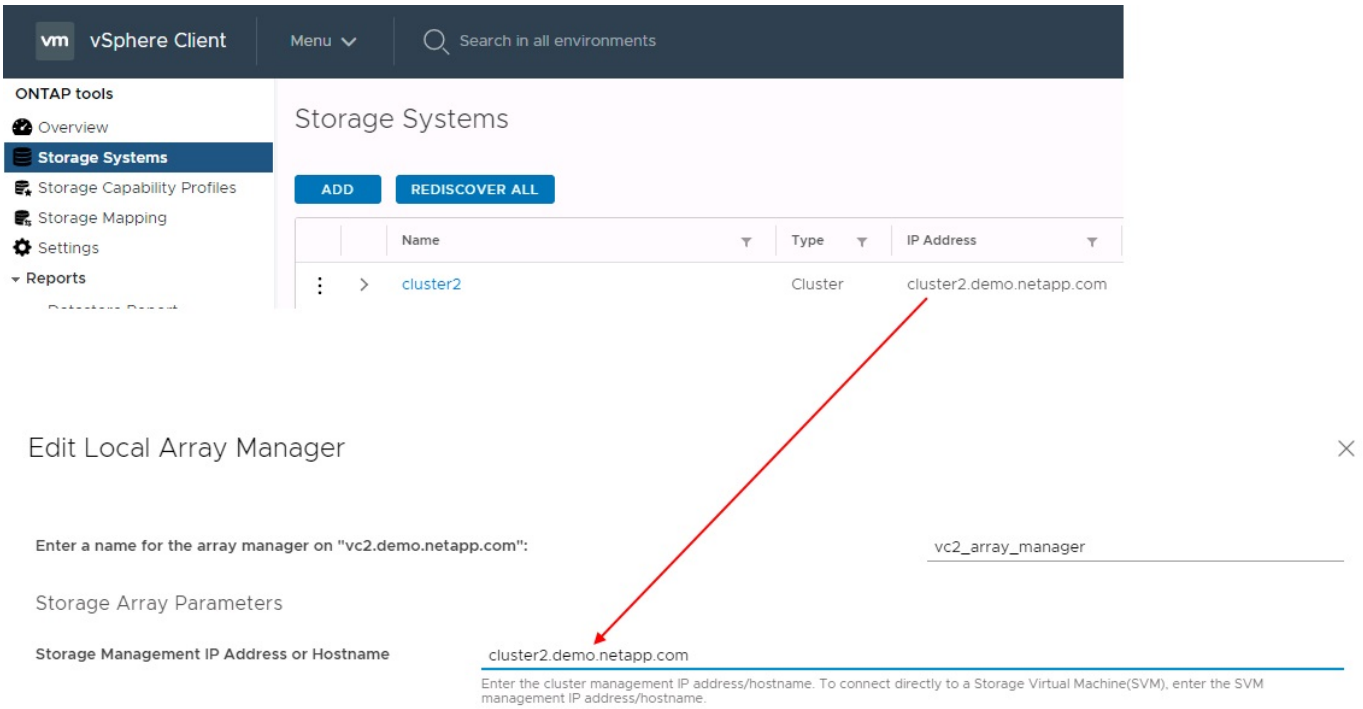
```
snap autodelete modify -volume -commitment try
```

- el tamaño automático del volumen debe establecerse en `grow` para los volúmenes que contienen almacenes de datos SAN y `grow_shrink` para almacenes de datos NFS. Obtenga más información sobre este tema en "Configure los volúmenes para que aumenten y reduzcan su tamaño automáticamente".
- SRM tiene un mejor rendimiento cuando el número de almacenes de datos y, por lo tanto, grupos de protección se minimizan en sus planes de recuperación. Por tanto, debería considerar la optimización para la densidad de las máquinas virtuales en entornos protegidos por SRM, donde el objetivo de tiempo de recuperación es de una importancia clave.
- Use el planificador de recursos distribuido (DRS) para equilibrar la carga en los clústeres ESXi protegidos y de recuperación. Recuerde que si tiene previsto realizar una conmutación tras recuperación, al ejecutar una nueva protección, los clústeres protegidos anteriormente se convertirán en los nuevos clústeres de recuperación. DRS ayudará a equilibrar la colocación en ambas direcciones.
- Siempre que sea posible, evite usar la personalización de IP con SRM, ya que esto puede aumentar su RTO.

Acerca de parejas de cabinas

Se crea un gestor de cabinas para cada pareja de cabinas. Con las herramientas SRM y ONTAP, el emparejamiento de cabinas se realiza con el ámbito de una SVM, incluso si utiliza credenciales de clúster. Esto le permite segmentar los flujos de trabajo de recuperación ante desastres entre inquilinos en función de los cuales se hayan asignado a gestionar las SVM. Puede crear varios administradores de cabina para un clúster determinado y pueden ser asimétricos. Es posible fan out o fan in entre diferentes clústeres de ONTAP 9. Por ejemplo, puede tener SVM-A y SVM-B en el clúster-1 que replica en SVM-C en el clúster-2, SVM-D en el clúster-3 o viceversa.

Al configurar parejas de cabinas en SRM, siempre debe añadirlas a SRM de la misma forma que las añadió a las herramientas de ONTAP, lo que significa que deben usar el mismo nombre de usuario, contraseña y LIF de gestión. Este requisito garantiza que el SRA se comunique correctamente con la matriz. La siguiente captura de pantalla ilustra cómo puede aparecer un clúster en las herramientas de ONTAP y cómo se puede añadir a un administrador de cabinas.



Acerca de los grupos de replicación

Los grupos de replicación contienen colecciones lógicas de máquinas virtuales que se recuperan juntas. Dado que la replicación de SnapMirror de ONTAP se produce en el nivel de volumen, todas las máquinas virtuales de un volumen se encuentran en el mismo grupo de replicación.

La consideración de los grupos de replicación es diversa y cómo se distribuyen los equipos virtuales entre los volúmenes de FlexVol. Agrupar equipos virtuales similares en el mismo volumen puede aumentar la eficiencia del almacenamiento con sistemas ONTAP anteriores que carecen de deduplicación a nivel de agregado, pero la agrupación aumenta el tamaño del volumen y reduce la concurrencia de I/O de volúmenes. El mejor equilibrio entre rendimiento y eficiencia del almacenamiento se puede lograr en los sistemas ONTAP modernos mediante la distribución de máquinas virtuales entre volúmenes de FlexVol en el mismo agregado, aprovechando así la deduplicación a nivel de agregado y ganando una mayor paralelización de I/O en múltiples volúmenes. Puede recuperar las máquinas virtuales en los volúmenes juntos porque un grupo de protección (tratado a continuación) puede contener varios grupos de replicación. La desventaja de esta distribución es que es posible que los bloques se transmitan a través de la conexión varias veces, ya que SnapMirror no tiene en cuenta la deduplicación de agregados.

Un aspecto final que se debe tener en cuenta para los grupos de replicación es que cada uno de ellos es, por su naturaleza, un grupo de consistencia lógico (que no se debe confundir con los grupos de consistencia SRM). Esto se debe a que todas las máquinas virtuales del volumen se transfieren juntas con la misma copia de Snapshot. Si tiene equipos virtuales que deben ser coherentes entre sí, considere almacenarlos en el mismo FlexVol.

Acerca de los grupos de protección

Los grupos de protección definen las máquinas virtuales y los almacenes de datos en grupos que se recuperan conjuntamente del sitio protegido. El sitio protegido es donde existen las máquinas virtuales configuradas en un grupo de protección durante las operaciones normales de estado constante. Es importante tener en cuenta que, aunque SRM puede mostrar varios administradores de cabinas para un grupo de protección, un grupo de protección no puede abarcar varios administradores de cabinas. Por este motivo, no debe abarcar los archivos de equipos virtuales entre almacenes de datos en diferentes SVM.

Acerca de los planes de recuperación

Los planes de recuperación definen qué grupos de protección se recuperan en el mismo proceso. Se pueden configurar varios grupos de protección en el mismo plan de recuperación. Además, para ofrecer más opciones para la ejecución de planes de recuperación, se puede incluir un solo grupo de protección en varios planes de recuperación.

Los planes de recuperación permiten a los administradores de SRM definir flujos de trabajo de recuperación asignando las máquinas virtuales a un grupo de prioridad de 1 (más alta) a 5 (más baja), siendo 3 (medio) el valor predeterminado. Dentro de un grupo de prioridad, las máquinas virtuales pueden configurarse para las dependencias.

Por ejemplo, su empresa podría tener una aplicación empresarial crítica de nivel 1 que dependa de un servidor Microsoft SQL para su base de datos. Por lo tanto, se deciden colocar las máquinas virtuales en el grupo de prioridad 1. Dentro del grupo de prioridad 1, comienza a planificar el pedido para que se traigan los servicios. Es probable que desee que el controlador de dominio de Microsoft Windows se inicie antes que el servidor Microsoft SQL, que tendría que estar en línea antes del servidor de aplicaciones, y así sucesivamente. Debe agregar todas estas máquinas virtuales al grupo de prioridades y, después, establecer las dependencias, dado que las dependencias solo se aplican dentro de un determinado grupo de prioridad.

NetApp recomienda encarecidamente trabajar con sus equipos de aplicaciones para comprender el orden de las operaciones necesarias en un escenario de conmutación por error y construir sus planes de recuperación según corresponda.

Probar la recuperación tras fallos

Como práctica recomendada, siempre realice una conmutación por error de prueba cada vez que se realice un cambio en la configuración del almacenamiento de VM protegido. Esto garantiza que, en caso de desastre, pueda confiar en que Site Recovery Manager pueda restaurar los servicios dentro del objetivo de RTO esperado.

NetApp también recomienda confirmar la funcionalidad de aplicaciones «en invitado» ocasionalmente, especialmente tras reconfigurar el almacenamiento de máquinas virtuales.

Cuando se realiza una operación de recuperación de pruebas, se crea una red privada de burbuja de pruebas en el host ESXi para los equipos virtuales. Sin embargo, esta red no está conectada automáticamente a ningún adaptador de red físico y, por lo tanto, no proporciona conectividad entre los hosts ESXi. Para permitir la comunicación entre máquinas virtuales que se ejecutan en diferentes hosts ESXi durante las pruebas de recuperación ante desastres, se crea una red privada física entre los hosts ESXi en el sitio de recuperación ante desastres. Para verificar que la red de prueba es privada, la red de burbuja de prueba se puede separar

físicamente o mediante VLAN o etiquetado VLAN. Esta red debe separarse de la red de producción porque, a medida que se recuperan los equipos virtuales, no se pueden colocar en la red de producción con direcciones IP que puedan entrar en conflicto con los sistemas de producción reales. Cuando se crea un plan de recuperación en SRM, es posible seleccionar la red de pruebas creada como la red privada para conectar los equipos virtuales a durante la prueba.

Una vez que la prueba se ha validado y ya no es necesaria, realice una operación de limpieza. La ejecución de la limpieza devuelve las máquinas virtuales protegidas a su estado inicial y restablece el plan de recuperación al estado Ready.

Consideraciones sobre la conmutación por error

Hay otros factores que se deben tener en cuenta a la hora de conmutar por error un sitio además del orden de las operaciones mencionado en esta guía.

Un problema que puede tener que lidiar es las diferencias de redes entre sitios. Es posible que algunos entornos puedan usar las mismas direcciones IP de red en el sitio primario y en el sitio de recuperación tras desastres. Esta capacidad se conoce como una configuración de red LAN virtual (VLAN) ampliada o extendida. Es posible que otros entornos tengan que utilizar diferentes direcciones IP de red (por ejemplo, diferentes VLAN) en el sitio principal con respecto al sitio de recuperación ante desastres.

VMware ofrece varias formas de resolver este problema. En primer lugar, las tecnologías de virtualización de redes como el centro de datos NSX-T de VMware abstraen toda la pila de redes de las capas 2 a 7 del entorno operativo, permitiendo soluciones más portátiles. Más información acerca de "Opciones de NSX-T con SRM".

SRM también le permite cambiar la configuración de red de un equipo virtual mientras se recupera. Esta reconfiguración incluye ajustes como las direcciones IP, las direcciones de puerta de enlace y la configuración del servidor DNS. Los diferentes ajustes de red, que se aplican a las VM individuales a medida que se recuperan, se pueden especificar en la configuración de la propiedad de una VM en el plan de recuperación.

Para configurar SRM de modo que aplique diferentes ajustes de red a varios equipos virtuales sin tener que editar las propiedades de cada uno del plan de recuperación, VMware ofrece una herramienta llamada DR-ip-customizer. Aprenda a usar esta utilidad, consulte "Documentación de VMware".

Vuelva a proteger

Después de una recuperación, el sitio de recuperación se convierte en el nuevo sitio de producción. Dado que la operación de recuperación rompió la replicación de SnapMirror, el nuevo sitio de producción no está protegido contra ningún desastre futuro. Una mejor práctica es proteger el nuevo site de producción en otro site inmediatamente después de una recuperación. Si el sitio de producción original está operativo, el administrador de VMware puede utilizar el sitio de producción original como un nuevo sitio de recuperación para proteger el nuevo sitio de producción, invirtiendo efectivamente la dirección de la protección. La reprotección solo está disponible en fallos no catastróficos. Por lo tanto, en algún momento deben recuperarse los servidores vCenter Server, los servidores ESXi, los servidores SRM y las bases de datos correspondientes originales. Si no están disponibles, deben crearse un nuevo grupo de protección y un nuevo plan de recuperación.

Conmutación tras recuperación

Una operación de conmutación tras recuperación es fundamentalmente una conmutación por error en una dirección diferente a la anterior. Como práctica recomendada, compruebe que el sitio original vuelve a los niveles aceptables de funcionalidad antes de intentar realizar la conmutación tras recuperación o, en otras palabras, la conmutación por error al sitio original. Si la instalación original sigue en peligro, deberá retrasar la conmutación tras recuperación hasta que se solucione el fallo lo suficiente.

Otra práctica recomendada para la conmutación tras recuperación es siempre realizar una conmutación al nodo de respaldo de prueba después de completar la reprotección y antes de llevar a cabo la conmutación tras recuperación final. Esto verifica que los sistemas en el sitio original pueden completar la operación.

Volver a proteger el sitio original

Después de la conmutación por recuperación, debe confirmar con todas las partes interesadas que sus servicios se han vuelto a la normalidad antes de ejecutar la reprotección de nuevo.

La ejecución de la reprotección después de la conmutación tras recuperación hace que el entorno vuelva a estar en el estado que estaba al principio, cuando la replicación de SnapMirror se ejecuta de nuevo desde el centro de producción al centro de recuperación.

Topologías de replicación

En ONTAP 9, los componentes físicos de un clúster son visibles para los administradores del clúster, pero no pueden ver directamente las aplicaciones y los hosts que utilizan el clúster. Los componentes físicos proporcionan un conjunto de recursos compartidos desde los cuales se construyen los recursos del clúster lógicos. Las aplicaciones y los hosts solo acceden a los datos a través de SVM que contienen volúmenes y LIF.

Cada SVM de NetApp se trata como una cabina en VMware vCenter Site Recovery Manager. VLSR admite ciertas distribuciones de replicación de cabina a cabina (o SVM a SVM).

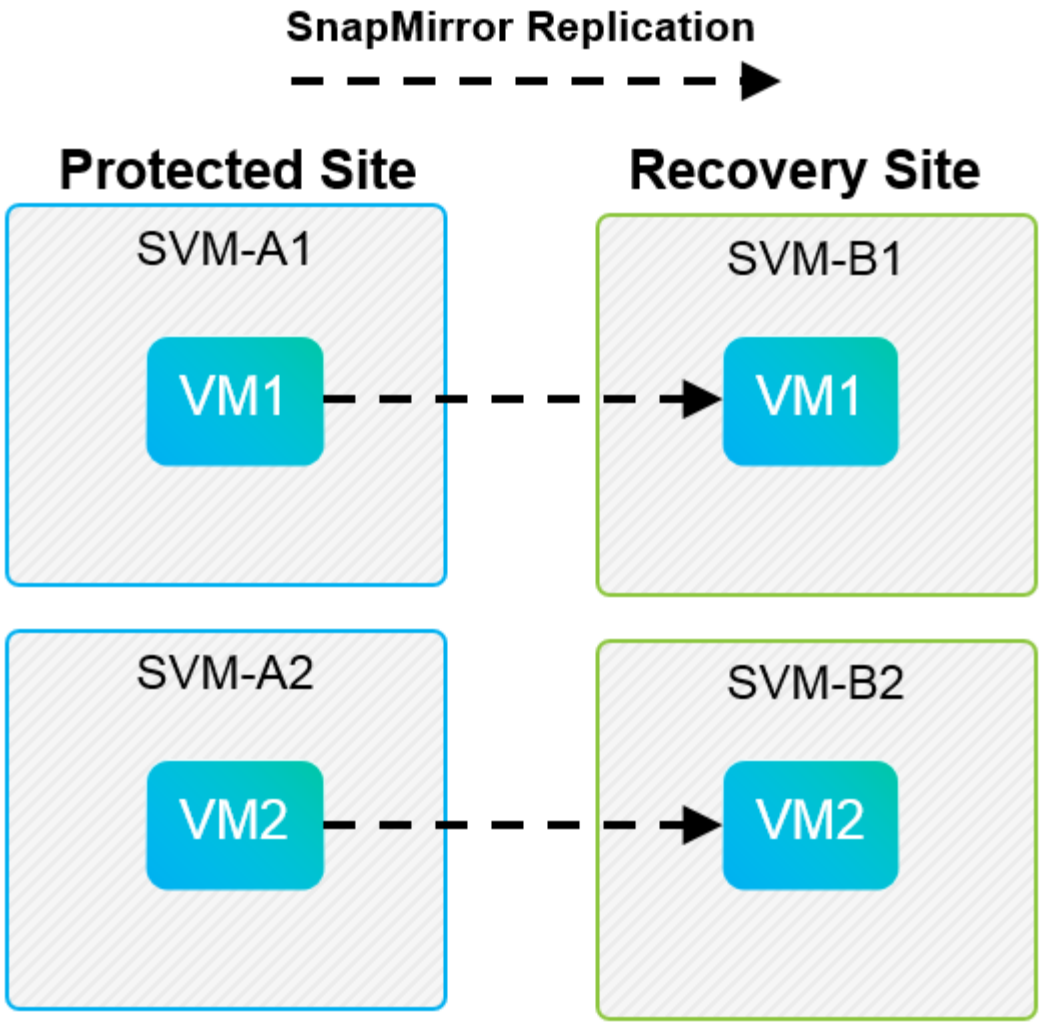
Una sola máquina virtual no puede poseer datos, Virtual Machine Disk (VMDK) o RDM, en más de una cabina de VLSR por los siguientes motivos:

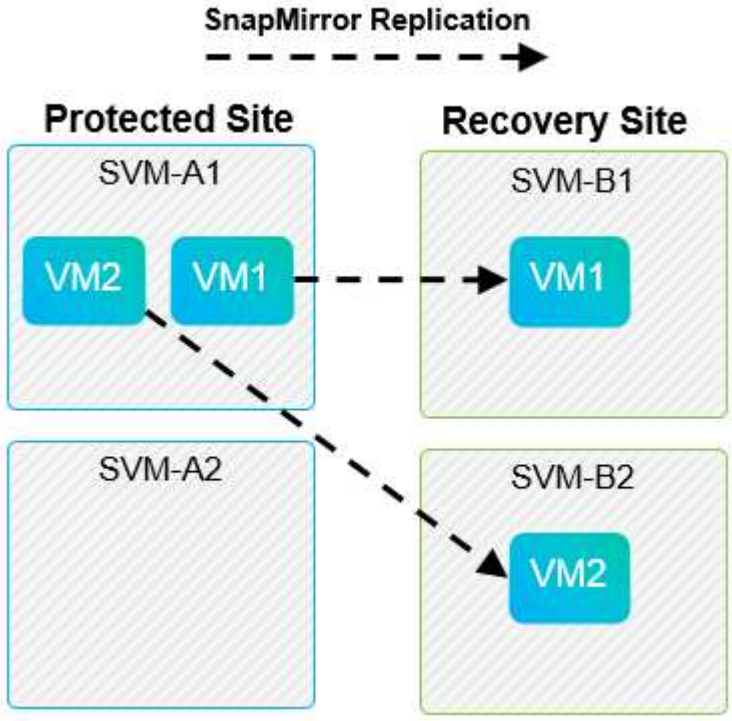
- VLSR solo ve la SVM, no una controladora física individual.
- Una SVM puede controlar los LUN y los volúmenes que abarcan varios nodos en un clúster.

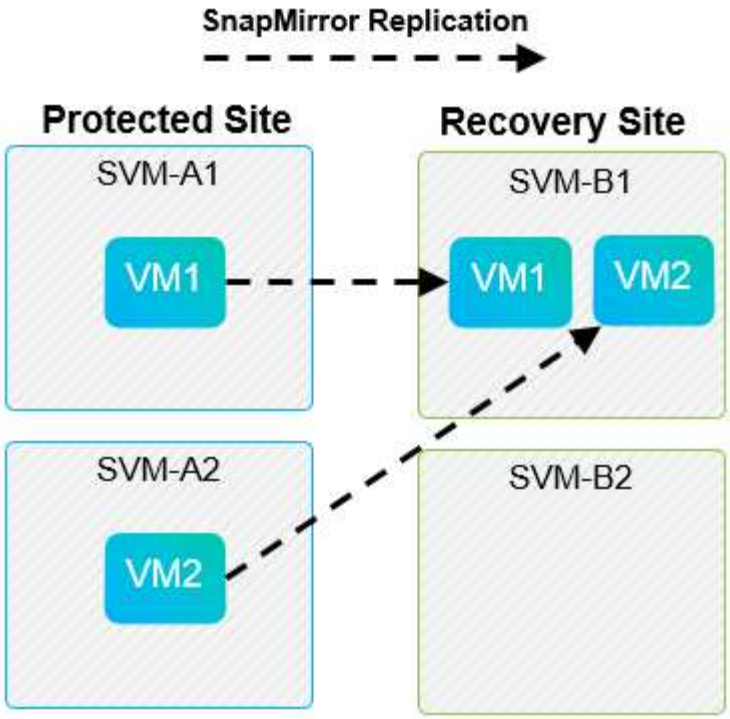
Mejor práctica
Para determinar la compatibilidad, tenga presente esta regla: Para proteger una máquina virtual con el VLSR y el SRA de NetApp, todas las partes de la máquina virtual deben existir en un solo SVM. Esta regla se aplica tanto al sitio protegido como al sitio de recuperación.

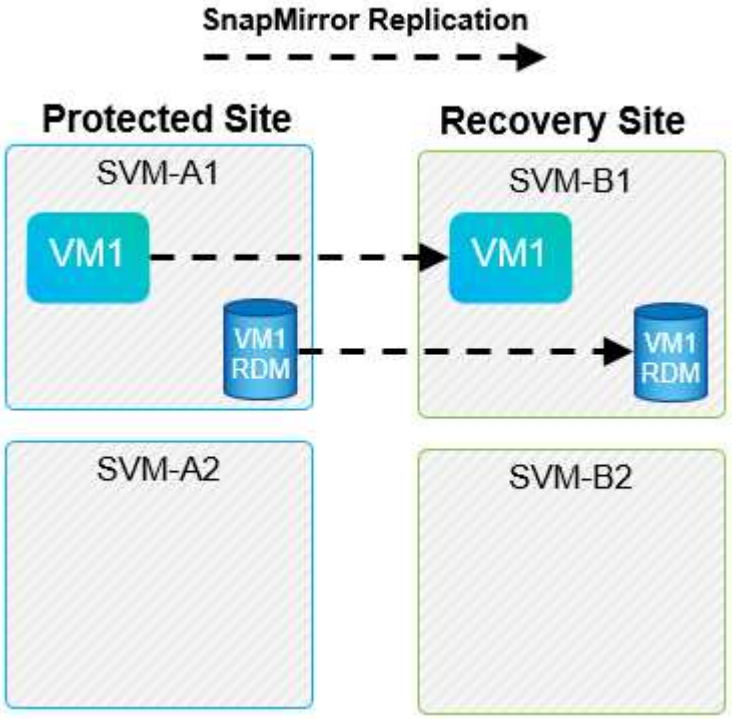
Distribuciones de SnapMirror compatibles

Las siguientes figuras muestran los escenarios de diseño de la relación de SnapMirror compatibles con VLSR y SRA. Cada equipo virtual de los volúmenes replicados posee datos en una sola cabina de VLSR (SVM) en cada sitio.


SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM1
SVM-B1
VM1
SVM-A2
VM2
SVM-B2
VM2

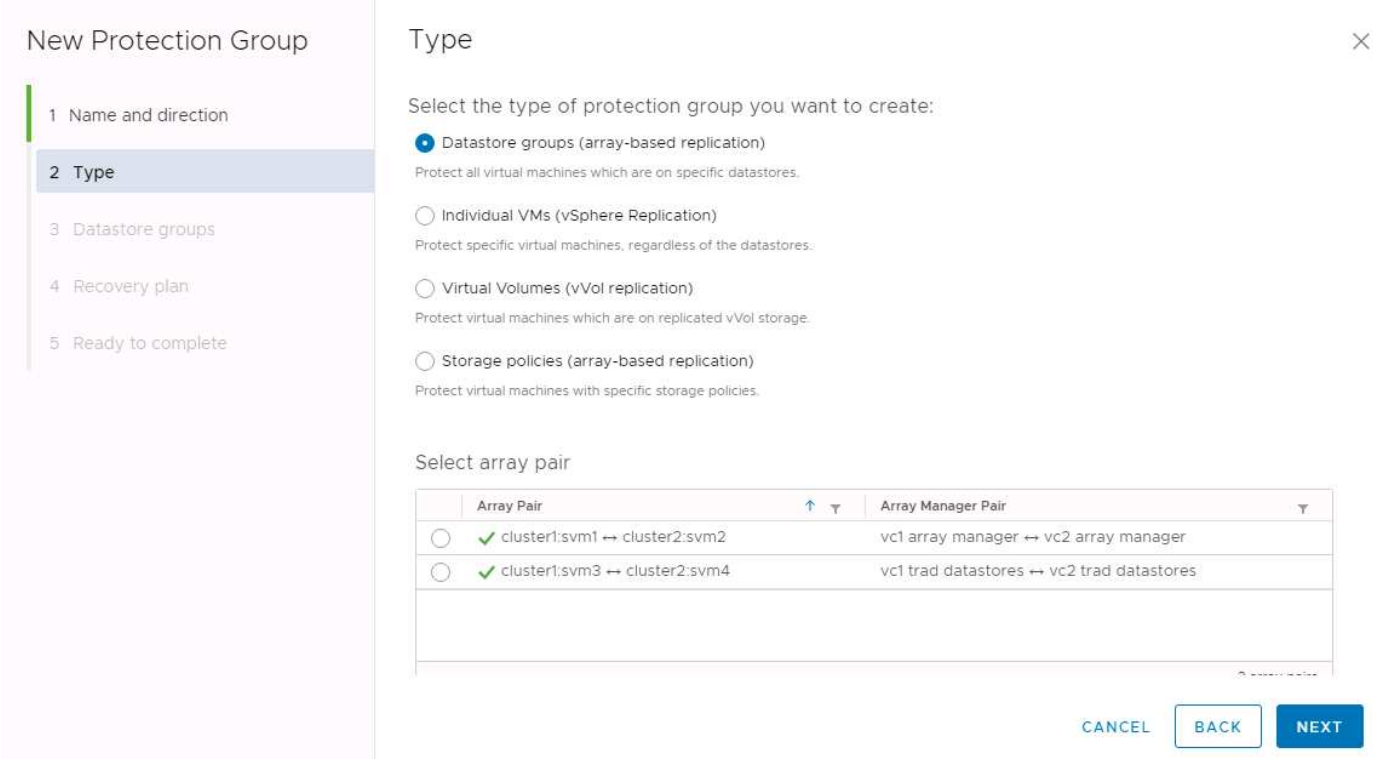

SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM2
VM1
SVM-B1
VM1
SVM-A2
SVM-B2
VM2





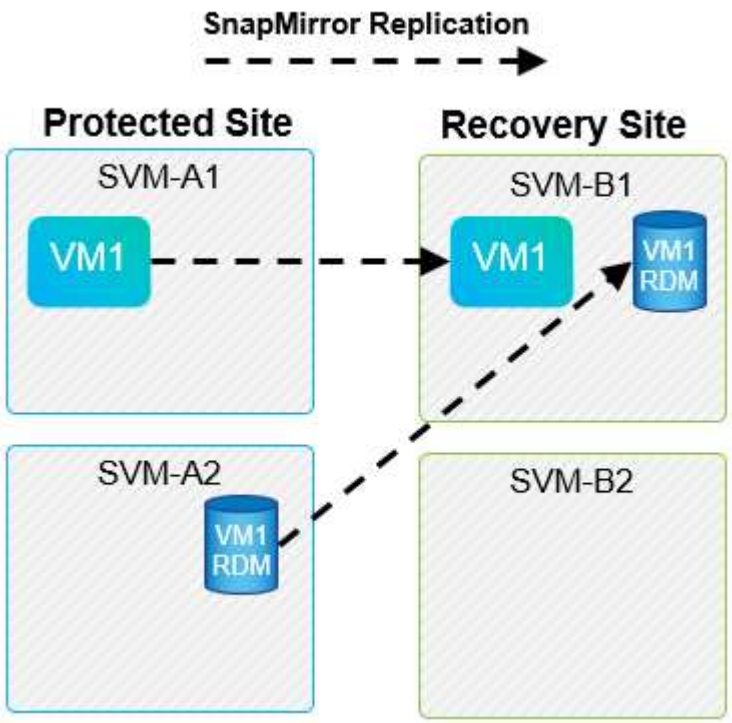
Diseños compatibles de Array Manager

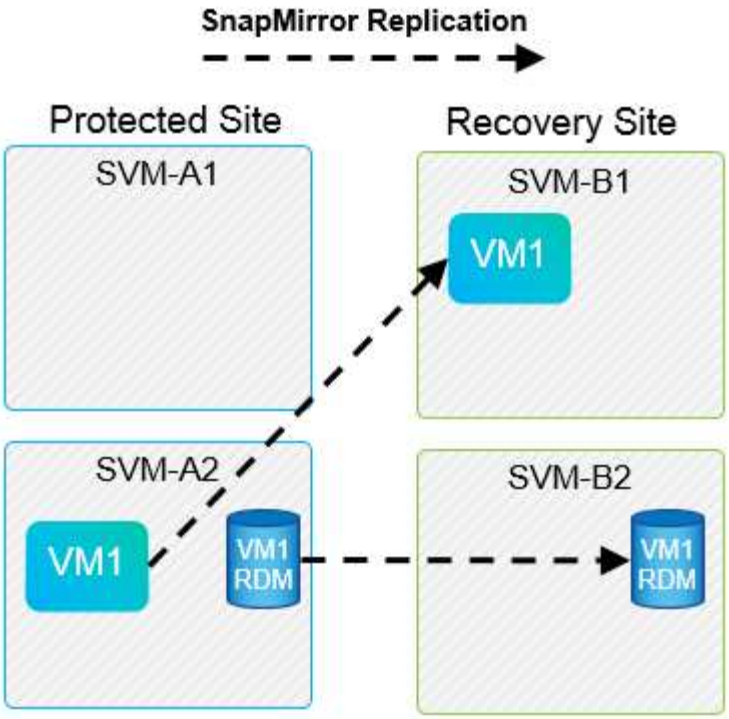
Cuando se utiliza la replicación basada en cabinas (ABR) en VLSR, los grupos de protección se aíslan en un solo par de cabina, como se muestra en la siguiente captura de pantalla. En este caso, `SVM1` y `SVM2` se relacionan con `SVM3` y `SVM4` en el sitio de recuperación. Sin embargo, es posible seleccionar solo una de las dos parejas de cabinas al crear un grupo de protección.



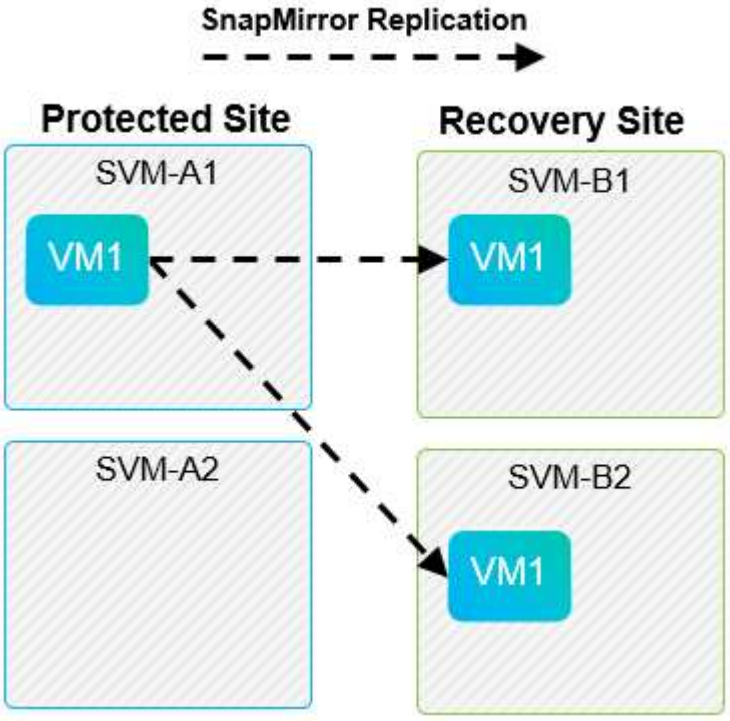
Diseños no admitidos

Las configuraciones no compatibles tienen datos (VMDK o RDM) en varias SVM que son propiedad de una máquina virtual individual. En los ejemplos que se muestran en las siguientes figuras, `VM1` no se puede configurar para protección con VLSR porque `VM1` tiene datos en dos SVM.





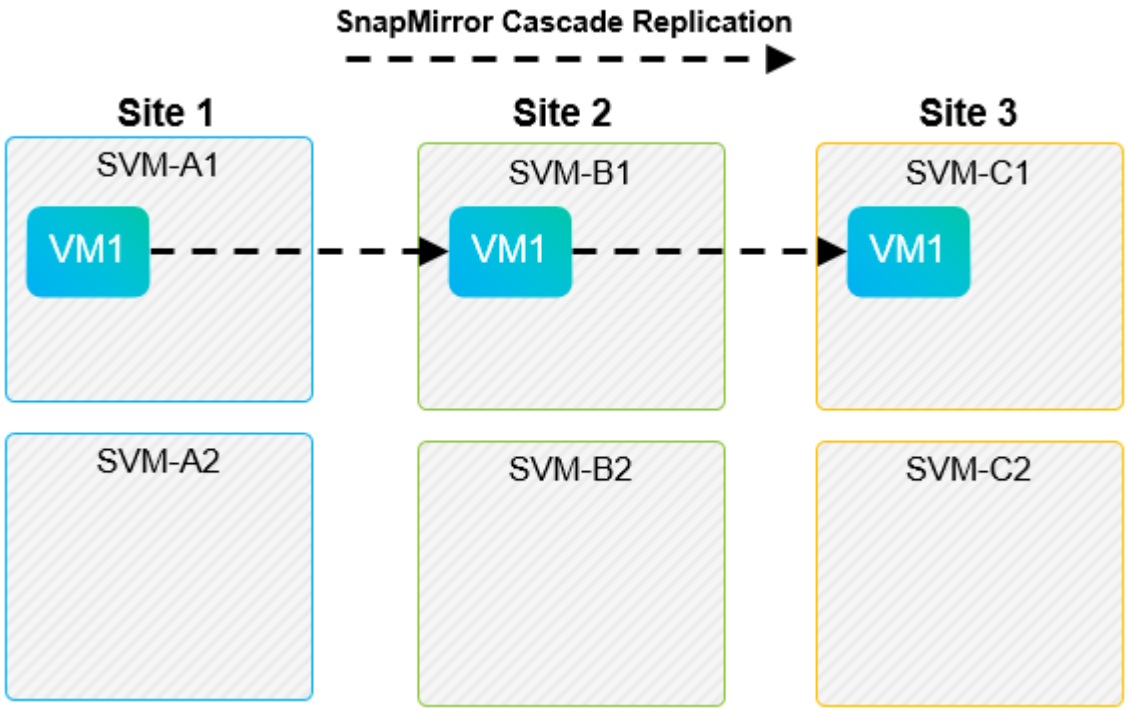
Toda relación de replicación en la que se replica un volumen individual de NetApp desde una SVM de origen a varios destinos en la misma SVM o en distintas SVM se denomina «fan-out» de SnapMirror. VLSR no es compatible con fan-out. En el ejemplo que se muestra en la siguiente figura, `VM1` no se puede configurar para protección en VLSR porque se replica con SnapMirror en dos ubicaciones diferentes.



Cascada de SnapMirror

VLSR no admite la configuración en cascada de relaciones de SnapMirror, en las que un volumen de origen se replica en un volumen de destino, y ese volumen de destino también se replica con SnapMirror en otro volumen de destino. En el caso que se muestra en la siguiente figura, VLSR no se puede utilizar para la

conmutación por error entre sitios.



SnapMirror y SnapVault

El software SnapVault de NetApp permite el backup a disco de datos empresariales entre sistemas de almacenamiento de NetApp. SnapVault y SnapMirror pueden coexistir en el mismo entorno. Sin embargo, VLSR admite la conmutación por error únicamente de las relaciones de SnapMirror.

El SRA de NetApp admite el `mirror-vault` tipo de política.

SnapVault fue reconstruido desde sus cimientos para ONTAP 8.2. Aunque los antiguos usuarios de Data ONTAP 7-Mode deberían encontrar similitudes, se han mejoras importantes en esta versión de SnapVault. Un avance importante es la capacidad de preservar las eficiencias del almacenamiento en los datos primarios durante las transferencias de SnapVault.

Un cambio de arquitectura importante es que SnapVault en ONTAP 9 se replica a nivel de volumen, frente a en el nivel de qtree, como es el caso de SnapVault en 7-Mode. Esta configuración significa que el origen de una relación de SnapVault debe ser un volumen y dicho volumen debe replicar en su propio volumen en el sistema secundario SnapVault.

En un entorno en el que se utiliza SnapVault, se crean específicamente copias Snapshot con nombre en el sistema de almacenamiento primario. En función de la configuración implementada, las instantáneas con nombre se pueden crear en el sistema primario mediante una programación de SnapVault o mediante una aplicación como NetApp Active IQ Unified Manager. Las copias Snapshot con nombre que se crean en el sistema primario se replican a continuación en el destino de SnapMirror y, desde allí, se almacenan en el destino de SnapVault.

Un volumen de origen se puede crear en una configuración en cascada en la que se replica un volumen a un destino de SnapMirror en el centro de recuperación ante desastres; a partir de ese punto, se realiza la copia en un destino de SnapVault. Un volumen de origen también puede crearse en una relación de dispersión en la que un destino es un destino de SnapMirror y el otro destino es un destino de SnapVault. Sin embargo, el SRA no reconfigura automáticamente la relación de SnapVault para usar el volumen de destino de SnapMirror

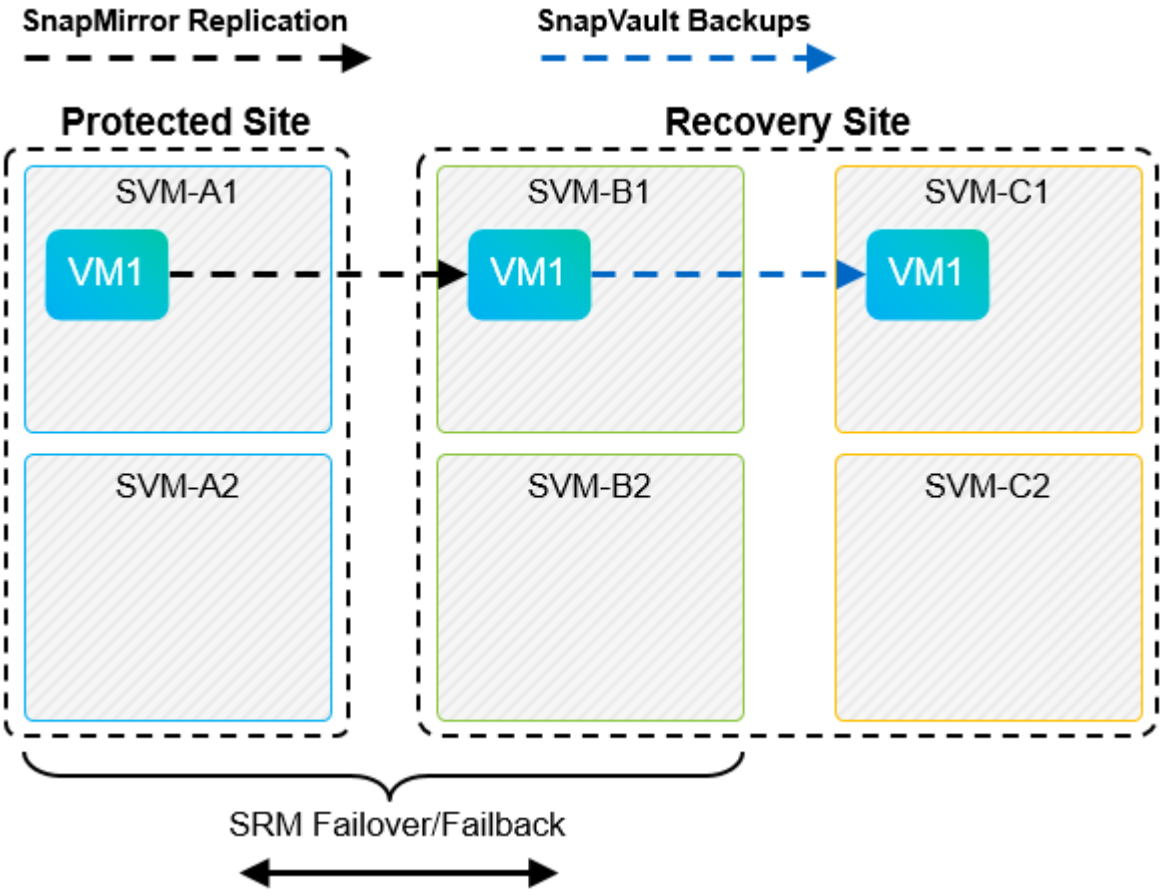
como origen del almacén cuando se produce la conmutación por error del VLSR o la reversión de la replicación.

Para obtener la información más reciente sobre SnapMirror y SnapVault para ONTAP 9, consulte "TR-4015 Guía de mejores prácticas para la configuración de SnapMirror para ONTAP 9."

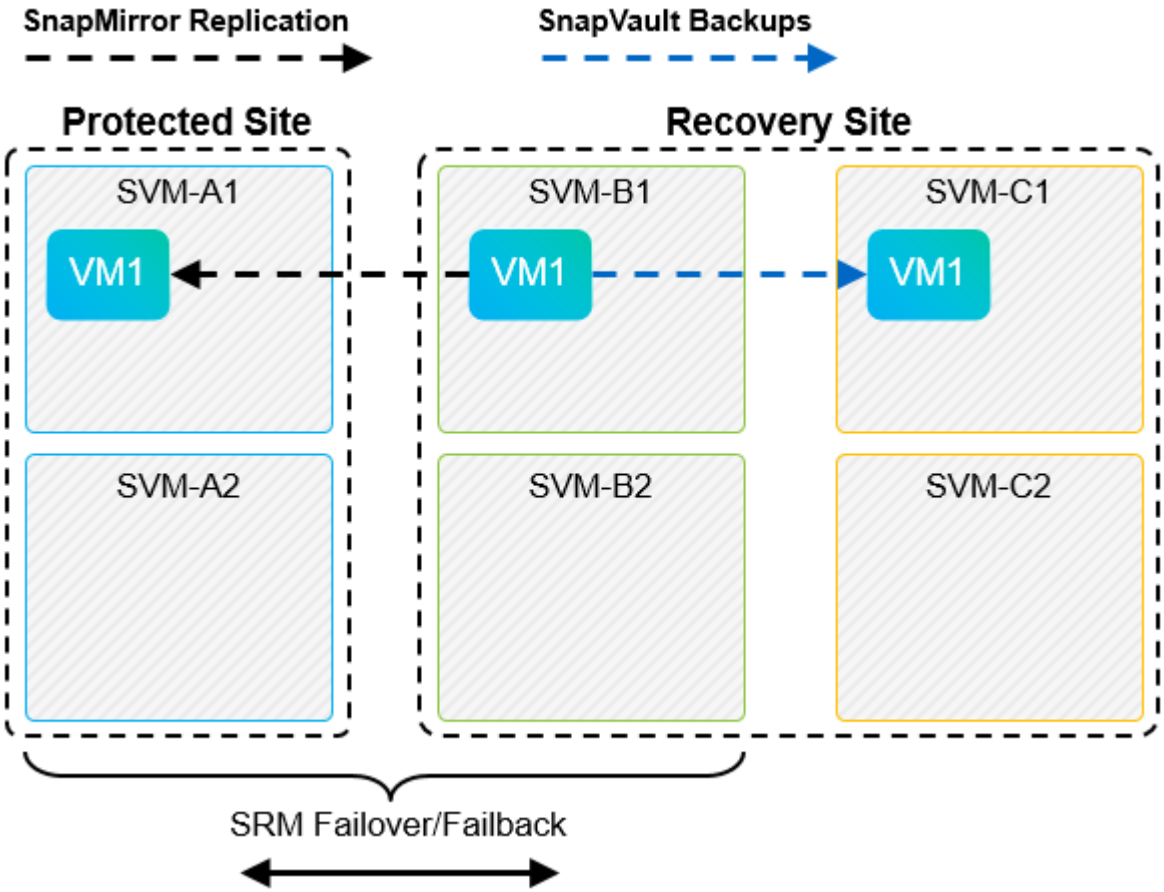
Mejor práctica
Si se emplean SnapVault y VLSR en el mismo entorno, NetApp recomienda utilizar una configuración en cascada de SnapMirror a SnapVault en la que los backups de SnapVault se realizan normalmente desde el destino de SnapMirror en el centro de recuperación ante desastres. En caso de desastre, esta configuración hace que el sitio primario sea inaccesible. Si se mantiene el destino de SnapVault en el centro de recuperación, los backups de SnapVault se pueden volver a configurar tras la conmutación por error para que los backups de SnapVault puedan continuar mientras estén en el centro de recuperación.

En un entorno VMware, cada almacén de datos tiene un identificador único universal (UUID) y cada máquina virtual tiene un ID de objeto gestionado único (MOID). VLSR no mantiene estos ID durante la conmutación por error o la conmutación tras recuperación. Dado que los UUID de almacenes de datos y los MOIDs de máquinas virtuales no se mantienen durante la conmutación por error por parte de VLSR, cualquier aplicación que dependa de estos identificadores se debe volver a configurar tras la conmutación por error de VLSR. Una aplicación de ejemplo es Active IQ Unified Manager de NetApp, que coordina la replicación de SnapVault con el entorno vSphere.

La siguiente figura muestra la configuración en cascada de SnapMirror a SnapVault. Si el destino de SnapVault se encuentra en el centro de recuperación ante desastres o en un sitio terciario que no se ve afectado por una interrupción en el centro principal, es posible volver a configurar el entorno para que los backups continúen tras la conmutación por error.



En la siguiente figura, se muestra la configuración una vez que se ha utilizado VLSR para revertir la replicación de SnapMirror al centro principal. También se ha reconfigurado el entorno para que los backups SnapVault se realicen desde el origen de SnapMirror. Esta configuración es una configuración de dispersión de SnapMirror SnapVault.



Cuando vsrm realiza una conmutación de retorno tras recuperación y una segunda reversión de las relaciones de SnapMirror, los datos de producción vuelven a estar en el sitio principal. Estos datos ahora están protegidos del mismo modo que antes la conmutación al centro de recuperación ante desastres, mediante backups de SnapMirror y SnapVault.

Uso de Qtrees en entornos de Site Recovery Manager

Los qtrees son directorios especiales que permiten aplicar cuotas del sistema de archivos para NAS. ONTAP 9 permite la creación de qtrees y pueden existir qtrees en los volúmenes replicados con SnapMirror. Sin embargo, SnapMirror no permite la replicación de qtrees individuales o a nivel de qtree. Toda la replicación de SnapMirror se realiza únicamente a nivel de volumen. Por este motivo, NetApp no recomienda el uso de qtrees con VLSR.

Entornos FC e iSCSI mixtos

Con los protocolos SAN compatibles (Fibre Channel, FCoE e iSCI), ONTAP 9 ofrece servicios LUN, esto es, la capacidad de crear y asignar LUN a los hosts conectados. Dado que el clúster se compone de varias controladoras, existen varias rutas lógicas que se gestionan mediante I/o multivía con cualquier LUN individual. En los hosts se utiliza ALUA (Asymmetric LUN Access) para que se seleccione la ruta optimizada a cada LUN Si la ruta optimizada a cualquier LUN cambia (por ejemplo, debido a que se mueve el volumen que lo contiene), ONTAP 9 reconoce automáticamente y se ajusta de forma no disruptiva para este cambio. Si la ruta optimizada deja de estar disponible, ONTAP puede cambiar a otra ruta disponible sin interrupciones.

El VLSR de VMware y el SRA de NetApp admiten el uso del protocolo FC en un sitio y el protocolo iSCSI en el otro sitio. Sin embargo, no admite el hecho de haber una combinación de almacenes de datos conectados a FC y almacenes de datos conectados a iSCSI en el mismo host ESXi o en hosts diferentes en el mismo clúster. Esta configuración no es compatible con VLSR porque, durante la conmutación por error de VLSR o la conmutación por error de prueba, VLSR incluye todos los iniciadores de FC e iSCSI de los hosts ESXi que están en la solicitud.

Mejor práctica
El VLSR y el SRA admiten protocolos mixtos de FC e iSCSI entre los sitios protegidos y de recuperación. Sin embargo, cada sitio debe configurarse con un solo protocolo, ya sea FC o iSCSI, y no con ambos protocolos en el mismo sitio. Si existe un requisito de tener configurados tanto los protocolos FC como iSCSI en el mismo sitio, NetApp recomienda que algunos hosts utilicen iSCSI y otros hosts utilicen FC. En este caso, NetApp también recomienda configurar las asignaciones de recursos de VLSR para que las máquinas virtuales se configuren para conmutar al nodo de respaldo en un grupo de hosts u otro.

Solución de problemas de VLSRM/SRM cuando se usa la replicación de vVols

Cuando se utilizan las herramientas de ONTAP 9.13P2, el flujo de trabajo que hay en VLSR y SRM es muy diferente cuando se usa la replicación vVols de lo que se utiliza con el SRA y los almacenes de datos tradicionales. Por ejemplo, no hay ningún concepto de administrador de cabinas. Como tal, `discoverarrays` y `discoverdevices` los comandos nunca se ven.

Para la solución de problemas, resulta beneficioso comprender los nuevos flujos de trabajo, que se enumeran a continuación:

1. QueryReplicationPeer: Descubre los acuerdos de replicación entre dos dominios de fallo.
2. QueryFaultDomain: Detecta la jerarquía de dominios de fallo.
3. QueryReplicationGroup: Detecta los grupos de replicación presentes en los dominios de origen o destino.
4. SyncReplicationGroup: Sincroniza los datos entre el origen y el destino.
5. QueryPointInTimeReplica: Detecta las réplicas de punto en tiempo en un destino.
6. TestFailoverReplicationGroupStart: Inicia la conmutación por error de prueba.
7. TestFailoverReplicationGroupStop: Finaliza la conmutación por error de prueba.
8. PromoteReplicationGroup: Promueve un grupo actualmente en pruebas a la producción.
9. PapreFailoverReplicationGroup: Prepara para una recuperación ante desastres.
10. FailoverReplicationGroup: Ejecuta la recuperación ante desastres.
11. ReverseReplicateGroup: Inicia la replicación inversa.
12. QueryMatchingContainer: Busca contenedores (junto con hosts o grupos de replicación) que puedan satisfacer una solicitud de aprovisionamiento con una directiva determinada.
13. QueryResourceMetadata: Descubre los metadatos de todos los recursos del proveedor VASA, la utilización de recursos puede devolverse como respuesta a la función queryMatchingContainer.

El error más común que se produce al configurar la replicación de vVols es no descubrir las relaciones de SnapMirror. Esto ocurre porque los volúmenes y las relaciones de SnapMirror se crean fuera del alcance de las herramientas de ONTAP. Por lo tanto, una práctica recomendada es asegurarse de que su relación con SnapMirror esté completamente inicializada y de que ha ejecutado una nueva detección en las herramientas

de ONTAP en ambos sitios antes de intentar crear un almacén de datos vVols replicado.

Información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- Herramientas de ONTAP para VMware vSphere 10.x Resources "https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab"
- Herramientas de ONTAP para VMware vSphere 9.x Resources "https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"
- TR-4597: VMware vSphere para ONTAP "https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"
- TR-4400: VMware vSphere Virtual Volumes con ONTAP "https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html"
- TR-4015 Guía de mejores prácticas para la configuración de SnapMirror para ONTAP 9 https://www.netapp.com/media/17229-tr4015.pdf?v=127202175503P
- Documentación de VMware Live Site Recovery "https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html"

Consulte el "Herramienta de matriz de interoperabilidad (IMT)"sitio de soporte de NetApp para confirmar que las versiones exactas del producto y las funciones descritas en este documento son compatibles con su entorno concreto. La cabina IMT de NetApp define los componentes y las versiones del producto que pueden utilizarse para crear configuraciones que sean compatibles con NetApp. Los resultados específicos dependen de la instalación que realice cada cliente de acuerdo con las especificaciones publicadas.

Clúster de almacenamiento vSphere Metro con ONTAP

Clúster de almacenamiento vSphere Metro con ONTAP

El hipervisor vSphere líder del sector de VMware se puede poner en marcha como un clúster ampliado conocido como vSphere Metro Storage Cluster (VMSC).

Las soluciones VMSC son compatibles con NetApp® MetroCluster™ y SnapMirror Active Sync (anteriormente conocido como continuidad empresarial de SnapMirror o SMBC) y proporcionan continuidad empresarial avanzada si uno o más dominios de fallo sufren una interrupción total. La resistencia a los diferentes modos de fallo depende de las opciones de configuración que elija.

Esta documentación sustituye a los informes técnicos publicados anteriormente *TR-4128: VSphere en NetApp MetroCluster*

Soluciones de disponibilidad continua para entornos vSphere

La arquitectura ONTAP es una plataforma de almacenamiento flexible y escalable que proporciona servicios SAN (FCP, iSCSI y NVMe-oF) y NAS (NFS v3 y v4,1) para almacenes de datos. Los sistemas de almacenamiento NetApp AFF, ASA y FAS utilizan el sistema operativo ONTAP para ofrecer protocolos adicionales para acceso al almacenamiento invitado, como S3 y SMB/CIFS.

NetApp MetroCluster utiliza la función de alta disponibilidad (conmutación por error de controladora o director

financiero) de NetApp para proteger frente a fallos de controladora. También incluye tecnología SyncMirror local, recuperación tras fallos en clúster en caso de desastre (conmutación por error en cluster en caso de desastre o CFOD), redundancia de hardware y separación geográfica para alcanzar altos niveles de disponibilidad. SyncMirror refleja de forma síncrona los datos en las dos mitades de la configuración de MetroCluster mediante la escritura de los datos en dos plexes: El plex local (en la bandeja local) que sirve los datos de forma activa y el plex remoto (en la bandeja remota) normalmente no ofrece datos. La redundancia de hardware se pone en marcha para todos los componentes de MetroCluster, como las controladoras, el almacenamiento, los cables, los switches (utilizados con Fabric MetroCluster) y los adaptadores.

La sincronización activa de NetApp SnapMirror, disponible en sistemas que no sean MetroCluster y en sistemas ASA R2, ofrece protección granular en almacenes de datos con protocolos FCP e iSCSI SAN. Le permite proteger todo el VMSC o proteger de forma selectiva las cargas de trabajo de alta prioridad. Ofrece acceso activo-activo tanto a sitios locales como remotos, a diferencia de NetApp MetroCluster, que es una solución activa-en espera. A partir de ONTAP 9.15.1, la sincronización activa de SnapMirror admite una funcionalidad activo-activo simétrica, lo que permite operaciones de I/O de lectura y escritura desde ambas copias de una LUN protegida con replicación síncrona bidireccional, lo que permite que ambas copias LUN sirvan operaciones de I/O localmente. Antes de ONTAP 9.15.1, la sincronización activa de SnapMirror solo admite configuraciones activo-activo asimétricas, en las que los datos del sitio secundario están proxy a la copia principal de una LUN.

Para crear un clúster HA/DRS de VMware en dos sitios, los hosts ESXi se usan y gestionan mediante una instancia de vCenter Server Appliance (VCSA). Las redes de gestión de vSphere, vMotion® y máquinas virtuales están conectadas a través de una red redundante entre los dos sitios. El servidor vCenter que gestiona el clúster HA/DRS puede conectarse a los hosts ESXi en ambos sitios y se debe configurar mediante vCenter HA.

Consulte "¿Cómo se crean y configuran clústeres en vSphere Client" Para configurar una alta disponibilidad de vCenter.

También debe consultar "Prácticas recomendadas para VMware vSphere Metro Storage Cluster" .

¿Qué es vSphere Metro Storage Cluster?

VSphere Metro Storage Cluster (VMSC) es una configuración certificada que protege las máquinas virtuales (VM) y los contenedores frente a fallos. Esto se logra mediante el uso de conceptos de almacenamiento extendidos junto con clústeres de hosts ESXi, que se distribuyen en diferentes dominios de fallo, como bastidores, edificios, campus o incluso ciudades. Las tecnologías de almacenamiento de sincronización activa de NetApp MetroCluster y SnapMirror se usan para proporcionar una protección de un objetivo de punto de recuperación cero (RPO=0) en los clústeres de hosts. La configuración de VMSC está diseñada para garantizar que los datos están siempre disponibles incluso si falla todo un «sitio» físico o lógico. Un dispositivo de almacenamiento que forme parte de la configuración de VMSC debe estar certificado tras someterse a un proceso de certificación VMSC exitoso. Todos los dispositivos de almacenamiento admitidos se pueden encontrar en el "Guía de compatibilidad de almacenamiento de VMware".

Si desea obtener más información sobre las directrices de diseño para vSphere Metro Storage Cluster, consulte la siguiente documentación:

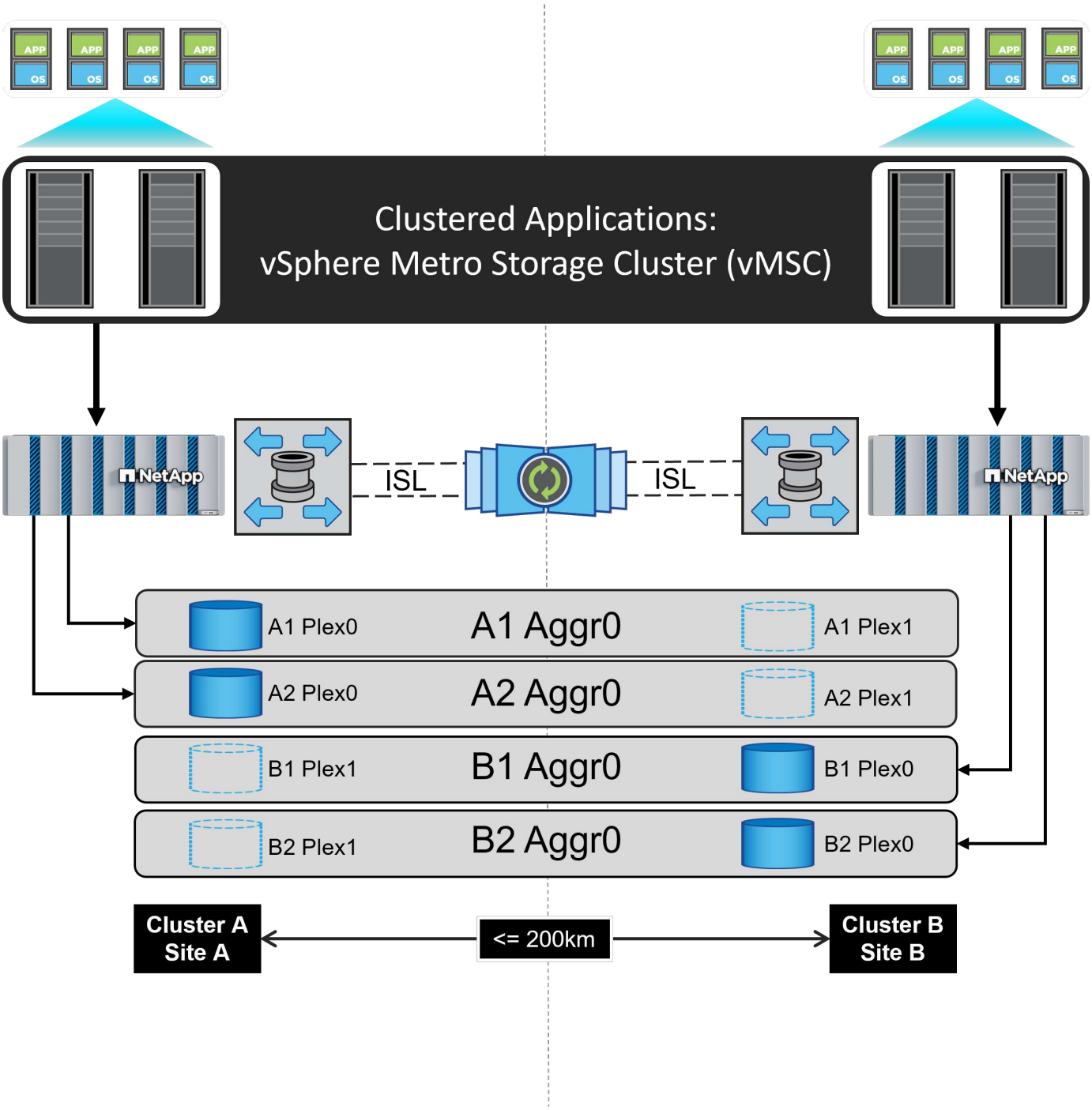
- "Compatibilidad de VMware vSphere con NetApp MetroCluster"
- "Compatibilidad de VMware vSphere con Continuidad del negocio de SnapMirror de NetApp" (Ahora conocido como SnapMirror active sync)

NetApp MetroCluster se puede poner en marcha en dos configuraciones diferentes para usarlas con vSphere:

- Stretch MetroCluster

- Fabric MetroCluster

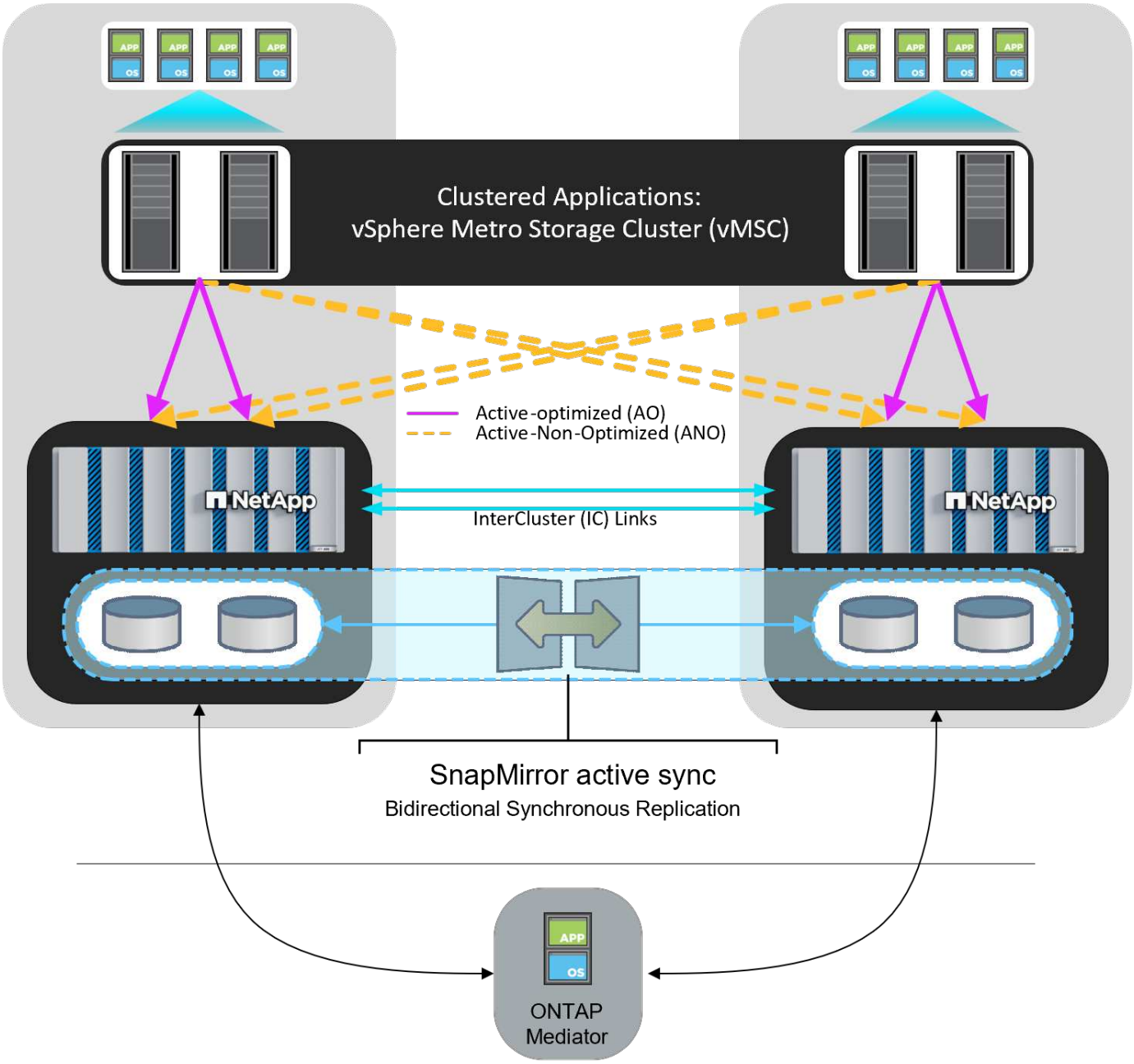
A continuación se muestra un diagrama topológico de alto nivel de MetroCluster de ampliación.



Consulte "Documentación de MetroCluster" Para obtener información específica sobre diseño e implementación para MetroCluster.

SnapMirror Active Sync también se puede poner en marcha de dos formas distintas.

- Asimétrico
- Sincronización activa simétrica (ONTAP 9.15.1)



Consulte "Documentos de NetApp" para obtener información específica sobre el diseño y la puesta en marcha de la sincronización activa de SnapMirror.

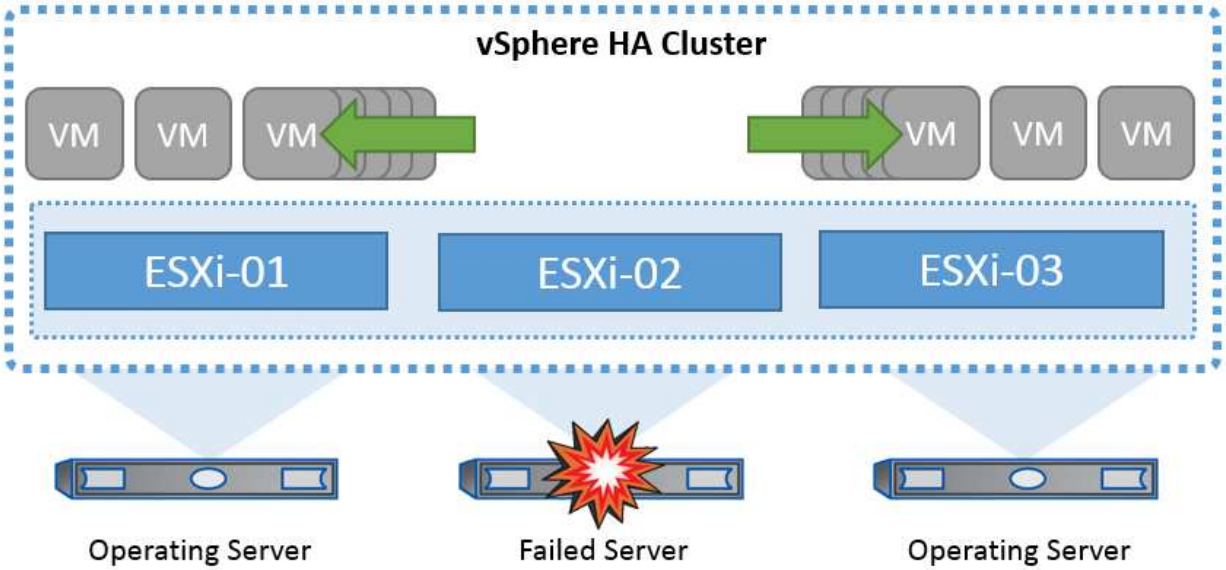
Descripción general de la solución de VMware vSphere

VCenter Server Appliance (VCSA) es el potente sistema de gestión centralizada y un panel único para vSphere que permiten a los administradores operar clústeres ESXi de forma eficiente. Facilita funciones clave como el aprovisionamiento de máquinas virtuales, la operación vMotion, alta disponibilidad, planificador de recursos distribuidos (DRS), Tanzu Kubernetes Grid, etc. Es un componente esencial en los entornos cloud de VMware y debe diseñarse teniendo en cuenta la disponibilidad del servicio.

Alta disponibilidad de vSphere

La tecnología de clúster de VMware agrupa los servidores ESXi en pools de recursos compartidos para máquinas virtuales y proporciona vSphere High Availability (HA). VSphere HA proporciona alta disponibilidad fácil de usar para aplicaciones que se ejecutan en máquinas virtuales. Cuando se habilita la función HA en el clúster, cada servidor ESXi mantiene la comunicación con otros hosts de modo que si algún host ESXi deja de responder o aísla, el clúster de alta disponibilidad puede negociar la recuperación de las máquinas virtuales que se estaban ejecutando en ese host ESXi entre los hosts supervivientes del clúster. En caso de fallo del sistema operativo invitado, la alta disponibilidad de vSphere puede reiniciar la máquina virtual afectada en el mismo servidor físico. VSphere HA permite reducir los tiempos de inactividad planificados, evitar tiempos de inactividad no planificados y recuperarse rápidamente de las interrupciones.

Un clúster de alta disponibilidad de vSphere que recupera las máquinas virtuales del servidor con errores.



Es importante entender que VMware vSphere no tiene conocimientos de la sincronización activa de NetApp MetroCluster o SnapMirror y ve todos los hosts ESXi del clúster de vSphere como hosts elegibles para las operaciones en clúster de alta disponibilidad en función de las configuraciones de afinidad de hosts y grupos de máquinas virtuales.

Detección de fallo de host

En cuanto se crea el clúster HA, todos los hosts del clúster participan en sus elecciones y uno de los hosts se convierte en un maestro. Cada esclavo realiza latidos de red al maestro y, a su vez, el maestro realiza latidos de red en todos los hosts esclavos. El host maestro de un clúster de alta disponibilidad de vSphere es responsable de detectar el fallo de hosts esclavos.

Según el tipo de error detectado, es posible que las máquinas virtuales que se ejecutan en los hosts deban conmutar al nodo de respaldo.

En un clúster de alta disponibilidad de vSphere se detectan tres tipos de fallos de host:

- Fallo: Un host deja de funcionar.
- Aislamiento: Un host se convierte en una red aislada.
- Partición: Un host pierde la conectividad de red con el host maestro.

El host maestro supervisa los hosts esclavos del cluster. Esta comunicación se realiza a través del intercambio

de latidos de la red cada segundo. Cuando el host maestro deja de recibir estos latidos de un host esclavo, comprueba si hay vida activa del host antes de declarar que el host ha fallado. La comprobación de vida que realiza el host maestro es determinar si el host esclavo está intercambiando latidos con uno de los almacenes de datos. Además, el host maestro comprueba si el host responde a los ping ICMP enviados a sus direcciones IP de gestión para detectar si simplemente está aislado de su nodo maestro o completamente aislado de la red. Para ello, haga ping en la puerta de enlace predeterminada. Se pueden especificar manualmente una o varias direcciones de aislamiento para mejorar la fiabilidad de la validación de aislamiento.

NetApp recomienda especificar un mínimo de dos direcciones de aislamiento adicionales, y que cada una de estas direcciones sea local de sitio. Esto mejorará la fiabilidad de la validación del aislamiento.

Respuesta de aislamiento del host

Isolation Response es una configuración de vSphere HA que determina la acción que se activa en máquinas virtuales cuando un host de un clúster de vSphere HA pierde sus conexiones de red de gestión, pero continúa ejecutándose. Hay tres opciones para esta configuración: «Desactivado», «Apagar y reiniciar equipos virtuales» y «Apagar y reiniciar equipos virtuales».

El apagado es mejor que el apagado, que no vacía los cambios más recientes en el disco o las transacciones de confirmación. Si los equipos virtuales no se apagan en 300 segundos, se apagan. Para cambiar el tiempo de espera, utilice la opción avanzada das.isolationshutdowntimeout.

Antes de que HA inicie la respuesta de aislamiento, primero comprueba si el agente maestro HA de vSphere posee el almacén de datos que contiene los archivos de configuración de la máquina virtual. Si no es así, el host no activará la respuesta de aislamiento, porque no hay ningún maestro para reiniciar las máquinas virtuales. El host comprobará periódicamente el estado del almacén de datos para determinar si un agente de alta disponibilidad de vSphere que posee el rol maestro.

NetApp recomienda establecer la respuesta de aislamiento del host en Desactivada.

Se puede producir una condición de cerebro dividido si un host se aísla o particiona desde el host maestro HA de vSphere y el maestro no puede comunicarse a través de los almacenes de datos de latido o mediante ping. El maestro declara que el host aislado está muerto y reinicia los equipos virtuales en otros hosts del cluster. Ahora existe una condición de cerebro dividido porque hay dos instancias de la máquina virtual en ejecución, solo una de las cuales puede leer o escribir los discos virtuales. Ahora se pueden evitar las condiciones del cerebro dividido configurando VM Component Protection (VMCP).

Protección de componentes de máquina virtual (VMCP)

Una de las mejoras de funciones de vSphere 6, relevante para la alta disponibilidad, es VMCP. VMCP proporciona protección mejorada contra todas las condiciones de pérdida permanente de dispositivos (APD) y de pérdida permanente de dispositivos (PDL) para bloques (FC, iSCSI, FCoE) y almacenamiento de archivos (NFS).

Pérdida permanente de dispositivo (PDL)

PDL es una condición que ocurre cuando un dispositivo de almacenamiento falla de forma permanente o se elimina de forma administrativa y no se espera que regrese. La cabina de almacenamiento NetApp emite un código de detección SCSI a ESXi que declara la pérdida permanente del dispositivo. En la sección Condiciones de fallo y Respuesta de VM de vSphere HA, puede configurar cuál debe ser la respuesta después de detectar una condición PDL.

NetApp recomienda establecer «Respuesta para el almacén de datos con PDL» en «**Apagar y reiniciar equipos virtuales**». Cuando se detecta esta condición, una máquina virtual se reinicia instantáneamente en un host en buen estado dentro del clúster de alta disponibilidad de vSphere.

Todas las rutas hacia abajo (APD)

APD es una condición que se produce cuando el host vuelve inaccesible a un dispositivo de almacenamiento y no hay rutas disponibles a la cabina. ESXi considera que esto es un problema temporal con el dispositivo y espera que vuelva a estar disponible.

Cuando se detecta una condición de APD, se inicia un temporizador. Después de 140 segundos, la condición APD se declara oficialmente, y el dispositivo se marca como APD Time Out. Una vez transcurridos los 140 segundos, HA comenzará a contar el número de minutos especificado en el APD de retraso para failover de VM. Cuando transcurra el tiempo especificado, HA reiniciará los equipos virtuales afectados. Puede configurar VMCP para que responda de manera diferente si lo desea (Desactivado, Incidir eventos o Apagar y reiniciar VM).

- NetApp recomienda configurar la respuesta para el almacén de datos con APD en «**Apagar y reiniciar VM (conservador)**».
- Conservative hace referencia a la probabilidad de que la alta disponibilidad pueda reiniciar equipos virtuales. Cuando se establece en Conservador, HA solo reiniciará la VM que se ve afectada por el APD si sabe que otro host puede reiniciarla. En caso de agresividad, HA intentará reiniciar la máquina virtual incluso si no conoce el estado de los otros hosts. Esto puede provocar que las máquinas virtuales no se reinicien si no hay ningún host con acceso al almacén de datos en el que se encuentra.
- Si se resuelve el estado de APD y se restaura el acceso al almacenamiento antes de que haya pasado el tiempo de espera, HA no reiniciará innecesariamente la máquina virtual a menos que lo configure explícitamente para hacerlo. Si se desea una respuesta, incluso cuando el entorno se ha recuperado de la condición APD, la respuesta para la recuperación APD después del tiempo de espera APD debe configurarse para restablecer las máquinas virtuales.
- NetApp recomienda configurar la respuesta para la recuperación de APD después del tiempo de espera de APD en Desactivado.

Implementación de VMware DRS para NetApp SnapMirror Active Sync

VMware DRS es una función que agrega los recursos de host en un clúster y se usa principalmente para equilibrar cargas dentro de un clúster de una infraestructura virtual. VMware DRS calcula principalmente los recursos de la CPU y la memoria para realizar el equilibrio de carga en un clúster. Como vSphere no es consciente de la agrupación en cluster ampliada, considera todos los hosts en ambos sitios al equilibrar la carga.

Implementación de VMware DRS para NetApp MetroCluster

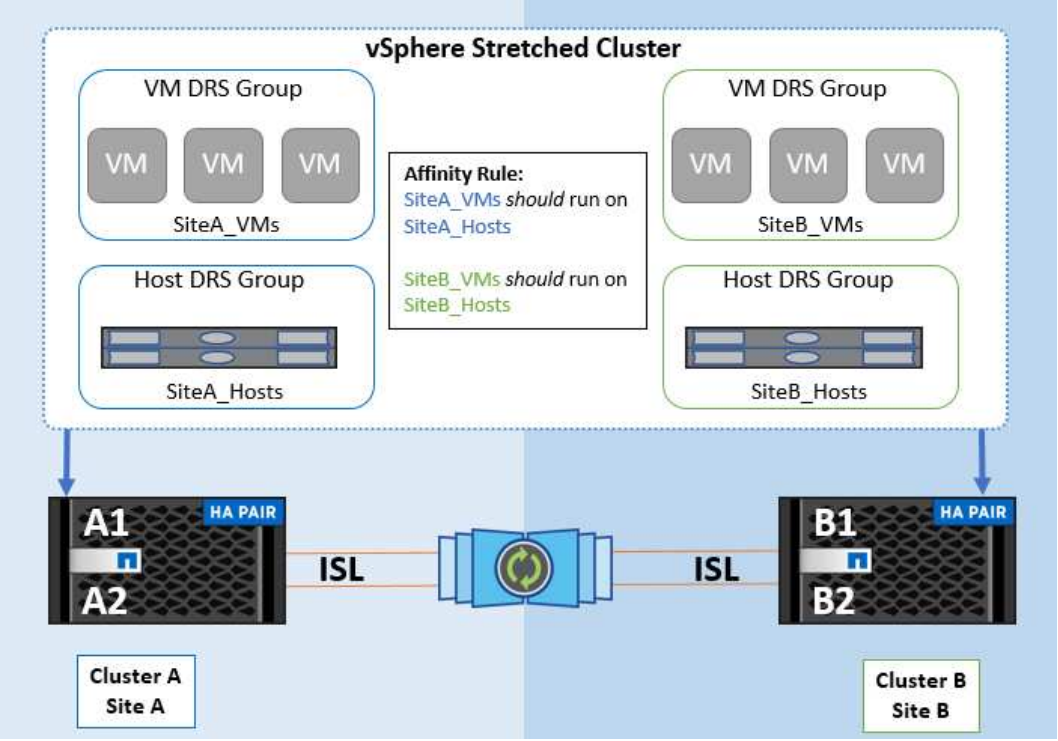
```
 To avoid cross-site traffic, NetApp recommends configuring DRS affinity
rules to manage a logical separation of VMs. This will ensure that unless
there is a complete site failure, HA and DRS will only use local hosts.
Si crea una regla de afinidad de DRS para su clúster, puede especificar
cómo aplica vSphere esa regla durante una conmutación al respaldo de una
máquina virtual.
```

Hay dos tipos de reglas que se pueden especificar el comportamiento de conmutación al nodo de respaldo de alta disponibilidad de vSphere:

- Las reglas de anti-afinidad de equipos virtuales obligan a los equipos virtuales especificados a permanecer separados durante las acciones de recuperación tras fallos.
- Las reglas de afinidad de host de VM colocan las máquinas virtuales especificadas en un host particular o un miembro de un grupo definido de hosts durante las acciones de conmutación por error.

Mediante el uso de reglas de afinidad de host de VM en VMware DRS, se puede tener una separación lógica entre el sitio A y el sitio B, de modo que la VM se ejecute en el host en el mismo sitio que la cabina que está configurada como la controladora de lectura/escritura primaria para un almacén de datos determinado. Además, las reglas de afinidad de host de VM permiten que las máquinas virtuales permanezcan locales en el almacenamiento, lo que, a su vez, verifica la conexión a la máquina virtual en caso de fallos de red entre los sitios.

A continuación se muestra un ejemplo de los grupos de hosts y las reglas de afinidad de las máquinas virtuales.



Best Practice

NetApp recomienda implementar reglas de «debería» en lugar de reglas de «obligación» porque vSphere HA las infringe en caso de fallo. El uso de reglas «imprescindibles» podría provocar interrupciones del servicio.

La disponibilidad de los servicios debe prevalecer siempre sobre el rendimiento. En el caso en el que falla un centro de datos completo, las reglas “imprescindibles” deben elegir hosts del grupo de afinidad de host de VM y, cuando el centro de datos no esté disponible, las máquinas virtuales no se reiniciarán.

Implementación de VMware Storage DRS con NetApp MetroCluster

La función VMware Storage DRS permite agregar almacenes de datos en una sola unidad y equilibra los discos de máquina virtual cuando se superan los umbrales de control de I/O de almacenamiento (SIOC).

El control de la I/O de almacenamiento se habilita de forma predeterminada en los clústeres DRS habilitados para Storage DRS. El control de las operaciones de I/O de almacenamiento permite a un administrador controlar la cantidad de I/O de almacenamiento que se asigna a máquinas virtuales durante periodos de congestión de I/O, lo que permite que las máquinas virtuales más importantes tengan preferencia por máquinas virtuales menos importantes para la asignación de recursos de E/S.

Storage DRS utiliza Storage vMotion para migrar los equipos virtuales a diferentes almacenes de datos dentro de un clúster de almacén de datos. En un entorno NetApp MetroCluster, una migración de máquinas virtuales debe controlarse dentro de los almacenes de datos de ese sitio. Por ejemplo, en condiciones ideales, la máquina virtual A, que se ejecuta en un host en el sitio A, debería migrar dentro de los almacenes de datos de la SVM en el sitio A. Si no lo hace, la máquina virtual continuará funcionando pero con un rendimiento degradado, ya que la lectura/escritura del disco virtual será desde la ubicación B a través de enlaces entre sitios.

*Cuando se utiliza el almacenamiento ONTAP, se recomienda desactivar el DRS de Almacenamiento.

- Por lo general, los DRS de almacenamiento no son necesarios ni se recomiendan para su uso con sistemas de almacenamiento de ONTAP.
- ONTAP proporciona sus propias funciones de eficiencia del almacenamiento, como la deduplicación, la compresión y la compactación, que pueden verse afectadas por Storage DRS.
- Si utiliza copias Snapshot de ONTAP, Storage vMotion dejaría detrás de la copia del equipo virtual en la copia Snapshot, lo que puede aumentar el uso del almacenamiento y puede afectar a las aplicaciones de backup como NetApp SnapCenter, que registran las máquinas virtuales y sus copias Snapshot de ONTAP.

Directrices de implementación y diseño de VMSC

Este documento describe las guías de diseño e implementación para VMSC con sistemas de almacenamiento ONTAP.

Configuración de almacenamiento de NetApp

Las instrucciones de configuración para NetApp MetroCluster están disponibles en "Documentación de MetroCluster". Las instrucciones para SnapMirror Active Sync (SMAS) también están disponibles en "Información general sobre la continuidad del negocio de SnapMirror".

Después de configurar MetroCluster, administrarlo es como administrar un entorno ONTAP tradicional. Puede configurar máquinas virtuales de almacenamiento (SVM) con diferentes herramientas, como la interfaz de línea de comandos (CLI), System Manager o Ansible. Una vez que se han configurado las SVM, cree interfaces lógicas (LIF), volúmenes y números de unidad lógica (LUN) en el clúster que se utilizarán para operaciones normales. Estos objetos se replicarán automáticamente en el otro clúster mediante la red de

conexión de clústeres.

Si no utiliza MetroCluster o tiene sistemas ONTAP que no son compatibles con MetroCluster, como los sistemas ASA R2, puede usar la sincronización activa de SnapMirror que proporciona protección granular de almacenes de datos y acceso activo-activo en varios clústeres de ONTAP de diferentes dominios de fallo. SMAS utiliza grupos de coherencia (CG) para garantizar la coherencia en orden de escritura entre uno o varios almacenes de datos y puede crear varios CG en función de los requisitos de su aplicación y de su almacén de datos. Los grupos de coherencia son especialmente útiles para aplicaciones que requieren sincronización de datos entre varios almacenes de datos. Por ejemplo, LVM invitados distribuidos entre almacenes de datos. SMAS también admite asignaciones de dispositivos sin procesar (RDM) y almacenamiento conectado mediante invitado con iniciadores iSCSI en los invitados. Puede obtener más información sobre los grupos de consistencia en "Información general sobre los grupos de consistencia".

Hay alguna diferencia en la gestión de una configuración VMSC con sincronización activa de SnapMirror en comparación con una MetroCluster. En primer lugar, SMAS es una configuración solo SAN, no se puede proteger ningún almacén de datos NFS con sincronización activa de SnapMirror. Segundo, debe asignar ambas copias de las LUN a los hosts ESXi para que accedan a los almacenes de datos replicados en ambos dominios de fallo. Tercero, debe crear uno o varios grupos de coherencia para los almacenes de datos que desea proteger con la sincronización activa de SnapMirror. Por último, debe crear una política de SnapMirror para los grupos de consistencia que creó. Todo esto puede realizarse fácilmente usando el asistente para proteger clúster del complemento vCenter de herramientas de ONTAP, o bien manualmente usando la CLI de ONTAP o System Manager.

Uso del complemento de herramientas de ONTAP para vCenter para SnapMirror

El complemento para vCenter para herramientas de ONTAP proporciona un método sencillo e intuitivo de configurar la sincronización activa de SnapMirror para VMSC. Es posible usar el complemento de herramientas de ONTAP para crear y gestionar relaciones de sincronización activa de SnapMirror entre dos clústeres de ONTAP. Este plugin proporciona una interfaz fácil de usar para establecer y gestionar estas relaciones de manera eficiente. Puede obtener más información sobre el complemento para vCenter de herramientas de ONTAP en "Herramientas de ONTAP para VMware vSphere", o ir directamente a "Proteja mediante la protección del clúster de hosts".

Configuración de VMware vSphere

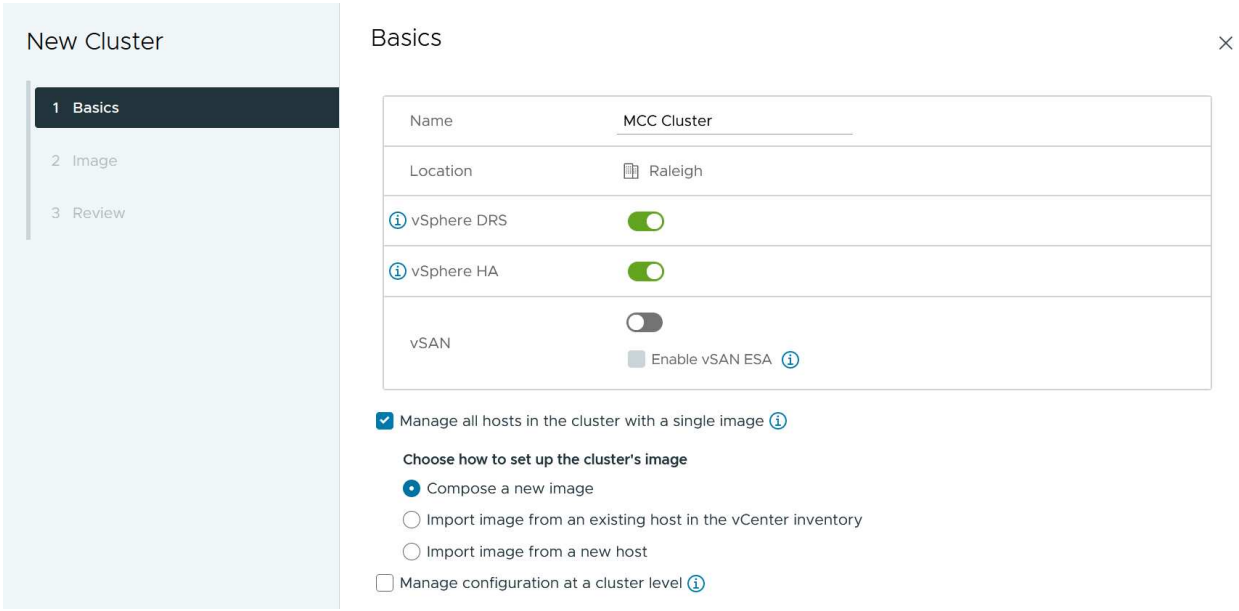
Cree un clúster de vSphere HA

La creación de un clúster de vSphere HA es un proceso de varios pasos que se documenta completamente en "Cómo se crean y configuran clústeres en vSphere Client en docs.vmware.com". En resumen, primero debe crear un clúster vacío y, después, utilizando vCenter, debe añadir hosts y especificar la alta disponibilidad de vSphere y otros ajustes del clúster.

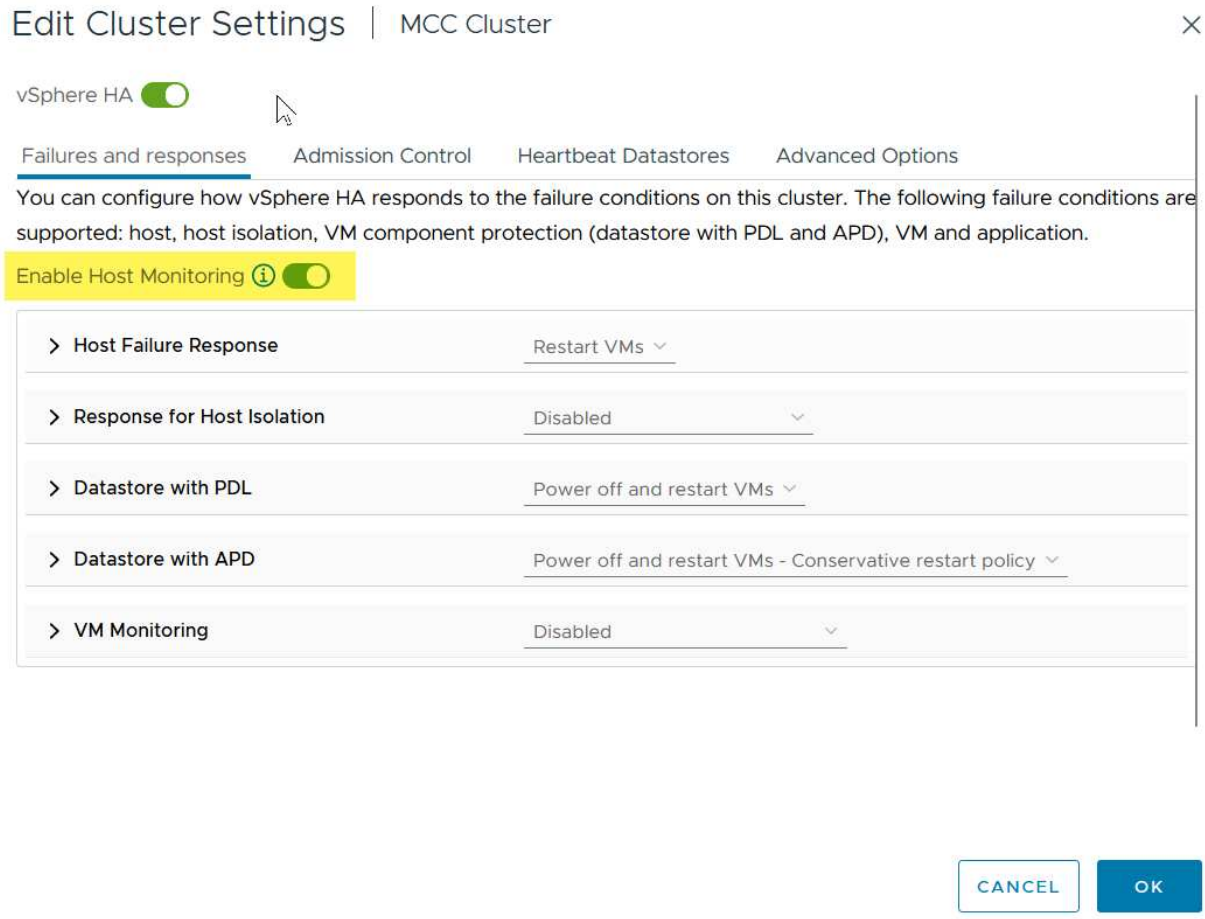
> Nada en este documento sustituye "Prácticas recomendadas para VMware vSphere Metro Storage Cluster". Este contenido se ofrece para facilitar la referencia y no sustituye la documentación oficial de VMware.

Para configurar un clúster de alta disponibilidad, realice los siguientes pasos:

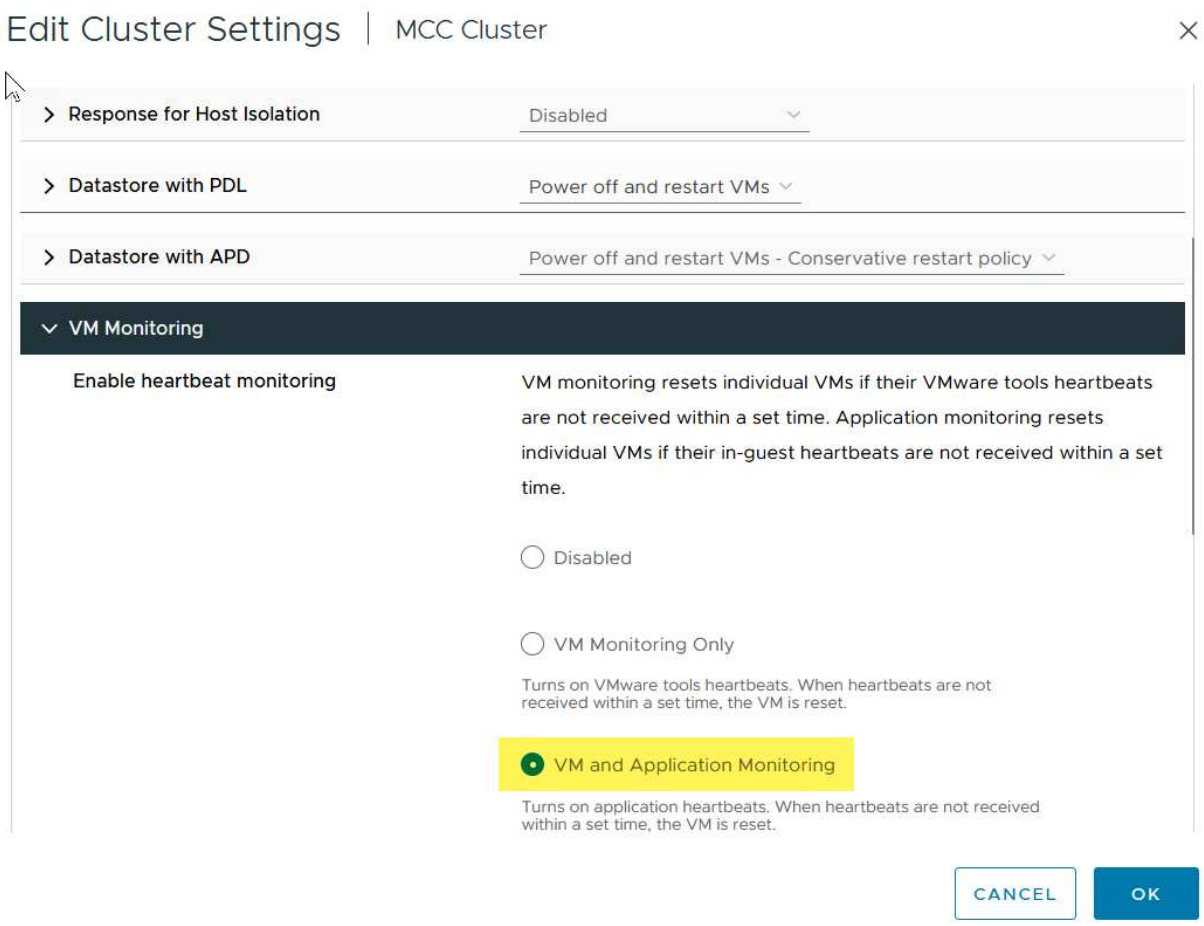
1. Conéctese a la interfaz de usuario de vCenter.
2. En Hosts and Clusters, vaya al centro de datos donde desea crear su clúster de alta disponibilidad.
3. Haga clic con el botón derecho en el objeto del centro de datos y seleccione New Cluster. En los conceptos básicos, asegúrese de haber habilitado vSphere DRS y vSphere HA. Complete el asistente.



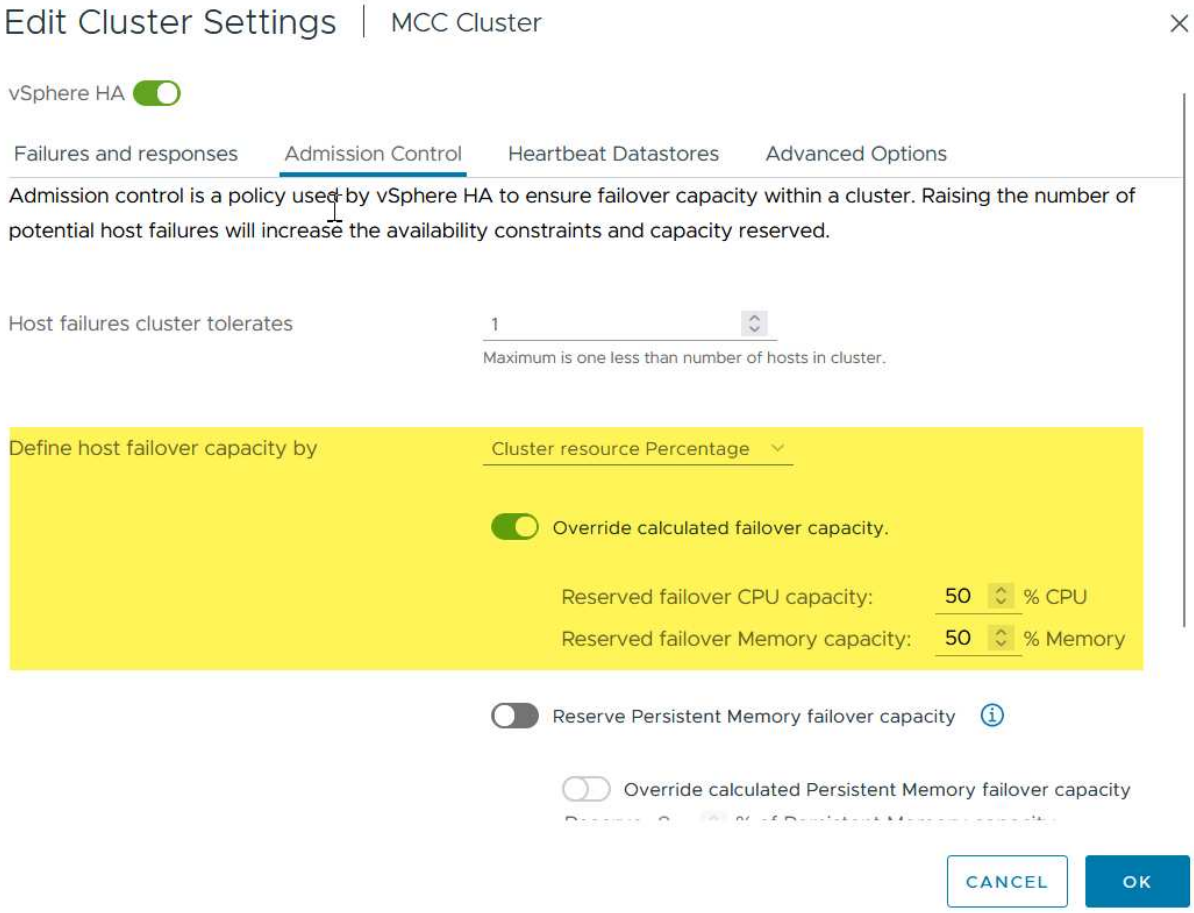
1. Seleccione el clúster y vaya a la pestaña Configure. Seleccione vSphere HA y haga clic en Edit.
2. En Supervisión de host, seleccione la opción Habilitar supervisión de host.



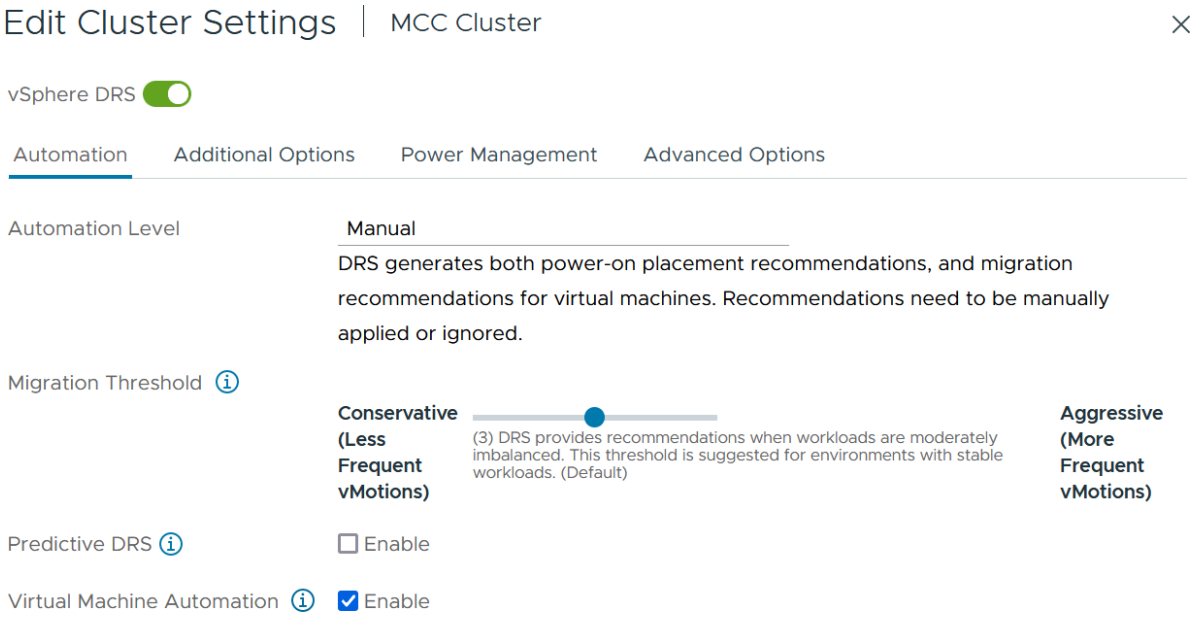
1. Mientras todavía está en la pestaña Fallos y Respuestas, en VM Monitoring, seleccione la opción VM Monitoring Only o VM and Application Monitoring.



1. En Control de admisión, establezca la opción de control de admisión de HA en Reserva de recursos de cluster; utilice 50% CPU/MEM.



1. Haga clic en OK.
2. Seleccione DRS y haga clic en EDIT.
3. Establezca el nivel de automatización en manual a menos que las aplicaciones lo requieran.



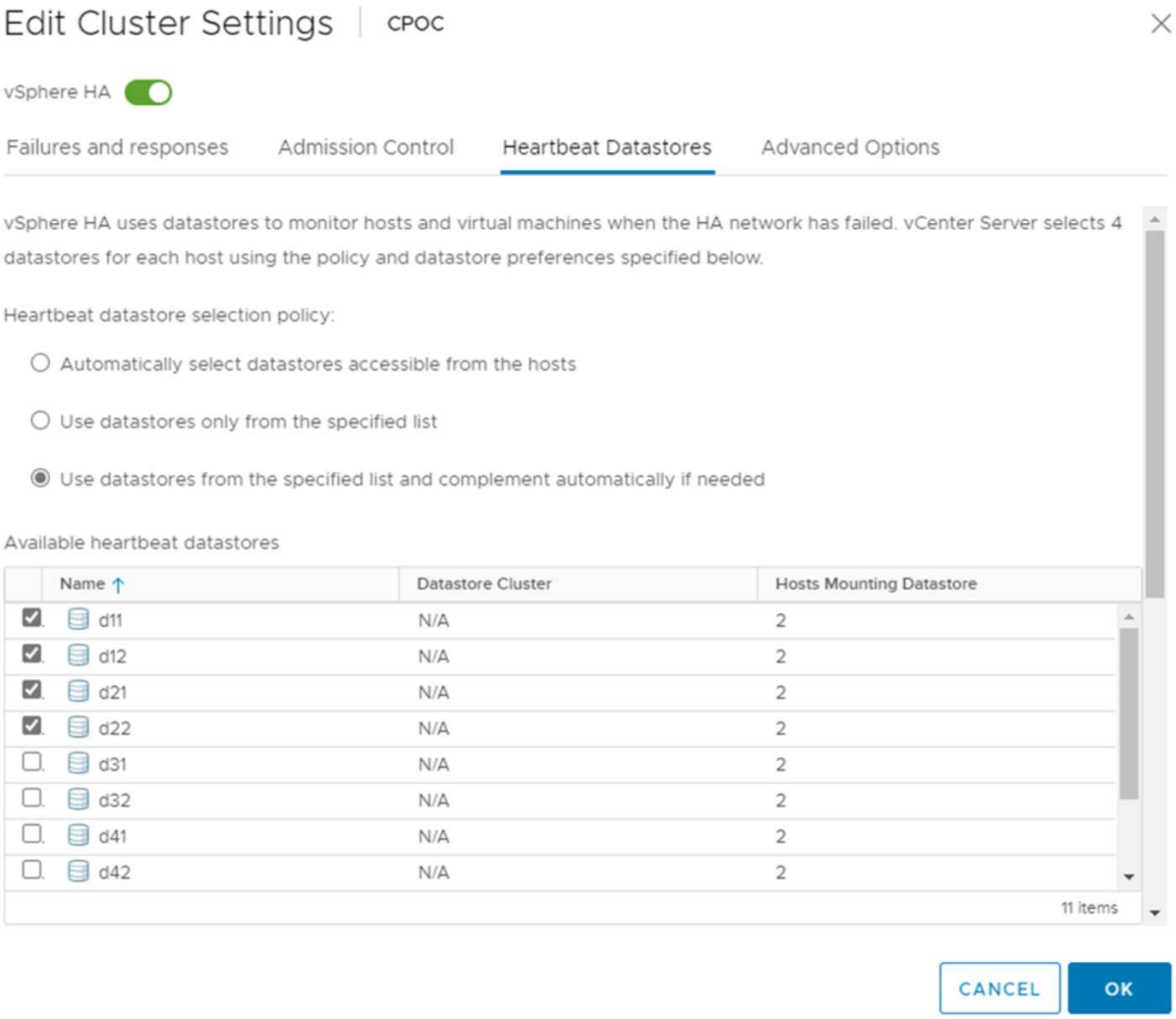
1. Habilite VM Component Protection, consulte "docs.vmware.com".
2. Se recomiendan las siguientes configuraciones adicionales de alta disponibilidad de vSphere para VMSC con MetroCluster:

Fallo	Respuesta
Error del host	Reiniciar las máquinas virtuales
Aislamiento de hosts	Deshabilitado
Almacén de datos con pérdida permanente de dispositivo (PDL)	Apagar y reiniciar los equipos virtuales
Almacén de datos con todas las rutas inactivas (APD)	Apagar y reiniciar los equipos virtuales
El huésped no es molesto	Restablecer las máquinas virtuales
Política de reinicio de máquinas virtuales	Determinado por la importancia del equipo virtual
Respuesta para el aislamiento del host	Apagar y reiniciar equipos virtuales
Respuesta para datastore con PDL	Apagar y reiniciar los equipos virtuales
Respuesta del almacén de datos con APD	Apagar y reiniciar equipos virtuales (conservador)
Demora en recuperación tras fallos de equipos virtuales para APD	3 minutos
Respuesta para la recuperación de APD con tiempo de espera APD	Deshabilitado
Supervisión de la sensibilidad de los equipos virtuales	Preajuste ALTO

Configurar almacenes de datos para Heartbeat

La alta disponibilidad de vSphere utiliza almacenes de datos para supervisar hosts y máquinas virtuales cuando se produce un error en la red de gestión. Es posible configurar la forma en la que vCenter selecciona los almacenes de datos de latido. Para configurar los almacenes de datos para latir, lleve a cabo los siguientes pasos:

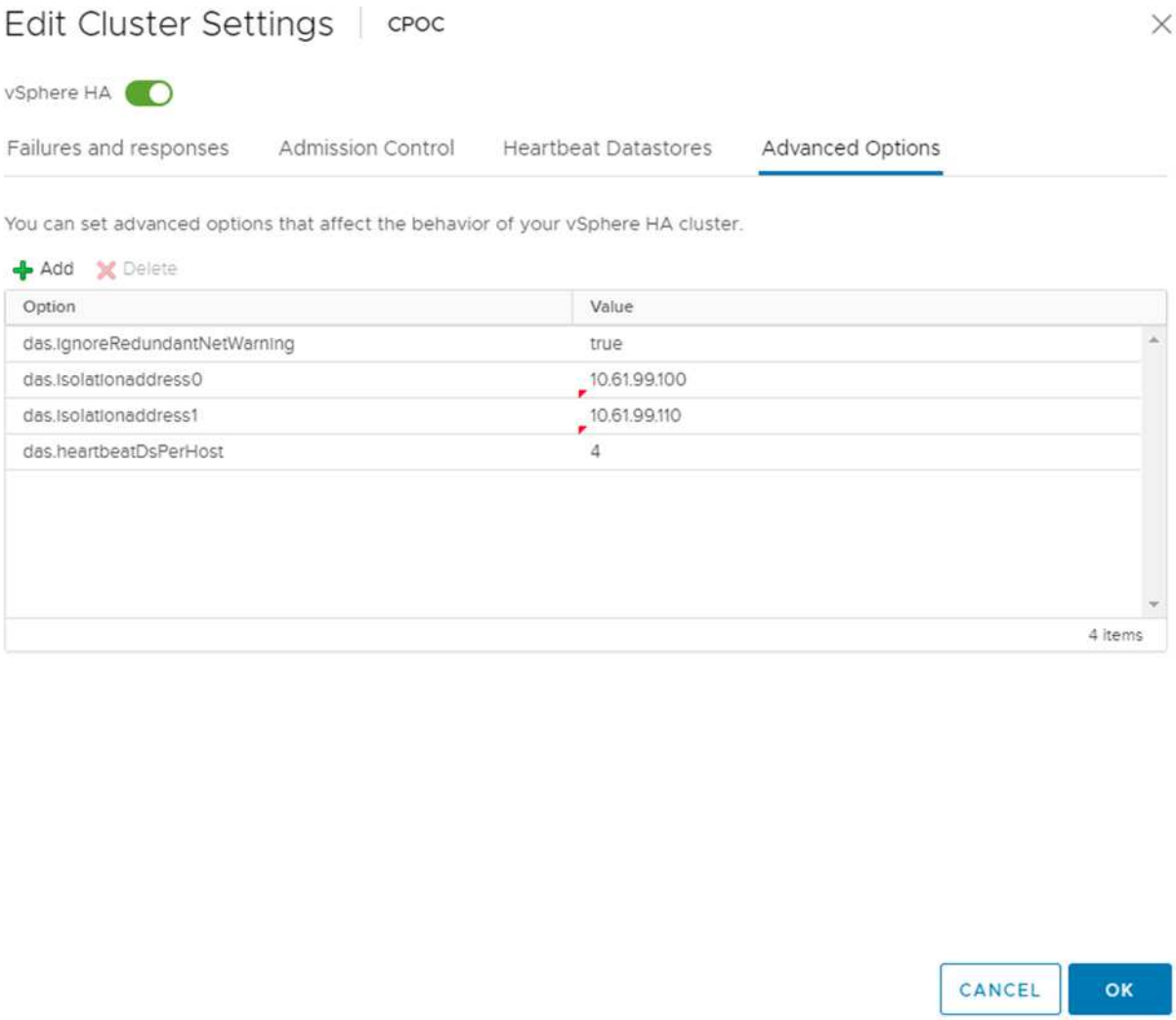
1. En la sección Datastore Heartbeat, seleccione Use datastores from the Specified List y complemente automáticamente si es necesario.
2. Seleccione los almacenes de datos que desee utilizar vCenter en ambos sitios y pulse OK.



Configurar opciones avanzadas

Los eventos de aislamiento se producen cuando los hosts dentro de un clúster de alta disponibilidad pierden la conectividad a la red u otros hosts del clúster. De forma predeterminada, vSphere HA utilizará la puerta de enlace predeterminada para su red de gestión como dirección de aislamiento predeterminada. Sin embargo, puede especificar direcciones de aislamiento adicionales para que el host haga ping para determinar si se debe activar una respuesta de aislamiento. Agregue dos IP de aislamiento que puedan hacer ping, una por sitio. No utilice la IP de la puerta de enlace. La configuración avanzada de HA de vSphere utilizada es das.isolationaddress. Puede utilizar las direcciones IP de ONTAP o Mediator para este fin.

Consulte "Prácticas recomendadas para VMware vSphere Metro Storage Cluster" para obtener más información.



Agregar una configuración avanzada llamada das.heartbeatDsPerHost puede aumentar el número de almacenes de datos de latido. Utilice cuatro almacenes de datos para el corazón (HB DSS): Dos por sitio. Utilice la opción Seleccionar de la lista pero complementar. Esto es necesario porque si un sitio falla, usted todavía necesita dos HB DSS. Sin embargo, dichas aplicaciones no tienen por qué estar protegidas con MetroCluster o SnapMirror con sincronización activa.

Consulte "Prácticas recomendadas para VMware vSphere Metro Storage Cluster" para obtener más información.

Afinidad de VMware DRS para NetApp MetroCluster

En esta sección creamos grupos DRS para equipos virtuales y hosts para cada sitio\clúster del entorno MetroCluster. A continuación, configuramos las reglas de VM\Host para alinear la afinidad de host de VM con los recursos de almacenamiento local. Por ejemplo, las máquinas virtuales de la dirección A pertenecen al grupo de máquinas virtuales sitea_vms y la ubicación A pertenecen al grupo de hosts sitea_hosts. A continuación, en VM\Host Rules, indicamos que sitea_vms debe ejecutarse en hosts en sitea_Hosts.

- NetApp recomienda encarecidamente la especificación **Debe ejecutarse en hosts del grupo** en lugar de la especificación **Debe ejecutarse en hosts del grupo**. En caso de que se produzca un fallo del host del sitio A, es necesario reiniciar las máquinas virtuales del sitio A en los hosts del sitio B a través de vSphere HA, pero la última especificación no permite a HA reiniciar los equipos virtuales en el sitio B, ya que es una regla estricta. La especificación anterior es una regla flexible y se infringirá en caso de alta disponibilidad, lo que permitirá la disponibilidad en lugar de rendimiento.
- Puede crear una alarma basada en eventos que se dispara cuando una máquina virtual viola una regla de afinidad VM-Host. En vSphere Client, agregue una nueva alarma para la máquina virtual y seleccione VM is Violating VM-Host Affinity Rule como activador de evento. Para obtener más información sobre la creación y edición de alarmas, consulte "Supervisión y rendimiento de vSphere"la documentación.

Crear grupos de hosts DRS

Para crear grupos de hosts DRS específicos del sitio A y del sitio B, realice los siguientes pasos:

1. En vSphere Web Client, haga clic con el botón derecho en el clúster en el inventario y seleccione Settings.
2. Haga clic en VM\Host Groups.
3. Haga clic en Añadir.
4. Escriba el nombre del grupo (por ejemplo, sitea_hosts).
5. En el menú Tipo, seleccione Grupo de hosts.
6. Haga clic en Agregar y seleccione los hosts deseados del sitio A y haga clic en Aceptar.
7. Repita estos pasos para agregar otro grupo de hosts para el sitio B.
8. Haga clic en Aceptar.

Crear grupos de máquinas virtuales DRS

Para crear grupos de máquinas virtuales DRS específicos del sitio A y del sitio B, realice los siguientes pasos:

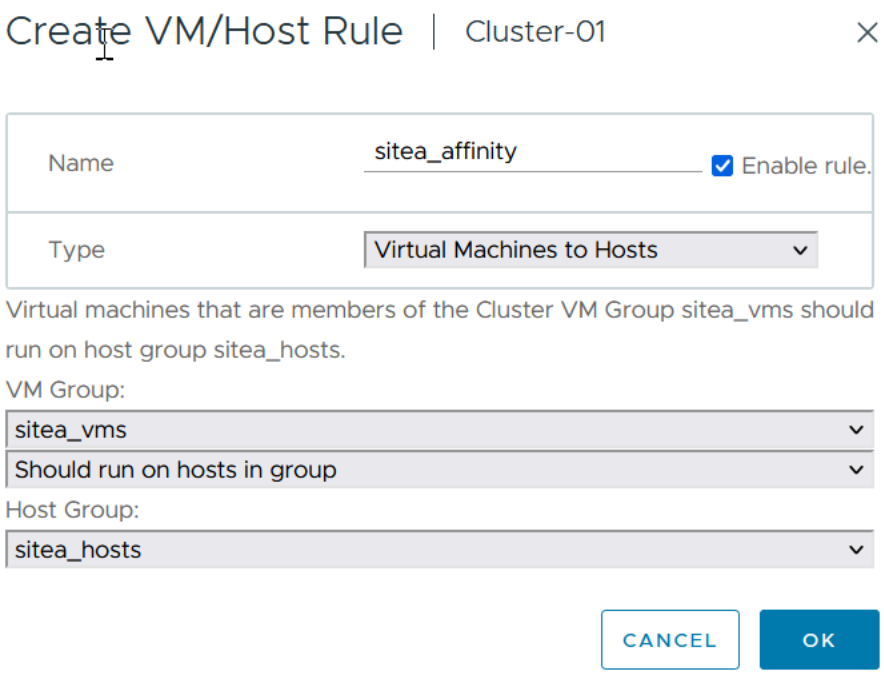
1. En vSphere Web Client, haga clic con el botón derecho en el clúster en el inventario y seleccione Settings.
2. Haga clic en VM\Host Groups.
3. Haga clic en Añadir.
4. Escriba el nombre del grupo (por ejemplo, sitea_vms).
5. En el menú Type, seleccione VM Group.
6. Haga clic en Add y seleccione las máquinas virtuales deseadas en el sitio A y, a continuación, haga clic en OK.
7. Repita estos pasos para agregar otro grupo de hosts para el sitio B.
8. Haga clic en Aceptar.

Crear reglas de host de VM

Para crear reglas de afinidad de DRS específicas para el sitio A y el sitio B, realice los siguientes pasos:

1. En vSphere Web Client, haga clic con el botón derecho en el clúster en el inventario y seleccione Settings.
2. Haga clic en VM\Host Rules.

3. Haga clic en Añadir.
4. Escriba el nombre de la regla (por ejemplo, sitea_affinity).
5. Compruebe que la opción Activar regla está activada.
6. En el menú Type, seleccione Virtual Machines to Hosts.
7. Seleccione el grupo de VM (por ejemplo, sitea_vms).
8. Seleccione el grupo Host (por ejemplo, sitea_Hosts).
9. Repita estos pasos para añadir otra regla VM\Host para el sitio B.
10. Haga clic en Aceptar.



Cree clústeres de almacenes de datos si es necesario

Para configurar un clúster de almacén de datos para cada sitio, complete los siguientes pasos:

1. Use el cliente web de vSphere, vaya al centro de datos donde reside el clúster de alta disponibilidad en Storage.
2. Haga clic con el botón derecho en el objeto del centro de datos y seleccione Storage > New Datastore Cluster.

*Cuando se utiliza el almacenamiento ONTAP, se recomienda desactivar el DRS de Almacenamiento.

- Por lo general, los DRS de almacenamiento no son necesarios ni se recomiendan para su uso con sistemas de almacenamiento de ONTAP.
- ONTAP proporciona sus propias funciones de eficiencia del almacenamiento, como la deduplicación, la compresión y la compactación, que pueden verse afectadas por Storage DRS.
- Si utiliza copias Snapshot de ONTAP, Storage vMotion dejaría detrás de la copia del equipo virtual en la copia Snapshot, lo que puede aumentar el uso del almacenamiento y puede afectar a las aplicaciones de backup como NetApp SnapCenter, que registran las máquinas virtuales y sus copias Snapshot de ONTAP.

1. Seleccione el clúster de alta disponibilidad y haga clic en Next.

1. Seleccione los almacenes de datos que pertenecen al sitio A y haga clic en Next.

1. Revise las opciones y haga clic en Finish.
2. Repita estos pasos para crear el clúster de almacenes de datos del sitio B y verifique que solo estén seleccionados los almacenes de datos del sitio B.

Disponibilidad del vCenter Server

Los dispositivos vCenter Server Appliances (VCSA) deben estar protegidos con alta disponibilidad de vCenter. La alta disponibilidad de vCenter le permite implementar dos VCSA en un par de alta disponibilidad activo-pasivo. Uno en cada dominio de fallo. Puede obtener más información sobre la alta disponibilidad de vCenter en "docs.vmware.com".

Resiliencia para eventos planificados y no planificados

NetApp MetroCluster y SnapMirror Active Sync son potentes herramientas que mejoran la alta disponibilidad y las operaciones no disruptivas del hardware de NetApp y del software ONTAP®.

Estas herramientas proporcionan protección en todo el sitio para todo el entorno de almacenamiento, lo que garantiza que los datos están siempre disponibles. Ya sea que utilice servidores independientes, clústeres de servidores de alta disponibilidad, contenedores o servidores virtualizados, la tecnología NetApp mantiene fácilmente la disponibilidad de almacenamiento en caso de interrupción total por pérdida de alimentación, refrigeración o conectividad de red, apagado del array de almacenamiento o error de funcionamiento.

MetroCluster y SnapMirror de sincronización activa proporcionan tres métodos básicos de continuidad de datos en caso de eventos previstos o no planificados:

- Componentes redundantes para protección contra fallos de un solo componente
- Toma de control local de alta disponibilidad para eventos que afectan a una única controladora
- Protección completa del sitio: Reanudación rápida del servicio al mover el almacenamiento y el acceso de clientes del clúster de origen al clúster de destino

Esto significa que las operaciones continúan sin problemas en caso de fallo de un único componente y vuelven automáticamente al funcionamiento redundante cuando se reemplaza el componente fallido.

Todos los clústeres de ONTAP, excepto los clústeres de un solo nodo (normalmente las versiones definidas por software, como ONTAP Select, por ejemplo), tienen funciones de alta disponibilidad incorporadas denominadas toma de control y retorno al nodo primario. Cada controladora del clúster se empareja con otra controladora, lo que forma una pareja de alta disponibilidad. Estos pares garantizan que cada nodo esté conectado localmente al almacenamiento.

La toma de control es un proceso automatizado en el que un nodo asume el almacenamiento del otro para mantener los servicios de datos. Giveback es el proceso inverso que restaura el funcionamiento normal. La toma de control puede planificarse, por ejemplo, al realizar tareas de mantenimiento del hardware o actualizaciones de ONTAP, o no planificadas, resultantes de un error de hardware o de alarma en el nodo.

Durante una toma de control, los LIF NAS en configuraciones de MetroCluster conmutan automáticamente al respaldo. Sin embargo, los LIF de SAN no conmutan al nodo de respaldo; seguirán utilizando la ruta directa a los números de unidad lógica (LUN).

Si quiere más información sobre la toma de control y el retorno al nodo primario de alta disponibilidad, consulte el "Información general sobre la gestión de parejas de HA". Vale la pena señalar que esta funcionalidad no es específica de la sincronización activa de MetroCluster o SnapMirror.

El cambio de sitio con MetroCluster se produce cuando un sitio está sin conexión o como una actividad planificada para el mantenimiento de todo el sitio. El sitio restante asume la propiedad de los recursos de almacenamiento (discos y agregados) del clúster sin conexión y las SVM del sitio con el que se ha producido el fallo se conectan y se reinician en el sitio de desastre, conservando su identidad completa para el acceso de clientes y host.

Con la sincronización activa de SnapMirror, dado que ambas copias se usan de forma activa a la vez, los hosts existentes seguirán funcionando. El Mediador de ONTAP es necesario para garantizar que la conmutación por error del sitio se produce correctamente.

Situaciones de fallo para VMSC con MetroCluster

En las siguientes secciones se resumen los resultados esperados de varios escenarios de fallo con sistemas VMSC y NetApp MetroCluster.

Fallo de ruta de almacenamiento única

En esta situación, si se produce un error en componentes como el puerto HBA, el puerto de red, el puerto del switch de datos de interfaz de usuario o un cable FC o Ethernet, esa ruta particular al dispositivo de almacenamiento se marca como muerta por el host ESXi. Si se configuran varias rutas para el dispositivo de almacenamiento proporcionando resiliencia en el puerto de HBA/red/switch, ESXi idealmente ejecuta una conmutación de rutas. Durante este periodo, las máquinas virtuales permanecen en ejecución sin que se vean afectadas, porque se cuida de la disponibilidad del almacenamiento mediante varias rutas al dispositivo de almacenamiento.

No hay ningún cambio en el comportamiento de MetroCluster en este escenario, y todos los almacenes de datos siguen estando intactos en sus sitios respectivos.

Best Practice

En entornos en los que se utilizan volúmenes NFS/iSCSI, NetApp recomienda tener al menos dos vínculos superiores de red configurados para el puerto NFS vmkernel en el vSwitch estándar y lo mismo en el grupo de puertos en el que se asigna la interfaz de NFS vmkernel para el vSwitch distribuido. La agrupación de NIC se puede configurar en activo-activo o activo-en espera.

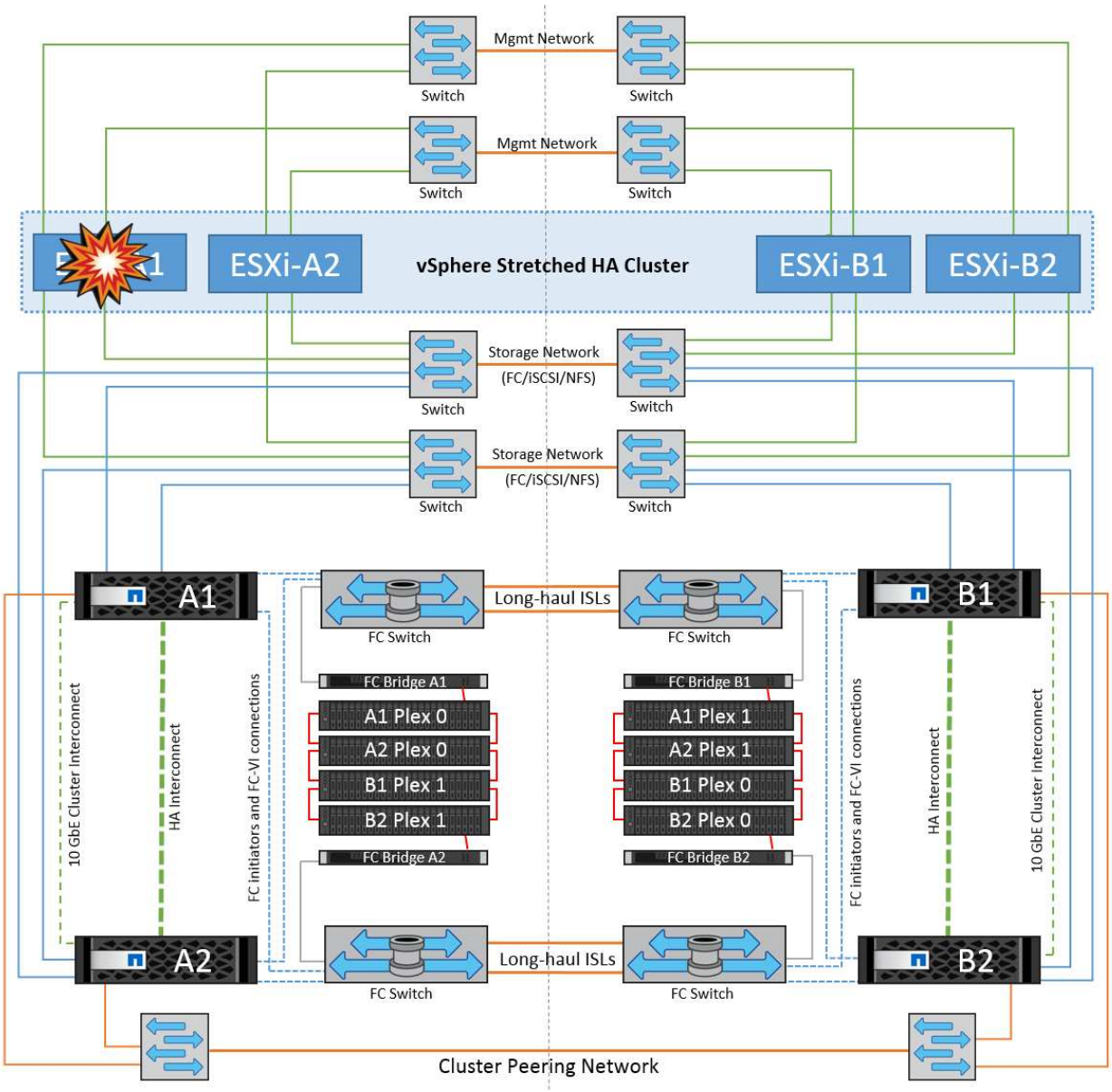
Además, para las LUN iSCSI, la multivía debe configurarse vinculando las interfaces de vmkernel con los adaptadores de red iSCSI. Si quiere más información, consulte la documentación de almacenamiento de vSphere.

Best Practice

En entornos en los que se usan LUN de Fibre Channel, NetApp recomienda tener al menos dos HBA, lo que garantiza la resistencia a nivel de HBA/puerto. NetApp también recomienda la división en zonas de un solo iniciador a un único destino como práctica recomendada para configurar la división en zonas.

Debe utilizarse Virtual Storage Console (VSC) para establecer normativas de accesos múltiples, porque establece normativas para todos los dispositivos de almacenamiento de NetApp nuevos y existentes.

Fallo de un host ESXi único



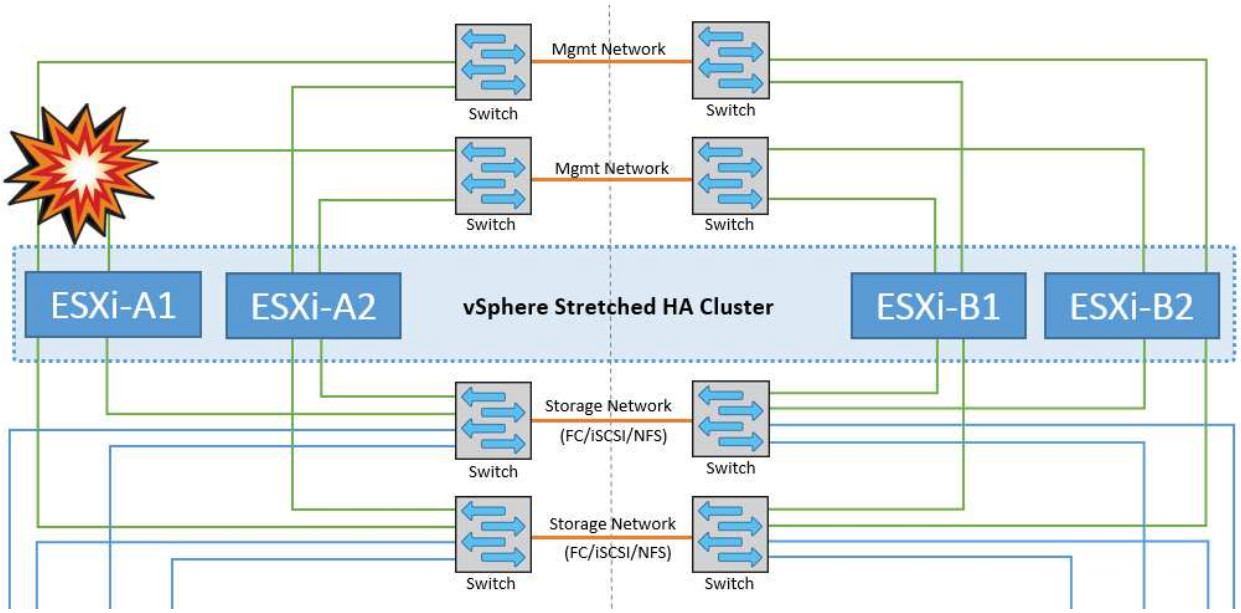
En esta situación, si hay un fallo de host ESXi, el nodo maestro del clúster de alta disponibilidad de VMware detecta el fallo del host porque ya no recibe los latidos de red. Para determinar si el host está realmente inactivo o sólo una partición de red, el nodo maestro supervisa los latidos del almacén de datos y, si están ausentes, realiza una comprobación final haciendo ping en las direcciones IP de gestión del host fallido. Si todas estas comprobaciones son negativas, el nodo maestro declara a este host un host fallido y todas las máquinas virtuales que se estaban ejecutando en este host fallido se reinician en el host superviviente del cluster.

Si se han configurado las reglas de afinidad de host y VM de DRS (las VM del grupo de VM sitea_vms deben ejecutar hosts en el grupo de hosts sitea_Hosts), el maestro de HA primero comprueba los recursos disponibles en el sitio A. Si no hay hosts disponibles en el sitio A, el maestro intenta reiniciar las máquinas virtuales en los hosts del sitio B.

Es posible que las máquinas virtuales se inicien en los hosts ESXi en el otro sitio si hay una restricción de recursos en el sitio local. Sin embargo, las reglas de afinidad de host y máquina virtual de DRS definidas corregirán si se viola alguna regla migrando las máquinas virtuales de nuevo a cualquier host ESXi sobreviviente en el sitio local. En los casos en que DRS se defina en manual, NetApp recomienda invocar DRS y aplicar las recomendaciones para corregir la ubicación de la máquina virtual.

No hay ningún cambio en el comportamiento de MetroCluster en este escenario y todos los almacenes de datos siguen estando intactos en sus sitios respectivos.

Aislamiento de hosts ESXi

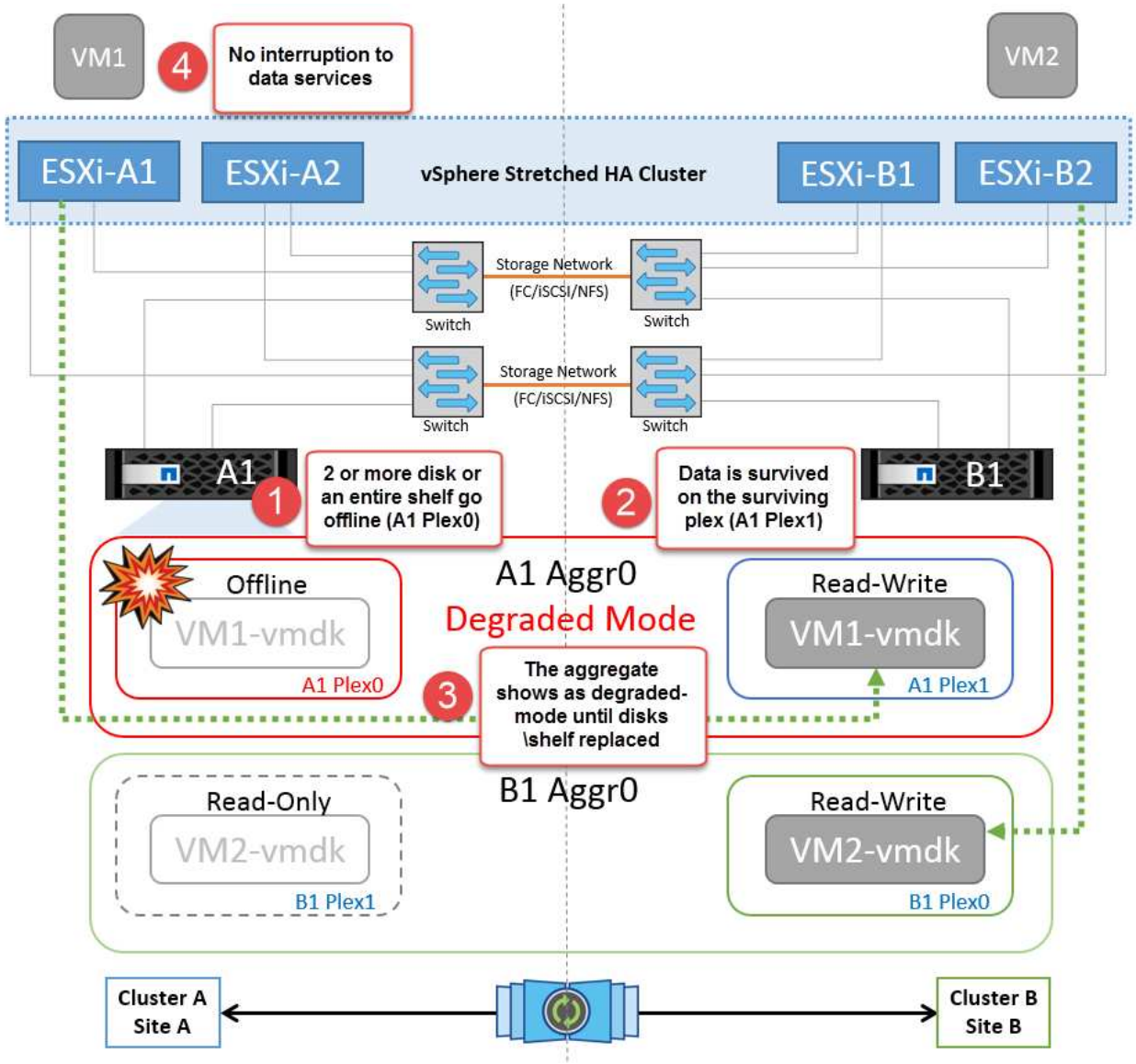


En esta situación, si la red de gestión del host ESXi está inactiva, el nodo principal del clúster de alta disponibilidad no recibirá ningún latido y, por lo tanto, este host se aísla en la red. Para determinar si ha fallado o solo está aislado, el nodo maestro comienza a supervisar el latido del almacén de datos. Si está presente, el nodo maestro declara que el host está aislado. Dependiendo de la respuesta de aislamiento configurada, el host puede optar por apagarse, apagar las máquinas virtuales o incluso dejar encendidas las máquinas virtuales. El intervalo predeterminado para la respuesta de aislamiento es de 30 segundos.

No hay ningún cambio en el comportamiento de MetroCluster en este escenario y todos los almacenes de datos siguen estando intactos en sus sitios respectivos.

Fallo de la bandeja de discos

En esta situación, se produce un fallo de más de dos discos o una bandeja entera. Los datos se sirven desde el plex superviviente sin interrupción de los servicios de datos. El fallo del disco puede afectar a un plex local o remoto. Los agregados se mostrarán como degradado porque solo está activo un plex. Una vez sustituidos los discos que han fallado, los agregados afectados se sincronizarán automáticamente para volver a compilar los datos. Tras realizar la resincronización, los agregados volverán automáticamente al modo reflejado normal. Si falla más de dos discos dentro de un mismo grupo RAID, es necesario reconstruir el plex.

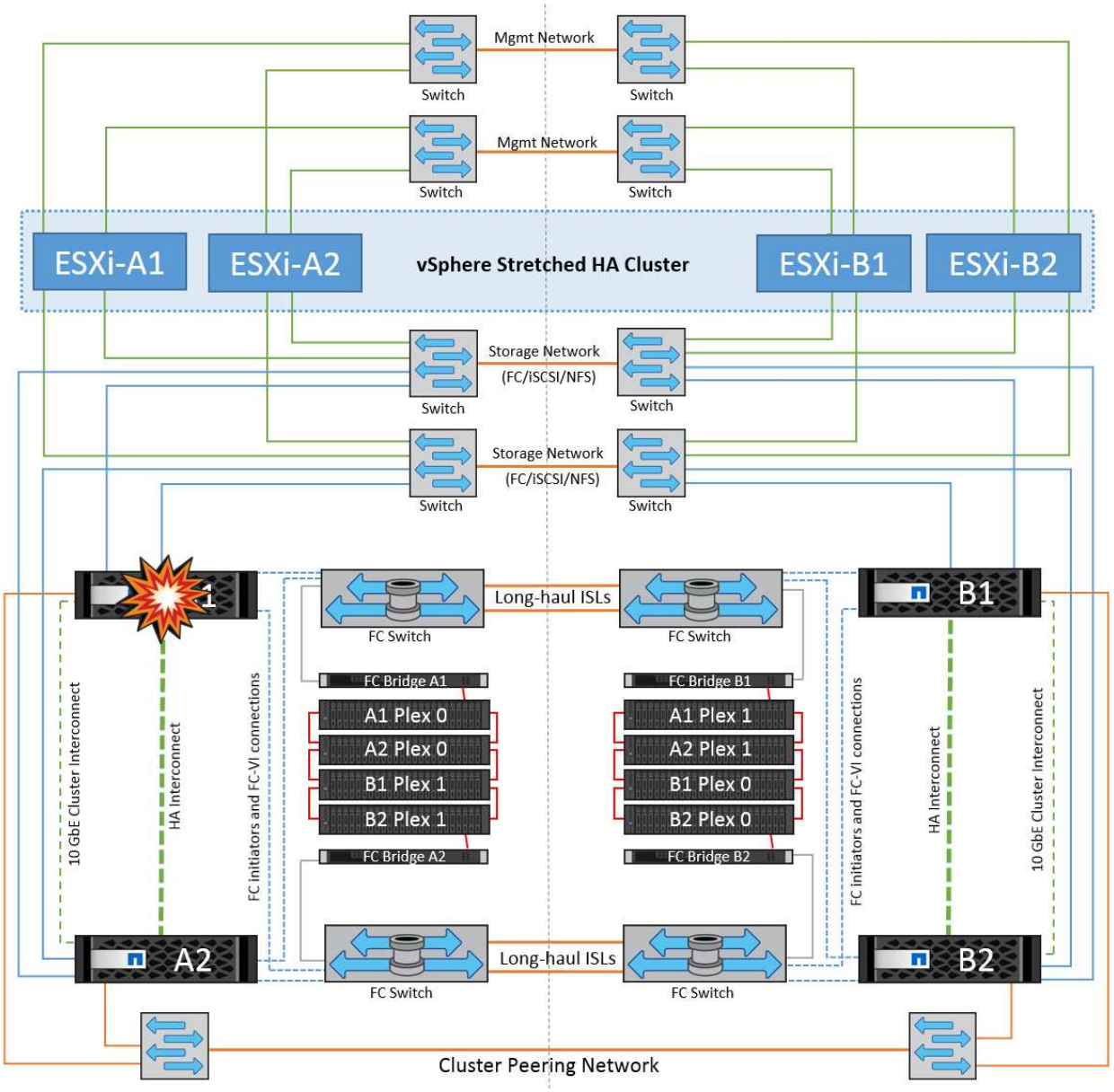


*[NOTA]

- Durante este periodo, no se ven afectadas las operaciones de I/O de las máquinas virtuales, pero el rendimiento está degradado porque se accede a los datos desde la bandeja de discos remota a través de enlaces ISL.

Fallo de una controladora de almacenamiento única

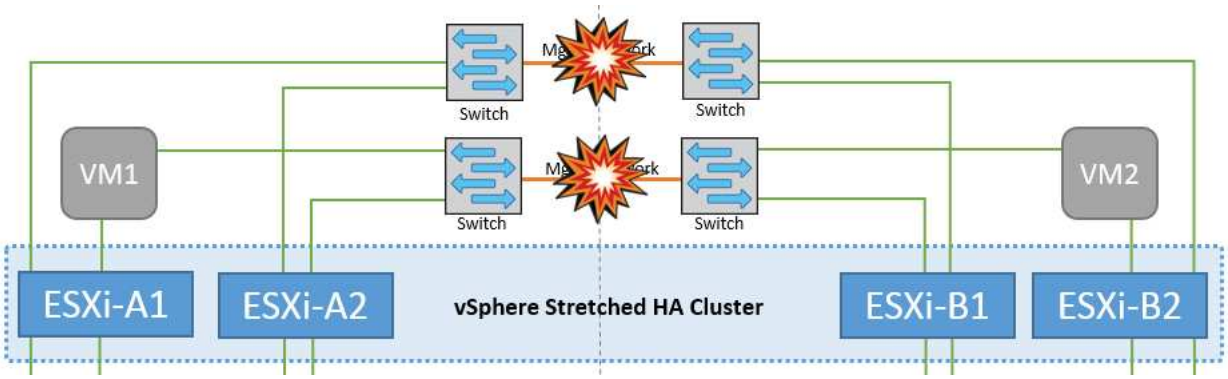
En este escenario, una de las dos controladoras de almacenamiento falla en un sitio. Dado que hay un par de alta disponibilidad en cada sitio, el fallo de un nodo de forma transparente activa automáticamente la conmutación al otro nodo. Por ejemplo, si falla el nodo A1, su almacenamiento y sus cargas de trabajo se transfieren automáticamente al nodo A2. Las máquinas virtuales no se verán afectadas porque todos los plexes permanecen disponibles. Los nodos del segundo sitio (B1 y B2) no se ven afectados. Además, vSphere HA no realizará ninguna acción porque el nodo principal del clúster seguirá recibiendo los latidos de red.



Si la conmutación al respaldo forma parte de un desastre gradual (el nodo A1 conmuta al nodo A2) y hay un fallo posterior de A2 o el fallo completo del sitio A, el cambio tras un desastre puede ocurrir en el sitio B.

Fallos de enlace de interinterruptor

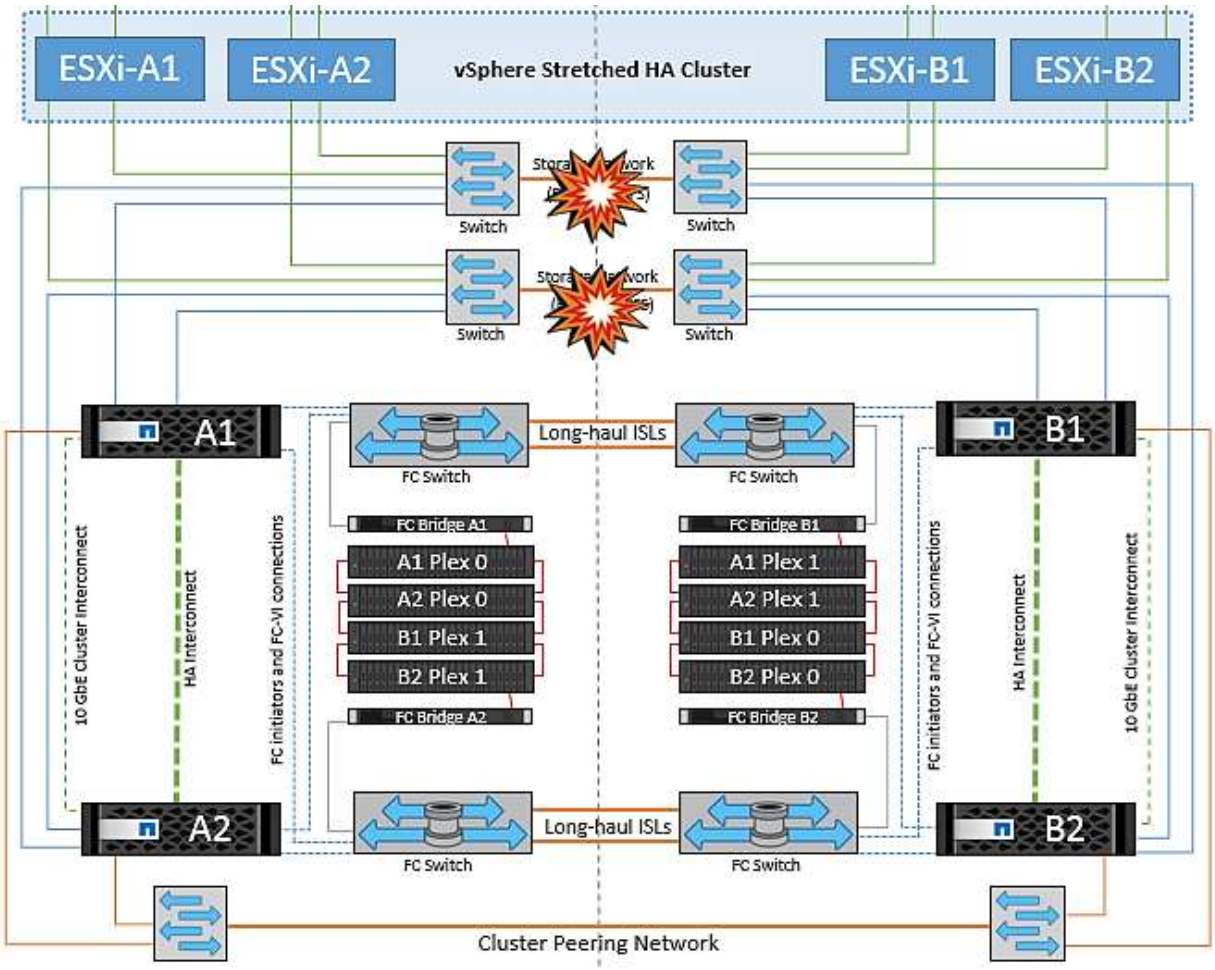
Fallo de enlace de interswitch en la red de gestión



En este escenario, si los enlaces ISL en la red de gestión de host de interfaz de usuario producen un error, los hosts ESXi del sitio A no podrán comunicarse con los hosts ESXi del sitio B. Esto dará lugar a una partición de red porque los hosts ESXi de un sitio concreto no podrán enviar los latidos de red al nodo maestro del clúster HA. Como tal, habrá dos segmentos de red debido a la partición y habrá un nodo maestro en cada segmento que protegerá las VM de fallos de host dentro del sitio en particular.

Durante este período, las máquinas virtuales permanecen en ejecución y no hay cambios en el comportamiento de MetroCluster en este escenario. Todos los almacenes de datos siguen estando intactos en sus respectivos sitios.

Fallo de enlace interswitch en la red de almacenamiento

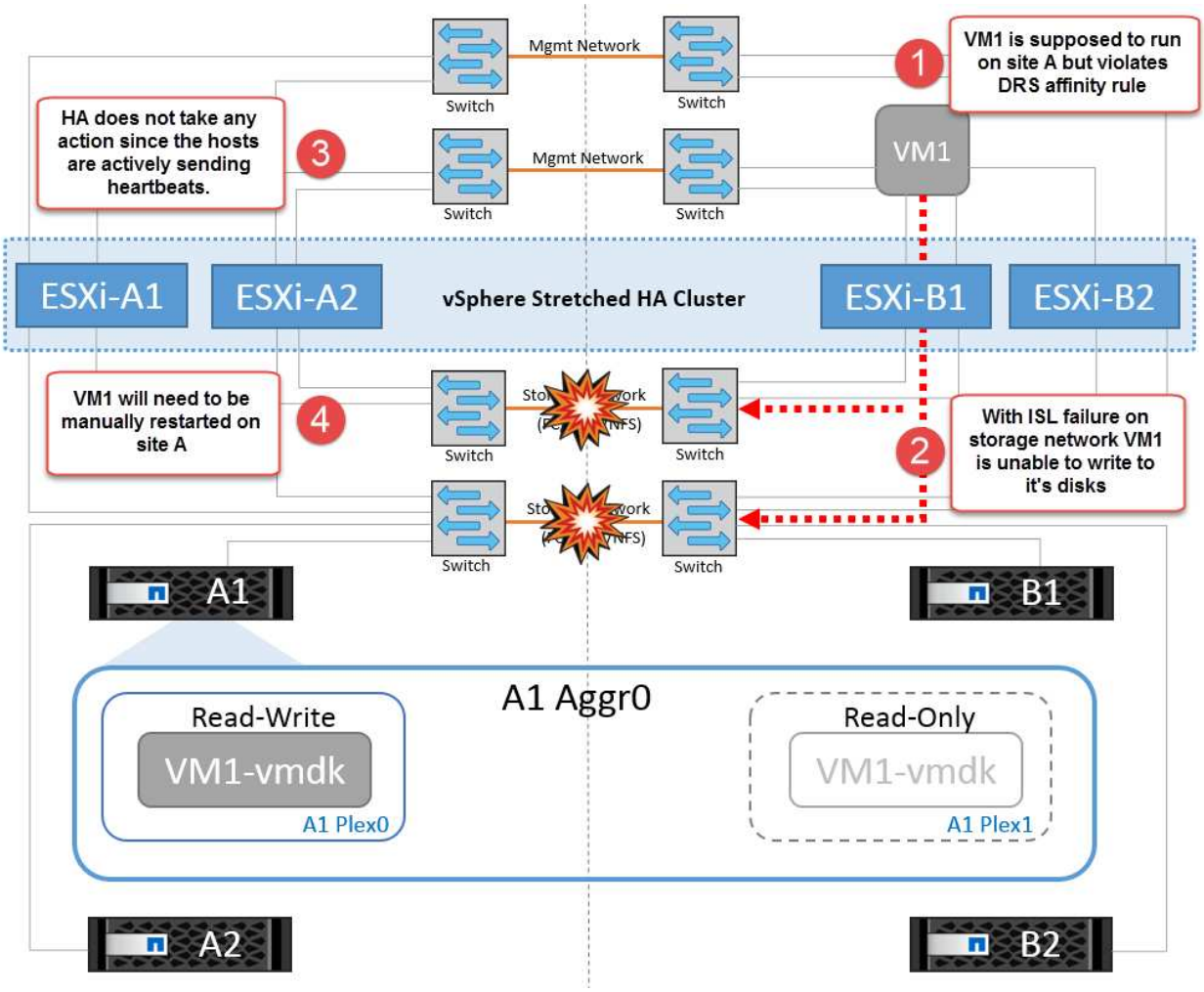


En este escenario, si los enlaces ISL en la red de almacenamiento de back-end fallan, los hosts del sitio A perderán acceso a los volúmenes de almacenamiento o las LUN del clúster B en el sitio B y viceversa. Las reglas de VMware DRS se definen de modo que la afinidad de sitios de almacenamiento host facilita que los equipos virtuales funcionen sin que el sitio se vea afectado.

Durante este período, las máquinas virtuales permanecen en ejecución en sus respectivos sitios y no hay cambios en el comportamiento de MetroCluster en este escenario. Todos los almacenes de datos siguen estando intactos en sus respectivos sitios.

Si por algún motivo se violó la regla de afinidad (por ejemplo, VM1, que se suponía que se ejecutaba desde la ubicación A donde sus discos residen en nodos del clúster local A, se está ejecutando en un host del sitio B), se accederá al disco de la máquina virtual de forma remota a través de enlaces ISL. Debido a un fallo de enlace ISL, VM1 ejecutándose en la instalación B no podría escribir en sus discos porque las rutas al volumen

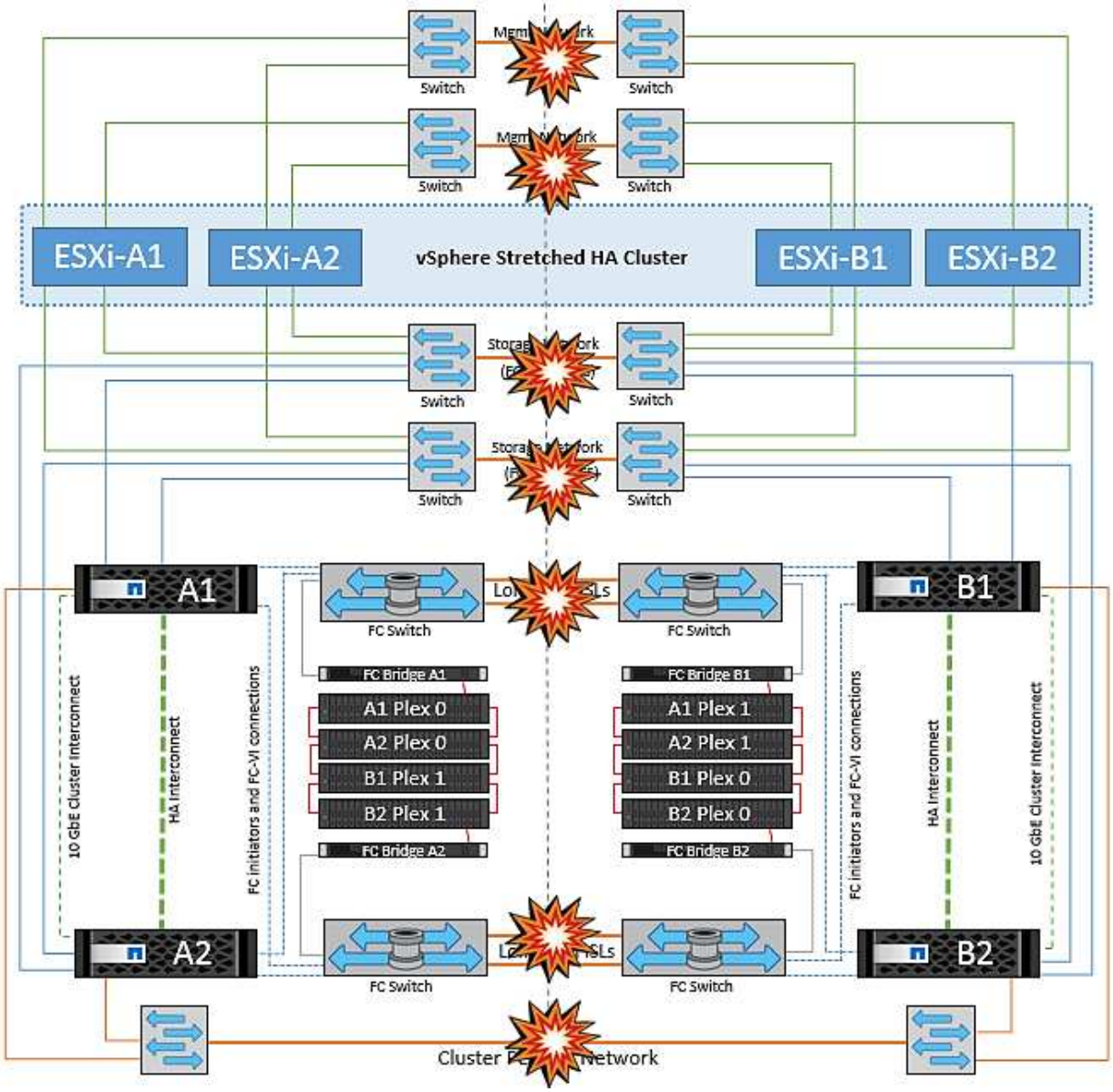
de almacenamiento están inactivas y la máquina virtual determinada está inactiva. En estos casos, VMware HA no realiza ninguna acción puesto que los hosts envían latidos de forma activa. Esas máquinas virtuales deben apagarse y encenderse manualmente en sus respectivos sitios. La siguiente figura ilustra una VM que viola una regla de afinidad DRS.



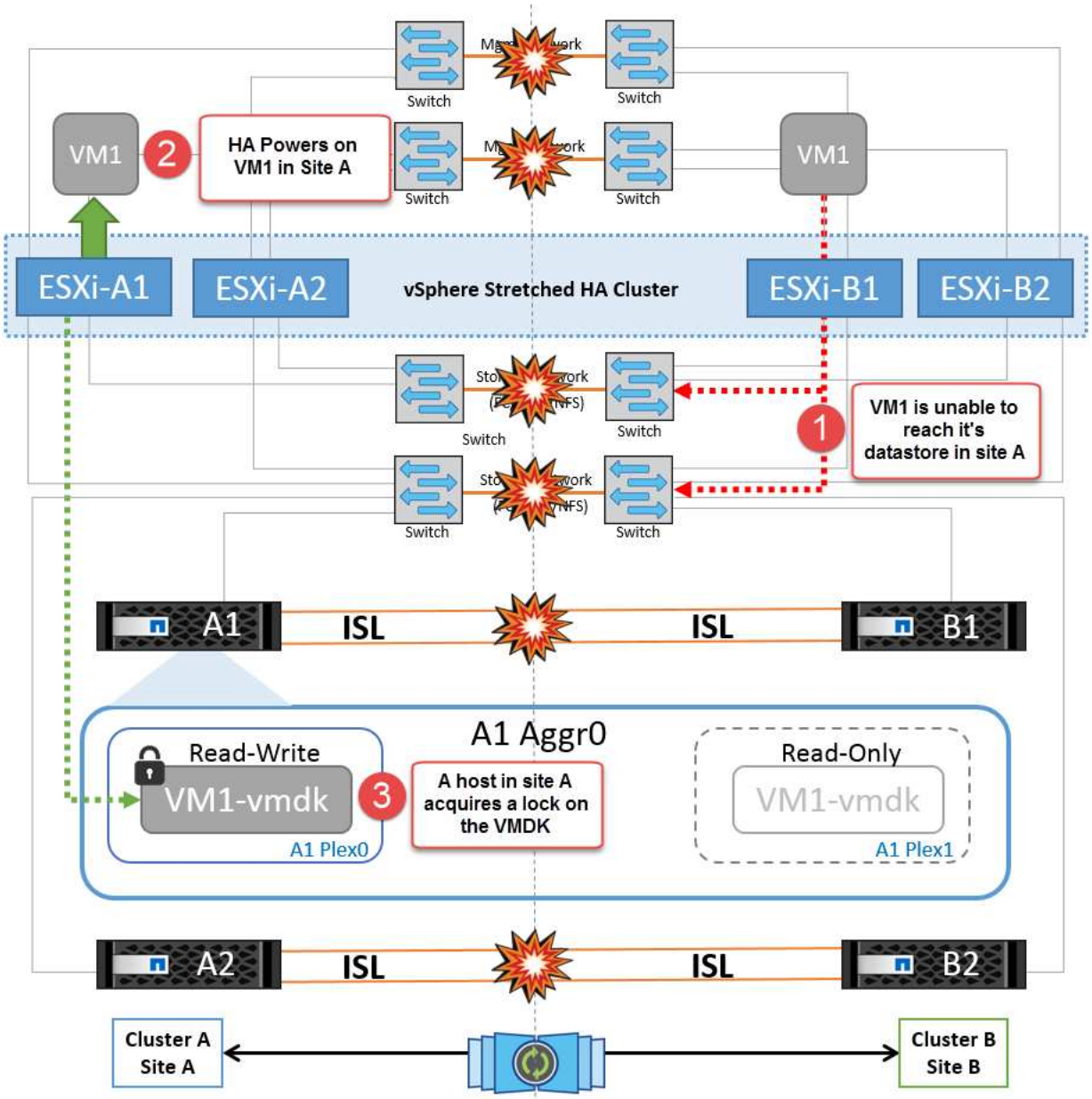
Todos los fallos de interswitch o la partición completa del centro de datos

En este escenario, todos los enlaces ISL entre los sitios están inactivos y los dos sitios están aislados uno de otro. Como se explicó en escenarios anteriores, como el fallo ISL en la red de gestión y en la red de almacenamiento, las máquinas virtuales no se ven afectadas por un fallo de ISL completo.

Una vez que los hosts ESXi hayan particionado entre sitios, el agente de alta disponibilidad de vSphere comprobará si hay latidos del almacén de datos y, en cada sitio, los hosts ESXi locales podrán actualizar los latidos del almacén de datos a sus respectivos volúmenes/LUN de lectura/escritura. Los hosts del sitio A asumirán que los otros hosts ESXi del sitio B han fallado porque no hay ningún latido de red/almacén de datos. VSphere HA en el sitio A intentará reiniciar las máquinas virtuales del sitio B, lo cual eventualmente fallará porque no se podrá acceder a los almacenes de datos del sitio B debido a un fallo del ISL del almacenamiento. Una situación similar se repite en el sitio B.



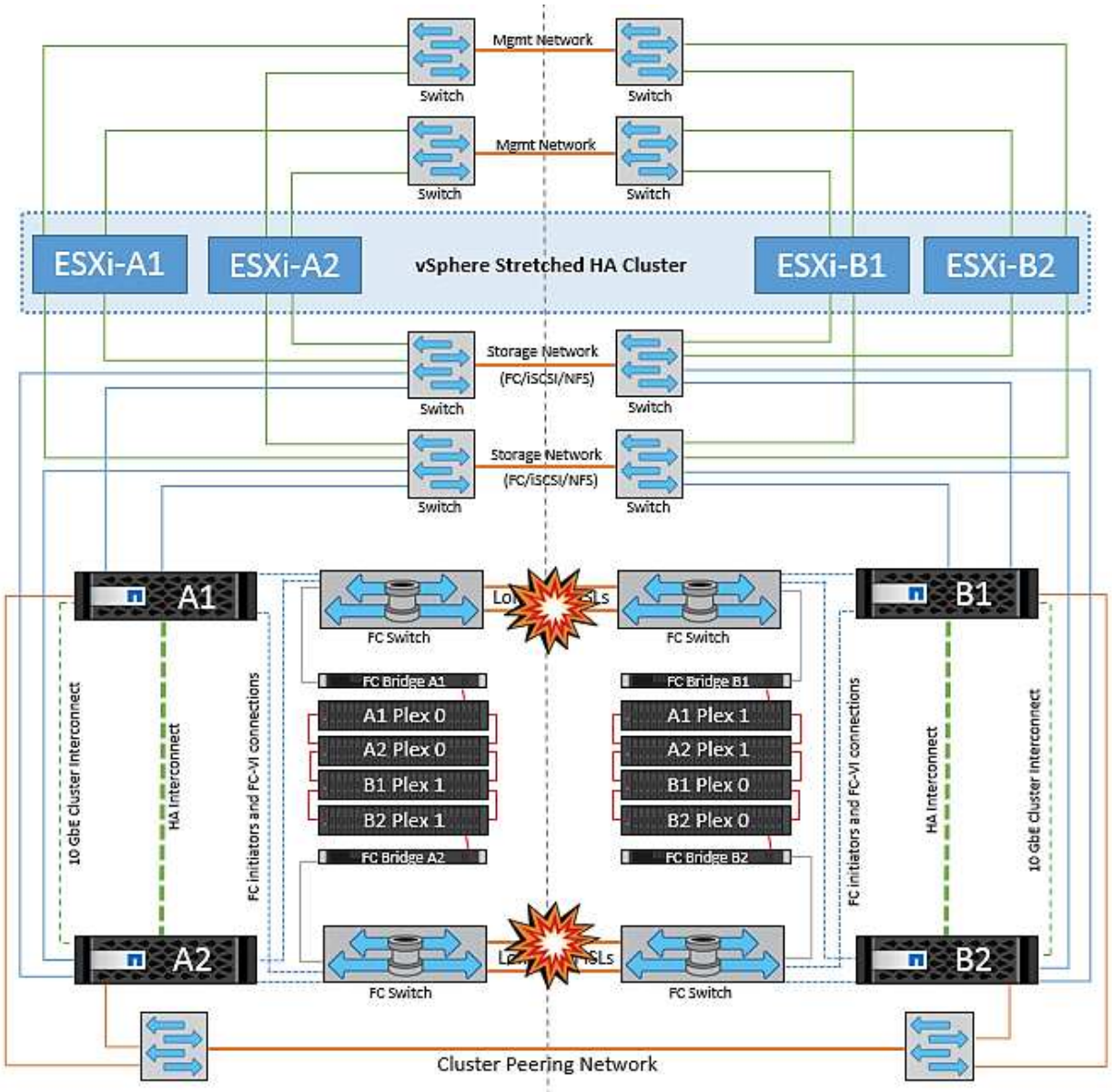
NetApp recomienda determinar si alguna máquina virtual ha infringido las reglas de DRS. Los equipos virtuales que se ejecuten desde un sitio remoto estarán inactivos ya que no podrán acceder al almacén de datos y vSphere HA reiniciará esa máquina virtual en el sitio local. Una vez que los enlaces ISL vuelvan a estar en línea, la máquina virtual que se estaba ejecutando en el sitio remoto se desactivará, ya que no puede haber dos instancias de máquinas virtuales ejecutándose con las mismas direcciones MAC.



Fallo de interswitch Link en ambas estructuras en NetApp MetroCluster

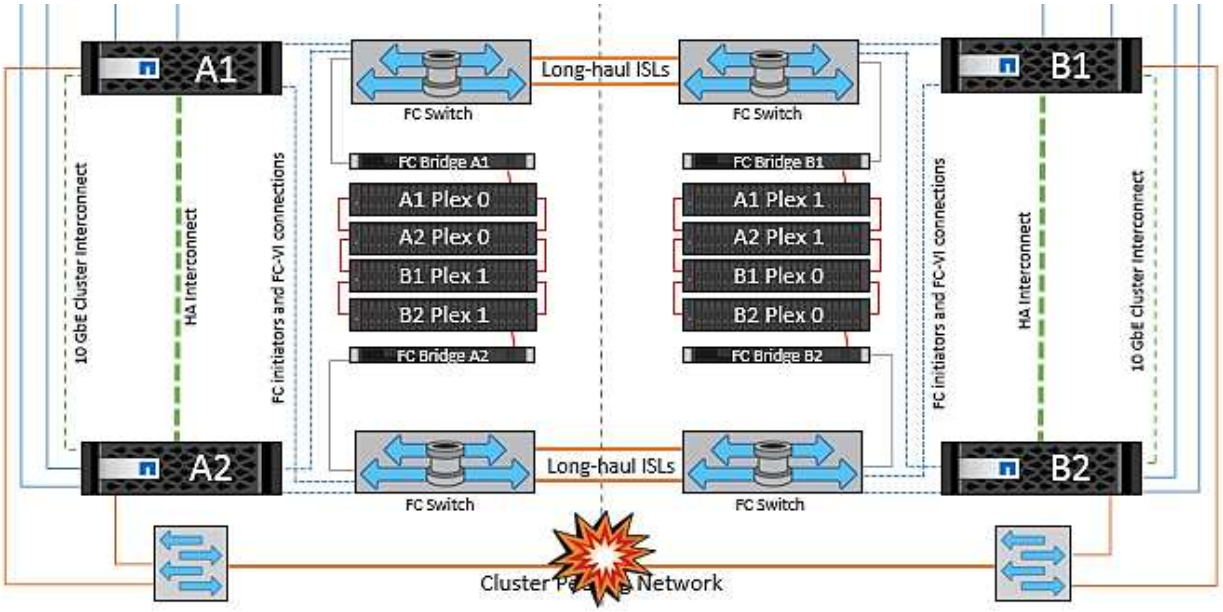
En un escenario en el que uno o varios ISL fallan, el tráfico continúa por los enlaces restantes. Si todos los ISL de ambas estructuras fallan, de modo que no hay ningún enlace entre los sitios para el almacenamiento y la replicación de NVRAM, cada controladora seguirá proporcionando sus datos locales. Cuando se restaura al menos un ISL, la resincronización de todos los complejos se realiza de forma automática.

Las escrituras que se produzcan después de que todos los ISL estén inactivos no se reflejarán en el otro sitio. Una conmutación de sitios en caso de desastre, mientras la configuración se encuentra en este estado, por lo tanto, incurriría en la pérdida de los datos que no se habían sincronizado. En este caso, se requiere intervención manual para la recuperación después del cambio. Si es probable que no haya ISL disponibles durante un largo período de tiempo, un administrador puede optar por cerrar todos los servicios de datos para evitar el riesgo de pérdida de datos si es necesario una conmutación por desastre. La realización de esta acción debe evaluarse para la probabilidad de que se produzca un desastre que requiera la conmutación del servicio antes de que esté disponible al menos un ISL. Como alternativa, si los ISL fallan en un escenario en cascada, un administrador podría activar una conmutación de sitios planificada a uno de los sitios antes de que todos los enlaces hayan fallado.



Fallo de enlace de clúster con conexión entre iguales

En un supuesto de fallo de enlace de clústeres con conexión entre iguales, dado que los ISL de estructura aún están activos, los servicios de datos (lecturas y escrituras) continúan en ambos sitios en ambos complejos. No se puede propagar ningún cambio de configuración del clúster (por ejemplo, añadir una nueva SVM o aprovisionar un volumen o un LUN en una SVM existente) al otro sitio. Estos se mantienen en los volúmenes de metadatos de CRS locales y se propagan automáticamente al otro cluster tras la recuperación del enlace de cluster entre iguales. Si se necesita una conmutación por error forzada antes de poder restaurar el enlace de clúster entre iguales, se volverán a reproducir automáticamente los cambios pendientes de configuración de clúster desde la copia replicada remota de los volúmenes de metadatos del sitio superviviente como parte del proceso de conmutación por error.



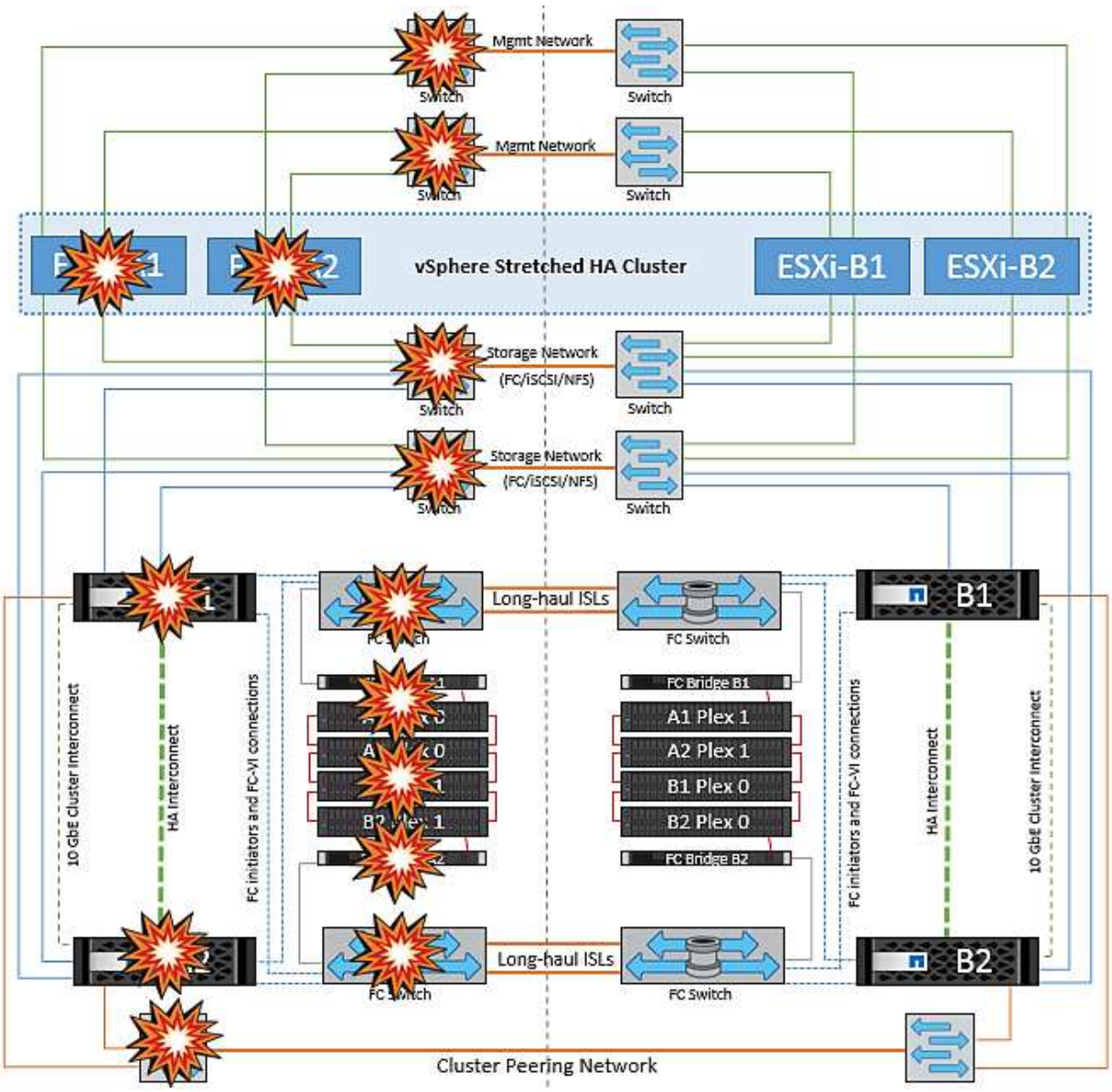
Fallo completo del sitio

En un supuesto de fallo del sitio A completo, los hosts ESXi del sitio B no obtendrán el latido de red de los hosts ESXi del sitio A porque están inactivos. El maestro de alta disponibilidad en el sitio B verificará que los latidos del almacén de datos no están presentes, declarará que los hosts del sitio A han fallado e intentará reiniciar el sitio A de los equipos virtuales en el sitio B. Durante este periodo, el administrador de almacenamiento realiza una conmutación de sitios para reanudar los servicios de los nodos fallidos en el sitio superviviente. Esto restaura todos los servicios de almacenamiento del sitio A en el sitio B. Después de que el sitio haya volúmenes o LUN disponibles en el sitio B, el agente maestro de alta disponibilidad intentará reiniciar el sitio A, máquinas virtuales del sitio B.

Si el intento del agente maestro HA de vSphere de reiniciar una máquina virtual (lo que implica registrarla y encenderla) falla, el reinicio se vuelve a intentar después de un retraso. El retardo entre reinicios se puede configurar hasta un máximo de 30 minutos. VSphere HA intenta estos reinicios durante un número máximo de intentos (seis intentos de forma predeterminada).

> El maestro de alta disponibilidad no inicia los intentos de reinicio hasta que el administrador de ubicación encuentra el almacenamiento adecuado, por lo que en caso de un fallo completo del sitio, sería después de que se haya realizado el cambio.

Si el sitio A se ha cambiado, un fallo posterior de uno de los nodos del sitio B superviviente se puede gestionar sin problemas mediante la conmutación al nodo superviviente. En este caso, solo un nodo realiza el trabajo de cuatro nodos. En este caso, la recuperación consistiría en realizar un retorno al nodo local. A continuación, cuando se restaura el sitio A, se realiza una operación de conmutación para restaurar el funcionamiento en estado constante de la configuración.



Seguridad de los productos

Herramientas de ONTAP para VMware vSphere

La ingeniería de software con Herramientas de ONTAP para VMware vSphere emplea las siguientes actividades de desarrollo seguro:

- **Modelado de amenazas.** el propósito del modelado de amenazas es descubrir defectos de seguridad en una característica, componente o producto al principio del ciclo de vida del desarrollo del software. Un modelo de amenaza es una representación estructurada de toda la información que afecta la seguridad de una aplicación. En esencia, es una visión de la aplicación y su entorno a través del objetivo de la seguridad.
- **Pruebas de seguridad de aplicaciones dinámicas (DAST).** esta tecnología está diseñada para detectar condiciones vulnerables en aplicaciones en su estado de funcionamiento. DAST prueba las interfaces HTTP y HTML expuestas de las aplicaciones web.
- **Moneda de código de terceros.** como parte del desarrollo de software con software de código abierto (OSS), debe tratar las vulnerabilidades de seguridad que pueden estar asociadas con cualquier OSS

incorporado en su producto. Esto es un esfuerzo continuo porque una nueva versión de OSS podría tener una vulnerabilidad recién descubierta reportada en cualquier momento.

- **Análisis de vulnerabilidades.** el propósito del análisis de vulnerabilidades es detectar vulnerabilidades de seguridad comunes y conocidas en los productos de NetApp antes de que se lancen a los clientes.
- * Pruebas de penetración.* la prueba de penetración es el proceso de evaluar un sistema, una aplicación web o una red para encontrar vulnerabilidades de seguridad que podrían ser explotadas por un atacante. Las pruebas de penetración (pruebas de Pen) en NetApp las realiza un grupo de empresas de terceros aprobadas y fiables. Su alcance de prueba incluye el lanzamiento de ataques contra una aplicación o software similar a intrusos hostiles o piratas informáticos que utilizan métodos o herramientas de explotación sofisticados.

Funciones de seguridad de los productos

Las herramientas de ONTAP para VMware vSphere incluyen las siguientes funciones de seguridad en cada versión.

- **Banner de inicio de sesión.** SSH está desactivado de forma predeterminada y sólo permite inicios de sesión de una vez si está activado desde la consola de VM. Se muestra el siguiente banner de inicio de sesión una vez que el usuario introduce un nombre de usuario en la solicitud de inicio de sesión:

  ADVERTENCIA: el acceso no autorizado a este sistema está prohibido y será procesado por ley. Al acceder a este sistema, acepta que sus acciones pueden supervisarse si se sospecha un uso no autorizado.

  Una vez que el usuario complete el inicio de sesión a través del canal SSH, se muestra el siguiente texto:

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Control de acceso basado en roles (RBAC).** dos tipos de controles RBAC están asociados con las herramientas ONTAP:
  - Privilegios nativos de vCenter Server
  - Privilegios específicos del plugin de vCenter. Para obtener más información, consulte "este enlace".
- **Canales de comunicaciones cifrados.** toda comunicación externa ocurre a través de HTTPS utilizando la versión 1.2 de TLS.
- **Exposición mínima del puerto.** sólo los puertos necesarios están abiertos en el firewall.

  En la siguiente tabla se describen los detalles de los puertos abiertos.

Puerto TCP v4/v6 #	Dirección	Función
8143	entrante	Conexiones HTTPS para la API de REST
8043	entrante	Conexiones HTTPS

Puerto TCP v4/v6 #	Dirección	Función
9060	entrante	Conexiones HTTPS Se utiliza para conexiones SOAP a través de https Este puerto se debe abrir para permitir que un cliente se conecte al servidor API de herramientas de ONTAP.
22	entrante	SSH (deshabilitado de forma predeterminada)
9080	entrante	Conexiones HTTPS - VP y SRA - conexiones internas sólo del bucle invertido
9083	entrante	Conexiones HTTPS: VP y SRA Se utiliza para conexiones SOAP a través de https
1162	entrante	VP paquetes de captura SNMP
1527	exclusivamente para uso interno	Puerto de base de datos Derby, sólo entre este equipo y él mismo, no se aceptan conexiones externas — sólo conexiones internas
443	bidireccional	Se utiliza para las conexiones a clústeres de ONTAP

- **Compatibilidad con certificados firmados por la entidad de certificación (CA).** las herramientas de ONTAP para VMware vSphere admiten certificados firmados por CA. Vea esto "artículo de base de conocimientos" si quiere más información.
- **Registro de auditoría.** los paquetes de soporte se pueden descargar y son extremadamente detallados. Las herramientas de ONTAP registran toda la actividad de inicio de sesión y cierre de sesión de los usuarios en un archivo de registro independiente. Las llamadas de API VASA se registran en un registro de auditoría de VASA dedicado (cxf.log local).
- **Políticas de contraseña.** se siguen las siguientes directivas de contraseñas:
  - Las contraseñas no han iniciado sesión en ningún archivo de registro.
  - Las contraseñas no se comunican en texto sin formato.
  - Las contraseñas se configuran durante el propio proceso de instalación.
  - El historial de contraseñas es un parámetro configurable.
  - La antigüedad mínima de la contraseña se establece en 24 horas.
  - El proceso de finalización automática de los campos de contraseña está desactivado.
  - Las herramientas de ONTAP cifran toda la información de credenciales almacenada mediante el hash SHA256.

Complemento de SnapCenter, VMware vSphere

La ingeniería de software del complemento SnapCenter de NetApp para VMware

vSphere utiliza las siguientes actividades de desarrollo seguro:

- **Modelado de amenazas.** el propósito del modelado de amenazas es descubrir defectos de seguridad en una característica, componente o producto al principio del ciclo de vida del desarrollo del software. Un modelo de amenaza es una representación estructurada de toda la información que afecta la seguridad de una aplicación. En esencia, es una visión de la aplicación y su entorno a través del objetivo de la seguridad.
- **Pruebas de seguridad de aplicaciones dinámicas (DAST).** Tecnologías diseñadas para detectar condiciones vulnerables en aplicaciones en estado en ejecución. DAST prueba las interfaces HTTP y HTML expuestas de las aplicaciones web.
- **Moneda de código de terceros.** como parte del desarrollo de software y el uso de software de código abierto (OSS), es importante abordar las vulnerabilidades de seguridad que pueden estar asociadas con OSS que se han incorporado a su producto. Se trata de un esfuerzo continuo, ya que la versión del componente OSS puede tener una vulnerabilidad recién descubierta reportada en cualquier momento.
- **Análisis de vulnerabilidades.** el propósito del análisis de vulnerabilidades es detectar vulnerabilidades de seguridad comunes y conocidas en los productos de NetApp antes de que se lancen a los clientes.
- * Pruebas de penetración.* la prueba de penetración es el proceso de evaluar un sistema, una aplicación web o una red para encontrar vulnerabilidades de seguridad que podrían ser explotadas por un atacante. Las pruebas de penetración (pruebas de Pen) en NetApp las realiza un grupo de empresas de terceros aprobadas y fiables. El alcance de su prueba incluye el lanzamiento de ataques contra una aplicación o software como intrusos hostiles o hackers que utilizan métodos o herramientas de explotación sofisticados.
- * Actividad de respuesta a incidentes de seguridad de los productos.* Las vulnerabilidades de seguridad se detectan tanto interna como externamente en la empresa y pueden representar un riesgo grave para la reputación de NetApp si no se tratan de manera puntual. Para facilitar este proceso, un equipo de respuesta a incidentes de seguridad de productos (PSIRT) informa y realiza un seguimiento de las vulnerabilidades.

Funciones de seguridad de los productos

El plugin de SnapCenter de NetApp para VMware vSphere incluye las siguientes funciones de seguridad en cada versión:

- **Acceso restringido al shell.** SSH está desactivado de forma predeterminada, y sólo se permiten inicios de sesión una vez si están habilitados desde la consola de VM.
- **Advertencia de acceso en el banner de inicio de sesión.** se muestra el siguiente banner de inicio de sesión después de que el usuario introduzca un nombre de usuario en el indicador de inicio de sesión:

  ADVERTENCIA: el acceso no autorizado a este sistema está prohibido y será procesado por ley. Al acceder a este sistema, acepta que sus acciones pueden supervisarse si se sospecha un uso no autorizado.

  Una vez que el usuario completa el inicio de sesión a través del canal SSH, se muestra la siguiente salida:

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Control de acceso basado en roles (RBAC).** dos tipos de controles RBAC están asociados con las herramientas ONTAP:
  - Privilegios nativos de vCenter Server.
  - Privilegios específicos del complemento de VMware vCenter. Para obtener más información, consulte "Control de acceso basado en roles (RBAC)".
- **Canales de comunicaciones cifrados.** toda comunicación externa ocurre a través de HTTPS utilizando TLS.
- **Exposición mínima del puerto.** sólo los puertos necesarios están abiertos en el firewall.

En la siguiente tabla se proporcionan los detalles de los puertos abiertos.

Número de puerto TCP v4/v6	Función
8144	Conexiones HTTPS para la API de REST
8080	Conexiones HTTPS para interfaz gráfica de usuario de OVA
22	SSH (deshabilitado de forma predeterminada)
3306	MySQL (sólo conexiones internas; las conexiones externas están deshabilitadas de forma predeterminada)
443	Nginx (servicios de protección de datos)

- **Compatibilidad con certificados firmados por entidad de certificación (CA).** el plugin de SnapCenter para VMware vSphere es compatible con la función de certificados firmados por CA. Consulte "Cómo crear o importar un certificado SSL al plugin de SnapCenter para VMware vSphere (SCV)".
- **Políticas de contraseña.** las siguientes directivas de contraseñas están en vigor:
  - Las contraseñas no han iniciado sesión en ningún archivo de registro.
  - Las contraseñas no se comunican en texto sin formato.
  - Las contraseñas se configuran durante el propio proceso de instalación.
  - Toda la información de credenciales se almacena mediante el hash SHA256.
- **Imagen del sistema operativo base.** el producto se entrega con el SO base Debian para OVA con acceso restringido y acceso al shell desactivado. Esto reduce el espacio necesario para los ataques. Todos los sistemas operativos base de la versión SnapCenter se actualizan con los parches de seguridad más recientes disponibles para obtener la máxima cobertura de seguridad.

NetApp desarrolla funciones de software y parches de seguridad con respecto al dispositivo del plugin de SnapCenter para VMware vSphere y, a continuación, se los libera a los clientes como una plataforma de software integrada. Dado que estos dispositivos incluyen dependencias específicas de sistemas suboperativos

de Linux y nuestro software exclusivo, NetApp recomienda no realizar cambios en el sistema operativo de subsistema, ya que esto tiene un gran potencial para afectar al dispositivo de NetApp. Esto podría afectar a la capacidad de NetApp para dar soporte al dispositivo. NetApp recomienda probar e implementar nuestra última versión de código para los dispositivos, ya que se los publica para resolver cualquier problema relacionado con la seguridad.

Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere

Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere 9,13

La guía de refuerzo de la seguridad para herramientas de ONTAP para VMware vSphere proporciona un conjunto completo de instrucciones para configurar los ajustes más seguros.

Estas guías se aplican tanto a las aplicaciones como al sistema operativo «guest» del propio dispositivo.

Verificación de la integridad de las herramientas de ONTAP para los paquetes de instalación de VMware vSphere 9,13

Existen dos métodos disponibles para que los clientes verifiquen la integridad de sus paquetes de instalación de herramientas de ONTAP.

1. Verificando las sumas de comprobación
2. Verificando la firma

Las sumas de comprobación se proporcionan en las páginas de descarga de los paquetes de instalación de OTV. Los usuarios deben verificar las sumas de comprobación de los paquetes descargados con la suma de comprobación proporcionada en la página de descarga.

Verificación de la firma del OVA de herramientas de ONTAP

El paquete de instalación de vApp se entrega en forma de tarball. Este tarball contiene certificados intermedios y raíz para el dispositivo virtual junto con un archivo README y un paquete OVA. El archivo README guía a los usuarios sobre cómo verificar la integridad del paquete OVA vApp.

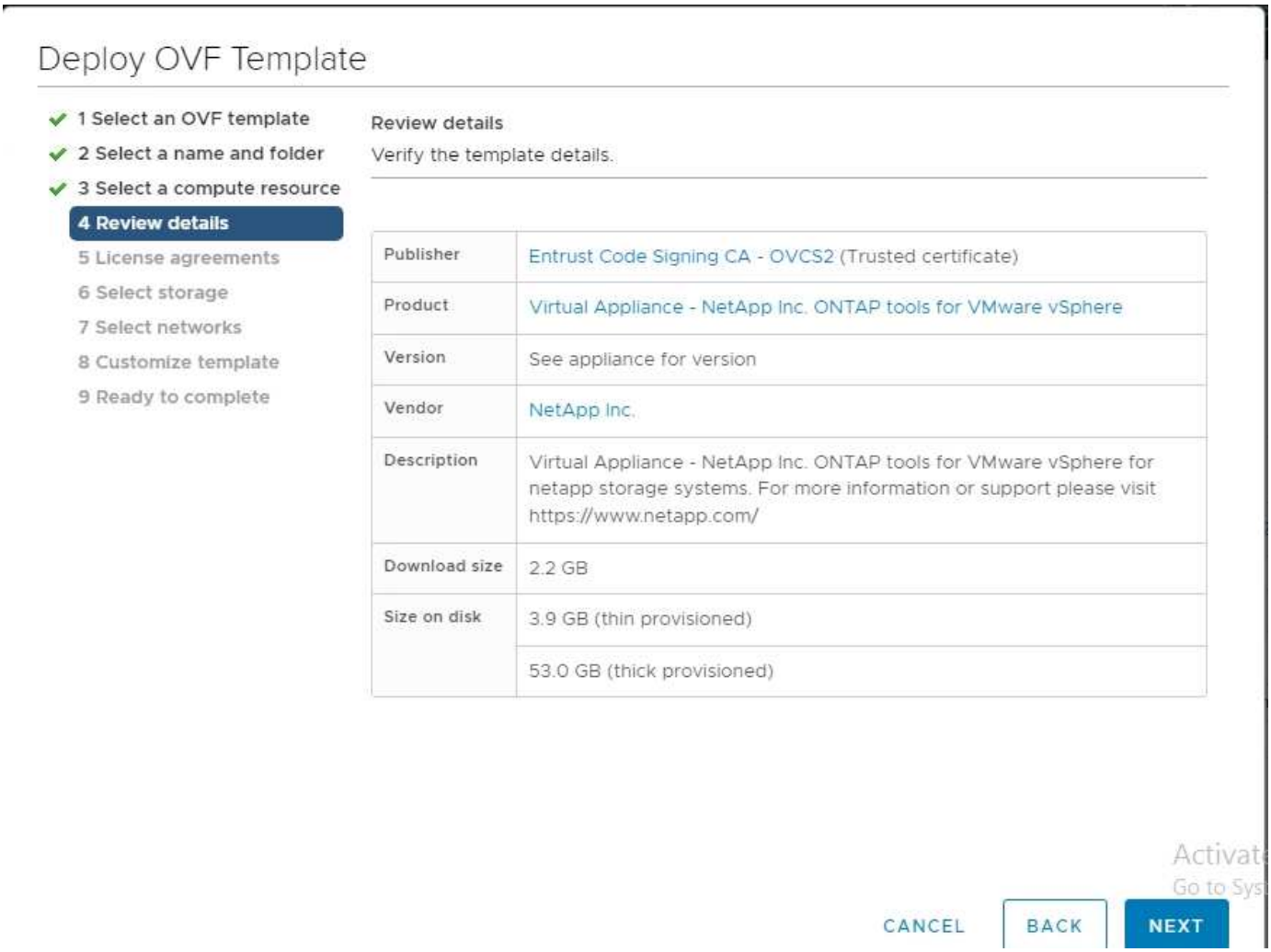
Los clientes también deben cargar el certificado raíz e intermedio proporcionado en la versión 7.0U3E de vCenter y versiones posteriores. Para versiones de vCenter entre 7.0.1 y 7,0.U3E, la funcionalidad de verificación del certificado no es compatible con VMware. Los clientes no deberán cargar ningún certificado para las versiones de vCenter 6.x.

Cargar el certificado raíz de confianza en vCenter

1. Inicie sesión con VMware vSphere Client en vCenter Server.
2. Especifique el nombre de usuario y la contraseña de administrator@vsphere.local u otro miembro del grupo Administradores de inicio de sesión único de vCenter. Si especificó un dominio diferente durante la instalación, inicie sesión como administrator@mydomain.
3. Desplácese hasta la IU de gestión de certificados: a. En el menú Inicio, seleccione Administración. b. En Certificados, haga clic en Gestión de certificados.

4. Si el sistema le solicita, introduzca las credenciales de vCenter Server.
5. En Certificados raíz de confianza, haga clic en Agregar.
6. Haga clic en Examinar y seleccione la ubicación del archivo .pem del certificado (OTV_OVA_INTER_ROOT_CERT_CHAIN.pem).
7. Haga clic en Añadir. El certificado se agrega a la tienda.

Consulte "Agregue un certificado raíz de confianza al almacén de certificados" si quiere más información. Al implementar una vApp (mediante el archivo OVA), la firma digital del paquete vApp se puede verificar en la página 'Detalles de revisión'. Si el paquete vApp descargado es genuino, la columna 'Publisher' muestra 'Trusted Certificate' (Certificado de confianza) (como en la siguiente captura de pantalla).



Verificación de la firma de las herramientas de ONTAP ISO y SRA tar.gz

NetApp comparte su certificado de firma de código con los clientes en la página de descarga del producto, junto con los archivos zip del producto para OTV-iso y sra.tgz.

Del certificado de firma de código, los usuarios pueden extraer la clave pública de la siguiente manera:

```
 #> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-
key name>
A continuación, se debe utilizar la clave pública para verificar la firma
para iso y el zip del producto tgz como se muestra a continuación:
```

```
 #> openssl dgst -sha256 -verify <public-key> -signature <signature-file>
<binary-name>
Ejemplo:
```

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-
for-vmware-vsphere-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-
vsphere-9.12-upgrade.iso
Verified OK  => response
```

Puertos y protocolos para las herramientas de ONTAP 9,13

A continuación se muestran los puertos y protocolos necesarios que permiten la comunicación entre herramientas de ONTAP para el servidor VMware vSphere y otras entidades como sistemas de almacenamiento gestionados, servidores y otros componentes.

Puertos de entrada y salida necesarios para OTV

Observe la siguiente tabla en la que se enumeran los puertos de entrada y salida necesarios para el correcto funcionamiento de las herramientas de ONTAP. Es importante asegurarse de que solo los puertos mencionados en la tabla estén abiertos para las conexiones de máquinas remotas, mientras que todos los demás puertos deben estar bloqueados para las conexiones de máquinas remotas. Esto ayudará a garantizar la seguridad de su sistema.

En la siguiente tabla se describen los detalles de los puertos abiertos.

Puerto TCP v4/v6 #	Dirección	Función
8143	entrante	Conexiones HTTPS para la API de REST
8043	entrante	Conexiones HTTPS
9060	entrante	Conexiones HTTPS Se utiliza para conexiones SOAP a través de HTTPS Este puerto se debe abrir para permitir que un cliente se conecte al servidor API de herramientas de ONTAP.
22	entrante	SSH (deshabilitado de forma predeterminada)

Puerto TCP v4/v6 #	Dirección	Función
9080	entrante	Conexiones HTTPS - VP y SRA - conexiones internas sólo del bucle invertido
9083	entrante	Conexiones HTTPS - VP y SRA Se utiliza para conexiones SOAP a través de HTTPS
1162	entrante	VP paquetes de captura SNMP
8443	entrante	Complemento remoto
1527	exclusivamente para uso interno	Puerto de base de datos Derby, solo entre este equipo y él mismo, conexiones externas no aceptadas — Solo conexiones internas
8150	exclusivamente para uso interno	El servicio de integridad de log se ejecuta en el puerto
443	bidireccional	Se utiliza para las conexiones a clústeres de ONTAP

Control del acceso remoto a la base de datos Derby

Los administradores pueden acceder a la base de datos derby con los siguientes comandos. Se puede acceder a él a través de las herramientas de ONTAP VM local, así como a un servidor remoto con los siguientes pasos:

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
connect 'jdbc:derby://<OTV-
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

Ejemplo:

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
ij version 10.15
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=[redacted]';
ij> show tables;
TABLE_SCHEM         |TABLE_NAME                    |REMARKS
------------------------------------------------------------------------
SYS                 |SYSALIASES                    |
SYS                 |SYSCHECKS                     |
SYS                 |SYSCOLPERMS                   |
SYS                 |SYSCOLUMNS                    |
SYS                 |SYSCONGLOMERATES              |
SYS                 |SYSCONSTRAINTS                |
SYS                 |SYSDEPENDS                    |
SYS                 |SYSFILES                      |
SYS                 |SYSFOREIGNKEYS                |
SYS                 |SYSKEYS                       |
SYS                 |SYSPERMS                      |
```

Herramientas de ONTAP para puntos de acceso de VMware vSphere 9,13 (usuarios)

La instalación de ONTAP Tools para VMware vSphere crea y utiliza tres tipos de usuarios:

1. Usuario del sistema: La cuenta de usuario raíz

2. Usuario de la aplicación: El usuario administrador, el usuario de mantenimiento y las cuentas de usuario de base de datos
3. Usuario de soporte: La cuenta de usuario diag

1. Usuario del sistema

El usuario System(root) se crea mediante la instalación de herramientas de ONTAP en el sistema operativo subyacente (Debian).

- Un usuario predeterminado del sistema “root” se crea en Debian mediante la instalación de herramientas de ONTAP. Su valor predeterminado está desactivado y se puede activar de forma ad hoc a través de la consola 'antigua'.

2. Usuario de la aplicación

El usuario de la aplicación se denomina usuario local en las herramientas de ONTAP. Se trata de usuarios creados en la aplicación de herramientas de ONTAP. La siguiente tabla muestra los tipos de usuarios de la aplicación:

Usuario	Descripción
Usuario administrador	Se crea durante la instalación de las herramientas de ONTAP y el usuario proporciona las credenciales al implementar las herramientas de ONTAP. Los usuarios tienen la opción de cambiar la 'contraseña' en 'consola antigua'. La contraseña caducará en 90 días y se espera que los usuarios cambien la misma.
Usuario de mantenimiento	Se crea durante la instalación de las herramientas de ONTAP y el usuario proporciona las credenciales al implementar las herramientas de ONTAP. Los usuarios tienen la opción de cambiar la 'contraseña' en 'consola antigua'. Se trata de un usuario de mantenimiento y se crea para ejecutar las operaciones de la consola de mantenimiento.
Usuario de base de datos	Se crea durante la instalación de las herramientas de ONTAP y el usuario proporciona las credenciales al implementar las herramientas de ONTAP. Los usuarios tienen la opción de cambiar la 'contraseña' en 'consola antigua'. La contraseña caducará en 90 días y se espera que los usuarios cambien la misma.

3. Usuario de apoyo (usuario diag)

Durante la instalación de las herramientas de ONTAP, se crea un usuario de soporte. Este usuario se puede utilizar para acceder a las herramientas de ONTAP en caso de cualquier problema o interrupción en el servidor y para recopilar registros. De forma predeterminada, este usuario está desactivado, pero se puede activar de forma específica a través de la consola 'antigua'. Es importante tener en cuenta que este usuario se desactivará automáticamente después de un período de tiempo determinado.

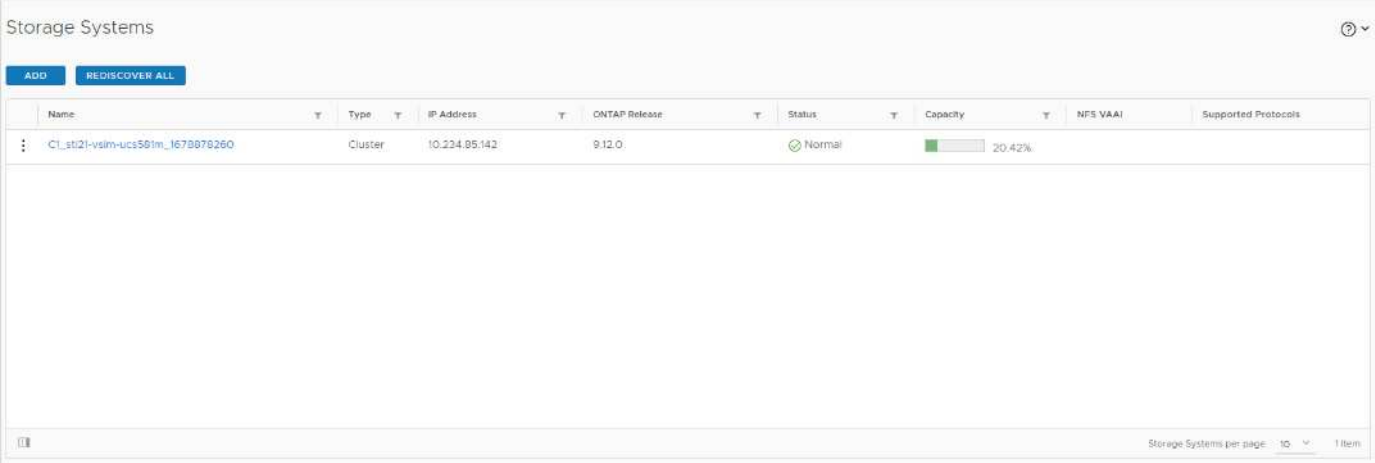
ONTAP TOOLS 9,13 TLS mutuo (autenticación basada en certificados)

Las versiones 9,7 y posteriores de ONTAP admiten la comunicación TLS mutua. A partir de ONTAP Tools para VMware y vSphere 9,12, el TLS mutuo se utiliza para la comunicación con clústeres recién añadidos (según la versión de ONTAP).

ONTAP

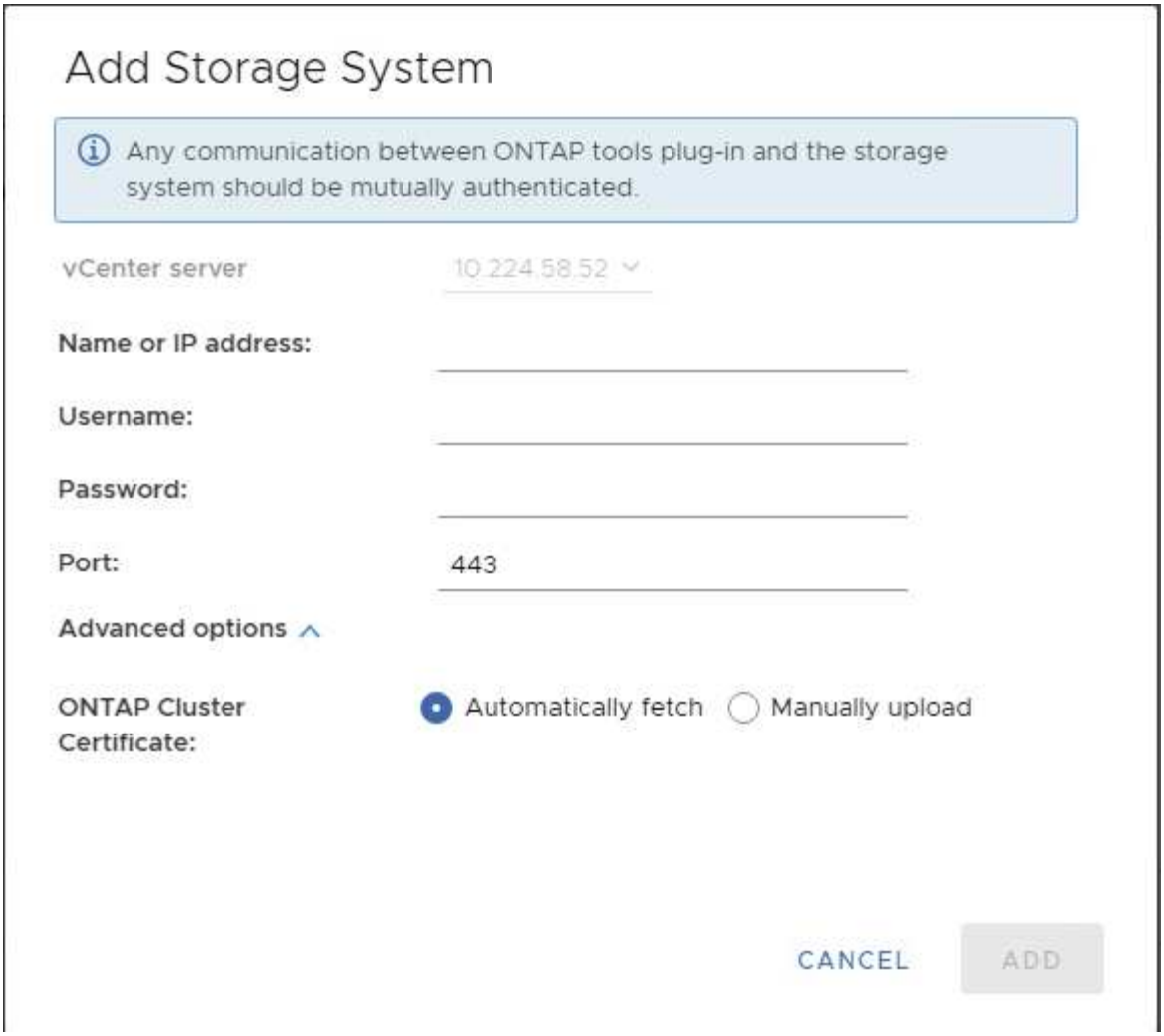
Para todos los sistemas de almacenamiento añadidos anteriormente: Durante una actualización, todos los sistemas de almacenamiento añadidos se volverán de confianza automáticamente y se configurarán los mecanismos de autenticación basados en certificados.

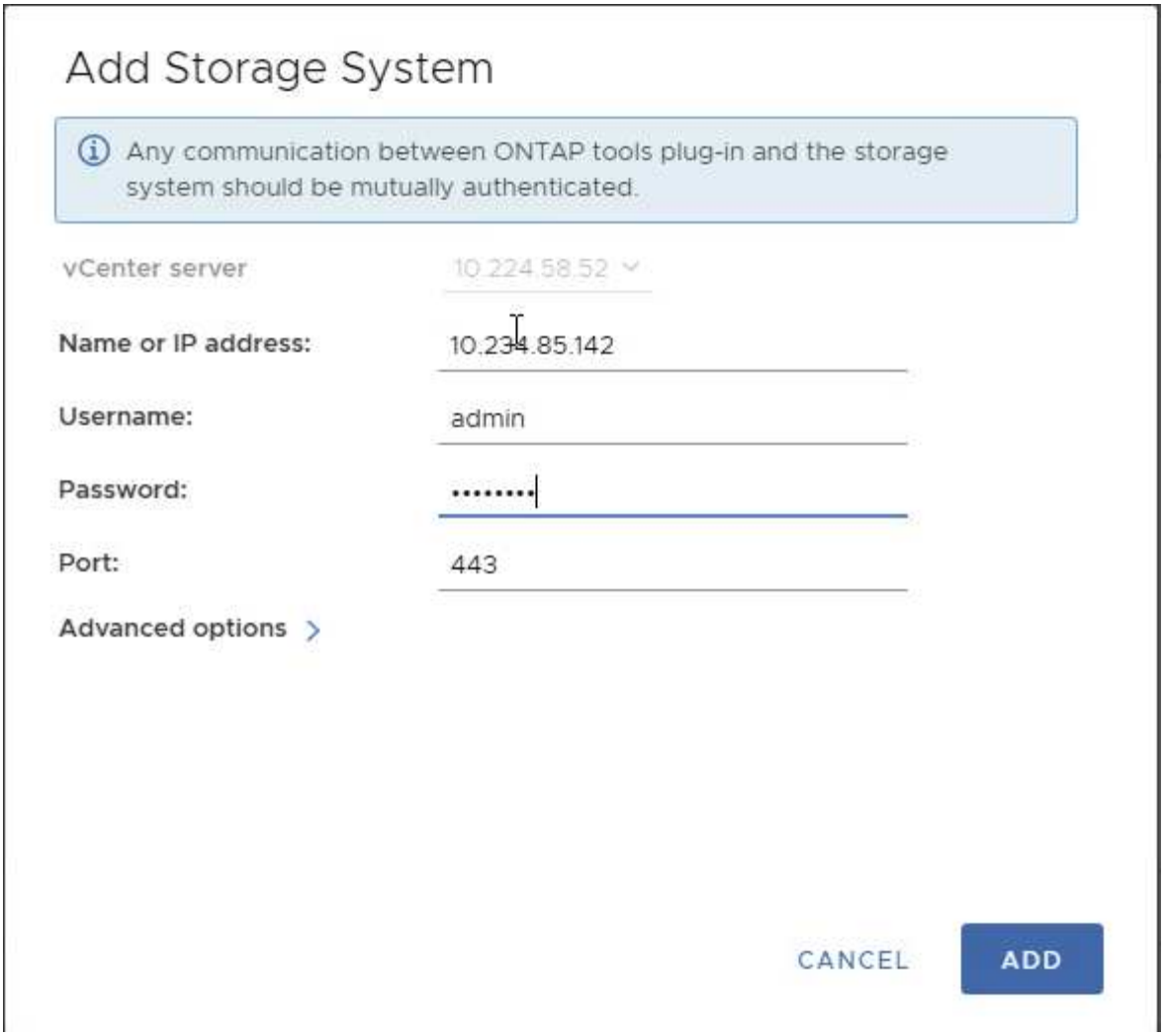
Como en la siguiente captura de pantalla, la página de configuración del clúster mostrará el estado de TLS mutuo (autenticación basada en certificado), configurado para cada clúster.

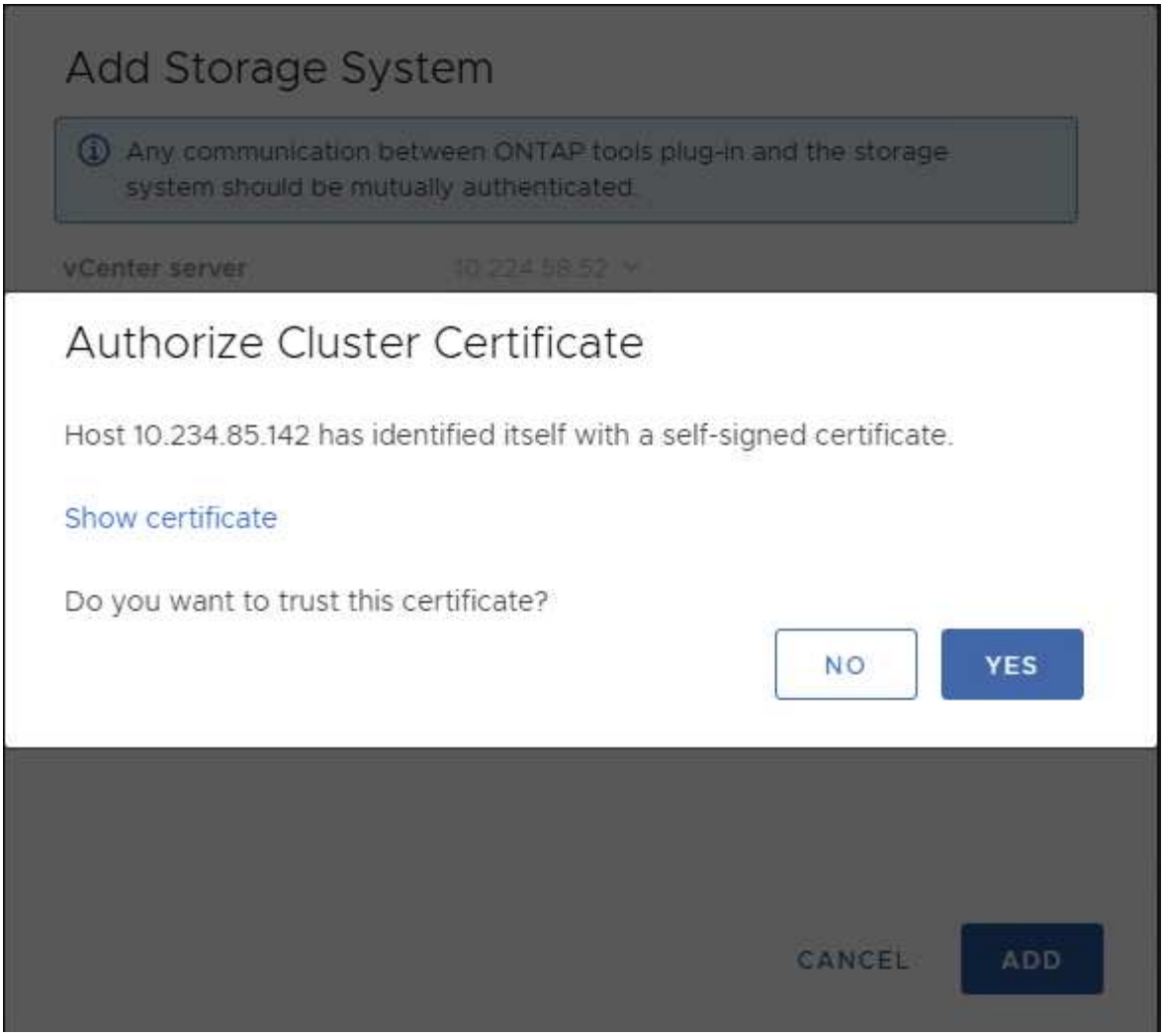


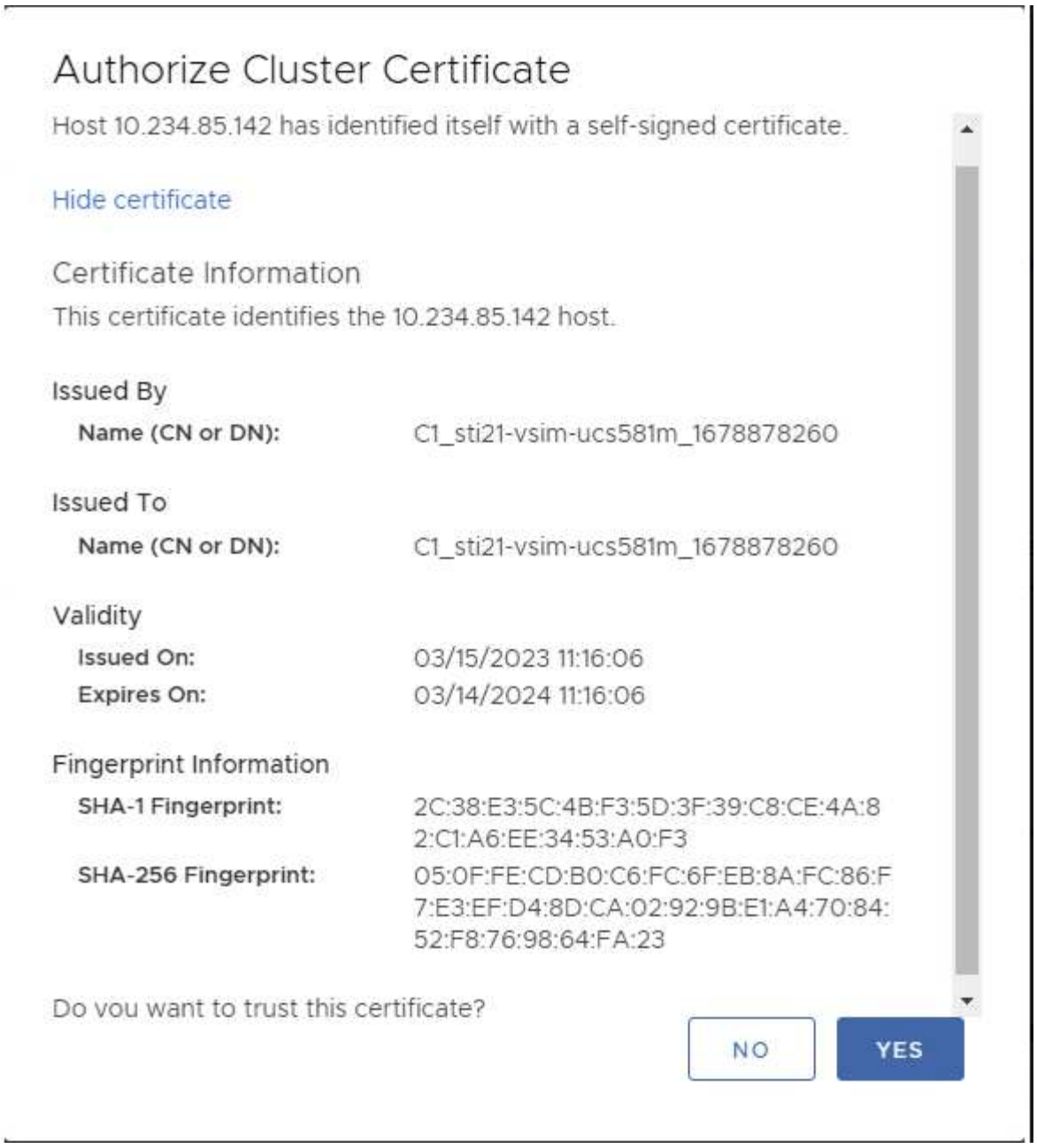
Cluster Add

Durante el flujo de trabajo de agregación de clústeres, si el clúster que se agrega admite MTLS, MTLS se configurará de forma predeterminada. El usuario no necesita realizar ninguna configuración para esto. La siguiente captura de pantalla muestra la pantalla presentada al usuario durante la adición del clúster.


Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
10.224.58.52
Name or IP address:
Username:
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
ADD


Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
10.224.58.52
Name or IP address:
10.234.85.142
Username:
admin
Password:
Port:
443
Advanced options
CANCEL
ADD

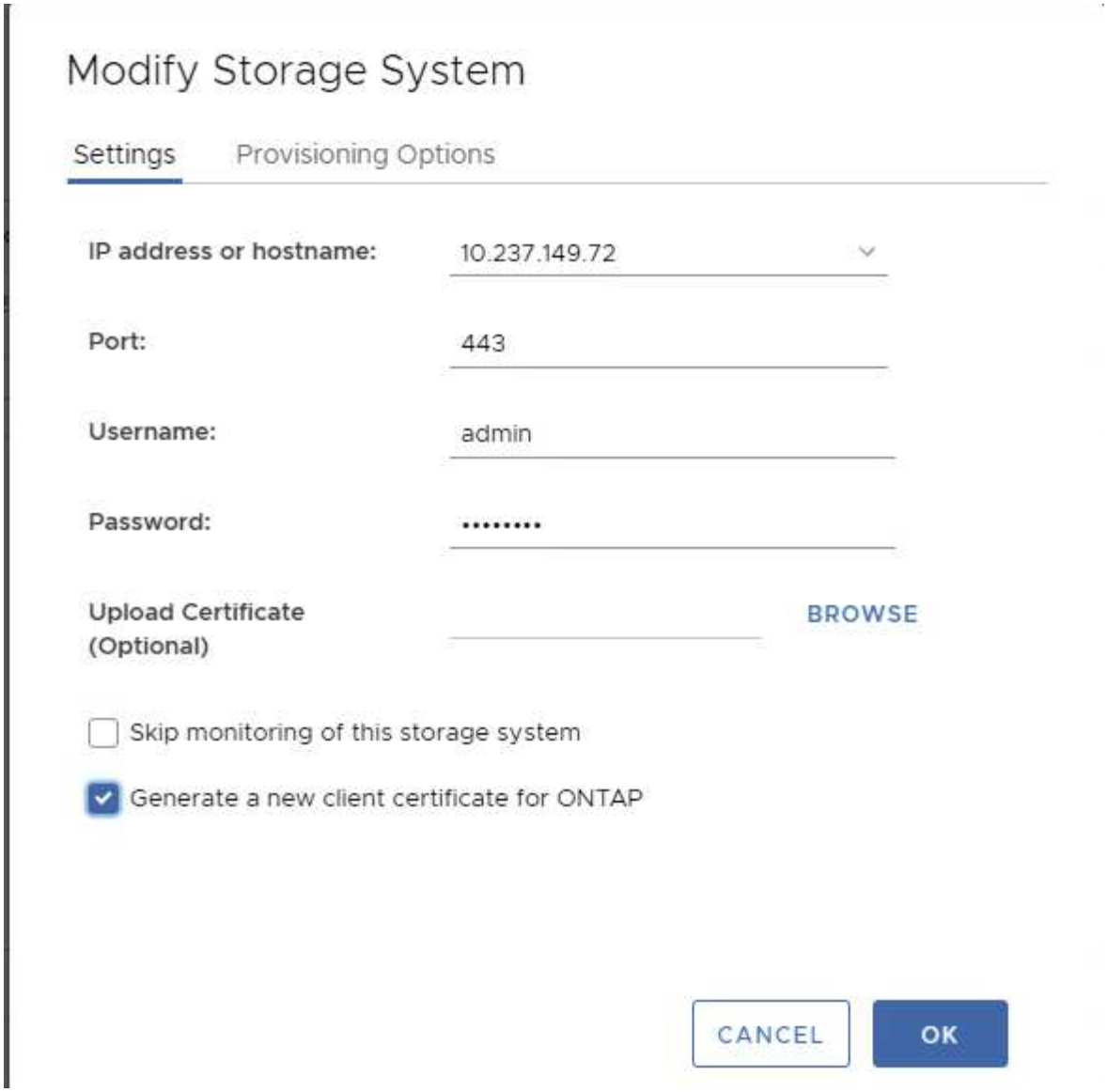

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
ADD

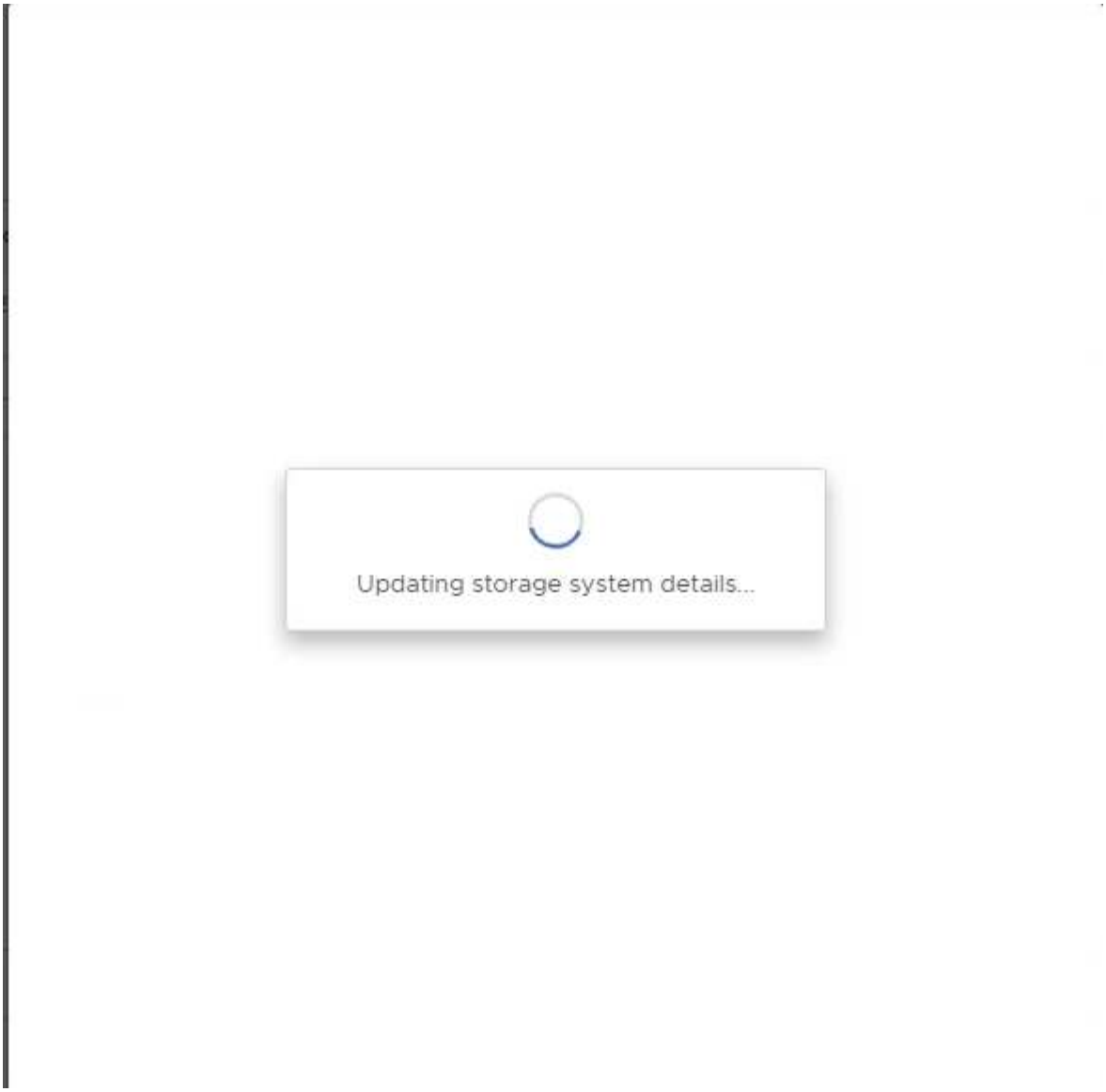


Edición de clúster

Durante la operación de edición del clúster, existen dos situaciones:

- Si el certificado ONTAP caduca, el usuario tendrá que obtener el nuevo certificado y cargarlo.
- Si el certificado OTV caduca, el usuario puede regenerarlo marcando la casilla de verificación.
  - *Generar un nuevo certificado de cliente para ONTAP.*


Modify Storage System
Settings
Provisioning Options
IP address or hostname:
10.237.149.72
Port:
443
Username:
admin
Password:
Upload Certificate (Optional)
BROWSE
Skip monitoring of this storage system
Generate a new client certificate for ONTAP
CANCEL
OK



Certificado HTTPS de ONTAP TOOLS 9,13

De manera predeterminada, las herramientas de ONTAP utilizan un certificado autofirmado que se crea automáticamente durante la instalación para proteger el acceso HTTPS a la interfaz de usuario web. Las herramientas de ONTAP ofrecen las siguientes funciones:

1. Regenerar certificado HTTPS

Durante la instalación de las herramientas de ONTAP, se instala un certificado de CA HTTPS y el certificado se almacena en el almacén de claves. El usuario tiene la opción de regenerar el certificado HTTPS a través de la consola de mantenimiento.

Se puede acceder a las opciones anteriores en la consola *maint* navegando a *'Configuración de la aplicación' → 'Volver a generar certificados'.*

Banner de inicio de sesión de ONTAP tools 9,13

Se muestra el siguiente banner de inicio de sesión después de que el usuario introduce un nombre de usuario en la pantalla de inicio de sesión. Tenga en cuenta que SSH está deshabilitado de forma predeterminada y solo permite inicios de sesión de una vez cuando se habilita desde la consola de VM.

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

Una vez que el usuario completa el inicio de sesión a través del canal SSH, se muestra el siguiente texto:

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

Tiempo de espera de inactividad para las herramientas de ONTAP 9,13

Para evitar el acceso no autorizado, se configura un tiempo de espera de inactividad, que cierra automáticamente la sesión de los usuarios inactivos durante un cierto período mientras se utilizan los recursos autorizados. Esto garantiza que solo los usuarios autorizados puedan acceder a los recursos y ayuda a mantener la seguridad.

- De forma predeterminada, las sesiones de vSphere Client se cierran tras 120 minutos de tiempo inactivo, lo cual requiere que el usuario inicie sesión nuevamente para reanudarse usando el cliente. Puede cambiar el valor de tiempo de espera editando el archivo webclient.properties. Puede configurar el tiempo de espera de vSphere Client "Configure el valor de tiempo de espera del cliente de vSphere"
- Las herramientas de ONTAP tienen un tiempo de cierre de sesión de la cli web de 30 minutos.

Número máximo de solicitudes simultáneas por usuario (protección de seguridad de red/ataque DOS) herramientas de ONTAP para VMware vSphere 9,13

Por defecto, el Núm. Máximo de solicitudes simultáneas por usuario es 48. El usuario root en las herramientas de ONTAP puede cambiar este valor en función de los requisitos de su entorno. **Este valor no debe establecerse en un valor muy alto, ya**

que proporciona un mecanismo contra ataques de denegación de servicio (DoS).

Los usuarios pueden modificar el número máximo de sesiones simultáneas y otros parámetros admitidos en el archivo ***/opt/netapp/vscserver/etc/dosfilterParams.json***.

Podemos configurar el filtro con los siguientes parámetros:

- ***delayMs***: El retraso en milisegundos dado a todas las solicitudes por encima del límite de tasa antes de que sean consideradas. Dar -1 para rechazar la solicitud.
- ***throttleMs***: Cuánto tiempo esperar el semáforo de forma asíncrona.
- ***maxRequestMs***: Cuánto tiempo se debe permitir que se ejecute esta solicitud.
- ***ipWhitelist***: Una lista separada por comas de direcciones IP que no se limitará la tasa. (Pueden ser IP de vCenter, ESXi y SRA)
- ***maxRequestsPerSec***: El número máximo de solicitudes de una conexión por segundo.

Valores predeterminados en el archivo *dosfilterParams*:

```
{"delayMs":"-1",
"throttleMs":"1800000",
"maxRequestMs":"300000",
"ipWhitelist":"10.224.58.52",
"maxRequestsPerSec":"48"}
```

Configuración del Protocolo de hora de red (NTP) para las herramientas ONTAP 9,13

A veces, pueden producirse problemas de seguridad debido a discrepancias en las configuraciones de tiempo de red. Es importante asegurarse de que todos los dispositivos dentro de una red tengan una configuración de tiempo precisa para evitar tales problemas.

Dispositivo virtual

Puede configurar los servidores NTP desde la consola de mantenimiento del dispositivo virtual. Los usuarios pueden agregar los detalles del servidor NTP en *Configuración del sistema* ⇒ *Agregar nuevo servidor NTP* opción

De forma predeterminada, el servicio para NTP es ntpd. Este es un servicio heredado y no funciona bien para máquinas virtuales en ciertos casos.

Debian

En Debian, el usuario puede acceder al archivo /etc/ntp.conf para obtener los detalles del servidor ntp.

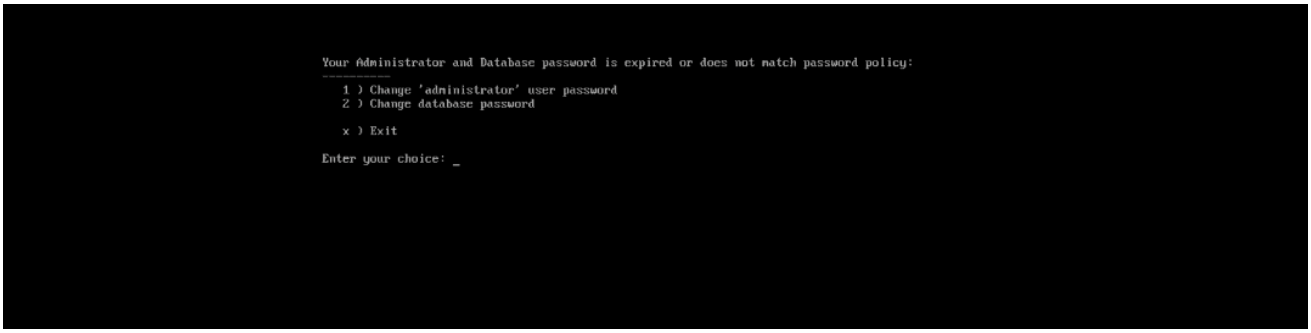
Políticas de contraseñas para las herramientas de ONTAP 9,13

Los usuarios que implementen las herramientas de ONTAP por primera vez o que actualicen a la versión 9,12 o posterior deberán seguir la política de contraseñas seguras

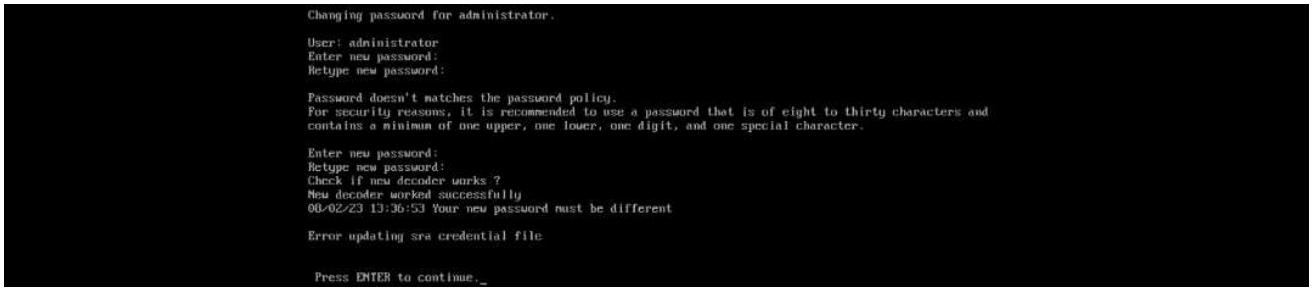
tanto para el administrador como para los usuarios de la base de datos. Durante el proceso de implementación, se solicitará a los nuevos usuarios que introduzcan sus contraseñas. Para los usuarios de brownfield que actualicen a la versión 9,12 o posterior, la opción de seguir la política de contraseñas seguras estará disponible en la consola de mantenimiento.

- Una vez que el usuario inicia sesión en la consola de mantenimiento, las contraseñas se verificarán con respecto al conjunto de reglas complejo y, si se detecta que no se siguen, se solicitará al usuario que restablezca la misma.
- La validez predeterminada de la contraseña es de 90 días y después de 75 días el usuario comenzará a recibir la notificación para cambiar la contraseña.
- Es necesario establecer una nueva contraseña en cada ciclo, el sistema no tomará la última contraseña como nueva contraseña.
- Cada vez que un usuario inicia sesión en la consola de mantenimiento, comprobará las políticas de contraseñas como las siguientes capturas de pantalla antes de cargar el menú principal:

- Si no sigue la política de contraseñas o su configuración de actualización desde las herramientas de ONTAP 9,11 o anteriores. A continuación, el usuario verá la siguiente pantalla para restablecer la contraseña:



- Si el usuario intenta establecer una contraseña débil o da la última contraseña de nuevo, el usuario verá el siguiente error:


Changing password for administrator.
User: administrator
Enter new password:
Retype new password:
Password doesn't matches the password policy.
For security reasons, it is recommended to use a password that is of eight to thirty characters and
contains a minimum of one upper, one lower, one digit, and one special character.
Enter new password:
Retype new password:
Check if new decoder works ?
New decoder worked successfully
08/02/23 13:36:53 Your new password must be different
Error updating sra credential file
Press ENTER to continue._

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

ONTAP

"Aviso para ONTAP 9.16.1" "Aviso para ONTAP 9.16.0" "Aviso para ONTAP 9.15.1" "Aviso para ONTAP 9.15.0" "Aviso para ONTAP 9.14.1" "Aviso para ONTAP 9.14.0" "Aviso para ONTAP 9.13.1" "Aviso para ONTAP 9.12.1" "Aviso para ONTAP 9.12.0" "Aviso para ONTAP 9.11.1" "Aviso para ONTAP 9.10.1" "Aviso para ONTAP 9.10.0" "Aviso para ONTAP 9.9.1" "Aviso para ONTAP 9.8" "Aviso para ONTAP 9,7" "Aviso para ONTAP 9,6" "Aviso para ONTAP 9,5" "Aviso para ONTAP 9,4" "Aviso para ONTAP 9,3" "Aviso para ONTAP 9,2" "Aviso para ONTAP 9,1"

Mediador de ONTAP para configuraciones IP de MetroCluster

"9.9.1 Aviso para Mediador ONTAP para configuraciones IP de MetroCluster" "9,8 Aviso para Mediador ONTAP para configuraciones IP de MetroCluster" "9,7 Aviso para Mediador ONTAP para configuraciones IP de MetroCluster"

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.