Replique y proteja datos

Cloud Manager 3.7

NetApp
October 23, 2024

This PDF was generated from https://docs.netapp.com/es-es/occm37/task_discovering_ontap.html on October 23, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Replique y proteja datos

Detectar y gestionar clústeres de ONTAP

Cloud Manager puede detectar los clústeres de ONTAP en su entorno local, en una configuración de almacenamiento privado de NetApp y en IBM Cloud. La detección de estos clústeres le permite replicar datos fácilmente en su entorno de cloud híbrido directamente desde Cloud Manager.

Detección de clústeres de ONTAP

Detectar un clúster de ONTAP en Cloud Manager le permite aprovisionar almacenamiento y replicar datos en el cloud híbrido.

Antes de empezar

Debe tener la dirección IP de gestión del clúster y la contraseña de la cuenta de usuario administrador para añadir el clúster a Cloud Manager.

Cloud Manager detecta los clústeres de ONTAP mediante HTTPS. Si utiliza directivas de firewall personalizadas, deben cumplir los siguientes requisitos:

- El host de Cloud Manager debe permitir el acceso HTTPS de salida a través del puerto 443.

  Si Cloud Manager se encuentra en AWS, el grupo de seguridad predefinido permite todas las comunicaciones salientes.

- El clúster ONTAP debe permitir el acceso HTTPS de entrada a través del puerto 443.

  La política de firewall "mgmt" predeterminada permite el acceso HTTPS entrante desde todas las direcciones IP. Si modificó esta política predeterminada o si creó su propia política de firewall, debe asociar el protocolo HTTPS con esa política y habilitar el acceso desde el host de Cloud Manager.

Pasos

1. En la página entornos de trabajo, haga clic en **descubrir** y seleccione **clúster ONTAP**.
2. En la página **Detalles del clúster ONTAP**, introduzca la dirección IP de administración del clúster, la contraseña de la cuenta de usuario administrador y la ubicación del clúster.

3. En la página Detalles, introduzca un nombre y una descripción para el entorno de trabajo y, a continuación, haga clic en **Ir**.

Resultado

Cloud Manager detecta el clúster. Ahora puede crear volúmenes, replicar datos a y desde el clúster, y ejecutar System Manager de OnCommand para realizar tareas avanzadas.

Aprovisionar volúmenes en clústeres de ONTAP

Cloud Manager le permite aprovisionar volúmenes NFS y CIFS en clústeres de ONTAP.

Antes de empezar

Debe configurarse NFS o CIFS en el clúster. Puede configurar NFS y CIFS con System Manager o la CLI.

Acerca de esta tarea

Es posible crear volúmenes en agregados existentes. No se pueden crear agregados nuevos desde Cloud Manager.

Pasos

1. En la página Working Environments, haga doble clic en el nombre del clúster de ONTAP en el que desea aprovisionar los volúmenes.
2. Haga clic en **Añadir nuevo volumen**.
3. En la página Crear nuevo volumen, introduzca los detalles del volumen y, a continuación, haga clic en **Crear**.

   Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Tamaño	El tamaño máximo que puede introducir depende en gran medida de si habilita thin provisioning, lo que le permite crear un volumen que sea mayor que el almacenamiento físico que hay disponible actualmente.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, Cloud Manager introduce un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también denominados listas de control de acceso o ACL). Es posible especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de Windows de dominio, debe incluir el dominio del usuario con el formato domain\username.
Perfil de uso	Los perfiles de uso definen las funciones de eficiencia del almacenamiento de NetApp habilitadas para un volumen.
Política de Snapshot	Una política de copia de Snapshot especifica la frecuencia y el número de copias de Snapshot de NetApp creadas automáticamente. Una copia snapshot de NetApp es una imagen del sistema de archivos puntual que no afecta al rendimiento y requiere un almacenamiento mínimo. Puede elegir la directiva predeterminada o ninguna. Es posible que no elija ninguno para los datos transitorios: Por ejemplo, tempdb para Microsoft SQL Server.

Replicación de datos entre sistemas

Puede replicar datos entre entornos de trabajo eligiendo una replicación de datos única para la transferencia de datos, o una programación recurrente para la recuperación ante desastres o la retención a largo plazo. Por ejemplo, puede configurar la replicación de datos desde un sistema ONTAP en las instalaciones a Cloud Volumes ONTAP para la recuperación ante desastres.

Cloud Manager simplifica la replicación de datos entre volúmenes en sistemas independientes con tecnologías SnapMirror y SnapVault. Solo tiene que identificar el volumen de origen y el de destino y, a continuación, elegir una programación y una política de replicación. Cloud Manager compra los discos necesarios, configura las relaciones, aplica la política de replicación y, a continuación, inicia la transferencia básica entre los volúmenes.

La transferencia básica incluye una copia completa de los datos de origen. Las transferencias posteriores contienen copias diferenciales de los datos de origen.

Requisitos de replicación de datos

Antes de poder replicar datos, debe confirmar que se cumplen requisitos específicos tanto para los sistemas Cloud Volumes ONTAP como para los clústeres de ONTAP.

Requisitos de versión

Debe verificar que los volúmenes de origen y destino ejecutan versiones de ONTAP compatibles antes de replicar los datos. Para obtener más detalles, consulte "Guía completa de protección de datos".

Requisitos específicos de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida necesarias: Específicamente, reglas para ICMP y los puertos 10000, 11104 y 11105.

  Estas reglas se incluyen en el grupo de seguridad predefinido.

- Para replicar datos entre dos sistemas Cloud Volumes ONTAP en subredes diferentes, las subredes deben enrutarse juntas (esta es la configuración predeterminada).
- Para replicar datos entre un sistema Cloud Volumes ONTAP en AWS y un sistema en Azure, debe tener una conexión VPN entre el VPC de AWS y la vnet de Azure.

Requisitos específicos de los clústeres de ONTAP

- Debe instalarse una licencia de SnapMirror activa.
- Si el clúster está en sus instalaciones, debe tener una conexión desde la red corporativa a AWS o Azure, que suele ser una conexión de VPN.
- Los clústeres de ONTAP deben cumplir con requisitos adicionales de subred, puerto, firewall y clúster.

  Para obtener detalles, consulte la Guía exprés de paridad de clústeres y SVM para su versión de ONTAP.

Configurar la replicación de datos entre sistemas

Puede replicar datos entre sistemas Cloud Volumes ONTAP y clústeres ONTAP eligiendo una replicación de datos única, que puede ayudarle a mover datos hacia y desde el cloud, o una programación recurrente, que puede ayudar con la recuperación ante desastres o la retención a largo plazo.

Acerca de esta tarea

Cloud Manager admite configuraciones sencillas, con ventilador y de protección de datos en cascada:

- En una configuración sencilla, la replicación se produce del volumen A al volumen B.
- En una configuración de fanout, la replicación se produce del volumen A a varios destinos.
- En una configuración en cascada, la replicación ocurre del volumen A al volumen B y del volumen B al volumen C.

Puede configurar las configuraciones de fanout y cascada en Cloud Manager configurando múltiples replicaciones de datos entre sistemas. Por ejemplo, replicando un volumen del sistema A al sistema B y, a continuación, replicando el mismo volumen del sistema B al sistema C.

Pasos

1. En la página entornos de trabajo, seleccione el entorno de trabajo que contiene el volumen de origen y, a continuación, arrástrelo al entorno de trabajo al que desea replicar el volumen:

2. Si aparecen las páginas Source y Destination peering Setup, seleccione todas las LIF de interconexión de clústeres para la relación de paridad de clústeres.

   La red de interconexión de clústeres se debe configurar de modo que los pares de clústeres tengan una conectividad de malla completa en función de par, lo que significa que cada par de clústeres de una relación de paridad de clústeres tiene conectividad entre todas sus LIF de interconexión de clústeres.

   Estas páginas aparecen si un clúster ONTAP que tiene varias LIF es el origen o el destino.

3. En la página Source Volume Selection, seleccione el volumen que desea replicar.
4. En la página Nombre del volumen de destino y clasificación por niveles, especifique el nombre del volumen de destino, elija un tipo de disco subyacente, cambie cualquiera de las opciones avanzadas y, a continuación, haga clic en **continuar**.

   Si el destino es un clúster de ONTAP, también debe especificar la SVM de destino y el agregado.

5. En la página Max Transfer Rate, especifique la velocidad máxima (en megabytes por segundo) a la que se pueden transferir los datos.
6. En la página Directiva de replicación, elija una de las directivas predeterminadas o haga clic en * Directivas adicionales* y, a continuación, seleccione una de las directivas avanzadas.

   Para obtener ayuda, consulte "Elegir una política de replicación".

   Si selecciona una política de backup (SnapVault) personalizada, las etiquetas asociadas con la política deben coincidir con las etiquetas de las copias de Snapshot en el volumen de origen. Para obtener más información, consulte "Cómo funcionan las políticas de backup".

7. En la página Schedule, seleccione una copia única o una programación recurrente.

   Hay varios horarios predeterminados disponibles. Si desea crear una programación diferente, debe crear una nueva en el clúster *Destination* mediante System Manager.

8. En la página Review, revise las selecciones y, a continuación, haga clic en **Go**.

Resultado

Cloud Manager inicia el proceso de replicación de datos. Puede ver detalles sobre la replicación en la página Replication Status.

Gestionar programaciones y relaciones de replicación de datos

Después de configurar la replicación de datos entre dos sistemas, puede gestionar la programación y la relación de replicación de datos desde Cloud Manager.

Pasos

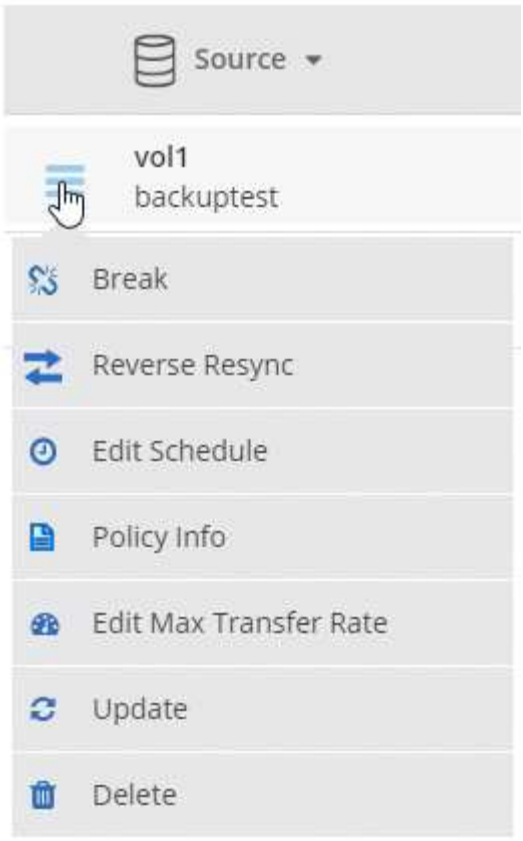
1. En la página entornos de trabajo, consulte el estado de replicación de todos los entornos de trabajo del área de trabajo o de un entorno de trabajo específico:

Opción	Acción
Todos los entornos de trabajo del espacio de trabajo	En la parte superior de Cloud Manager, haga clic en **Estado de replicación**.
Un entorno de trabajo específico	Abra el entorno de trabajo y haga clic en **replicaciones**.

2. Revisar el estado de las relaciones de replicación de datos para verificar que están en buen estado.

   Si el estado de una relación está inactivo y el estado de reflejo no se ha inicializado, debe inicializar la relación desde el sistema de destino para que la replicación de datos se realice de acuerdo con la programación definida. Puede inicializar la relación mediante System Manager o la interfaz de línea de comandos (CLI). Estos estados pueden aparecer cuando el sistema de destino falla y, a continuación, vuelve a estar online.

3. Seleccione el icono de menú junto al volumen de origen y, a continuación, elija una de las acciones disponibles.



En la siguiente tabla se describen las acciones disponibles:

Acción	Descripción
Interrumpir	Rompe la relación entre los volúmenes de origen y de destino, y activa el volumen de destino para acceder a los datos. Esta opción suele utilizarse cuando el volumen de origen no puede servir datos debido a eventos como datos dañados, una eliminación accidental o un estado sin conexión. Para obtener información sobre la configuración de un volumen de destino para el acceso a los datos y la reactivación de un volumen de origen, consulte la Guía exprés de recuperación de desastres de volúmenes de ONTAP 9.
Resincronizcar	Vuelve a establecer una relación rota entre volúmenes y reanuda la replicación de datos de acuerdo con la programación definida. Cuando se resincronizan los volúmenes, el contenido del volumen de destino se sobrescribe con el contenido del volumen de origen. Para realizar una resincronización inversa, que resincronizará los datos del volumen de destino con el volumen de origen, consulte "Guía exprés de recuperación de desastres de volúmenes de ONTAP 9".
Resincronización inversa	Revierte los roles de los volúmenes de origen y destino. El contenido del volumen de origen original se sobrescribe con el contenido del volumen de destino. Esto es útil cuando se desea reactivar un volumen de origen que se desconectó. No se conservan todos los datos escritos en el volumen de origen original entre la última replicación de datos y la hora en la que se deshabilitó el volumen de origen.

Acción	Descripción
Editar programación	Le permite elegir una programación diferente para la replicación de datos.
Información sobre políticas	Muestra la política de protección asignada a la relación de replicación de datos.
Editar velocidad máxima de transferencia	Permite editar la frecuencia máxima (en kilobytes por segundo) a la que se pueden transferir los datos.
Actualizar	Inicia una transferencia incremental para actualizar el volumen de destino.
Eliminar	Elimina la relación de protección de datos entre los volúmenes de origen y de destino, lo que significa que ya no se produce la replicación de datos entre los volúmenes. Esta acción no activa el volumen de destino para acceder a los datos. Esta acción también elimina la relación de paridad entre clústeres y la relación entre iguales de máquinas virtuales de almacenamiento (SVM), si no hay otras relaciones de protección de datos entre los sistemas.

Resultado

Después de seleccionar una acción, Cloud Manager actualiza la relación o la programación.

Elegir una política de replicación

Es posible que necesite ayuda para elegir una política de replicación al configurar la replicación de datos en Cloud Manager. Una política de replicación define cómo el sistema de almacenamiento replica los datos de un volumen de origen a un volumen de destino.

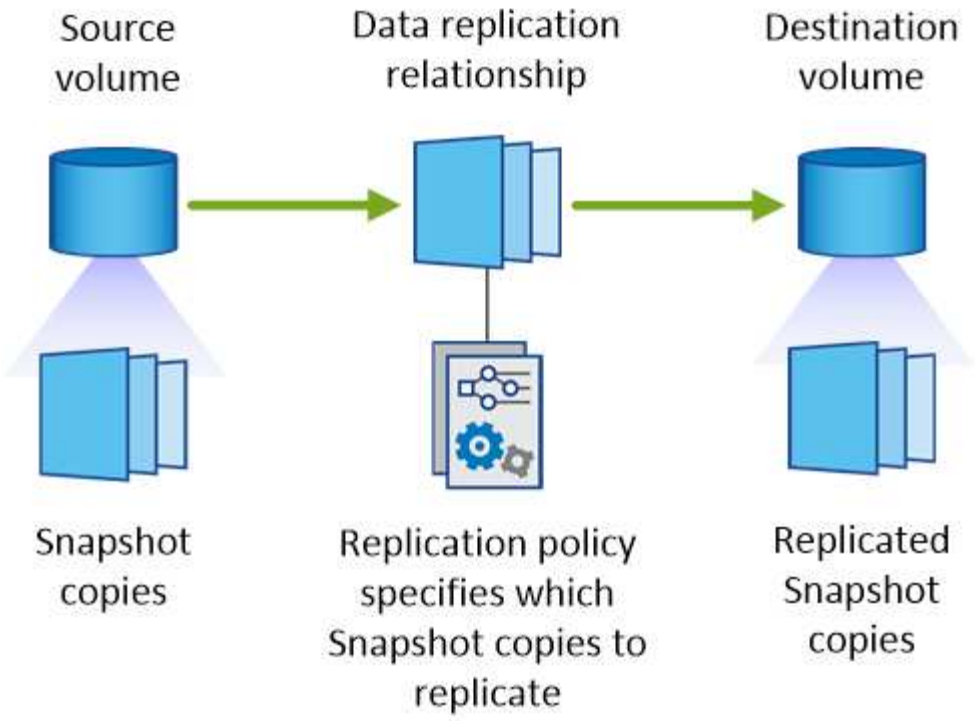
Lo que hacen las políticas de replicación

El sistema operativo ONTAP crea automáticamente backups llamados copias snapshot. Una copia Snapshot es una imagen de solo lectura de un volumen que captura el estado del sistema de archivos en un momento específico.

Cuando se replican datos entre sistemas, se replican copias Snapshot de un volumen de origen a un volumen de destino. Una política de replicación especifica las copias de Snapshot que se van a replicar del volumen de origen al volumen de destino.

Las normativas de replicación también se conocen como políticas de *protection* porque se alimentan de las tecnologías SnapMirror y SnapVault, que proporcionan protección de recuperación ante desastres y backup y recuperación de datos de disco a disco.

En la siguiente imagen, se muestra la relación entre las copias Snapshot y las políticas de replicación:



Tipos de políticas de replicación

Existen tres tipos de políticas de replicación:

- Una directiva *Mirror* replica las copias Snapshot recién creadas en un volumen de destino.

  Es posible usar estas copias Snapshot para proteger el volumen de origen como preparación para la recuperación ante desastres o para la replicación de datos que se realiza una vez. Puede activar el volumen de destino para acceder a los datos en cualquier momento.

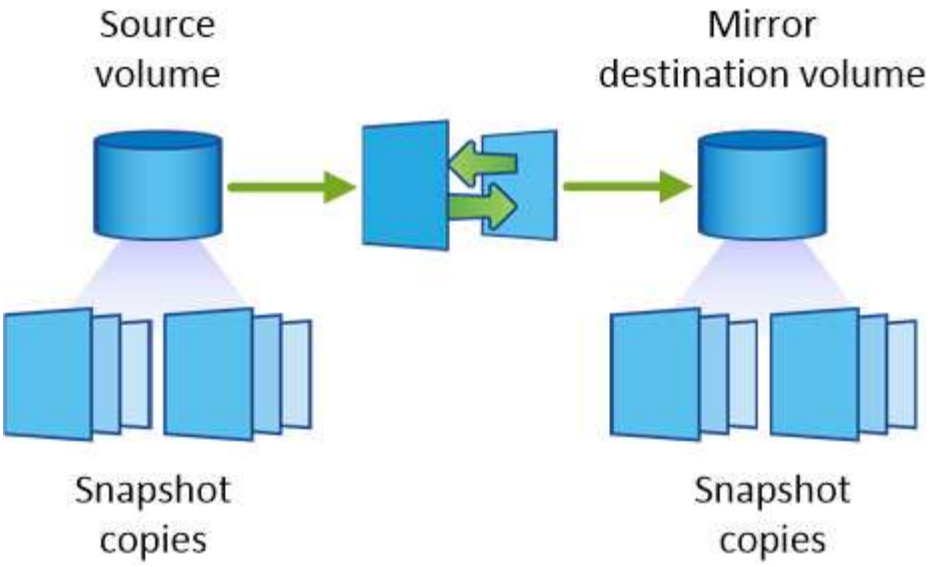
- Una política de *Backup* replica copias Snapshot específicas a un volumen de destino y, normalmente, las conserva durante un período de tiempo más largo del que tendría en el volumen de origen.

  Puede restaurar datos de estas copias Snapshot cuando se dañen o se pierdan datos, y conservarlas para cumplir los estándares y otros fines relacionados con la regulación.

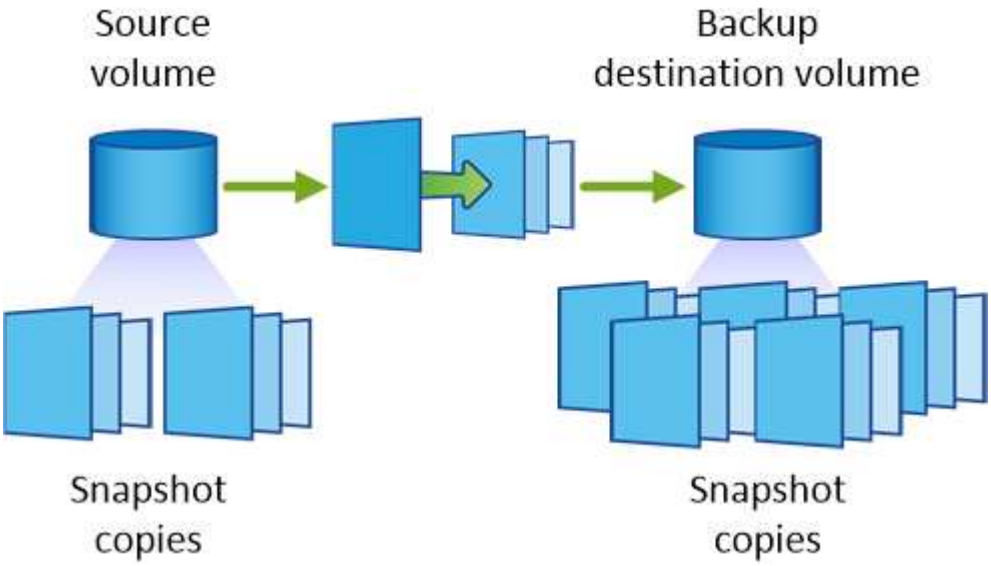
- Una política de *Mirror and Backup* proporciona recuperación ante desastres y retención a largo plazo.

  Cada sistema incluye una política predeterminada de copia de seguridad y copia de seguridad, que funciona bien en muchas situaciones. Si necesita políticas personalizadas, puede crear propias con System Manager.

En las siguientes imágenes, se muestra la diferencia entre las políticas de reflejo y backup. Una política de mirroring refleja las copias Snapshot disponibles en el volumen de origen.



Normalmente, una política de backup retiene copias Snapshot durante más tiempo del que se conservan en el volumen de origen:



Cómo funcionan las políticas de backup

A diferencia de las políticas de mirroring, las políticas de backup (SnapVault) replican copias Snapshot específicas a un volumen de destino. Es importante comprender cómo funcionan las políticas de backup si desea utilizar sus propias políticas en lugar de las predeterminadas.

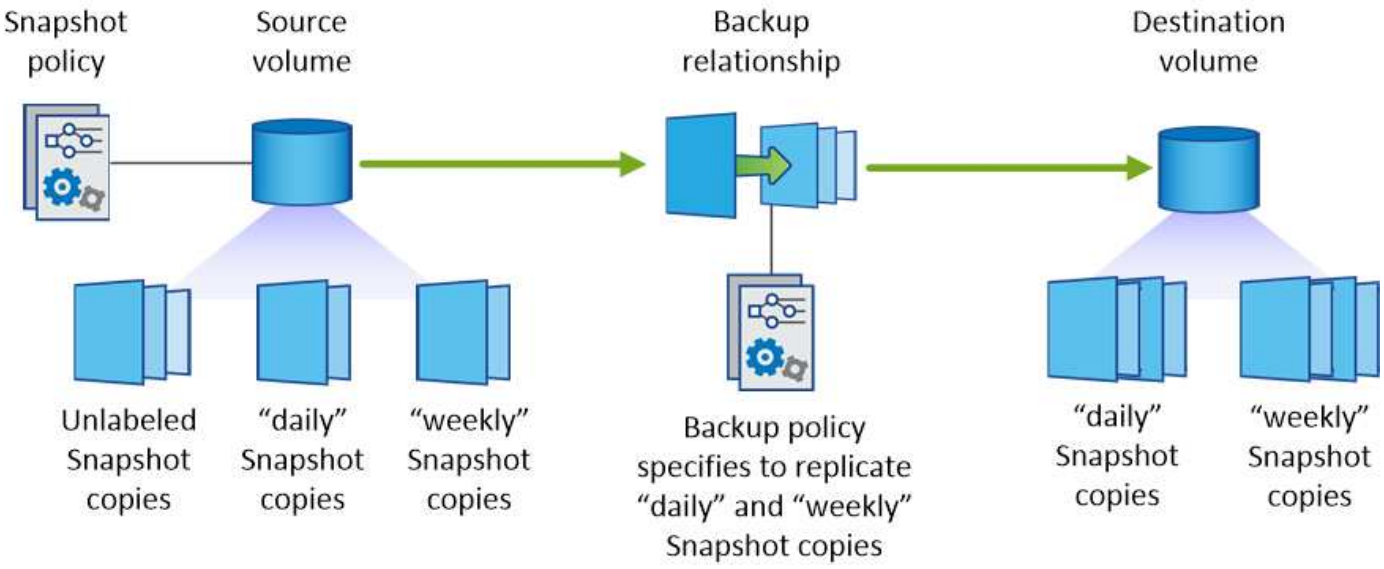
Descripción de la relación entre las etiquetas de copia de Snapshot y las políticas de backup

Una política de Snapshot define el modo en que el sistema crea copias Snapshot de los volúmenes. La política especifica cuándo crear las copias Snapshot, cuántas copias se deben conservar y cómo etiquetarlas. Por ejemplo, un sistema puede crear una copia Snapshot todos los días a las 12:10 a.m., retener las dos copias más recientes y etiquetarlas "diarias".

Una política de backup incluye reglas que especifican las etiquetas que las copias Snapshot se replican en un volumen de destino y cuántas copias se retendrán. Las etiquetas definidas en una política de backup deben coincidir con una o más etiquetas definidas en una política de Snapshot. De lo contrario, el sistema no puede

replicar ninguna copia Snapshot.

Por ejemplo, una política de backup que incluya las etiquetas "diaria" y "semanal" provoca la replicación de copias Snapshot que solo incluyen esas etiquetas. No se replican ninguna otra copia Snapshot, como se muestra en la siguiente imagen:



Directivas predeterminadas y personalizadas

La política de Snapshot predeterminada crea copias de SnapVault cada hora, cada día y cada semana, y conserva seis copias de Snapshot cada hora, dos días y dos semanas.

Puede utilizar fácilmente una política de backup predeterminada con la política de Snapshot predeterminada. Las normativas de backup predeterminadas replican las copias snapshot diarias y semanales, y conservan siete copias snapshot diarias y 52 semanales.

Si crea directivas personalizadas, las etiquetas definidas por dichas directivas deben coincidir. Puede crear políticas personalizadas mediante System Manager.

Realizar backups de datos en Amazon S3

Backup en S3 es una función complementaria para Cloud Volumes ONTAP que ofrece funcionalidades de backup y restauración totalmente gestionadas para la protección y el archivado a largo plazo de sus datos en el cloud. Los backups se almacenan en el almacenamiento de objetos de S3, independientemente de las copias Snapshot de volúmenes que se utilicen para la recuperación o el clonado a corto plazo.

Cuando se habilita Backup en S3, el servicio realiza un backup completo de los datos. Todos los backups adicionales son incrementales, lo que significa que solo se realiza un backup de los bloques modificados y los nuevos bloques.

"Visite Cloud Central de NetApp para obtener más información sobre los precios".

Tenga en cuenta que debe usar Cloud Manager para todas las operaciones de backup y restauración. Cualquier acción que se haga directamente desde ONTAP o Amazon S3 tendrá como resultado una configuración no compatible.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Verifique la compatibilidad con la configuración

Compruebe lo siguiente:

- Cloud Volumes ONTAP 9.4 o una versión posterior se ejecuta en una región AWS admitida: N. Virginia, Oregón, Irlanda, Frankfurt o Sydney
- Se ha suscrito al nuevo "Oferta Cloud Manager Marketplace"
- El puerto TCP 5010 está abierto para el tráfico saliente en el grupo de seguridad para Cloud Volumes ONTAP (está abierto de forma predeterminada)
- El puerto TCP 8088 está abierto para tráfico saliente en el grupo de seguridad para Cloud Manager (está abierto de forma predeterminada)
- Desde Cloud Manager se puede acceder al siguiente extremo:

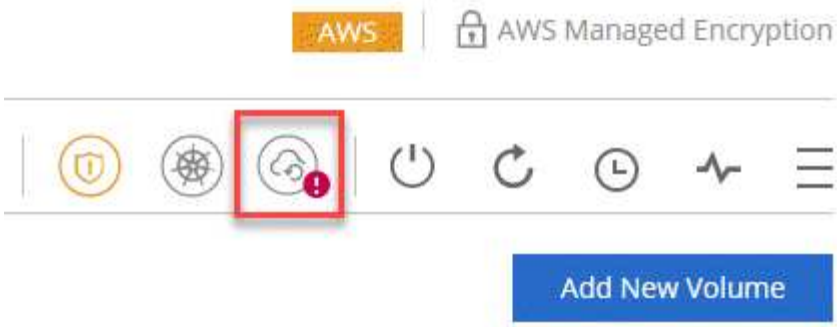
  https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

- Hay espacio para que Cloud Manager asigne hasta dos extremos de VPC de interfaz en el VPC (el límite de AWS por VPC es de 20).
- Cloud Manager tiene permiso para usar los permisos de extremo de VPC que se enumeran en las versiones más recientes "Política de Cloud Manager":

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

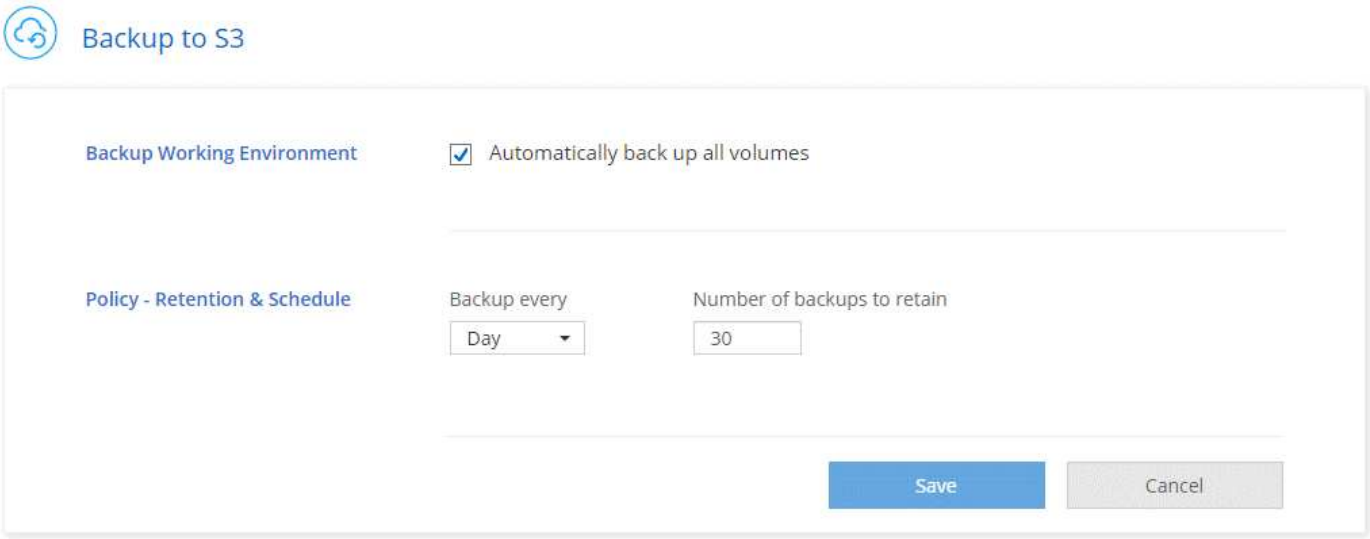
Habilite Backup en S3 en su sistema nuevo o existente

- Nuevos sistemas: La función Backup en S3 está habilitada de forma predeterminada en el asistente del entorno de trabajo. Asegúrese de mantener la opción habilitada.
- Sistemas existentes: Abra el entorno de trabajo, haga clic en el icono de configuración de copia de seguridad y habilite las copias de seguridad.



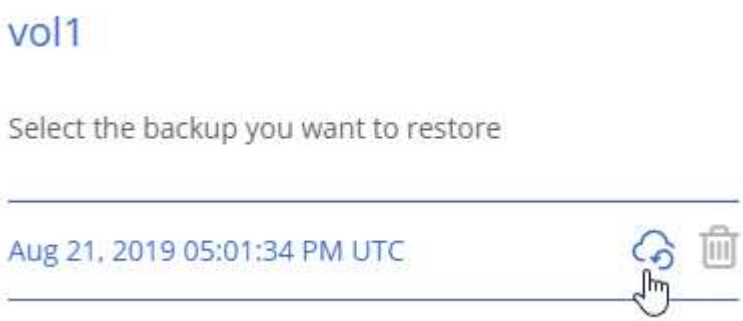
Si es necesario, modifique la política de backup

La política predeterminada realiza backups de los volúmenes todos los días y retiene 30 copias de backup de cada volumen. Si es necesario, puede cambiar la cantidad de copias de backup que se conservan.



Restaure sus datos, según sea necesario

En la parte superior de Cloud Manager, haga clic en **copia de seguridad y restauración**, seleccione un volumen, seleccione una copia de seguridad y, a continuación, restaure los datos de la copia de seguridad a un volumen nuevo.



Requisitos

Lea los siguientes requisitos para asegurarse de que tenga una configuración compatible antes de comenzar a realizar el backup de volúmenes en S3.

Versiones de ONTAP compatibles

El backup en S3 es compatible con Cloud Volume ONTAP 9.4 y versiones posteriores.

Regiones admitidas de AWS

El backup en S3 es compatible con Cloud Volumes ONTAP en las siguientes regiones de AWS:

- Este DE EE. UU. (N. Virginia)
- Oeste DE EE. UU. (Oregón)
- UE (Irlanda)
- UE (Frankfurt)
- APAC (Sidney)

Se requieren permisos de AWS

El rol IAM que proporciona permisos a Cloud Manager debe incluir lo siguiente:

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

Requisito de suscripción de AWS

A partir del lanzamiento de la versión 3.7.3, hay una nueva suscripción de Cloud Manager disponible en AWS Marketplace. Esta suscripción permite la puesta en marcha de los sistemas Cloud Volumes ONTAP 9.6 y posteriores de PAYGO y la función Backup to S3. Necesita hacerlo "suscríbase a esta nueva suscripción a Cloud Manager" Antes de habilitar Backup en S3. La facturación de la función Backup to S3 se realiza mediante esta suscripción.

Requisitos de puertos

- El puerto TCP 5010 debe estar abierto para el tráfico saliente de Cloud Volumes ONTAP al servicio de respaldo.
- El puerto TCP 8088 debe estar abierto para tráfico saliente en el grupo de seguridad para Cloud Manager.

  Estos puertos ya están abiertos si se usan los grupos de seguridad predefinidos. No obstante, si ha utilizado los suyos, deberá abrir estos puertos.

Acceso a Internet de salida

Asegúrese de que se pueda acceder al siguiente extremo desde Cloud Manager: https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

Cloud Manager se pone en contacto con este extremo para añadir su ID de cuenta de AWS a la lista de usuarios permitidos para Backup en S3.

Extremos de la interfaz VPC

Cuando se habilita la función Backup en S3, Cloud Manager crea un extremo de interfaz VPC en el VPC, donde se ejecuta Cloud Volumes ONTAP. Este *terminal de backup* se conecta al VPC de NetApp, donde se ejecuta el backup a S3. Si restaura un volumen, Cloud Manager crea un extremo de la interfaz adicional VPC, que es el *restore Endpoint*.

Todos los sistemas Cloud Volumes ONTAP adicionales del VPC utilizan estos dos extremos de VPC.

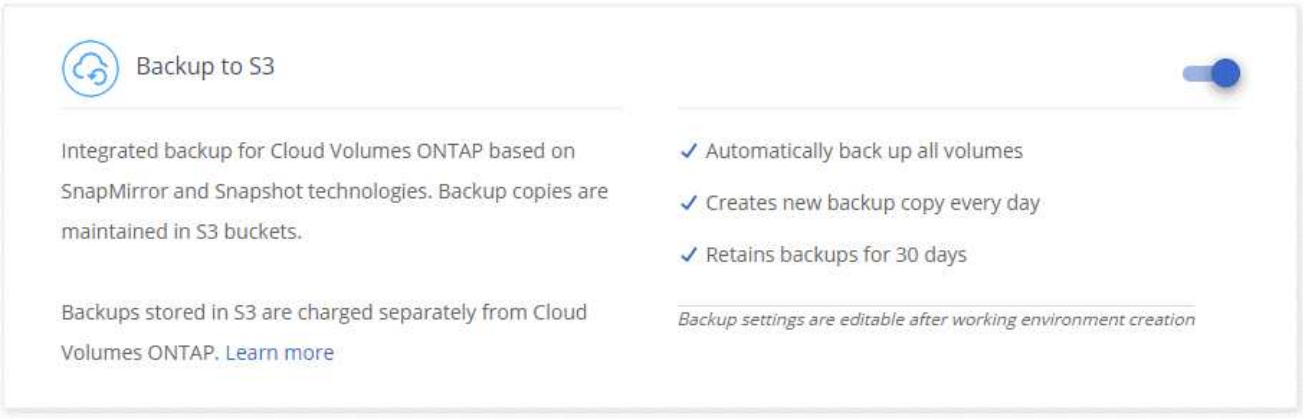
"El límite predeterminado para los extremos de VPC de la interfaz es de 20 por VPC". Asegúrese de que VPC no haya alcanzado el límite antes de habilitar la función.

Habilitar backups en S3 en un nuevo sistema

La función Backup to S3 está habilitada de manera predeterminada en el asistente del entorno de trabajo. Asegúrese de mantener la opción habilitada.

Pasos

1. Haga clic en **Crear Cloud Volumes ONTAP**.
2. Seleccione Amazon Web Services como proveedor de cloud y, a continuación, elija un único nodo o sistema de alta disponibilidad.
3. Rellene la página Details & Credentials.
4. En la página copia de seguridad en S3, deje activada la función y haga clic en **continuar**.



5. Complete las páginas del asistente para implementar el sistema.

Resultado

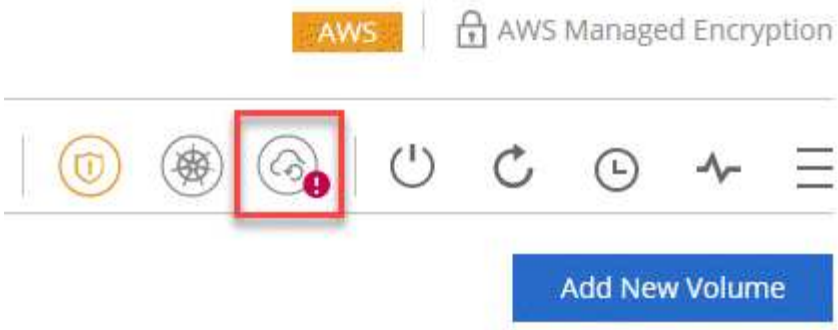
La función Backup to S3 está habilitada en el sistema y realiza un backup de volúmenes todos los días y retiene 30 copias de backup. Aprenda a modificar la retención de backup.

Habilitar backups en S3 en un sistema existente

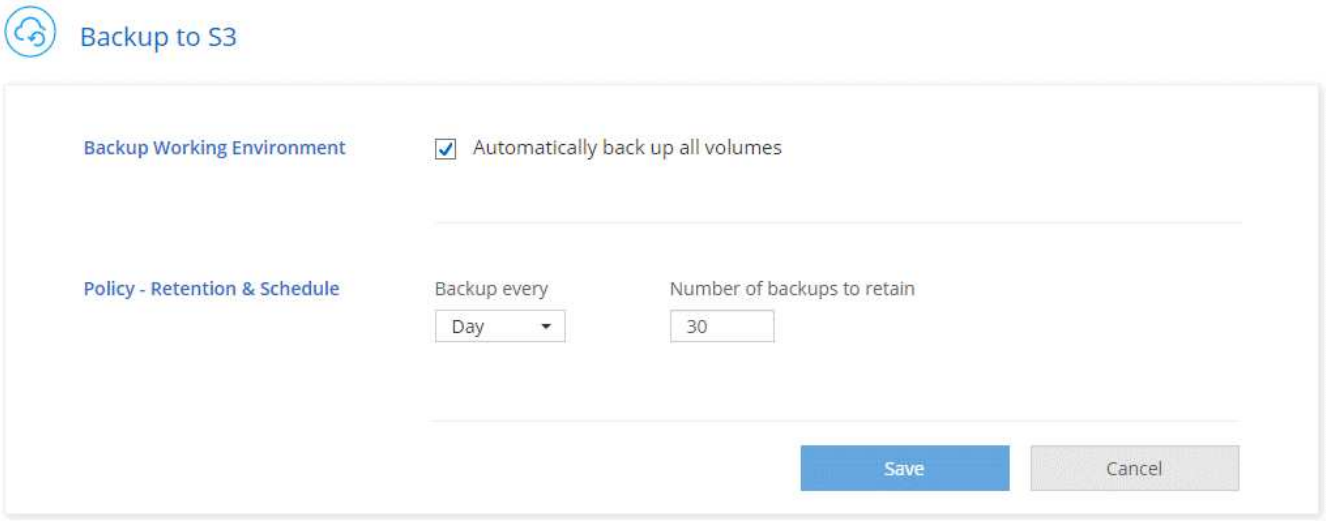
Es posible habilitar backups en S3 en un sistema Cloud Volumes ONTAP existente, siempre que se ejecute una configuración compatible. Para obtener más información, consulte Requisitos.

Pasos

1. Abra el entorno de trabajo.
2. Haga clic en el icono de configuración de copia de seguridad.



3. Seleccione **copia de seguridad automática de todos los volúmenes**.
4. Elija su retención de copia de seguridad y, a continuación, haga clic en **Guardar**.



Resultado

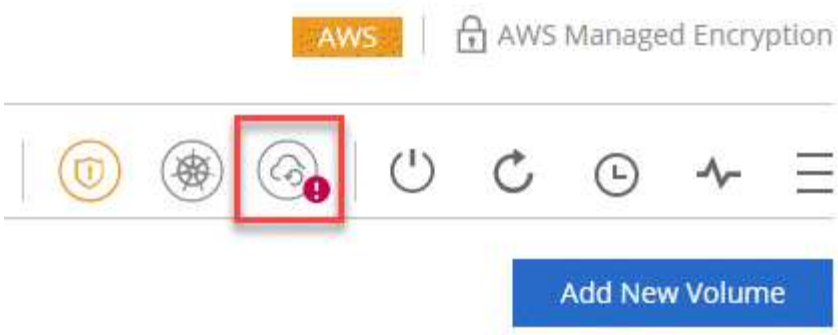
La función Backup to S3 comienza a tomar los backups iniciales de cada volumen.

Cambiar la retención de backups

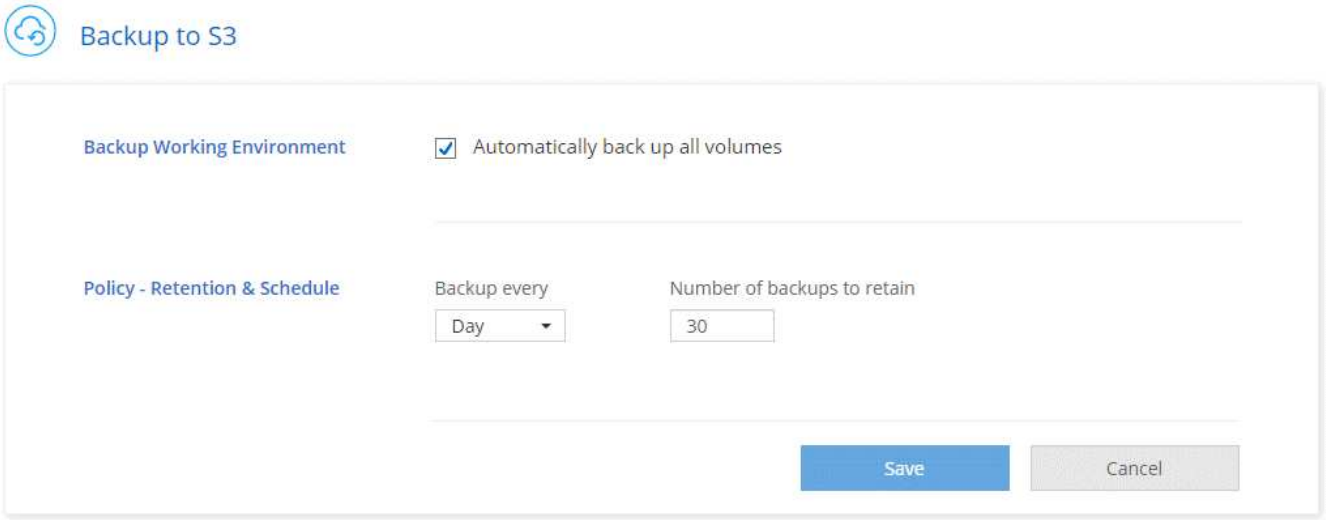
La política predeterminada realiza backups de los volúmenes todos los días y retiene 30 copias de backup de cada volumen. Es posible cambiar el número de copias de backup que se conservan.

Pasos

1. Abra el entorno de trabajo.
2. Haga clic en el icono de configuración de copia de seguridad.



3. Cambie la retención de la copia de seguridad y, a continuación, haga clic en **Guardar**.



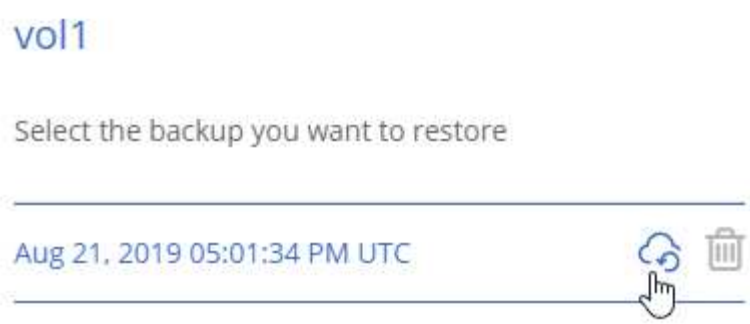
Restaurar un volumen

Cuando restaura datos de un backup, Cloud Manager realiza una restauración completa de un volumen en un volumen *new*. Puede restaurar los datos en el mismo entorno de trabajo o en otro de trabajo.

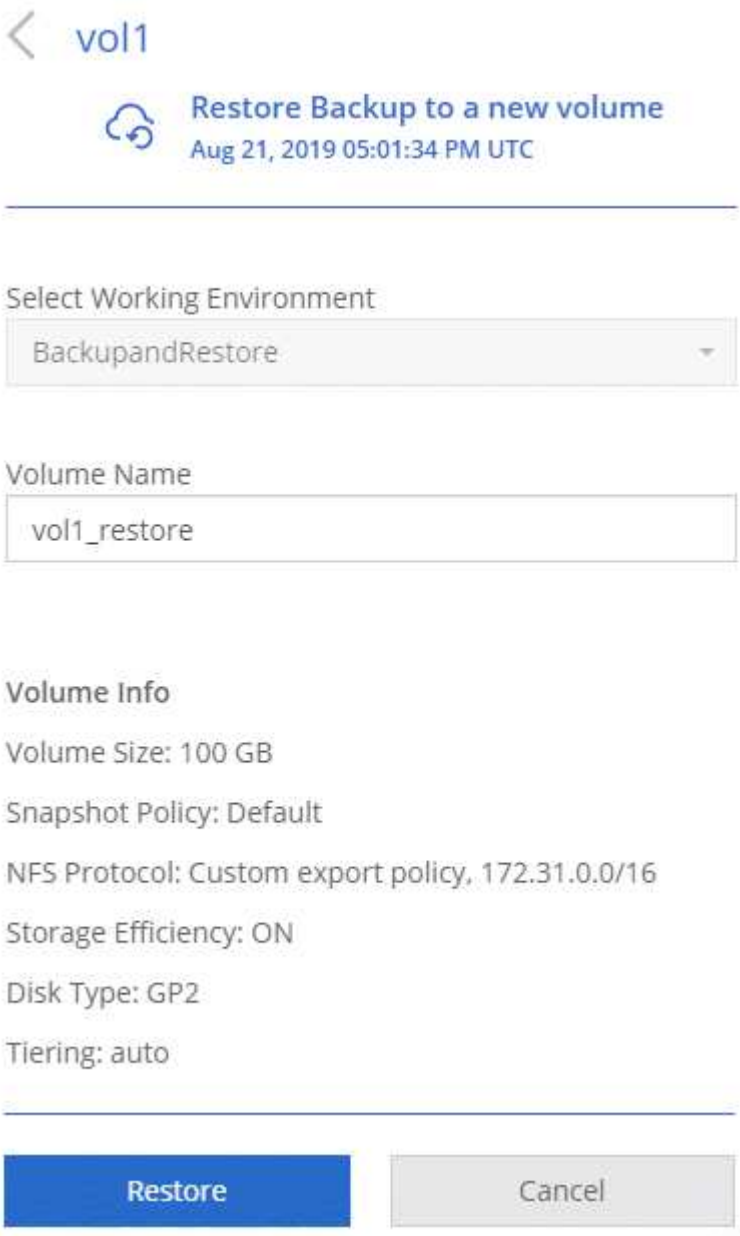
Pasos

1. En la parte superior de Cloud Manager, haga clic en **copia de seguridad y restauración**.
2. Seleccione el volumen que desea restaurar.

3. Busque el backup desde el que desea restaurar y haga clic en el icono de restauración.



4. Seleccione el entorno de trabajo al que desea restaurar el volumen.
5. Escriba un nombre para el volumen.
6. Haga clic en **Restaurar**.

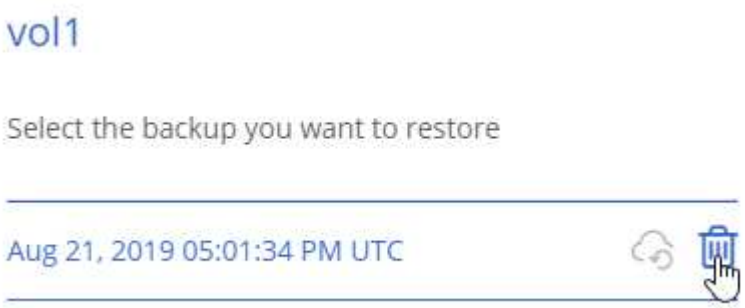


Eliminar backups

Todos los backups se retienen en S3 hasta que se los elimina de Cloud Manager. Los backups no se eliminan al eliminar un volumen o al eliminar el sistema Cloud Volumes ONTAP.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **copia de seguridad y restauración**.
2. Seleccionar un volumen.
3. Busque el backup que desea eliminar y haga clic en el icono de eliminar.



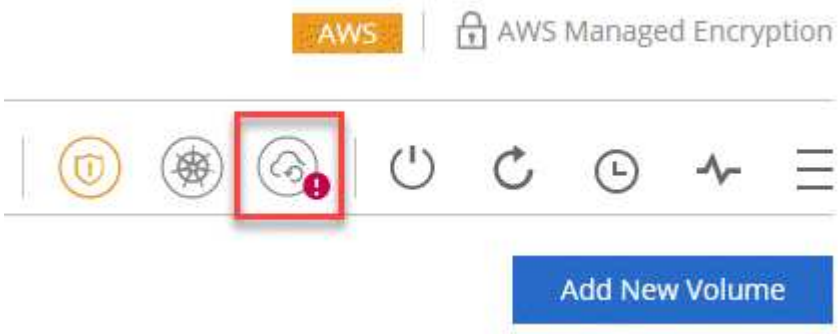
4. Confirme que desea eliminar el backup.

Deshabilitar los backups en S3

Al deshabilitar los backups en S3, se deshabilitan los backups de cada volumen del sistema. No se eliminarán los backups existentes.

Pasos

1. Abra el entorno de trabajo.
2. Haga clic en el icono de configuración de copia de seguridad.



3. Desactivar **hacer una copia de seguridad automática de todos los volúmenes** y, a continuación, hacer clic en **Guardar**.

Cómo funciona el backup en S3

En las siguientes secciones, se proporciona más información sobre la función Backup to S3.

La ubicación de los backups

Las copias de backup se almacenan en un bloque de S3 propiedad de NetApp, en la misma región donde se encuentra el sistema Cloud Volumes ONTAP.

Los backups son incrementales

Tras el primer backup completo de sus datos, todos los backups adicionales son incrementales, lo que significa que solo se realiza un backup de los bloques modificados y los nuevos bloques.

Los backups se realizan a medianoche

Los backups diarios comienzan justo después de la medianoche cada día. En este momento, no puede programar operaciones de backup a una hora específica del usuario.

Las copias de backup están asociadas con su cuenta de Cloud Central

Las copias de backup se asocian con "Cuenta de Cloud Central" En el que reside Cloud Manager.

Si tiene varios sistemas Cloud Manager en la misma cuenta de Cloud Central, cada sistema Cloud Manager mostrará la misma lista de backups. Que incluye los backups asociados con las instancias de Cloud Volumes ONTAP desde otros sistemas de Cloud Manager.

La política de respaldo es de todo el sistema

La cantidad de backups que se retendrán se define en el nivel del sistema. No puede establecer una política diferente para cada volumen del sistema.

Seguridad

Los datos de los backups se protegen con conexiones HTTPS en reposo con cifrado AES de 256 bits y TLS 1.2.

Los datos viajan a través de enlaces de Direct Connect seguros al servicio, y permanecen protegidos en reposo gracias al cifrado de 256 bits de AES. A continuación, los datos cifrados se escriben en el cloud mediante conexiones HTTPS TLS 1.2. Además, los datos también se trasladan a Amazon S3 solo a través de conexiones terminales, de manera que no se envía tráfico por Internet.

A cada usuario se le asigna una clave de inquilino, además de una clave de cifrado general propiedad del servicio. Este requisito es similar a necesitar un par de claves para abrir un cliente seguro en un banco. Todas las claves, como credenciales de cloud, se almacenan de forma segura mediante el servicio y solo están restringidas a cierto personal de NetApp responsable de mantenimiento del servicio.

Limitaciones

- Si utiliza cualquiera de los siguientes tipos de instancia, un sistema Cloud Volumes ONTAP puede realizar un backup de un máximo de 20 volúmenes a S3:
  - m4.xlarge
  - m5.xlarge
  - r4.xlarge
  - r5.xlarge
- Los volúmenes que cree fuera de Cloud Manager no se podrán realizar automáticamente backups en S3.

Por ejemplo, si crea un volumen desde la CLI de ONTAP, la API de ONTAP o System Manager, no se creará un backup automático de ese volumen.

Si desea realizar un backup de estos volúmenes, debe deshabilitar la función Backup en S3 y, a continuación, volver a habilitarla.

- Cuando restaura datos de un backup, Cloud Manager realiza una restauración completa de un volumen en un volumen *new*. No se realiza automáticamente backups de este nuevo volumen en S3.

  Si se desea realizar un backup de volúmenes creados desde una operación de restauración, se debe deshabilitar la función Backup en S3 y, luego, volver a habilitarla.

- Es posible realizar backups de volúmenes con un tamaño mínimo de 50 TB.
- El backup en S3 puede mantener hasta 245 backups totales de un volumen.
- El almacenamiento WORM no es compatible en un sistema Cloud Volumes ONTAP cuando se habilita el backup en S3.

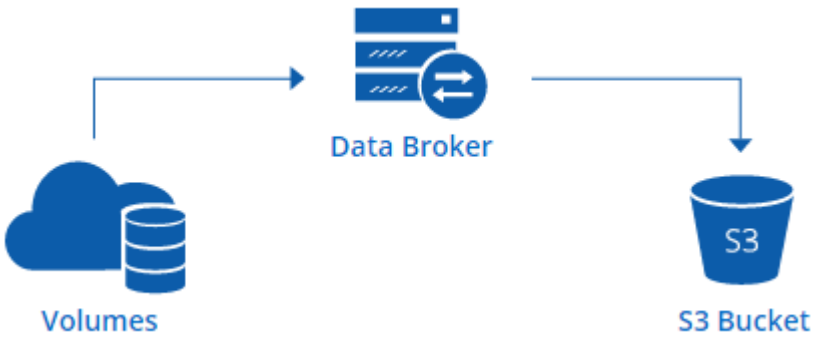
Sincronizando datos en Amazon S3

Puede sincronizar datos de ONTAP Volumes en un bloque de Amazon S3 mediante la integración de un entorno de trabajo con "Cloud Sync de NetApp". A continuación, puede utilizar los datos sincronizados como una copia secundaria o para el procesamiento de datos con servicios de AWS como EMR y Redshift.

Cómo funciona la función de sincronización con S3

Puede integrar un entorno de trabajo con el servicio Cloud Sync en cualquier momento. Cuando se integra un entorno de trabajo, el servicio Cloud Sync sincroniza los datos de los volúmenes seleccionados en un único bloque de S3. La integración funciona con entornos de trabajo de Cloud Volumes ONTAP, así como clústeres de ONTAP que están en las instalaciones o forman parte de una configuración de almacenamiento privado de NetApp (NPS).

Para sincronizar los datos, el servicio inicia una instancia de agente de datos en el VPC. Cloud Sync utiliza un agente de datos por entorno de trabajo para sincronizar datos de volúmenes en un bloque de S3. Después de la sincronización inicial, el servicio sincroniza los datos modificados una vez al día a medianoche.



Si desea realizar acciones Cloud Sync avanzadas, vaya directamente al servicio Cloud Sync. A partir de ahí, puede realizar acciones como sincronizar de S3 con un servidor NFS, elegir distintos bloques S3 para volúmenes y modificar programaciones.

prueba gratuita de 14 días

Si usted es un nuevo usuario de Cloud Sync, sus primeros 14 días son gratis. Después de que finalice la prueba gratuita, deberá pagar por cada *SYNC Relationship* a una tarifa por hora o mediante la compra de licencias. Cada volumen que se sincroniza con un bloque de S3 se considera una relación de sincronización. Puede configurar ambas opciones de pago directamente desde Cloud Sync en la página Configuración de licencia.

Cómo obtener ayuda

Use las siguientes opciones para cualquier soporte relacionado con la función Cloud Manager Sync to S3 o con Cloud Sync en general:

- Comentarios generales sobre productos: ng-cloudsync-contact@netapp.com
- Opciones de soporte técnico:
  - Comunidades Cloud Sync de NetApp
  - Chat en el producto (en la esquina inferior derecha de Cloud Manager)

Integración de un entorno de trabajo con el servicio Cloud Sync

Si desea sincronizar volúmenes en Amazon S3 directamente desde Cloud Manager, debe integrar el entorno de trabajo con el servicio Cloud Sync.

[] | *https://img.youtube.com/vi/3hOtLs70_xE/maxresdefault.jpg*

Pasos

1. Abra un entorno de trabajo y haga clic en **Sincronizar a S3**.
2. Haga clic en **Sincronizar** y siga las indicaciones para sincronizar los datos con S3.

No es posible sincronizar los volúmenes de protección de datos en S3. Los volúmenes deben ser editables.

Gestión de relaciones de sincronización de volúmenes

Tras integrar un entorno de trabajo con el servicio Cloud Sync, puede sincronizar volúmenes adicionales, detener la sincronización de un volumen y eliminar la integración con Cloud Sync.

Pasos

1. En la página entornos de trabajo, haga doble clic en el entorno de trabajo en el que desea gestionar las relaciones de sincronización.
2. Si desea activar o desactivar la sincronización con S3 para un volumen, seleccione el volumen y, a continuación, haga clic en **Sincronizar con S3** o **Eliminar relación de sincronización**.
3. Si desea eliminar todas las relaciones de sincronización de un entorno de trabajo, haga clic en la ficha **Sincronizar a S3** y, a continuación, haga clic en **Eliminar sincronización**.

   Esta acción no elimina los datos sincronizados del bloque de S3. Si el agente de datos no se está utilizando en ninguna otra relación de sincronización, el servicio Cloud Sync elimina el agente de datos.

Información de copyright

Copyright © 2024 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.