



Administre sus máquinas virtuales y datos de almacenamiento

AFX

NetApp
February 10, 2026

Tabla de contenidos

Administre sus máquinas virtuales y datos de almacenamiento	1
Administrar datos	1
Prepárese para administrar los datos de su sistema de almacenamiento AFX	1
Crear y configurar un volumen en un sistema de almacenamiento AFX	3
Administrar los volúmenes del sistema de almacenamiento AFX	4
Crear y configurar un bucket S3 en un sistema de almacenamiento AFX	4
Administrar los depósitos del sistema de almacenamiento AFX	5
Supervisar y solucionar problemas de un sistema de almacenamiento AFX	5
Proteger datos	5
Prepárese para proteger los datos de su sistema de almacenamiento AFX	5
Crear un grupo de consistencia en un sistema de almacenamiento AFX	6
Administrar grupos de consistencia en un sistema de almacenamiento AFX	7
Crear una instantánea en un sistema de almacenamiento AFX	8
Administrar instantáneas en un sistema de almacenamiento AFX	11
Crear una relación de pares SVM entre clústeres en un sistema de almacenamiento AFX	12
Administrar la replicación de instantáneas en un sistema de almacenamiento AFX	12
Administrar las políticas y los cronogramas de protección de datos del sistema de almacenamiento AFX	17
Datos seguros	19
Prepárese para proteger los datos de su sistema de almacenamiento AFX	19
Cifrar datos en reposo en un sistema de almacenamiento AFX	19
Conexiones IP seguras en sus sistemas de almacenamiento AFX	20
Administración adicional para un sistema de almacenamiento AFX SVM	21
Gestión y rendimiento del almacenamiento	21
Protección de datos	22
Seguridad	22
Monitoreo de eventos y rendimiento de ONTAP	22
Información relacionada	22

Administre sus máquinas virtuales y datos de almacenamiento

Administrar datos

Prepárese para administrar los datos de su sistema de almacenamiento AFX

Antes de administrar sus datos AFX, debe familiarizarse con los conceptos y capacidades básicos.



Dado que muchos de los conceptos y procedimientos de administración disponibles en los sistemas AFF y FAS son los mismos que los de los sistemas de almacenamiento AFX, revisar la documentación de Unified ONTAP puede resultar útil. Consulte los enlaces en [Información relacionada](#) Para obtener más información.

Terminología y opciones

Hay varios términos relacionados con el almacenamiento AFX con los que debes estar familiarizado.

Volumen flexible

Un FlexVol es un tipo de contenedor lógico utilizado en sistemas de almacenamiento AFX. Los volúmenes FlexVol se pueden expandir, contraer, mover y copiar de manera eficiente. También se pueden dividir en unidades más manejables usando qtrees y se puede limitar el uso de recursos usando cuotas.

FlexGroup

Un volumen FlexGroup es un contenedor NAS escalable que proporciona alto rendimiento y distribución automática de carga. Cada uno consta de múltiples volúmenes que comparten el tráfico de forma transparente. Los volúmenes FlexGroup ofrecen varios beneficios, entre ellos mayor escalabilidad y rendimiento, además de una gestión simplificada.

FlexCache

FlexCache es una tecnología de almacenamiento en caché de ONTAP que crea réplicas dispersas y escribibles de volúmenes en el mismo clúster de ONTAP o en diferentes. Está diseñado para mejorar el rendimiento del acceso a los datos al acercarlos a los usuarios, lo que puede generar un rendimiento más rápido con un espacio más pequeño. FlexCache es particularmente útil para flujos de trabajo de lectura intensiva y ayuda a descargar el tráfico de volúmenes con mucho acceso.

Cubo S3

Un bucket S3 es un contenedor de almacenamiento que contiene objetos o datos en la nube. Con ONTAP, un bucket NAS S3 es una asignación entre un nombre de bucket S3 y una ruta NAS, lo que permite el acceso de S3 a cualquier parte de un espacio de nombres SVM con volúmenes y estructura de directorio existentes.

contenedor de datos

En el contexto de un sistema AFX, un contenedor de datos es un término genérico y puede ser un volumen o un depósito S3.

Árbol Q

Un qtree es una subdivisión lógica dentro de un volumen que puedes crear para administrar y organizar datos. Permite especificar sus propiedades y estilo de seguridad (NTFS o UNIX) y puede heredar políticas

de exportación de su volumen padre o tener las suyas propias. Los Qtrees pueden contener archivos y directorios, y a menudo se utilizan para administrar permisos y cuotas de forma más granular dentro de un volumen.

Cuota

Una cuota en ONTAP es un límite establecido en la cantidad de espacio de almacenamiento o número de archivos que puede usar un usuario, grupo o qtree. Las cuotas se utilizan para administrar y controlar el uso de recursos dentro de un sistema de almacenamiento, garantizando que ningún usuario o aplicación pueda consumir una cantidad excesiva de recursos.

Enlace troncal de sesión NFS

El enlace troncal NFS es una tecnología que permite a los clientes NFS v4.1 abrir múltiples conexiones a diferentes LIF en el servidor NFS. Esto aumenta la velocidad de transferencia de datos y proporciona resiliencia a través de múltiples rutas al exportar volúmenes a clientes con capacidad de enlace troncal. Las LIF deben estar en el mismo nodo para participar en el enlace troncal.

Para habilitar el trunking, debe tener un SVM configurado para NFS y NFSv4.1 debe estar habilitado. También requiere volver a montar todos los clientes NFSv4.x después de un cambio de configuración, lo que puede resultar disruptivo. Los procedimientos de soporte y configuración para enlaces troncales NFS son los mismos para todos los sistemas ONTAP . Obtenga más información sobre ["Troncalización NFS"](#)

Análisis del sistema de archivos

File System Analytics (FSA) es una función de ONTAP que proporciona visibilidad en tiempo real del uso de archivos y las tendencias de capacidad de almacenamiento dentro de los volúmenes FlexGroup o FlexVol . Elimina la necesidad de herramientas externas al ofrecer información sobre la utilización del almacenamiento y las oportunidades de optimización. FSA proporciona vistas detalladas en varios niveles de la jerarquía del sistema de archivos de un volumen, incluidos los niveles de SVM, volumen, directorio y archivo.

Opciones de migración de datos

Hay varias opciones de migración de datos. El objetivo es migrar datos externos a un clúster AFX.

Migración de datos desde sistemas AFF o FAS

Está disponible una ruta de migración totalmente integrada de los sistemas AFF o FAS (que ejecutan la personalidad Unified ONTAP) a AFX mediante las siguientes tecnologías:

- SnapMirror
- Migración de SVM
- SVM DR

Además, los volúmenes FlexCache se pueden conectar entre sistemas AFX y AFF o FAS en cualquier dirección.

Migración de datos desde una fuente que no es ONTAP

La migración de datos desde sistemas que no sean ONTAP se puede realizar mediante operaciones de copia a nivel de archivo. utilidades de copia rápida como ["XCP"](#) o ["Copiar y sincronizar"](#) Puede utilizarse junto con utilidades estándar como RoboCopy (para SMB) y rsync (para NFS), así como con herramientas de terceros como DataDobi.

Limitaciones migratorias

Puede replicar datos de sistemas AFF o FAS a AFX si el volumen de datos de origen no contiene LUN o espacios de nombres NVMe. Al replicar desde sistemas AFX a AFF o FAS, la versión mínima de ONTAP compatible con el sistema AFF o FAS es 9.16.1. Esta es la primera versión de ONTAP que admite el equilibrio de capacidad avanzado.

Muestra una descripción general de tu almacenamiento

Para comenzar a administrar sus datos AFX, debe mostrar una descripción general del almacenamiento.

Acerca de esta tarea

Puede acceder a todos los volúmenes y depósitos definidos para el clúster AFX. Cada uno de ellos se considera un contenedor de datos.

Pasos

1. En el Administrador del sistema, seleccione **Almacenamiento** y luego **Descripción general**
2. Junto a **Volúmenes**, seleccione → para mostrar una lista de volúmenes.
3. Junto a **Cubos**, seleccione → para mostrar una lista de depósitos.
4. Actualice o cree un contenedor de datos según sea necesario.

Información relacionada

- ["Obtenga información sobre el análisis del sistema de archivos ONTAP."](#)
- ["Administración adicional de AFX SVM"](#)
- ["Prepárese para administrar su sistema AFX"](#)
- ["Migrar un SVM del sistema AFX"](#)
- ["Herramienta de matriz de interoperabilidad de NetApp"](#)

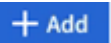
Crear y configurar un volumen en un sistema de almacenamiento AFX

Puede crear un volumen y adjuntarlo a una SVM. Cada volumen se puede exponer a los clientes mediante uno de los protocolos de acceso compatibles con AFX.

Acerca de esta tarea

Al crear un volumen, debe proporcionar una cantidad mínima de detalles de configuración. Se pueden proporcionar detalles adicionales durante la creación o posteriormente editando el volumen. Debe seleccionar la SVM para el volumen si ha creado SVM adicionales.

Pasos

1. En el Administrador del sistema, seleccione **Almacenamiento** y luego **Volúmenes**.
2. Seleccionar  y proporcionar la configuración básica incluyendo nombre, capacidad y optimización.
3. Opcionalmente, seleccione **Más opciones** para obtener una configuración adicional relacionada con la protección de datos, SnapLock y el acceso NFS.
4. Seleccionar **Guardar** para agregar el volumen.

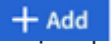
Administrar los volúmenes del sistema de almacenamiento AFX

Hay varias tareas administrativas que puede realizar como parte de la administración de los volúmenes definidos en su clúster AFX.

Crear un qtree

Un qtree es una subdivisión lógica dentro de un volumen que puede crear para organizar y administrar datos.

Pasos

1. En el Administrador del sistema, seleccione **Almacenamiento** y luego **Qtrees**.
2. Seleccionar  y proporcionar la configuración básica, incluido el nombre, el volumen y el estilo de seguridad; opcionalmente, configurar una cuota.
3. Seleccione **Guardar** para agregar el qtree.

Crear una cuota

Una cuota es un límite establecido en la cantidad de espacio de almacenamiento o número de archivos que puede usar un usuario, grupo o qtree. Las cuotas se utilizan para administrar y controlar el uso de recursos dentro de un sistema AFX.

Pasos

1. En el Administrador del sistema, seleccione **Almacenamiento** y luego **Cuotas**.
2. Seleccione la pestaña **Uso** para mostrar una lista de las cuotas activas en todos los volúmenes.
3. Seleccione la pestaña **Volúmenes** para mostrar una lista de los volúmenes definidos en el clúster AFX; seleccione un volumen específico para mostrar información adicional.
4. Para definir una cuota, seleccione la pestaña **Reglas**.
5. Proporcione los detalles de configuración, incluido el objetivo de cuota, el tipo y los límites.
6. Seleccione **Guardar** para agregar la cuota.

Crear y configurar un bucket S3 en un sistema de almacenamiento AFX

Puede crear un depósito y adjuntarlo a una SVM. Cada bucket se puede exponer a clientes que utilizan el protocolo de acceso S3 compatible con AFX.

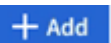
Acerca de esta tarea

Al crear un depósito, debe proporcionar una cantidad mínima de detalles de configuración. Se pueden proporcionar detalles adicionales durante la creación o posteriormente editando el depósito. Debe seleccionar la SVM para el depósito si ha creado SVM adicionales.

Antes de empezar

Debe configurar el servicio S3 para la SVM para que los clientes puedan acceder al depósito.

Pasos

1. En el Administrador del sistema, seleccione **Almacenamiento** y luego **Depósitos**.
2. Seleccionar  y proporcionar la configuración básica, incluido el nombre y la capacidad.
3. Opcionalmente, seleccione **Más opciones** para realizar configuraciones adicionales relacionadas con la protección de datos, el bloqueo y los permisos.

4. Seleccione **Guardar** para agregar el depósito.

Administrar los depósitos del sistema de almacenamiento AFX

Hay varias tareas administrativas que puede realizar como parte de la gestión de los buckets AFX S3 y el acceso del cliente. La configuración y el soporte de S3 en AFX son los mismos que los que se proporcionan con Unified ONTAP. Consulte la documentación de Unified ONTAP para obtener más detalles.

Información relacionada

["Obtenga más información sobre la configuración de ONTAP S3"](#)

Supervisar y solucionar problemas de un sistema de almacenamiento AFX

El sistema AFX incluye varias opciones para monitorear el almacenamiento que administra cada clúster.

Mostrar clientes NAS

Puede mostrar una lista de los clientes NFS y SMB/CIFS conectados actualmente al clúster AFX.

Pasos

1. En el Administrador del sistema, seleccione **Clientes** en el panel de navegación.
2. Seleccione la pestaña **NFS** o **SMB/CIFS** según desee.
3. Personalice la visualización, así como la búsqueda y descarga de información del cliente según sea necesario.

Información relacionada

- ["Prepárese para administrar sus datos AFX"](#)

Proteger datos

Prepárese para proteger los datos de su sistema de almacenamiento AFX

Antes de proteger sus datos de AFX, debe familiarizarse con algunos de los conceptos y capacidades clave.



Debido a que muchos de los conceptos y procedimientos de administración disponibles en los sistemas AFF y FAS son los mismos que los de los sistemas de almacenamiento AFX, es recomendable revisar la documentación de Unified ONTAP para ["Protección de datos y recuperación ante desastres"](#) Puede ser útil.

Terminología y opciones

Hay varios términos relacionados con la protección de datos de AFX que debe conocer.

Snapshot

Una instantánea es una imagen de un volumen, de solo lectura y en un punto determinado del tiempo. Es una tecnología fundamental para los servicios de replicación y protección de datos de ONTAP.

Grupo de consistencia

Un grupo de consistencia es una colección de volúmenes que se administran como una sola unidad. Puede crear grupos de consistencia para simplificar la administración del almacenamiento y la protección de datos para las cargas de trabajo de las aplicaciones. Por ejemplo, puede tomar instantáneas de varios volúmenes en una operación utilizando el grupo de consistencia en lugar de los volúmenes individuales.

Grupo de consistencia jerárquica

Los grupos de consistencia jerárquica se introdujeron con ONTAP 9.16.1 y están disponibles con AFX. Con una estructura jerárquica, uno o más grupos de consistencia se pueden configurar como hijos de un padre. Estos grupos jerárquicos le permiten aplicar políticas de instantáneas individuales a grupos de consistencia secundarios y replicar las instantáneas de todos los secundarios en un clúster remoto como una sola unidad replicando al primario.

SnapLock

SnapLock es una función de ONTAP que le permite proteger sus archivos moviéndolos a un estado de escritura única y lectura múltiple (WORM). Esto evita la modificación o eliminación durante un período de retención específico. Los volúmenes SnapLock creados no se pueden convertir a partir de volúmenes que no sean SnapLock después de la creación en función de la retención.

Limitaciones de la protección de datos de AFX

Debe conocer los límites y restricciones de protección de datos de ONTAP aplicados por el sistema de almacenamiento AFX.

SnapMirror sincrónico (SM-S)

Existe una limitación de escala al usar SM-S. Se puede tener un máximo de 400 relaciones en un solo clúster del sistema AFX.

Información relacionada

- ["Administración adicional de AFX SVM"](#)
- ["Prepárese para administrar su sistema AFX"](#)

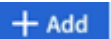
Crear un grupo de consistencia en un sistema de almacenamiento AFX

Puede crear grupos de consistencia para simplificar la administración del almacenamiento y la protección de datos para las cargas de trabajo de las aplicaciones. Un grupo de consistencia puede basarse en volúmenes existentes o nuevos.

Antes de empezar

Si planea crear uno o más volúmenes nuevos, debe consultar las opciones de configuración al crear un nuevo volumen.

Pasos

1. En el Administrador del sistema, seleccione **Protección** y luego **Grupos de consistencia**.
2. Seleccionar  y elige uno de:

- Uso de volúmenes existentes
 - Uso de nuevos volúmenes NAS
3. Proporcione los detalles de configuración, incluido el nombre, los volúmenes, el tipo de aplicación y la protección.
 4. Seleccione **Agregar**.

Información relacionada

- ["Administrar grupos de consistencia"](#)
- ["Crear y configurar un volumen AFX"](#)

Administrar grupos de consistencia en un sistema de almacenamiento AFX

Puede administrar los grupos de consistencia en un sistema AFX. Esto puede simplificar la administración de su almacenamiento.

Agregar protección de datos de instantáneas a un grupo de consistencia

Cuando agrega protección de datos de instantáneas a un grupo de consistencia, se pueden tomar instantáneas locales del grupo de consistencia a intervalos regulares según un cronograma predefinido.

Pasos

1. En el Administrador del sistema, seleccione **Protección** y luego **Grupos de consistencia**.
2. Coloque el cursor sobre el grupo de consistencia que desea proteger.
3. Seleccionar  ; luego seleccione **Editar**.
4. En **Protección local**, seleccione **Programar instantáneas**.
5. Seleccione una política de instantáneas.

Acepte la política de instantáneas predeterminada, seleccione una política existente o cree una nueva.

Opción	Pasos
Seleccionar una política de instantáneas existente	Seleccionar  junto a la política predeterminada; luego seleccione la política existente que desea utilizar.

Opción	Pasos
Crear una nueva política de instantáneas	- Seleccionar + Add ; luego ingrese el nombre de la nueva política. - Seleccione el alcance de la política. - En Horarios seleccione + Add . - Seleccione el nombre que aparece debajo de Nombre del programa; luego seleccione ▼ . - Seleccione el cronograma de políticas. - En Máximo de instantáneas, ingrese la cantidad máxima de instantáneas que desea conservar del grupo de consistencia. - Opcionalmente, en *Etiqueta SnapMirror * ingrese una etiqueta SnapMirror . - Seleccione Guardar.

6. Seleccione **Editar**.

Información relacionada

- ["Obtenga más información sobre los grupos de consistencia de ONTAP"](#)

Crear una instantánea en un sistema de almacenamiento AFX

Para realizar una copia de seguridad de los datos de su sistema AFX, debe crear una instantánea. Puede crear una instantánea manualmente o programarla para que se cree automáticamente mediante un grupo de consistencia.

Antes de empezar

Una instantánea es una copia local, de solo lectura, de sus datos que puede usar para restaurar volúmenes a puntos específicos en el tiempo. Las instantáneas se pueden crear manualmente a pedido o automáticamente a intervalos regulares según un ["Política y programación de instantáneas"](#) .

La política y la programación de instantáneas especifican los detalles, incluido cuándo crear las instantáneas, cuántas copias conservar, cómo nombrarlas y cómo etiquetarlas para la replicación. Por ejemplo, un sistema podría crear una instantánea todos los días a las 12:10 a. m., conservar las dos copias más recientes, nombrarlas "diarias" (con una marca de tiempo adjunta) y etiquetarlas como "diarias" para su replicación.

Tipos de instantáneas

Puede crear una instantánea a pedido de un solo volumen o de un grupo de consistencia. También puede crear instantáneas automatizadas de un grupo de consistencia que contenga varios volúmenes. Sin embargo, no es posible crear instantáneas automatizadas de un solo volumen.

- Instantáneas a pedido

Puede crear una instantánea a pedido de un volumen en cualquier momento. No es necesario que el volumen sea miembro de un grupo de consistencia para estar protegido por una instantánea a pedido. Si crea una instantánea de un volumen que es miembro de un grupo de consistencia, los demás volúmenes del grupo de consistencia no se incluyen en la instantánea. Cuando se crea una instantánea a pedido de

un grupo de consistencia, se incluyen todos los volúmenes del grupo de consistencia.

- **Instantáneas automatizadas**

Se crean instantáneas automatizadas según las definiciones de políticas de instantáneas. Para aplicar una política de instantáneas a un volumen para la creación automática de instantáneas, los volúmenes deben ser miembros del mismo grupo de consistencia. Si aplica una política de instantáneas a un grupo de consistencia, todos los volúmenes del grupo de consistencia estarán protegidos.

Crear una instantánea

Crear una instantánea de un volumen o grupo de consistencia.

Instantánea de un grupo de consistencia

Pasos

1. En el Administrador del sistema, seleccione **Protección** y luego **Grupos de consistencia**.
2. Coloque el cursor sobre el nombre del grupo de consistencia que desea proteger.
3. Seleccionar  ; luego seleccione **Proteger**.
4. Si desea crear una instantánea inmediata a pedido, en **Protección local**, seleccione **Agregar una instantánea ahora**.

La protección local crea la instantánea en el mismo clúster que contiene el volumen.

- a. Ingrese un nombre para la instantánea o acepte el nombre predeterminado; luego, opcionalmente, ingrese una etiqueta SnapMirror .

La etiqueta SnapMirror es utilizada por el destino remoto.

5. Si desea crear instantáneas automatizadas utilizando una política de instantáneas, seleccione **Programar instantáneas**.

- a. Seleccione una política de instantáneas.

Acepte la política de instantáneas predeterminada, seleccione una política existente o cree una nueva.

Opción	Pasos
Seleccionar una política de instantáneas existente	Seleccionar  junto a la política predeterminada; luego seleccione la política existente que desea utilizar.
Crear una nueva política de instantáneas	i. Seleccionar  Add ; luego ingrese los parámetros de la política de instantáneas. ii. Seleccione Agregar política.

6. Si desea replicar sus instantáneas en un clúster remoto, en **Protección remota**, seleccione **Replicar en un clúster remoto**.

- a. Seleccione el clúster de origen y la máquina virtual de almacenamiento; luego, seleccione la política de replicación.

La transferencia de datos inicial para la replicación comienza inmediatamente de forma predeterminada.

7. Seleccione **Guardar**.

Instantánea de un volumen

Pasos

1. En el Administrador del sistema, seleccione **Almacenamiento** y luego **Volúmenes**.
2. Coloque el cursor sobre el nombre del volumen que desea proteger.
3. Seleccionar  ; luego seleccione **Proteger**. Si desea crear una instantánea inmediata a pedido, en **Protección local**, seleccione **Agregar una instantánea ahora**.

La protección local crea la instantánea en el mismo clúster que contiene el volumen.

4. Ingrese un nombre para la instantánea o acepte el nombre predeterminado; luego, opcionalmente, ingrese una etiqueta SnapMirror .

La etiqueta SnapMirror es utilizada por el destino remoto.

5. Si desea crear instantáneas automatizadas utilizando una política de instantáneas, seleccione **Programar instantáneas**.

- a. Seleccione una política de instantáneas.

Acepte la política de instantáneas predeterminada, seleccione una política existente o cree una nueva.

Opción	Pasos
Seleccionar una política de instantáneas existente	Seleccionar  junto a la política predeterminada; luego seleccione la política existente que desea utilizar.
Crear una nueva política de instantáneas	i. Seleccionar  Add ; luego ingrese los parámetros de la política de instantáneas. ii. Seleccione Agregar política.

6. Si desea replicar sus instantáneas en un clúster remoto, en **Protección remota**, seleccione **Replicar en un clúster remoto**.

- a. Seleccione el clúster de origen y la máquina virtual de almacenamiento; luego, seleccione la política de replicación.

La transferencia de datos inicial para la replicación comienza inmediatamente de forma predeterminada.

7. Seleccione **Guardar**.

Información relacionada

- ["Crear una política de instantáneas de ONTAP"](#)

Administrar instantáneas en un sistema de almacenamiento AFX

Puede administrar instantáneas en su sistema AFX. Consulte la documentación de Unified ONTAP para obtener más detalles.

Información relacionada

- ["Crear una política de instantáneas de ONTAP"](#)
- ["Proteger los volúmenes de ONTAP FlexGroup mediante instantáneas"](#)

Crear una relación de pares SVM entre clústeres en un sistema de almacenamiento AFX

Una relación de pares define las conexiones de red que permiten que los clústeres y las máquinas virtuales (VM) de almacenamiento intercambien datos de forma segura. Puede crear una relación de pares entre máquinas virtuales de almacenamiento en diferentes clústeres para habilitar la protección de datos y la recuperación ante desastres mediante SnapMirror.

Antes de empezar

Debe haber establecido una relación de pares de clúster entre los clústeres locales y remotos antes de poder crear una relación de pares de VM de almacenamiento. "[Crear una relación de pares de clúster](#)" Si aún no lo has hecho.

Pasos

1. En el Administrador del sistema, seleccione **Protección > Descripción general**.
2. En **Pares de máquinas virtuales de almacenamiento**, seleccione **Agregar un par de máquinas virtuales de almacenamiento**.
3. Seleccione la VM de almacenamiento en el clúster local; luego, seleccione la VM de almacenamiento en el clúster remoto.
4. Seleccione **Agregar un par de VM de almacenamiento**.

Información relacionada

- "[Aprenda más sobre las relaciones entre pares](#)" .

Administrar la replicación de instantáneas en un sistema de almacenamiento AFX

La replicación de instantáneas es un proceso en el que los grupos de consistencia de su sistema AFX se copian a una ubicación geográficamente remota. Después de la replicación inicial, los cambios en los grupos de consistencia se copian a la ubicación remota según una política de replicación. Los grupos de consistencia replicados se pueden utilizar para la recuperación ante desastres o la migración de datos.

Para configurar la replicación de instantáneas, debe establecer una relación de replicación entre su sistema de almacenamiento AFX y la ubicación remota. La relación de replicación está gobernada por una política de replicación. Durante la configuración del clúster se crea una política predeterminada para replicar todas las instantáneas. Puede utilizar la política predeterminada o, opcionalmente, crear una nueva política.

Paso 1: Crear una relación de pares de clúster

Antes de poder proteger sus datos replicándolos en un clúster remoto, debe crear una relación de pares de clúster entre el clúster local y el remoto.

Antes de empezar

Los requisitos previos para el peering de clústeres son los mismos para los sistemas AFX que para otros sistemas ONTAP . "[Revise los requisitos previos para el peering de clústeres](#)" .

Pasos

1. En el clúster local, en el Administrador del sistema, seleccione **Clúster > Configuración**.

2. En **Configuración entre clústeres**, junto a **Pares de clúster**, seleccione  , luego seleccione **Agregar un par del clúster**.
3. Seleccione **Iniciar clúster remoto**; esto genera una frase de contraseña que utilizará para autenticarse con el clúster remoto.
4. Después de generar la frase de contraseña para el clúster remoto, péguela en **Frase de contraseña** en el clúster local.
5. Seleccionar  **Add** ; luego ingrese la dirección IP de la interfaz de red entre clústeres.
6. Seleccione **Iniciar peering de clúster**.

¿Que sigue?

Ha emparejado un clúster AFX local con un clúster remoto. Ahora puede crear una relación de replicación.

Paso 2: Opcionalmente, cree una política de replicación

La política de replicación de instantáneas define cuándo se replican en el sitio remoto las actualizaciones realizadas en el clúster AFX.

Pasos

1. En el Administrador del sistema, seleccione **Protección > Políticas**; luego seleccione **Políticas de replicación**.
2. Seleccionar  **Add** .
3. Ingrese un nombre para la política de replicación o acepte el nombre predeterminado; luego ingrese una descripción.
4. Seleccione el **Alcance de la política**.

Si desea aplicar la política de replicación a todo el clúster, seleccione **Clúster**. Si desea que la política de replicación se aplique solo al volumen en una máquina virtual de almacenamiento específica, seleccione **Máquina virtual de almacenamiento**.

5. Seleccione el **Tipo de política**.

Opción	Pasos
Copiar datos al sitio remoto después de escribirlos en la fuente.	a. Seleccione Asincrónico. b. En Transferir instantáneas desde la fuente, acepte el programa de transferencia predeterminado o seleccione uno diferente. c. Seleccione para transferir todas las instantáneas o crear reglas para determinar qué instantáneas transferir. d. Opcionalmente, habilite la compresión de red.
Escribir datos en los sitios de origen y remotos simultáneamente.	a. Seleccione Sincrónico.

6. Seleccione **Guardar**.

¿Que sigue?

Ha creado una política de replicación y ahora está listo para crear una relación de replicación entre su sistema

AFX y su ubicación remota.

Paso 3: Crear una relación de replicación

Una relación de replicación de instantáneas establece una conexión entre su sistema AFX y una ubicación remota para que pueda replicar grupos de consistencia en un clúster remoto. Los grupos de consistencia replicados se pueden utilizar para la recuperación ante desastres o para la migración de datos.

Para protegerse contra ataques de ransomware, cuando configura su relación de replicación, puede seleccionar bloquear las instantáneas de destino. Las instantáneas bloqueadas no se pueden eliminar de forma accidental o maliciosa. Puede utilizar instantáneas bloqueadas para recuperar datos si un volumen se ve comprometido por un ataque de ransomware.

Antes de empezar

Cree una relación de replicación con o sin instantáneas de destino bloqueadas.

Con instantáneas bloqueadas

Pasos

1. En el Administrador del sistema, seleccione **Protección > Grupos de consistencia**.
2. Seleccione un grupo de consistencia.
3. Seleccionar  ; luego seleccione **Proteger**.
4. En **Protección remota**, seleccione **Replicar a un clúster remoto**.
5. Seleccione la **Política de replicación**.

Debe seleccionar una política de replicación *vault*.

6. Seleccione **Configuración de destino**.
7. Seleccione **Bloquear instantáneas de destino para evitar su eliminación**.
8. Introduzca el período máximo y mínimo de retención de datos.
9. Para retrasar el inicio de la transferencia de datos, desmarque **Iniciar transferencia inmediatamente**.

La transferencia de datos inicial comienza inmediatamente de forma predeterminada.

10. Opcionalmente, para anular el programa de transferencia predeterminado, seleccione **Configuración de destino** y, a continuación, seleccione **Anular programa de transferencia**.

Su horario de traslado debe ser de un mínimo de 30 minutos para ser compatible.

11. Seleccione **Guardar**.

Sin instantáneas bloqueadas

Pasos

1. En el Administrador del sistema, seleccione **Protección > Replicación**.
2. Seleccione para crear la relación de replicación con el destino local o la fuente local.

Opción	Pasos
Destinos locales	a. Seleccione Destinos locales, luego seleccione . b. Busque y seleccione el grupo de consistencia de origen. El grupo de consistencia <i>source</i> hace referencia al grupo de consistencia en el clúster local que desea replicar.

Opción	Pasos
Fuentes locales	a. Seleccione Fuentes locales y luego seleccione  . b. Busque y seleccione el grupo de consistencia de origen. El grupo de consistencia <i>source</i> hace referencia al grupo de consistencia en el clúster local que desea replicar. c. En Destino de replicación, seleccione el clúster al que se replicará; luego, seleccione la máquina virtual de almacenamiento.

3. Seleccione una política de replicación.

4. Para retrasar el inicio de la transferencia de datos, seleccione **Configuración de destino**; luego desmarque **Iniciar transferencia inmediatamente**.

La transferencia de datos inicial comienza inmediatamente de forma predeterminada.

5. Opcionalmente, para anular el programa de transferencia predeterminado, seleccione **Configuración de destino** y, a continuación, seleccione **Anular programa de transferencia**.

Su horario de traslado debe ser de un mínimo de 30 minutos para ser compatible.

6. Seleccione **Guardar**.

¿Que sigue?

Ahora que ha creado una política y una relación de replicación, su transferencia de datos inicial comienza según lo definido en su política de replicación. Opcionalmente, puede probar su conmutación por error de replicación para verificar que pueda ocurrir una conmutación por error exitosa si su sistema AFX se desconecta.

Paso 4: Pruebe la conmutación por error de replicación

De manera opcional, valide que pueda servir con éxito datos desde volúmenes replicados en un clúster remoto si el clúster de origen está fuera de línea.

Pasos

1. En el Administrador del sistema, seleccione **Protección > Replicación**.
2. Coloque el cursor sobre la relación de replicación que desea probar y luego seleccione  .
3. Seleccione **Prueba de conmutación por error**.
4. Ingrese la información de conmutación por error y luego seleccione **Probar conmutación por error**.

¿Que sigue?

Ahora que sus datos están protegidos con la replicación de instantáneas para la recuperación ante desastres, debería [Cifre sus datos en reposo](#) para que no se pueda leer si un disco en su sistema AFX se reutiliza, se devuelve, se extravía o se lo roban.

Administrar las políticas y los cronogramas de protección de datos del sistema de almacenamiento AFX

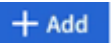
Puede utilizar políticas de instantáneas para proteger los datos en sus grupos de consistencia según una programación automatizada. Los programas de políticas dentro de las políticas de instantáneas determinan la frecuencia con la que se toman instantáneas.

Crear un nuevo programa de políticas de protección

Una programación de política de protección define la frecuencia con la que se ejecuta una política de instantáneas. Puede crear programaciones para que se ejecuten en intervalos regulares según una cantidad de días, horas o minutos. Por ejemplo, puede crear un programa para que se ejecute cada hora o para que se ejecute solo una vez al día. También puedes crear programaciones para que se ejecuten en momentos específicos en días específicos de la semana o del mes. Por ejemplo, puedes crear un cronograma para que se ejecute a las 12:15 a. m. el día 20 de cada mes.

Definir varios programas de políticas de protección le brinda la flexibilidad de aumentar o disminuir la frecuencia de las instantáneas para diferentes aplicaciones. Esto le permite proporcionar un mayor nivel de protección y un menor riesgo de pérdida de datos para sus cargas de trabajo críticas que lo que podría ser necesario para cargas de trabajo menos críticas.

Pasos

1. Seleccione **Protección** y luego **Políticas**; luego seleccione **Programación**.
2. Seleccionar  **Add** .
3. Ingrese un nombre para la programación; luego seleccione los parámetros de la programación.
4. Seleccione **Guardar**.

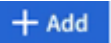
¿Que sigue?

Ahora que ha creado un nuevo programa de políticas, puede utilizar el programa recién creado dentro de sus políticas para definir cuándo se toman las instantáneas.

Crear una política de instantáneas

Una política de instantáneas define la frecuencia con la que se toman instantáneas, la cantidad máxima de instantáneas permitidas y durante cuánto tiempo se conservan las instantáneas.

Pasos

1. En el Administrador del sistema, seleccione **Protección** y luego **Políticas**; luego seleccione **Políticas de instantáneas**.
2. Seleccionar  **Add** .
3. Introduzca un nombre para la política de instantáneas.
4. Seleccione **Clúster** para aplicar la política a todo el clúster. Seleccione **VM de almacenamiento** para aplicar la política a una VM de almacenamiento individual.
5. Seleccione **Agregar una programación**; luego ingrese la programación de la política de instantáneas.
6. Seleccione **Agregar política**.

¿Que sigue?

Ahora que ha creado una política de instantáneas, puede aplicarla a un grupo de consistencia. Se tomarán

instantáneas del grupo de consistencia según los parámetros que configure en su política de instantáneas.

Aplicar una política de instantáneas a un grupo de consistencia

Aplique una política de instantáneas a un grupo de consistencia para crear, conservar y etiquetar automáticamente instantáneas del grupo de consistencia.

Pasos

1. En el Administrador del sistema, seleccione **Protección** y luego **Políticas**; luego seleccione **Políticas de instantáneas**.
2. Coloque el cursor sobre el nombre de la política de instantáneas que desea aplicar.
3. Seleccionar  ; luego seleccione **Aplicar**.
4. Seleccione los grupos de consistencia a los que desea aplicar la política de instantáneas; luego seleccione **Aplicar**.

¿Que sigue?

Ahora que sus datos están protegidos con instantáneas, debería ["establecer una relación de replicación"](#) para copiar sus grupos de consistencia a una ubicación geográficamente remota para realizar copias de seguridad y recuperación ante desastres.

Editar, eliminar o deshabilitar una política de instantáneas

Edite una política de instantáneas para modificar el nombre de la política, la cantidad máxima de instantáneas o la etiqueta SnapMirror . Elimine una política para eliminarla y sus datos de respaldo asociados de su clúster. Deshabilite una política para detener temporalmente la creación o transferencia de instantáneas especificadas por la política.

Pasos

1. En el Administrador del sistema, seleccione **Protección** y luego **Políticas**; luego seleccione **Políticas de instantáneas**.
2. Coloque el cursor sobre el nombre de la política de instantáneas que desea editar.
3. Seleccionar  ; luego seleccione **Editar**, **Eliminar** o **Deshabilitar**.

Resultado

Ha modificado, eliminado o deshabilitado la política de instantáneas.

Editar una política de replicación

Edite una política de replicación para modificar la descripción de la política, el programa de transferencia y las reglas. También puede editar la política para habilitar o deshabilitar la compresión de red.

Pasos

1. En el Administrador del sistema, seleccione **Protección** y luego **Políticas**.
2. Seleccione **Políticas de replicación**.
3. Coloque el cursor sobre la política de replicación que desea editar; luego seleccione  .
4. Seleccione **Editar**.
5. Actualice la política; luego seleccione **Guardar**.

Datos seguros

Prepárese para proteger los datos de su sistema de almacenamiento AFX

Antes de administrar sus datos AFX, debe familiarizarse con los principales conceptos y capacidades.

Terminología y opciones

Hay varios términos relacionados con la seguridad de datos de AFX con los que debe estar familiarizado.

Ransomware

El ransomware es un software malicioso que cifra los archivos y los hace inaccesibles para el usuario. Generalmente se exige algún tipo de pago para descifrar los datos. ONTAP ofrece soluciones de protección contra ransomware a través de funciones como Autonomous Ransomware Protection (ARP).

Cifrado

El cifrado es el proceso de convertir datos a un formato seguro que no se puede leer fácilmente sin la autorización adecuada. ONTAP ofrece tecnologías de cifrado basadas en software y hardware para proteger los datos en reposo. Esto garantiza que no se pueda leer si el medio de almacenamiento se reutiliza, se devuelve, se extravía o se roba. Estas soluciones de cifrado se pueden gestionar mediante un servidor de administración de claves externo o mediante el administrador de claves integrado proporcionado por ONTAP. Referirse a ["Cifrar datos en reposo en un sistema de almacenamiento AFX"](#) Para más información.

Certificados digitales y PKI

Un certificado digital es un documento electrónico que se utiliza para demostrar la propiedad de una clave pública. La clave pública y la clave privada asociada se pueden utilizar de diversas maneras, incluso para establecer la identidad, generalmente como parte de un marco de seguridad más amplio, como TLS e IPsec. Estas claves, así como los protocolos de soporte y los estándares de formato, forman la base de la infraestructura de clave pública (PKI). Referirse a ["Administrar certificados en un sistema de almacenamiento AFX"](#) Para más información.

Seguridad del Protocolo de Internet

IPsec es un estándar de Internet que proporciona encriptación, integridad y autenticación de datos en tránsito para el tráfico que fluye entre puntos finales de la red a nivel de IP. Asegura todo el tráfico IP entre ONTAP y los clientes, incluidos los protocolos de nivel superior como NFS y SMB. IPsec brinda protección contra repeticiones maliciosas y ataques del tipo "man-in-the-middle" en sus datos. Referirse a ["Conexiones IP seguras en sus sistemas de almacenamiento AFX"](#) Para más información.

Información relacionada

- ["Administración adicional de AFX SVM"](#)
- ["Prepárese para administrar su sistema AFX"](#)

Cifrar datos en reposo en un sistema de almacenamiento AFX

Puede cifrar sus datos a nivel de hardware y software para obtener protección de doble capa. Cuando se cifran datos en reposo, no se pueden leer si el medio de almacenamiento se reutiliza, se devuelve, se extravía o se roba.

NetApp Storage Encryption (NSE) admite el cifrado de hardware mediante unidades de autocifrado (SED). Los SED cifran los datos a medida que se escriben. Cada SED contiene una clave de cifrado única. Los datos cifrados almacenados en la SED no se pueden leer sin la clave de cifrado de la SED. Los nodos que intentan leer desde un SED deben estar autenticados para acceder a la clave de cifrado del SED. Los nodos se autentican obteniendo una clave de autenticación de un administrador de claves y luego presentando dicha clave al SED. Si la clave de autenticación es válida, el SED le dará al nodo su clave de cifrado para acceder a los datos que contiene.

Antes de empezar

Utilice el administrador de claves integrado de AFX o un administrador de claves externo para entregar claves de autenticación a sus nodos. Además de NSE, también puedes habilitar el cifrado de software para agregar otra capa de seguridad a tus datos.

Pasos

1. En el Administrador del sistema, seleccione **Clúster** y luego **Configuración**.
2. En la sección **Seguridad**, en **Cifrado**, seleccione **Configurar**.
3. Configurar el administrador de claves.

Opción	Pasos
Configurar el administrador de claves integrado	a. Seleccione Administrador de claves integrado para agregar los servidores de claves. b. Introduzca una frase de contraseña.
Configurar un administrador de claves externo	a. Seleccione Administrador de claves externo para agregar los servidores de claves. b. Seleccionar + Add para agregar los servidores clave. c. Agregue los certificados CA del servidor KMIP. d. Agregue los certificados de cliente KMIP.

4. Seleccione **Cifrado de doble capa** para habilitar el cifrado de software.
5. Seleccione **Guardar**.

Información relacionada

- ["Cifrado"](#)

Conexiones IP seguras en sus sistemas de almacenamiento AFX

Seguridad IP (IPsec) es un estándar de protocolo de Internet que proporciona encriptación, integridad y autenticación de datos para el tráfico que fluye entre los puntos finales de la red a nivel de IP. Puede utilizar IPsec para mejorar la seguridad de la red front-end entre un clúster AFX y los clientes.

Configuración de IPsec en un sistema AFX

Los procedimientos de configuración de IPsec para los sistemas de almacenamiento AFX son los mismos que

para los sistemas AFF y FAS , con la excepción de las tarjetas controladoras de interfaz de red (NIC) compatibles que se utilizan con la función de descarga de hardware. Referirse a ["Prepárese para configurar la seguridad IP para la red ONTAP."](#) Para más información.

Función de descarga de hardware

Varias de las operaciones criptográficas de IPsec, como el cifrado y las comprobaciones de integridad, se pueden descargar a una tarjeta NIC compatible en su sistema AFX. Esto puede mejorar significativamente el rendimiento y el rendimiento del tráfico de red protegido por IPsec.



A partir de ONTAP 9.18.1, la función de descarga de hardware de IPsec se amplía para admitir el tráfico IPv6.

Las siguientes tarjetas NIC son compatibles con la función de descarga de hardware IPsec en sistemas de almacenamiento AFX a partir de ONTAP 9.17.1:

- X50130B (controlador Ethernet 2p, 40G/100G)
- X50131B (controlador Ethernet 2p, 40G/100G/200G/400G)

Consulte la ["NetApp Hardware Universe"](#) para obtener más información sobre las tarjetas compatibles con la versión ONTAP que se ejecuta en su sistema AFX.

Información relacionada

- ["Prepárese para configurar la seguridad IP para la red ONTAP."](#)
- ["NetApp Hardware Universe"](#)

Administración adicional para un sistema de almacenamiento AFX SVM

Además de la administración típica de AFX SVM, es posible que haya otras tareas que deba realizar según su entorno. La mayoría de las tareas adicionales se pueden realizar mediante el Administrador del sistema, aunque en algunos casos es posible que sea necesario utilizar la CLI.



Las características y la administración de ONTAP descritas son comunes a los sistemas de almacenamiento AFX y a los sistemas AFF o FAS que ejecutan Unified ONTAP. Se incluyen enlaces a la documentación relevante de Unified ONTAP según corresponda.

Gestión y rendimiento del almacenamiento

Hay varias funciones opcionales de administración y rendimiento de almacenamiento que puede configurar y usar con su implementación de AFX.

Gestión de almacenamiento NAS de ONTAP

El almacenamiento conectado a red (NAS) proporciona almacenamiento de archivos dedicado al que pueden acceder varios clientes en la red. ONTAP admite varios protocolos NAS. Referirse a ["Gestión de almacenamiento NAS"](#) Para más información.

Volúmenes ONTAP FlexCache

FlexCache es una función de almacenamiento en caché remoto de ONTAP . Acerca los datos a los clientes lo que mejora el rendimiento del acceso y reduce costes. La creación de un volumen FlexCache , que inicialmente copia solo los metadatos del sistema de archivos de origen, simplifica la distribución de archivos y reduce el tráfico WAN. Referirse a ["Obtenga más información sobre los volúmenes ONTAP FlexCache"](#) Para más información.

Volúmenes de ONTAP FlexGroup

Un volumen FlexGroup consta de varios volúmenes miembros que comparten el tráfico de forma automática y transparente. Los volúmenes FlexGroup ofrecen varios beneficios, incluido alto rendimiento y gestión simplificada. Referirse a ["Configuración del volumen de FlexGroup"](#) Para más información.

Protección de datos

Hay varias funciones de protección de datos opcionales que puede configurar y utilizar con su implementación de AFX.

Grupos de consistencia

Un grupo de consistencia es una colección de volúmenes que se administran como una sola unidad. Referirse a ["Obtenga más información sobre los grupos de consistencia de ONTAP"](#) Para más información.

SnapLock

Puede proteger sus archivos convirtiéndolos a un estado de escritura única y lectura múltiple (WORM) a nivel de volumen. SnapLock admite dos modos. El modo de cumplimiento garantiza que los archivos no se puedan eliminar hasta que expire su período de retención, lo que atiende mandatos gubernamentales o específicos de la industria. El modo empresarial permite a los usuarios privilegiados eliminar archivos antes de que expire su período de retención. Referirse a ["Obtenga más información sobre ONTAP SnapLock"](#) Para más información.

Seguridad

Hay varias funciones de seguridad opcionales que puede configurar y usar con su implementación de AFX.

Política

FPolicy es un marco de notificación de acceso a archivos que se utiliza para monitorear y administrar eventos de acceso a archivos en máquinas virtuales de almacenamiento (SVM). Puede utilizar FPolicy para crear políticas que definan qué operaciones de archivos supervisar y, opcionalmente, bloquear, según los criterios que usted defina. FPolicy se utiliza comúnmente para auditoría de seguridad, cumplimiento y gobernanza de datos. Referirse a ["Obtenga más información sobre las soluciones ONTAP FPolicy."](#) Para más información.

Monitoreo de eventos y rendimiento de ONTAP

Puede supervisar la salud y el rendimiento de un clúster. Esto incluye la configuración de alertas para eventos y la gestión de notificaciones para alertas de salud del sistema. Referirse a ["Monitoreo de eventos, rendimiento y salud"](#) Para más información.

Información relacionada

- ["Preguntas frecuentes sobre los sistemas de almacenamiento AFX"](#)

- "Administración adicional para clústeres AFX"

Información de copyright

Copyright © 2026 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.