



Gestione los archivos WORM

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

- Gestione los archivos WORM 1
 - Gestione los archivos WORM 1
 - Los archivos cumplen CON WORM. 1
 - Confirmar copias Snapshot a WORM en un destino de almacén 5
 - Refleje los archivos WORM para la recuperación ante desastres. 8
 - Conserve los archivos WORM durante su litigio gracias a su conservación legal 12
 - Información general acerca de Delete WORM files 13

Gestione los archivos WORM

Gestione los archivos WORM

Puede gestionar archivos WORM de las siguientes formas:

- "Los archivos cumplen CON WORM"
- "Confirmar copias Snapshot a WORM en un destino de almacén"
- "Refleje los archivos WORM para la recuperación ante desastres"
- "Conserve los archivos WORM durante su proceso de litigio"
- "Eliminar los archivos WORM"

Los archivos cumplen CON WORM

Puede confirmar archivos a WORM (escritura única y lectura múltiple) o bien manualmente, o bien conserva los archivos automáticamente. También puede crear archivos flexibles WORM.

Confirmar los archivos a WORM manualmente

Los archivos se comprometen a WORM manualmente haciendo que el archivo sea de solo lectura. Puede utilizar cualquier comando o programa adecuado a través de NFS o CIFS para cambiar el atributo de lectura y escritura de un archivo a sólo lectura. Puede optar por confirmar los archivos manualmente si desea garantizar que una aplicación haya terminado de escribir en un archivo de modo que el archivo no se confirme prematuramente o si hay problemas de escalado para el analizador de compromiso automático debido a un gran número de volúmenes.

Lo que necesitará

- El archivo que desea confirmar debe residir en un volumen de SnapLock.
- El archivo debe ser editable.

Acerca de esta tarea

El tiempo de la instancia de ComplianceClock del volumen se escribe en `ctime` campo del archivo cuando se ejecuta el comando o el programa. La hora de la instancia de ComplianceClock determina cuándo se ha alcanzado el tiempo de retención del archivo.

Pasos

1. Utilice un comando o programa adecuado para cambiar el atributo de lectura y escritura de un archivo a sólo lectura.

En un shell UNIX, utilice el siguiente comando para crear un archivo denominado `document.txt` solo lectura:

```
chmod -w document.txt
```

En un shell de Windows, utilice el siguiente comando para crear un archivo denominado `document.txt`

solo lectura:

```
attrib +r document.txt
```

Confirmar archivos a WORM automáticamente

La función de compromiso automático de SnapLock le permite confirmar los archivos automáticamente a WORM. La función de compromiso automático confirma un archivo en estado WORM en un volumen SnapLock si el archivo no cambió en el período de compromiso automático duración. La función de compromiso automático está deshabilitada de forma predeterminada.

Lo que necesitará

- Los archivos que desea confirmar automáticamente deben residir en un volumen de SnapLock.
- El volumen SnapLock debe estar en línea.
- El volumen SnapLock debe ser un volumen de lectura/escritura.



La función SnapLock autocommit analiza todos los archivos del volumen y confirma un archivo si cumple con el requisito de compromiso automático. Es posible que haya un intervalo de tiempo entre cuando el archivo esté listo para la confirmación automática y cuando el escáner de confirmación automática de SnapLock lo confirme realmente. Sin embargo, el sistema de archivos sigue protegiendo el archivo de las modificaciones y eliminaciones en cuanto sea apto para la confirmación automática.

Acerca de esta tarea

El *autocommit Period* especifica la cantidad de tiempo que los archivos deben permanecer sin cambios antes de que se autocomprometan. Al cambiar un archivo antes de que haya transcurrido el período de compromiso automático, se reinicia el período de compromiso automático del archivo.

En la siguiente tabla se muestran los posibles valores para el período de compromiso automático:

Valor	Unidad	Notas
ninguno	-	El valor predeterminado.
5 - 5256000	minutos	-
1 - 87600	horas	-
1 - 3650	días	-
1 - 120	meses	-
1 - 10	años	-



El valor mínimo es de 5 minutos y el valor máximo es de 10 años.

Pasos

1. Los archivos de confirmación automática en un volumen SnapLock a WORM:

```
volume snaplock modify -vserver SVM_name -volume volume_name -autocommit  
-period autocommit_period
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando confirma automáticamente los archivos en el volumen `vol1` De SVM `vs1`, siempre y cuando los archivos permanezcan inalterados durante 5 horas:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit  
-period 5hours
```

Crear un archivo ampliable WORM

Un archivo ampliable WORM conserva los datos escritos de forma incremental, como las entradas del registro. Puede utilizar cualquier comando o programa adecuado para crear un archivo que pueda adaptarse A WORM o la función SnapLock *volume append mode* para crear archivos WORM adaptados de forma predeterminada.

Utilice un comando o programa para crear un archivo que puede adaptarse A WORM

Puede utilizar cualquier comando o programa adecuado a través de NFS o CIFS para crear un archivo ampliable WORM. Un archivo ampliable WORM conserva los datos escritos de forma incremental, como las entradas del registro. Los datos se agregan al archivo en fragmentos de 256 KB. A medida que se escribe cada fragmento, el fragmento anterior se convierte en CON protección WORM. No se puede eliminar el archivo hasta que haya transcurrido el período de retención.

Lo que necesitará

El archivo ampliable WORM debe residir en un volumen SnapLock.

Acerca de esta tarea

Los datos no tienen que escribirse secuencialmente en el fragmento de 256 KB activo. Cuando se escriben datos en el byte $n \times 256\text{KB} + 1$ del archivo, el segmento de 256 KB anterior se protege WORM.

Pasos

1. Utilice un comando o programa adecuado para crear un archivo de longitud cero con el tiempo de retención deseado.

En un shell de UNIX, utilice el comando siguiente para establecer una hora de retención de 21 de noviembre de 2020 6:00 a.m. en un archivo de longitud cero denominado `document.txt`:

```
touch -a -t 202011210600 document.txt
```

2. Utilice un comando o programa adecuado para cambiar el atributo de lectura y escritura del archivo a sólo lectura.

En un shell UNIX, utilice el siguiente comando para crear un archivo denominado `document.txt` solo

lectura:

```
chmod 444 document.txt
```

3. Utilice un comando o programa adecuado para cambiar el atributo de lectura y escritura del archivo a grabable.



Este paso no se considera un riesgo de cumplimiento de normativas porque no hay datos en el archivo.

En un shell UNIX, utilice el siguiente comando para crear un archivo denominado `document.txt` modificable:

```
chmod 777 document.txt
```

4. Utilice un comando o programa adecuado para iniciar la escritura de datos en el archivo.

En un shell UNIX, utilice el comando siguiente para escribir datos en `document.txt`:

```
echo test data >> document.txt
```



Vuelva a cambiar los permisos de archivo a sólo lectura cuando ya no necesite agregar datos al archivo.

Use el modo de adición de volúmenes para crear archivos WORM flexibles

A partir de ONTAP 9.3, se puede utilizar la función SnapLock *volume append mode* (VAM) para crear archivos WORM flexibles de forma predeterminada. Un archivo ampliable WORM conserva los datos escritos de forma incremental, como las entradas del registro. Los datos se agregan al archivo en fragmentos de 256 KB. A medida que se escribe cada fragmento, el fragmento anterior se convierte en CON protección WORM. No se puede eliminar el archivo hasta que haya transcurrido el período de retención.

Lo que necesitará

- El archivo ampliable WORM debe residir en un volumen SnapLock.
- El volumen SnapLock debe estar desmontado y vacío de las copias Snapshot y los archivos creados por el usuario.

Acerca de esta tarea

Los datos no tienen que escribirse secuencialmente en el fragmento de 256 KB activo. Cuando se escriben datos en el byte $n \times 256\text{KB} + 1$ del archivo, el segmento de 256 KB anterior se protege WORM.

Si especifica un período de compromiso automático para el volumen, se comprometen a WORM los archivos flexibles que no se modifican durante un período superior al período de compromiso automático a WORM.



No se admite el VAM en los volúmenes de registros de auditoría de SnapLock.

Pasos

1. Activar VAM:

```
volume snaplock modify -vserver SVM_name -volume volume_name -is-volume-append  
-mode-enabled true|false
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando habilita VAM sobre el volumen vol1 De SVMvs1:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume  
-append-mode-enabled true
```

2. Utilice un comando o programa adecuado para crear archivos con permisos de escritura.

De forma predeterminada, los archivos se pueden APPWORM.

Confirmar copias Snapshot a WORM en un destino de almacén

Puede usar SnapLock para SnapVault para proteger CON WORM las copias Snapshot en el almacenamiento secundario. Todas las tareas básicas de SnapLock se realizan en el destino del almacén. El volumen de destino es de solo lectura montado automáticamente, por lo que no es necesario confirmar explícitamente las copias Snapshot a WORM; por lo tanto, no se admiten la creación de copias Snapshot programadas en el volumen de destino mediante políticas de SnapMirror.

Antes de empezar

- El clúster de origen debe ejecutar ONTAP 8.2.2 o una versión posterior.
- Los agregados de origen y destino deben tener 64 bits.
- El volumen de origen no puede ser un volumen de SnapLock.
- Los volúmenes de origen y destino deben crearse en clústeres con una relación entre iguales con SVM.

Para obtener más información, consulte ["Conexión de clústeres entre iguales"](#).

- Si se deshabilita el crecimiento automático de un volumen, el espacio libre en el volumen de destino debe ser al menos un cinco por ciento mayor que el espacio usado en el volumen de origen.

Acerca de esta tarea

El volumen de origen puede usar almacenamiento de NetApp o de terceros. Para el almacenamiento que no sea de NetApp, debe usar la virtualización de FlexArray.



No puede cambiar el nombre de una copia Snapshot que esté comprometida con el estado WORM.

Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock.



Los LUN no son compatibles con los volúmenes de SnapLock. Los LUN se admiten en volúmenes de SnapLock solo en casos en los que las copias de Snapshot creadas en un volumen distinto de SnapLock se transfieren a un volumen de SnapLock para la protección como parte de la relación de almacén de SnapLock. Los LUN no son compatibles con los volúmenes de SnapLock de lectura/escritura. Las copias Snapshot a prueba de manipulaciones son compatibles tanto con los volúmenes de origen como con los volúmenes de destino de SnapMirror que contienen LUN.

A partir de ONTAP 9.14.1, puede especificar períodos de retención para etiquetas de SnapMirror específicas en la política de SnapMirror de la relación de SnapMirror, de modo que las copias Snapshot replicadas del volumen de origen al de destino se conserven durante el período de retención especificado en la regla. Si no se especifica ningún período de retención, se utiliza el período de retención predeterminado del volumen de destino.

A partir de ONTAP 9.13.1, puede restaurar instantáneamente una copia Snapshot bloqueada en el volumen SnapLock de destino de una relación de almacén de SnapLock mediante la creación de un FlexClone con el `snaplock-type` Opción establecida en «non-snaplock» y especificando la copia Snapshot como la «parent-snapshot» al ejecutar la operación de creación de clones de volúmenes. Más información acerca de "[Creación de un volumen FlexClone con un tipo de SnapLock](#)".

Para las configuraciones de MetroCluster, debe tener en cuenta lo siguiente:

- Solo puede crear relaciones de SnapVault entre varias SVM sincronizada en origen, no entre una SVM sincronizada en origen y una SVM sincronizada en destino.
- Puede crear una relación de SnapVault entre un volumen en una SVM sincronizada en origen y una SVM que sirva datos.
- Puede crear una relación de SnapVault entre un volumen en una SVM que sirva datos y un volumen de DP en una SVM sincronizada en origen.

En la siguiente ilustración, se muestra el procedimiento para inicializar una relación de almacén de SnapLock:

Pasos

1. Identifique el clúster de destino.
2. En el clúster de destino, "[Instale la licencia de SnapLock](#)", "[Inicialice el reloj de cumplimiento](#)", Y, si está utilizando una versión de ONTAP anterior a 9.10.1, "[Cree un agregado de SnapLock](#)".
3. En el clúster de destino, cree un volumen de destino de SnapLock de tipo DP que tiene el mismo tamaño o mayor que el volumen de origen:

```
volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name  
-snaplock-type compliance|enterprise -type DP -size size
```



A partir de ONTAP 9.10.1, los volúmenes de SnapLock y otros de SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado de SnapLock separado si se utiliza ONTAP 9.10.1. La opción `volume -snaplock-type` se utiliza para especificar el tipo de volumen Compliance o Enterprise SnapLock. En las versiones de ONTAP anteriores a ONTAP 9.10.1, el modo SnapLock, Compliance o Enterprise, se hereda del agregado. No se admiten los volúmenes de destino con versión flexible. La configuración de idioma del volumen de destino debe coincidir con la configuración de idioma del volumen de origen.

El siguiente comando crea una SnapLock de 2 GB Compliance volumen denominado dstvolB pulg SVM2 en el agregado node01_aggr:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. En el clúster de destino, establezca el período de retención predeterminado, tal como se describe en [Establecer el período de retención predeterminado](#).



Un volumen SnapLock que es un destino de almacén tiene asignado un período de retención predeterminado. El valor correspondiente a este período se establece inicialmente en un mínimo de 0 años para volúmenes de SnapLock Enterprise y un máximo de 30 años para volúmenes de SnapLock Compliance. Cada copia de Snapshot de NetApp se compromete con el primer período de retención predeterminado. El período de retención se puede ampliar más adelante, si fuera necesario. Para obtener más información, consulte [Establecer información general sobre el tiempo de retención](#).

5. [Cree una nueva relación de replicación](#) Entre el origen que no es de SnapLock y el nuevo destino de SnapLock que creó en el paso 3.

En este ejemplo, se crea una nueva relación de SnapMirror con el volumen de SnapLock de destino dstvolB utilizar una política de XDPDefault Para almacenar las copias snapshot etiquetadas como diaria y semanal en una programación horaria:

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```



[Cree una política de replicación personalizada](#) o a [programación personalizada](#) si los valores predeterminados disponibles no son adecuados.

6. En la SVM de destino, inicialice la relación de SnapVault creada en el paso 5:

snapmirror initialize -destination-path destination_path

El siguiente comando inicializa la relación entre el volumen de origen srcvolA encendido SVM1 y el volumen de destino dstvolB encendido SVM2:

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

7. Después de inicializar y de estar inactiva la relación, utilice `snapshot show` Comando en el destino para comprobar el tiempo de caducidad de la SnapLock aplicado a las copias Snapshot replicadas.

En este ejemplo, se enumeran las copias Snapshot en el volumen dstvolB Que tienen la etiqueta de SnapMirror y la fecha de caducidad de SnapLock:

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields  
snapmirror-label, snaplock-expiry-time
```

Información relacionada

["Relaciones entre iguales de clústeres y SVM"](#)

["Backup de volúmenes mediante SnapVault"](#)

Refleje los archivos WORM para la recuperación ante desastres

Puede usar SnapMirror para replicar archivos WORM a otra ubicación geográfica a efectos de recuperación ante desastres y otros fines. Tanto el volumen de origen como el de destino deben configurarse para SnapLock, y ambos volúmenes deben tener el mismo modo SnapLock, Compliance o Enterprise. Se replican todas las propiedades clave de la SnapLock del volumen y los archivos.

Requisitos previos

Los volúmenes de origen y destino deben crearse en clústeres con una relación entre iguales con SVM. Para obtener más información, consulte ["Relaciones entre iguales de clústeres y SVM"](#).

Acerca de esta tarea

- A partir de ONTAP 9.5, puede replicar archivos WORM con la relación de tipo XDP (protección de datos ampliada) de SnapMirror en lugar de la relación de tipo DP (protección de datos). El modo XDP es independiente de las versiones de ONTAP y es capaz de diferenciar los archivos almacenados en el mismo bloque, facilitando de este modo la resincronización de los volúmenes replicados de modo de cumplimiento. Para obtener información sobre cómo convertir una relación de tipo DP existente a una relación de tipo XDP, consulte ["Protección de datos"](#).
- Una operación de resincronización de tipo DP relación SnapMirror genera un error en un volumen de modo de cumplimiento si SnapLock determina que provocará la pérdida de datos. Si una operación de resincronización falla, puede utilizar el `volume clone create` comando para crear un clon del volumen de destino. A continuación, puede volver a sincronizar el volumen de origen con el clon.
- Una relación de SnapMirror del tipo XDP entre volúmenes compatibles con SnapLock admite una resincronización después de una interrupción aunque los datos del destino hayan divergido del origen posterior a la interrupción.

En un resincronización, cuando se detecta una divergencia de datos entre el destino de origen más allá de la instantánea común, se corta una nueva instantánea en el destino para capturar esta divergencia. La nueva snapshot y la snapshot común están bloqueadas con un tiempo de retención de la siguiente manera:

- La hora de caducidad del volumen del destino
- Si el tiempo de caducidad del volumen es pasado o no se ha establecido, la copia de Snapshot se bloquea durante un período de 30 días
- Si el destino tiene retenciones legales, el período de caducidad real del volumen se oculta y aparece como "indefinido", sin embargo la instantánea se bloquea durante el período de caducidad real del volumen.

Si el volumen de destino tiene un período de caducidad posterior al origen, se conserva el período de caducidad del destino y no se sobrescribe con el período de caducidad del volumen de origen posterior a la resincronización.

Si el destino tiene retenciones legales en él que difieren de la fuente, no se permite una resincronización. El origen y el destino deben tener idénticas retenciones legales o todas las retenciones legales del destino deben liberarse antes de intentar realizar una resincronización.

Una copia Snapshot bloqueada en el volumen de destino creada para capturar los datos divergentes se puede copiar en el origen con la CLI ejecutando el `snapmirror update -s snapshot` comando. La instantánea una vez copiada seguirá bloqueada en la fuente.


- No se admiten las relaciones de protección de datos de SVM.
- No se admiten las relaciones de protección de datos con uso compartido de carga.

En la siguiente ilustración, se muestra el procedimiento para inicializar una relación de SnapMirror:

System Manager

A partir de ONTAP 9.12.1, puede usar System Manager para configurar la replicación de SnapMirror de archivos WORM.

Pasos

1. Vaya a **almacenamiento > volúmenes**.
2. Haga clic en **Mostrar/Ocultar** y seleccione **Tipo de SnapLock** para visualizar la columna en la ventana **volúmenes**.
3. Busque un volumen de SnapLock.
4. Haga clic en  Y seleccione **proteger**.
5. Elija el clúster de destino y la máquina virtual de almacenamiento de destino.
6. Haga clic en **más opciones**.
7. Seleccione **Mostrar políticas heredadas** y seleccione **DPDefault (Legacy)**.
8. En la sección **Detalles de la configuración de destino**, seleccione **Anular programa de transferencia** y seleccione **por hora**.
9. Haga clic en **Guardar**.
10. A la izquierda del nombre del volumen de origen, haga clic en la flecha para expandir los detalles del volumen y, en el lado derecho de la página, consulte los detalles de la protección remota de SnapMirror.
11. En el clúster remoto, vaya a **Relaciones de protección**.
12. Busque la relación y haga clic en el nombre del volumen de destino para ver los detalles de la relación.
13. Compruebe que el tipo de SnapLock del volumen de destino y otra información de SnapLock.

CLI

1. Identifique el clúster de destino.
2. En el clúster de destino, ["Instale la licencia de SnapLock"](#), ["Inicialice el reloj de cumplimiento"](#), Y, si está utilizando una versión de ONTAP anterior a 9.10.1, ["Cree un agregado de SnapLock"](#).
3. En el clúster de destino, cree un volumen de destino de SnapLock de tipo DP es el mismo tamaño que el volumen de origen o mayor:

```
volume create -vserver SVM_name -volume volume_name -aggregate  
aggregate_name -snaplock-type compliance|enterprise -type DP -size size
```



A partir de ONTAP 9.10.1, los volúmenes de SnapLock y otros de SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado de SnapLock separado si se utiliza ONTAP 9.10.1. La opción `volume -snaplock-type` se utiliza para especificar el tipo de volumen Compliance o Enterprise SnapLock. En las versiones de ONTAP anteriores a ONTAP 9.10.1, el modo SnapLock (Compliance o Enterprise) se hereda del agregado. No se admiten los volúmenes de destino con versión flexible. La configuración de idioma del volumen de destino debe coincidir con la configuración de idioma del volumen de origen.

El siguiente comando crea una SnapLock de 2 GB Compliance volumen denominado `dstvolB` en el agregado `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate  
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. En la SVM de destino, cree una política de SnapMirror:

```
snapmirror policy create -vserver SVM_name -policy policy_name
```

El siguiente comando crea la política de toda la SVM SVM1-mirror:

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. En la SVM de destino, cree una programación de SnapMirror:

```
job schedule cron create -name schedule_name -dayofweek day_of_week -hour  
hour -minute minute
```

El siguiente comando crea una programación de SnapMirror con el nombre weekendcron:

```
SVM2::> job schedule cron create -name weekendcron -dayofweek  
"Saturday, Sunday" -hour 3 -minute 0
```

6. En la SVM de destino, cree una relación de SnapMirror:

```
snapmirror create -source-path source_path -destination-path  
destination_path -type XDP|DP -policy policy_name -schedule schedule_name
```

El siguiente comando crea una relación de SnapMirror entre el volumen de origen srcvolA encendido SVM1 y el volumen de destino dstvolB encendido SVM2, y asigna la directiva SVM1-mirror y el programa weekendcron:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination  
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule  
weekendcron
```



El tipo XDP está disponible en ONTAP 9.5 y posterior. Debe usar el tipo de DP en ONTAP 9.4 y versiones anteriores.

7. En la SVM de destino, inicialice la relación de SnapMirror:

```
snapmirror initialize -destination-path destination_path
```

El proceso de inicialización realiza una *transferencia basal* al volumen de destino. SnapMirror realiza una copia Snapshot del volumen de origen y, a continuación, transfiere la copia y todos los bloques de datos que hace referencia al volumen de destino. También transfiere cualquier otra copia Snapshot del volumen de origen al volumen de destino.

El siguiente comando inicializa la relación entre el volumen de origen `srcvolA` encendido SVM1 y el volumen de destino `dstvolB` encendido SVM2:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Información relacionada

["Relaciones entre iguales de clústeres y SVM"](#)

["Preparación para la recuperación ante desastres de volúmenes"](#)

["Protección de datos"](#)

Conserve los archivos WORM durante su litigio gracias a su conservación legal

A partir de ONTAP 9.3, puede conservar archivos WORM en modo de cumplimiento durante un litigio con la función *Legal Hold*.

Lo que necesitará

- Debe ser un administrador de SnapLock para realizar esta tarea.

["Cree una cuenta de administrador de SnapLock"](#)

- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

Acerca de esta tarea

Un archivo de retención legal se comporta como un archivo WORM con un período de retención indefinido. Es su responsabilidad especificar cuándo termina el período de retención legal.

El número de archivos que se pueden colocar en una conservación legal depende del espacio disponible en el volumen.

Pasos

1. Inicie una conservación legal:

```
snaplock legal-hold begin -litigation-name litigation_name -volume volume_name -path path_name
```

El siguiente comando inicia una retención legal para todos los archivos de `vol1`:

```
cluster1::> snaplock legal-hold begin -litigation-name litigation1 -volume vol1 -path /
```

2. Terminar una conservación legal:

```
snaplock legal-hold end -litigation-name litigation_name -volume volume_name -path path_name
```

El siguiente comando finaliza una retención legal para todos los archivos de `vol1`:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume  
vol1 -path /
```

Información general acerca de Delete WORM files

Puede eliminar archivos WORM en modo de empresa durante el período de retención mediante la función de eliminación con privilegios. Antes de poder usar esta función, debe crear una cuenta de administrador de SnapLock y, a continuación, utilizar la cuenta, habilitar la función.

Cree una cuenta de administrador de SnapLock

Para realizar una eliminación con privilegios, debe tener privilegios de administrador de SnapLock. Estos privilegios se definen en el rol `vsadmin-snaplock`. Si todavía no ha asignado ese rol, puede solicitar al administrador de clúster que cree una cuenta de administrador de SVM con el rol de administrador de SnapLock.

Lo que necesitará

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

Pasos

1. Cree una cuenta de administrador de SVM con el rol de administrador de SnapLock:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

El siguiente comando habilita la cuenta de administrador de SVM `SnapLockAdmin` con los predefinidos `vsadmin-snaplock` función a la que acceder SVM1 con una contraseña:

```
cluster1::> security login create -vserver SVM1 -user-or-group-name  
SnapLockAdmin -application ssh -authmethod password -role vsadmin-  
snaplock
```

Active la función de eliminación con privilegios

Debe habilitar explícitamente la función de eliminación con privilegios en el volumen de Enterprise que contiene los archivos WORM que desea eliminar.

Acerca de esta tarea

El valor de `-privileged-delete` la opción determina si la eliminación con privilegios está habilitada. Los valores posibles son `enabled`, `disabled`, y `permanently-disabled`.



`permanently-disabled` es el estado del terminal. No se puede habilitar la eliminación con privilegios en el volumen después de establecer el estado en `permanently-disabled`.

Pasos

1. Habilitar la eliminación con privilegios para un volumen de SnapLock Enterprise:

```
volume snaplock modify -vserver SVM_name -volume volume_name -privileged  
-delete disabled|enabled|permanently-disabled
```

El siguiente comando habilita la función de eliminación con privilegios para el volumen de empresa dataVol encendido SVM1:

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged  
-delete enabled
```

Elimine los archivos WORM de modo empresarial

Puede utilizar la función de eliminación con privilegios para eliminar archivos WORM en modo de empresa durante el período de retención.

Lo que necesitará

- Debe ser un administrador de SnapLock para realizar esta tarea.
- Debe haber creado un registro de auditoría de SnapLock y habilitado la función de eliminación privilegiada en el volumen empresarial.

Acerca de esta tarea

No puede utilizar una operación de eliminación privilegiada para eliminar un archivo WORM caducado. Puede utilizar el `volume file retention show` Comando para ver el tiempo de retención del archivo WORM que desea eliminar. Para obtener más información, consulte la página man del comando.

Paso

1. Eliminar un archivo WORM en un volumen empresarial:

```
volume file privileged-delete -vserver SVM_name -file file_path
```

El siguiente comando elimina el archivo /vol/dataVol/f1 En la SVM SVM1:

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```


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.