Protección autónoma de ransomware

ONTAP 9

NetApp
August 31, 2024

Tabla de contenidos

Protección autónoma de ransomware

Información general sobre la protección de ransomware autónoma

A partir de ONTAP 9.10.1, la función de protección de ransomware autónoma (ARP) utiliza análisis de cargas de trabajo en entornos NAS (NFS y SMB) para detectar de forma proactiva y advertir sobre una actividad anormal que puede indicar un ataque de ransomware.

Cuando se sospecha una presencia de un ataque, ARP también crea nuevas copias Snapshot, además de la protección existente frente a copias Snapshot programadas.

Licencias y habilitación

ARP requiere una licencia. ARP está disponible con el "Licencia ONTAP ONE". Si no tiene la licencia ONTAP One, hay otras licencias disponibles para usar ARP, que varían en función de la versión de ONTAP.

Lanzamientos de ONTAP	Licencia
ONTAP 9.11.1 y versiones posteriores	Antiransomware
ONTAP 9.10.1	MT_EK_MGMT (gestión de claves multi-tenant)

- Si actualiza a ONTAP 9.11.1 o una versión posterior y ARP ya está configurado en el sistema, no necesita adquirir la nueva licencia contra ransomware. Para las nuevas configuraciones ARP, se requiere la nueva licencia.
- Si va a revertir de ONTAP 9.11.1 o posterior a ONTAP 9.10.1 y habilitó ARP con la licencia Anti-ransomware, verá un mensaje de advertencia y es posible que deba volver a configurar ARP. "Aprenda sobre cómo revertir ARP".

Puede configurar ARP por volumen mediante System Manager o la CLI de ONTAP.

Estrategia de protección contra ransomware ONTAP

Una estrategia efectiva de detección de ransomware debe incluir más que una única capa de protección.

Una analogía sería las características de seguridad de un vehículo. No dependes de una sola característica, como un cinturón de seguridad, para protegerte por completo en caso de accidente. Las bolsas de aire, los frenos antibloqueo y la advertencia de colisión frontal son características de seguridad adicionales que conducirán a un resultado mucho mejor. La protección contra ransomware debe verse de la misma manera.

Aunque ONTAP incluye funciones como FPolicy, copias Snapshot, SnapLock y el asesor digital de Active IQ para ayudarle a protegerse del ransomware, la siguiente información se centra en la función ARP integrada con funcionalidades de aprendizaje automático.

Para obtener más información sobre otras funciones antiransomware de ONTAP, consulte "La cartera de protección de NetApp y ransomware".

Lo que ARP detecta

ARP está diseñado para proteger contra ataques de denegación de servicio en los que el atacante retiene datos hasta que se pague un rescate. ARP ofrece detección de ransomware en tiempo real basada en:

- Identificación de los datos entrantes como texto cifrado o sin formato.
- Análisis, que detecta
  - **Entropía**: Una evaluación de la aleatoriedad de los datos en un archivo
  - **Tipos de extensión de archivo**: Una extensión que no se ajusta al tipo de extensión normal
  - **IOPS de archivo**: Un aumento en la actividad de volumen anormal con cifrado de datos (a partir de ONTAP 9.11.1)

ARP puede detectar la propagación de la mayoría de ataques de ransomware solo una pequeña cantidad de archivos se cifran, toman medidas automáticamente para proteger los datos y avisan de que se está produciendo un ataque sospechoso.

> Ningún sistema de detección o prevención de ransomware puede garantizar completamente la seguridad de un ataque de ransomware. Aunque es posible que un ataque no se detecte, ARP actúa como una capa adicional importante de defensa si el software antivirus no ha podido detectar una intrusión.

Modos de aprendizaje y activos

ARP tiene dos modos:

- **Aprendizaje** (o modo “dry run”)
- **Activo** (o modo “habilitado”)

Cuando habilita ARP, se ejecuta en *modo de aprendizaje*. En el modo de aprendizaje, el sistema ONTAP desarrolla un perfil de alerta basado en las áreas de análisis: Entropía, tipos de extensiones de archivos e IOPS de archivos. Después de ejecutar ARP en el modo de aprendizaje durante el tiempo suficiente para evaluar las características de la carga de trabajo, puede cambiar al modo activo y empezar a proteger los datos. Una vez que ARP ha cambiado al modo activo, ONTAP crea copias snapshot de ARP para proteger los datos en caso de que se detecte una amenaza.

Se recomienda dejar ARP en modo de aprendizaje durante 30 días. A partir de ONTAP 9.13.1, ARP determina automáticamente el intervalo óptimo del período de aprendizaje y automatiza el switch, que puede ocurrir antes de 30 días.

En el modo activo, si una extensión de archivo se marca como anormal, debe evaluar la alerta. Puede actuar en la alerta para proteger sus datos o puede marcar la alerta como un falso positivo. Al marcar una alerta como falso positivo, se actualiza el perfil de alerta. Por ejemplo, si la alerta se activa con una nueva extensión de archivo y marca la alerta como un falso positivo, no recibirá una alerta la próxima vez que se observe la extensión de archivo. El comando `security anti-ransomware volume workload-behavior show` muestra las extensiones de archivo que se han detectado en el volumen. (Si ejecuta este comando al principio del modo de aprendizaje y muestra una representación precisa de los tipos de archivo, no debe utilizar esos datos como base para pasar al modo activo, ya que ONTAP sigue recopilando otras métricas).

A partir de ONTAP 9.11.1, se pueden personalizar los parámetros de detección para ARP. Para obtener más información, consulte Administrar los parámetros de detección de ataques ARP.

Evaluación de amenazas y copias Snapshot de ARP

En el modo activo, ARP evalúa la probabilidad de amenaza en función de los datos entrantes medidos con respecto a los análisis aprendidos. Se asigna una medición cuando ARP detecta una amenaza:

- **Bajo**: La detección más temprana de una anomalía en el volumen (por ejemplo, se observa una nueva extensión de archivo en el volumen).
- **Moderado**: Se observan múltiples archivos con la misma extensión de archivo Never-seen-before.
  - En ONTAP 9.10.1, el umbral para escalar a moderado es de 100 archivos o más. A partir de ONTAP 9.11.1, la cantidad de archivo es modificable; su valor predeterminado es 20.

En un caso de amenaza baja, ONTAP detecta una anomalía y crea una copia Snapshot del volumen para crear el mejor punto de recuperación. ONTAP antepone el nombre de la copia Snapshot de ARP con `Anti-ransomware-backup` para que sea fácilmente identificable, por ejemplo `Anti_ransomware_backup.2022-12-20_1248`.

La amenaza se escala a moderada después de que ONTAP ejecuta un informe de análisis para determinar si la anormalidad coincide con un perfil de ransomware. Las amenazas que permanecen en el nivel bajo se registran y son visibles en la sección **Eventos** de System Manager. Cuando la probabilidad de ataque es moderada, ONTAP genera una notificación EMS que le solicita que evalúe la amenaza. ONTAP no envía alertas sobre amenazas bajas, sin embargo, a partir de ONTAP 9.14.1, usted puede modificar la configuración de alertas. Para obtener más información, consulte Responda a actividades anormales.

Puede ver información sobre una amenaza, independientemente del nivel, en la sección **Eventos** de System Manager o con la `security anti-ransomware volume show` comando.

Las copias Snapshot de ARP se conservan durante un mínimo de dos días. A partir de ONTAP 9.11.1, puede modificar la configuración de retención. Para obtener más información, consulte Modifique las opciones para las copias Snapshot.

Cómo recuperar los datos en ONTAP después de un ataque de ransomware

Cuando se sospecha la existencia de un ataque, el sistema toma una copia snapshot para el volumen en ese momento específico y bloquea esa copia. Si más tarde se confirma el ataque, el volumen se puede restaurar mediante la copia snapshot de ARP.

Las copias snapshot bloqueadas no se pueden eliminar de forma normal. Sin embargo, si más tarde decide marcar el ataque como un falso positivo, la copia bloqueada se eliminará.

Con el conocimiento de los ficheros afectados y el tiempo del ataque, es posible recuperar de forma selectiva los ficheros afectados de varias copias snapshot, en lugar de simplemente revertir el volumen completo a una de las copias snapshot.

De este modo, ARP se basa en la protección de datos ONTAP y la tecnología de recuperación ante desastres demostradas para responder a ataques de ransomware. Consulte los siguientes temas para obtener más información sobre cómo recuperar datos.

- "Recuperar desde copias Snapshot (System Manager)"
- "Restaurar archivos desde copias Snapshot (CLI)"
- "Recuperación inteligente de ransomware"

Casos de uso y consideraciones sobre la protección de Ransomware autónoma

La protección autónoma de Ransomwware (ARP) está disponible para cargas de trabajo NAS que comiencen con ONTAP 9.10.1. Antes de implementar ARP, debe tener en cuenta los usos recomendados y las configuraciones compatibles, así como las implicaciones de rendimiento.

Configuraciones admitidas y no admitidas

Al decidir usar ARP, es importante asegurarse de que la carga de trabajo de su volumen sea adecuada para ARP y que cumpla con las configuraciones del sistema requeridas.

Cargas de trabajo adecuadas

ARP es adecuado para:

- En almacenamiento NFS
- Directorios iniciales Windows o Linux

  Debido a que los usuarios podían crear archivos con extensiones que no se detectaron en el período de aprendizaje, existe una mayor posibilidad de falsos positivos en esta carga de trabajo.

- Imágenes y vídeo

  Por ejemplo, historiales médicos y datos de automatización de diseño electrónico (EDA)

Cargas de trabajo poco adecuadas

ARP no es adecuado para:

- Cargas de trabajo con una gran frecuencia de creación o eliminación de archivos (cientos de miles de archivos en pocos segundos, por ejemplo, cargas de trabajo de prueba/desarrollo).
- La detección de amenazas de ARP depende de su capacidad para reconocer un aumento inusual en la actividad de creación, cambio de nombre o eliminación de archivos. Si la aplicación en sí es el origen de la actividad de archivos, no se puede distinguir eficazmente de la actividad de ransomware.
- Cargas de trabajo en las que la aplicación o el host cifran datos.
  ARP depende de distinguir los datos entrantes como cifrados o no cifrados. Si la propia aplicación está cifrando los datos, se reduce la eficacia de la función. Sin embargo, la característica puede seguir funcionando según la actividad del archivo (eliminar, sobrescribir o crear, o crear o cambiar el nombre con una nueva extensión de archivo) y el tipo de archivo.

Configuraciones admitidas

ARP está disponible para volúmenes NFS y SMB en sistemas ONTAP on-premises que empiezan por ONTAP 9.10.1.

La compatibilidad con otras configuraciones y tipos de volúmenes está disponible en las siguientes versiones de ONTAP:

	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Volúmenes protegidos con SnapMirror asíncrono	✓	✓	✓	✓		
SVM protegido con SnapMirror asíncrono (recuperación ante desastres de SVM)	✓	✓	✓	✓		
Movilidad de datos de SVM (`vserver migrate`)	✓	✓	✓	✓		
Volúmenes de FlexGroup	✓	✓	✓			
Verificación de varios administradores	✓	✓	✓			

Interoperabilidad de SnapMirror y ARP

A partir de ONTAP 9.12.1, ARP es compatible con volúmenes de destino asíncronos de SnapMirror. ARP no es ** compatible con SnapMirror Synchronous.

Si un volumen de origen de SnapMirror tiene la función ARP habilitada, el volumen de destino de SnapMirror adquiere automáticamente el estado de configuración ARP (aprendizaje, habilitado, etc.), datos de entrenamiento ARP y Snapshot creadas con ARP del volumen de origen. No se requiere habilitación explícita.

Mientras que el volumen de destino consta de copias Snapshot de solo lectura (RO), no se realiza el procesamiento ARP en sus datos. Sin embargo, cuando el volumen de destino de SnapMirror se convierte en Read-write (RW), ARP se habilita automáticamente en el volumen de destino que se convierte en RW. El volumen de destino no requiere ningún procedimiento de aprendizaje adicional además de lo que ya se ha registrado en el volumen de origen.

En ONTAP 9.10.1 y 9.11.1, SnapMirror no transfiere el estado de configuración de ARP, los datos de formación y las copias Snapshot de los volúmenes de origen a destino. Por ello, cuando el volumen de destino de SnapMirror se convierte en RW, ARP en el volumen de destino debe habilitarse explícitamente en el modo de aprendizaje después de la conversión.

ARP y máquinas virtuales

ARP es compatible con máquinas virtuales (VM). La detección de ARP se comporta de manera diferente para los cambios dentro y fuera de la VM. No se recomienda ARP para cargas de trabajo con archivos de alta entropía dentro del equipo virtual.

Realizar cambios fuera de la máquina virtual

ARP puede detectar cambios de extensión de archivo en un volumen NFS fuera de la VM si una nueva extensión entra en el volumen cifrado o cambia una extensión de archivo. Los cambios detectables en la extensión de archivo son:

- .vmx
- .vmxf
- .vmdk
- -flat.vmdk
- .nvram
- .vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .log
- -\#.log

Cambios dentro de la VM

Si el ataque de ransomware se dirige a la máquina virtual y los archivos dentro de la máquina virtual se alteran sin hacer cambios fuera de la máquina virtual, ARP detecta la amenaza si la entropía predeterminada de la máquina virtual es baja (por ejemplo, archivos .txt, .docx o .mp4). Aunque ARP crea una instantánea de protección en este escenario, no genera una alerta de amenaza porque las extensiones de archivo fuera de la VM no se han manipulado.

Si, por defecto, los archivos son de alta entropía (por ejemplo, archivos .gzip o protegidos con contraseña), las capacidades de detección de ARP son limitadas. ARP todavía puede tomar instantáneas proactivas en este caso; sin embargo, no se activará ninguna alerta si las extensiones de archivo no se han manipulado externamente.

Configuraciones no admitidas

ARP no es compatible con las siguientes configuraciones del sistema:

- Entornos ONTAP S3
- Entornos SAN

ARP no admite las siguientes configuraciones de volumen:

- FlexGroup Volumes (en ONTAP 9.10.1 a 9.12.1. A partir de ONTAP 9.13.1, los volúmenes de FlexGroup son compatibles)
- Volúmenes FlexCache (ARP es compatible con los volúmenes FlexVol de origen, pero no con los volúmenes de caché)
- Volúmenes sin conexión
- Volúmenes solo DE SAN
- Volúmenes de SnapLock

- SnapMirror síncrono
- SnapMirror asíncrono (solo no se admite en ONTAP 9.10.1 y 9.11.1). Se admite SnapMirror asíncrono a partir de ONTAP 9.12.1. Para obtener más información, consulte [snapmirror].)
- Volúmenes restringidos
- Volúmenes raíz de equipos virtuales de almacenamiento
- Volúmenes de máquinas virtuales de almacenamiento detenidas

Consideraciones de rendimiento y frecuencia de ARP

ARP puede tener un impacto mínimo en el rendimiento del sistema, ya que se mide el rendimiento y los picos de IOPS. El impacto de la función ARP depende de las cargas de trabajo de volumen específicas. Para cargas de trabajo comunes, se recomiendan los siguientes límites de configuración:

Características de las cargas de trabajo	Límite de volúmenes recomendado por nodo	Degradación del rendimiento cuando se supera el límite de volumen por nodo pasada:[*]
Con una gran cantidad de lecturas o se pueden comprimir los datos.	150	4 % del valor máximo de IOPS
Gran cantidad de escrituras y los datos no se pueden comprimir.	60	10 % de IOPS máximo

Aprobado:[*] el rendimiento del sistema no se degrada más allá de estos porcentajes, independientemente del número de volúmenes añadidos por encima de los límites recomendados.

Dado que la analítica ARP se ejecuta en una secuencia priorizada, a medida que aumenta el número de volúmenes protegidos, la analítica se ejecuta en cada volumen con menos frecuencia.

Verificación multi-admin con volúmenes protegidos con ARP

A partir de ONTAP 9.13.1, puede habilitar la verificación multiadministrador (MAV) para obtener seguridad adicional con ARP. MAV garantiza que al menos dos o más administradores autenticados deben desactivar ARP, pausar ARP o marcar un ataque sospechoso como falso positivo en un volumen protegido. Aprenda cómo "Habilite MAV para volúmenes protegidos por ARP".

Debe definir administradores para un grupo MAV y crear reglas MAV para el `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, y. `security anti-ransomware volume attack clear-suspect` Comandos ARP que desea proteger. Cada administrador del grupo MAV debe aprobar cada nueva solicitud de regla y. "Vuelva a agregar la regla MAV" Dentro de los ajustes de MAV.

A partir de ONTAP 9.14.1, ARP ofrece alertas para la creación de una instantánea ARP y para la observación de una nueva extensión de archivo. De forma predeterminada, las alertas correspondientes a estos eventos están deshabilitadas. Las alertas pueden establecerse en el nivel del volumen o SVM. Puede crear reglas MAV en el nivel de la SVM mediante `security anti-ransomware vserver event-log modify` o a nivel de volumen con `security anti-ransomware volume event-log modify`.

Siguientes pasos

- "Habilite la protección de ransomware autónoma"
- "Habilite MAV para volúmenes protegidos por ARP"

Habilite la protección de ransomware autónoma

A partir de ONTAP 9.10.1, la protección de ransomware autónoma (ARP) puede habilitarse en volúmenes nuevos o existentes. Primero debe habilitar ARP en el modo de aprendizaje, en el cual el sistema analiza la carga de trabajo para caracterizar el comportamiento normal. Puede habilitar ARP en un volumen existente, o bien crear un volumen nuevo y habilitar ARP desde el principio.

Acerca de esta tarea

Siempre debe habilitar ARP inicialmente en modo de aprendizaje (o ejecución en seco). Si se inicia en modo activo, se pueden producir demasiados informes de falsos positivos.

Se recomienda que deje que ARP se ejecute en modo de aprendizaje durante un mínimo de 30 días. A partir de ONTAP 9.13.1, ARP determina automáticamente el intervalo óptimo del período de aprendizaje y automatiza el switch, que puede ocurrir antes de 30 días. Para obtener más información, consulte "Modos de aprendizaje y activos".

> En los volúmenes existentes, los modos de aprendizaje y activos solo se aplican a los datos recién escritos, no a los datos ya existentes en el volumen. Los datos existentes no se analizan y analizan, ya que se asumen las características del tráfico de datos normal anterior según los nuevos datos una vez habilitado para ARP el volumen.

Antes de empezar

- Debe tener una máquina virtual de almacenamiento (SVM) habilitada para NFS o SMB (o ambos).
- La licencia correcta Debe estar instalado para la versión de ONTAP.
- Debe tener carga de trabajo NAS con clientes configurados.
- El volumen que desea establecer ARP debe estar protegido y debe tener un activo "ruta de unión".
- El volumen debe estar lleno por debajo del 100%.
- Se recomienda configurar el sistema EMS para enviar notificaciones por correo electrónico, que incluirán avisos de actividad ARP. Para obtener más información, consulte "Configure eventos de EMS para que envíen notificaciones por correo electrónico".
- A partir de ONTAP 9.13.1, se recomienda habilitar la verificación multiadministrador (MAV) para que se necesiten dos o más administradores de usuarios autenticados para la configuración de protección autónoma contra ransomware (ARP). Para obtener más información, consulte "Habilite la verificación multiadministradora".

Active ARP

Puede habilitar ARP mediante System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

Pasos

1. Seleccione **Almacenamiento > Volúmenes** y, a continuación, seleccione el volumen que desea proteger.
2. En la pestaña **Seguridad** de la vista general **Volúmenes**, selecciona **Estado** para cambiar de Desactivado a Activado en el modo de aprendizaje en la casilla **Anti-ransomware**.
3. Cuando finalice el período de aprendizaje, cambie ARP al modo activo.

   > A partir de ONTAP 9.13.1, ARP determina automáticamente el intervalo óptimo del período de aprendizaje y automatiza el switch. Puede hacerlo "Deshabilite este ajuste en la máquina virtual de almacenamiento asociada" si desea controlar el modo de aprendizaje al modo activo, cambie manualmente.

   a. Selecciona **Almacenamiento > Volúmenes** y, a continuación, selecciona el volumen que esté listo para el modo activo.
   b. En la pestaña **Seguridad** del resumen **Volúmenes**, selecciona **Cambiar** al modo activo en el cuadro Anti-ransomware.
4. Puede verificar el estado ARP del volumen en la casilla **Anti-ransomware**.

   Para mostrar el estado ARP para todos los volúmenes: En el panel **Volúmenes**, seleccione **Mostrar/Ocultar** y, a continuación, asegúrese de que el estado **Anti-ransomware** esté marcado.

CLI

El proceso para habilitar ARP con la CLI es diferente si la habilita en un volumen existente en lugar de en un volumen nuevo.

Habilite ARP en un volumen existente

1. Modifique un volumen existente para habilitar la protección contra ransomware en el modo de aprendizaje:

   ```
   security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
   ```

   Si ejecuta ONTAP 9.13.1 o posterior, el aprendizaje adaptativo se activa para que el cambio al estado activo se realice automáticamente. Si no desea que este comportamiento se habilite automáticamente, cambie la configuración en el nivel de SVM en todos los volúmenes asociados:

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

2. Cuando el periodo de aprendizaje haya terminado, modifique el volumen protegido para cambiar al modo activo si no se ha realizado automáticamente:

   ```
   security anti-ransomware volume enable -volume vol_name -vserver svm_name
   ```

   También se puede cambiar al modo activo con el comando modify volume:

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   active
   ```

3. Verifique el estado ARP del volumen.

   ```
   security anti-ransomware volume show
   ```

Habilite ARP en un nuevo volumen

1. Crea un nuevo volumen con la protección antiransomware habilitada antes de aprovisionar los datos.

   ```
   volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size
   nn -anti-ransomware-state dry-run -junction-path /path_name
   ```

   Si ejecuta ONTAP 9.13.1 o posterior, el aprendizaje adaptativo se activa para que el cambio al estado activo se realice automáticamente. Si no desea que este comportamiento se habilite automáticamente, cambie la configuración en el nivel de SVM en todos los volúmenes asociados:

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

2. Cuando el periodo de aprendizaje haya terminado, modifique el volumen protegido para cambiar al modo activo si no se ha realizado automáticamente:

   ```
   security anti-ransomware volume enable -volume vol_name -vserver svm_name
   ```

   También se puede cambiar al modo activo con el comando modify volume:

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   active
   ```

3. Verifique el estado ARP del volumen.

   ```
   security anti-ransomware volume show
   ```

Habilite la protección de ransomware autónoma de forma predeterminada en nuevos volúmenes

A partir de ONTAP 9.10.1, puede configurar máquinas virtuales de almacenamiento (SVM) de modo que los nuevos volúmenes estén habilitados por defecto para protección de ransomware autónoma (ARP) en el modo de aprendizaje.

Acerca de esta tarea

De manera predeterminada, se crean nuevos volúmenes con ARP en el modo deshabilitado. Puede modificar este ajuste en System Manager y con la CLI. Los volúmenes que están habilitados de forma predeterminada se establecen en ARP en modo de aprendizaje (o ejecución seca).

ARP solo se habilitará en los volúmenes creados en la SVM después de modificar la configuración. ARP no estará habilitado en los volúmenes existentes. Aprenda cómo "Habilite ARP en un volumen existente".

A partir de ONTAP 9.13.1, el aprendizaje adaptativo se ha agregado a la analítica ARP, y el cambio del modo de aprendizaje al modo activo se realiza automáticamente. Para obtener más información, consulte "Modos de aprendizaje y activos".

Antes de empezar

- La licencia correcta Debe estar instalado para la versión de ONTAP.
- El volumen debe estar lleno por debajo del 100%.
- Las rutas de unión deben estar activas.
- A partir de ONTAP 9.13.1, se recomienda habilitar la verificación multiadministrador (MAV) para que se necesiten dos o más administradores de usuarios autenticados para las operaciones anti-ransomware. "Leer más".

Cambie ARP del modo de aprendizaje al modo activo

A partir de ONTAP 9.13.1, el aprendizaje adaptativo se ha añadido a la analítica ARP. El cambio del modo de aprendizaje al modo activo se realiza automáticamente. La decisión autónoma de ARP de cambiar automáticamente del modo de aprendizaje al modo activo se basa en los ajustes de configuración de las siguientes opciones:

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

Después de 30 días de aprendizaje, un volumen se cambia automáticamente al modo activo incluso si una o más de estas condiciones no se cumplen. Es decir, si el cambio automático está activado, el volumen cambia al modo activo después de un máximo de 30 días. El valor máximo de 30 días es fijo y no modificable.

Para obtener más información sobre las opciones de configuración de ARP, incluidos los valores predeterminados, consulte la "Referencia de comandos de la ONTAP".

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para habilitar ARP de manera predeterminada.

System Manager

1. Seleccione **Almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento que contiene los volúmenes que desea proteger con ARP.
2. Navega a la pestaña **Settings**. En **Seguridad**, localice el mosaico **Anti-ransomware** y luego seleccione
3. Marque la casilla para habilitar ARP para volúmenes NAS. Marque la casilla adicional para habilitar ARP en todos los volúmenes NAS elegibles en la máquina virtual de almacenamiento.

> Si ha actualizado a ONTAP 9.13.1, el ajuste **Cambie automáticamente del modo de aprendizaje al modo activo después de suficiente aprendizaje** se habilita automáticamente. Esto permite a ARP determinar el intervalo óptimo del período de aprendizaje y automatizar el cambio al modo activo. Desactive el ajuste si desea realizar la transición manual al modo activo.

CLI

1. Modifique una SVM existente para habilitar ARP de forma predeterminada en volúmenes nuevos:
   `vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run`

   En la CLI, también puede crear una SVM nueva con ARP habilitada de forma predeterminada para volúmenes nuevos.
   `vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]`

   Si ha actualizado a ONTAP 9.13.1 o posterior, el aprendizaje adaptativo se activa para que el cambio al estado activo se realice automáticamente. Si no desea que este comportamiento se habilite automáticamente, utilice el siguiente comando:

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

Detenga la protección de ransomware autónoma para excluir eventos de carga de trabajo del análisis

Si espera eventos de carga de trabajo inusuales, puede suspender temporalmente y reanudar el análisis de la protección de ransomware autónoma (ARP) en cualquier momento.

A partir de ONTAP 9.13.1, puede habilitar la verificación multiadministrador (MAV) para que se requieran dos o más administradores de usuarios autenticados para pausar ARP. "Leer más".

Acerca de esta tarea

Durante una pausa de ARP, no se registran eventos ni se realiza ninguna acción para las nuevas escrituras. No obstante, la operación de análisis continúa para registros anteriores en segundo plano.

No utilice la función de desactivación ARP para pausar el análisis. Al hacerlo, se deshabilita ARP en el volumen y se pierde toda la información existente acerca del comportamiento de la carga de trabajo adquirida. Esto requeriría un reinicio del período de aprendizaje.

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para pausar ARP.

System Manager

1. Seleccione **Almacenamiento > Volúmenes** y, a continuación, seleccione el volumen donde desea pausar ARP.
2. En la pestaña **Seguridad** de la vista general de volúmenes, selecciona **Pausa anti-ransomware** en la casilla **Anti-ransomware**.

> A partir de ONTAP 9.13.1, si utiliza MAV para proteger la configuración ARP, la operación de pausa le solicita la aprobación de uno o más administradores adicionales. "La aprobación debe recibirse de todos los administradores" Asociado al grupo de aprobación MAV o la operación fallará.

CLI

1. Poner en pausa ARP en un volumen:

   ```
   security anti-ransomware volume pause -vserver svm_name -volume vol_name
   ```

2. Para reanudar el procesamiento, utilice `resume` comando:

   ```
   security anti-ransomware volume resume -vserver svm_name -volume vol_name
   ```

3. **Si está utilizando MAV (disponible con ARP a partir de ONTAP 9.13.1) para proteger su configuración ARP,** la operación de pausa le pedirá que obtenga la aprobación de uno o más administradores adicionales. Se debe recibir la aprobación de todos los administradores asociados al grupo de aprobación MAV o la operación fallará.

   Si utiliza MAV y una operación de pausa esperada necesita aprobaciones adicionales, cada aprobador de grupo MAV realiza lo siguiente:

   a. Mostrar la solicitud:

      ```
      security multi-admin-verify request show
      ```

   b. Apruebe la solicitud:

      ```
      security multi-admin-verify request approve -index[number returned from show request]
      ```

      La respuesta del último aprobador de grupo indica que el volumen se ha modificado y que el estado de ARP está en pausa.

      Si utiliza MAV y es un aprobador de grupo MAV, puede rechazar una solicitud de operación de pausa:

   ```
   security multi-admin-verify request veto -index[number returned from show request]
   ```

Gestiona los parámetros de detección de ataques de protección autónoma frente a ransomware

A partir de ONTAP 9.11.1, se pueden modificar los parámetros de detección de ransomware en un volumen específico habilitado para la protección autónoma contra ransomware e informar un aumento conocido como actividad normal de los archivos. El ajuste de los parámetros de detección ayuda a mejorar la precisión de los informes según la carga de trabajo del volumen específico.

Cómo funciona la detección de ataques

Cuando la protección autónoma contra ransomware (ARP) está en modo de aprendizaje, desarrolla valores básicos para los comportamientos de volumen. Son entropía, extensiones de archivos y, a partir de ONTAP 9.11.1, IOPS. Estas líneas de base se utilizan para evaluar las amenazas de ransomware. Para obtener más información sobre estos criterios, consulte Lo que ARP detecta.

En ONTAP 9.10.1, ARP emite una advertencia si detecta las dos condiciones siguientes:

- más de 20 archivos con extensiones de archivo no observadas anteriormente en el volumen
- alta entropía de datos

A partir de ONTAP 9.11.1, ARP emite una advertencia de amenaza si se cumple *only* una condición. Por ejemplo, si se observan más de 20 archivos con extensiones de archivo que no se han observado previamente en el volumen en un período de 24 horas, ARP lo clasificará como una amenaza *independientemente* de la entropía observada. (Los valores de archivo de 24 hora y 20 son los valores predeterminados, que se pueden modificar).

A partir de ONTAP 9.14.1, se pueden configurar alertas cuando ARP observa una nueva extensión de archivo y cuando ARP crea una instantánea. Para obtener más información, consulte [modify-alerts]

Ciertos volúmenes y cargas de trabajo requieren parámetros de detección diferentes. Por ejemplo, el volumen compatible con ARP puede alojar numerosos tipos de extensiones de archivo, en cuyo caso es posible que desee modificar el recuento de umbrales para extensiones de archivo nunca vistas hasta un número mayor que el predeterminado de 20 o deshabilitar las advertencias basadas en extensiones de archivo nunca vistas. A partir de ONTAP 9.11.1, puedes modificar los parámetros de detección de ataques para que se adapten mejor a tus cargas de trabajo específicas.

Modificar los parámetros de detección de ataques

Dependiendo de los comportamientos esperados de su volumen con ARP habilitado, es posible que desee modificar los parámetros de detección de ataques.

Pasos

1. Ver los parámetros de detección de ataques existentes:

```
security anti-ransomware volume attack-detection-parameters show -vserver
svm_name -volume volume_name
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
                                                Vserver Name : vs1
                                                 Volume Name : vol1
            Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                  Is Detection Based on File Create Rate? : true
                  Is Detection Based on File Rename Rate? : true
                  Is Detection Based on File Delete Rate? : true
           Is Detection Relaxing Popular File Extensions? : true
                High Entropy Data Surge Notify Percentage : 100
                 File Create Rate Surge Notify Percentage : 100
                 File Rename Rate Surge Notify Percentage : 100
                 File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 20
       Never Seen before File Extensions Duration in Hour : 24
```

2. Todos los campos mostrados se pueden modificar con valores booleanos o enteros. Para modificar un campo, utilice la `security anti-ransomware volume attack-detection-parameters modify` comando.

   Para obtener una lista completa de parámetros, consulte "Referencia de comandos de la ONTAP".

Informe de sobretensiones conocidas

ARP continúa modificando los valores de línea base para los parámetros de detección, incluso en modo activo. Si conoce aumentos en su actividad de volumen, ya sea un aumento puntual o un aumento característico de una nueva normalidad, debe informar de ello como seguro. Informar manualmente de estas subidas como seguras ayuda a mejorar la precisión de las evaluaciones de amenazas de ARP.

Informe de un aumento puntual

1. Si se produce un aumento puntual en circunstancias conocidas y desea que ARP informe de un aumento similar en circunstancias futuras, borre el aumento del comportamiento de la carga de trabajo:

   ```
   security anti-ransomware volume workload-behavior clear-surge -vserver
   svm_name -volume volume_name
   ```

Modificar sobretensiones de línea base

1. Si una sobretensión informada debe considerarse un comportamiento normal de la aplicación, notifique la sobretensión como tal para modificar el valor de sobretensión de línea base.

   ```
   security anti-ransomware volume workload-behavior update-baseline-from-surge
   -vserver svm_name -volume volume_name
   ```

Configurar alertas ARP

A partir de ONTAP 9.14.1, ARP permite especificar alertas para dos eventos ARP:

- Observación de la nueva extensión de archivo en un volumen
- Creación de una instantánea ARP

Es posible establecer alertas para estos dos eventos en volúmenes individuales o para toda la SVM. Si se habilitan alertas para la SVM, las configuraciones de alerta solo heredan los volúmenes creados después de habilitar la alerta. De manera predeterminada, las alertas no están habilitadas en ningún volumen.

Las alertas de eventos se pueden controlar con verificación multiadministrador. Para obtener más información, consulte Verificación multi-admin con volúmenes protegidos con ARP.

System Manager

Configure alertas para un volumen

1. Navega a **volúmenes**. Seleccione el volumen individual para el cual desea modificar la configuración.
2. Seleccione la pestaña **Seguridad** y luego **Configuración de seguridad de eventos**.
3. Para recibir alertas de **Nueva extensión de archivo detectada** y **Instantánea de ransomware creada**, seleccione el menú desplegable bajo el encabezado **Gravedad**. Modifique la configuración de **No generar evento** a **Aviso**.
4. Selecciona **Guardar**.

Configure alertas para una SVM

1. Desplácese hasta **Storage VM** y seleccione la SVM para la que desea habilitar la configuración.
2. Bajo el encabezado **Seguridad**, localiza la tarjeta **Anti-ransomware**. Seleccione ⋮ a continuación **Editar gravedad de evento de ransomware**.
3. Para recibir alertas de **Nueva extensión de archivo detectada** y **Instantánea de ransomware creada**, seleccione el menú desplegable bajo el encabezado **Gravedad**. Modifique la configuración de **No generar evento** a **Aviso**.
4. Selecciona **Guardar**.

CLI

Configure alertas para un volumen

- Para configurar alertas para una nueva extensión de archivo:

  ```
  security anti-ransomware volume event-log modify -vserver svm_name -is
  -enabled-on-new-file-extension-seen true
  ```

- Para configurar alertas para la creación de una instantánea ARP:

  ```
  security anti-ransomware volume event-log modify -vserver svm_name -is
  -enabled-on-snapshot-copy-creation true
  ```

- Confirme la configuración con el `anti-ransomware volume event-log show` comando.

Configure alertas para una SVM

- Para configurar alertas para una nueva extensión de archivo:

  ```
  security anti-ransomware vserver event-log modify -vserver svm_name -is
  -enabled-on-new-file-extension-seen true
  ```

- Para configurar alertas para la creación de una instantánea ARP:

  ```
  security anti-ransomware vserver event-log modify -vserver svm_name -is
  -enabled-on-snapshot-copy-creation true
  ```

- Confirme la configuración con el `security anti-ransomware vserver event-log show` comando.

Más información

- "Comprende los ataques autónomos de protección frente a ransomware y el snapshot autónomo de protección frente a ransomware"

Responda a actividades anormales

Cuando la protección de ransomware autónoma (ARP) detecta actividad anormal en un volumen protegido, emite una advertencia. Debe evaluar la notificación para determinar si la actividad es aceptable (falso positivo) o si un ataque parece malicioso.

Acerca de esta tarea

ARP muestra una lista de archivos sospechosos cuando detecta cualquier combinación de alta entropía de datos, actividad de volumen anormal con cifrado de datos y extensiones de archivo inusuales.

Cuando se emita la advertencia, responda designando la actividad del archivo de una de las dos formas siguientes:

- **Falso positivo**

  Se espera el tipo de archivo identificado en la carga de trabajo y se puede ignorar.

- **Potencial ataque de ransomware**

  El tipo de archivo identificado no es esperado en su carga de trabajo y debe tratarse como un ataque potencial.

En ambos casos, la monitorización normal se reanuda después de actualizar y borrar los avisos. ARP registra su evaluación en el perfil de evaluación de amenazas, utilizando su elección para supervisar las actividades de archivo posteriores.

En caso de sospecha de un ataque, debes determinar si se trata de un ataque, responder a él si es así y restaurar los datos protegidos antes de borrar los avisos. "Obtenga más información sobre cómo recuperarse de un ataque de ransomware".

Si restaura un volumen completo, no hay avisos que borrar.

Antes de empezar

ARP debe estar ejecutándose en modo activo.

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para responder a una tarea anormal.

System Manager

1. Cuando recibas una notificación de “actividad anormal”, sigue el enlace. Alternativamente, navega a la pestaña **Seguridad** de la vista general **Volúmenes**.

   Las advertencias se muestran en el panel **Overview** del menú **Events**.

2. Cuando aparezca un mensaje de “actividad de volumen anormal detectada”, consulte los archivos sospechosos.

   En la pestaña **Seguridad**, selecciona **Ver tipos de archivos sospechosos**.

3. En el cuadro de diálogo **tipos de archivo sospechosos**, examine cada tipo de archivo y márquelo como “falso positivo” o “ataque potencial de ransomware”.

Si seleccionó este valor…	Realice esta acción…
Falso positivo	Seleccione **Actualizar** y **Borrar tipos de archivos sospechosos** para registrar su decisión y reanudar el monitoreo normal de ARP. A partir de ONTAP 9.13.1, si está utilizando MAV para proteger su configuración ARP, la operación claramente sospechosa le solicita que obtenga la aprobación de uno o más administradores adicionales. "La aprobación debe recibirse de todos los administradores" Asociado al grupo de aprobación MAV o la operación fallará.
Posible ataque de ransomware	Responda al ataque y restaure datos protegidos. A continuación, seleccione **Actualizar** y **Borrar tipos de archivos sospechosos** para registrar su decisión y reanudar el monitoreo ARP normal. No hay ningún tipo de archivo sospechoso que borrar si se restaura un volumen completo.

CLI

1. Cuando reciba una notificación de un ataque de ransomware sospechoso, compruebe la hora y la gravedad del ataque:

   `security anti-ransomware volume show -vserver` *`svm_name`* `-volume` *`vol_name`*

   Salida de muestra:

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

   También puede comprobar los mensajes de EMS:

```
event log show -message-name callhome.arw.activity.seen
```

2. Generar un informe de ataque y anotar la ubicación de salida:

   ```
   security anti-ransomware volume attack generate-report -volume vol_name
   -dest-path file_location/
   ```

   Salida de muestra:

   ```
   Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
   "vs0:vol1/"
   ```

3. Ver el informe en un sistema cliente de administración. Por ejemplo:

   ```
   [root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08

   19  "9/14/2021 01:03:23"   test_dir_1/test_file_1.jpg.lckd
   20  "9/14/2021 01:03:46"   test_dir_2/test_file_2.jpg.lckd
   21  "9/14/2021 01:03:46"   test_dir_3/test_file_3.png.lckd`
   ```

4. Realice una de las siguientes acciones en función de su evaluación de las extensiones de archivo:

   - Falso positivo

     Introduzca el siguiente comando para registrar su decisión, agregando la nueva extensión a la lista de los permitidos y reanudar la supervisión anti-ransomware normal:
     `anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true`

     Utilice uno de los siguientes parámetros para identificar las extensiones:
     `[-seq-no integer]` Número de secuencia del archivo en la lista de sospechosos.
     `[-extension text, … ]` Extensiones de archivo
     `[-start-time date_time -end-time date_time]` Horas de inicio y finalización del intervalo de archivos que se van a borrar, con el formato "MM/DD/AAAA HH:MM:SS".

   - Ataque potencial de ransomware

     Responda al ataque y. "Recupere los datos de la instantánea de backup creada por ARP". Después de recuperar los datos, introduzca el siguiente comando para registrar su decisión y reanudar la supervisión normal de ARP:

     ```
     anti-ransomware volume attack clear-suspect -vserver svm_name -volume
     vol_name [extension identifiers] -false-positive false
     ```

     Utilice uno de los siguientes parámetros para identificar las extensiones:
     `[-seq-no integer]` Número de secuencia del archivo en la lista de sospechosos
     `[-extension text, … ]` Extensión de archivo
     `[-start-time date_time -end-time date_time]` Horas de inicio y finalización del intervalo de archivos que se van a borrar, con el formato "MM/DD/AAAA HH:MM:SS".

No hay ningún tipo de archivo sospechoso que borrar si se restaura un volumen completo. Se eliminará la instantánea de copia de seguridad creada por ARP y se borrará el informe de ataque.

5. Si está utilizando MAV y se espera `clear-suspect` La operación necesita aprobaciones adicionales, cada aprobador del grupo MAV debe:

   a. Mostrar la solicitud:

      `security multi-admin-verify request show`

   b. Apruebe la solicitud para reanudar la supervisión normal antiransomware:

      `security multi-admin-verify request approve -index[`*`number returned from show request`*`]`

   La respuesta del último aprobador de grupo indica que el volumen se ha modificado y se registra un falso positivo.

6. Si está utilizando MAV y es un aprobador de grupo MAV, también puede rechazar una solicitud clara sospechosa:

   `security multi-admin-verify request veto -index[`*`number returned from show request`*`]`

Más información

- "KB: Comprender los ataques autónomos de protección frente a ransomware y la instantánea de protección autónoma frente a ransomware".

Restaure los datos después de un ataque de ransomware

Autonomous Ransomware Protection (ARP) crea copias Snapshot denominadas `Anti_ransomware_backup` cuando detecta una posible amenaza de ransomware. Puede usar una de estas copias Snapshot de ARP u otra copia Snapshot del volumen para restaurar los datos.

Acerca de esta tarea

Si el volumen tiene relaciones de SnapMirror, replique manualmente todas las copias de reflejo del volumen inmediatamente después de restaurar desde una copia de Snapshot. Si no lo hace, puede provocar copias reflejadas inutilizables que se deban eliminar y volver a crear.

Para restaurar desde una copia Snapshot que no sea la `Anti_ransomware_backup` Snapshot Después de identificar un ataque del sistema, primero debe liberar la instantánea ARP.

Si no se ha informado de ningún ataque al sistema, primero debe restaurar desde el `Anti_ransomware_backup` Y luego complete una restauración posterior del volumen de la copia Snapshot que elija.

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para restaurar los datos.

System Manager

Restaurar después de un ataque al sistema

1. Para restaurar desde la instantánea ARP, vaya al paso dos. Para restaurar desde una copia snapshot anterior, primero debe liberar el bloqueo en la instantánea ARP.
   a. Seleccione **almacenamiento > volúmenes**.
   b. Seleccione **Seguridad** y luego **Ver tipos de archivos sospechosos**
   c. Marque los archivos como "False positive" .
   d. Seleccione **Actualizar** y **Borrar tipos de archivos sospechosos**
2. Mostrar las copias Snapshot en los volúmenes:

   Selecciona **Almacenamiento > Volúmenes** y, a continuación, selecciona el volumen y **Copias instantáneas**.
3. Seleccione ⋮ junto a la copia Snapshot que desea restaurar y luego **Restaurar**.

Restaurar si no se identificó un ataque del sistema

1. Mostrar las copias Snapshot en los volúmenes:

   Selecciona **Almacenamiento > Volúmenes** y, a continuación, selecciona el volumen y **Copias instantáneas**.
2. Selecciónelos ⋮ y elija la `Anti_ransomware_backup` instantánea.
3. Seleccione **Restaurar**.
4. Vuelva al menú **Copias de instantánea** y, a continuación, elija la copia de instantánea que desee utilizar. Seleccione **Restaurar**.

CLI

Restaurar después de un ataque al sistema

1. Para restaurar desde la copia snapshot de ARP, vaya al paso dos. Para restaurar datos de copias snapshot anteriores, debe liberar el bloqueo de la instantánea ARP.

   ⓘ Solo es necesario liberar la SnapLock antiransomware antes de restaurar desde copias de Snapshot anteriores si utiliza el `volume snap restore` comando como se describe a continuación. Si va a restaurar datos utilizando Flex Clone, Single File Snap Restore u otros métodos, esto no es necesario.

   Marcar el ataque como «falso positivo» y «claro sospechoso»:
   `anti-ransomware volume attack clear-suspect -vserver` *`svm_name`* `-volume` *`vol_name`* `[`*`extension identifiers`*`] -false-positive true`
   Utilice uno de los siguientes parámetros para identificar las extensiones:
   `[-seq-no` *`integer`*`]` Número de secuencia del archivo en la lista de sospechosos.
   `[-extension` *`text`*`, … ]` Extensiones de archivo
   `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` Horas de inicio y finalización del intervalo de archivos que se van a borrar, con el formato "MM/DD/AAAA HH:MM:SS".
2. Enumere las copias Snapshot en un volumen:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

El ejemplo siguiente muestra las copias Snapshot en `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. Restaure el contenido de un volumen de una copia Snapshot:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

En el ejemplo siguiente se restaura el contenido de `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

Restaurar si no se identificó un ataque del sistema

1. Enumere las copias Snapshot en un volumen:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

El ejemplo siguiente muestra las copias Snapshot en `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaure el contenido de un volumen de una copia Snapshot:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

En el ejemplo siguiente se restaura el contenido de `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

3. Repita los pasos 1 y 2 para restaurar el volumen con la copia Snapshot que desee.

Más información

- "KB: Prevención y recuperación de ransomware en ONTAP"

Modifique las opciones de las copias automáticas Snapshot

A partir de ONTAP 9.11.1, puede utilizar la interfaz de línea de comandos para controlar la configuración de retención de copias de Snapshot de protección autónoma frente a ransomware (ARP) que se generan automáticamente en respuesta a ataques de ransomware sospechosos.

Antes de empezar

Solo puede modificar las opciones de ARP Snapshots en una SVM de nodo.

Pasos

1. Para mostrar todas las opciones actuales de copias de Snapshot de ARP, introduzca:
`vserver options -vserver` *`svm_name`* `arw*`

> La `vserver options` es un comando oculto. Para ver la página man, introduzca `man vserver options` En la CLI de ONTAP.

2. Para mostrar la configuración de copia de Snapshot de ARP actual seleccionada, introduzca: `vserver options -vserver svm_name -option-name arw_setting_name`
3. Para modificar la configuración de una copia Snapshot de ARP, introduzca: `vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value`

   Se pueden modificar los siguientes ajustes:

Ajuste ARW	Descripción
`arw.snap.max.count`	Especifica la cantidad máxima de copias de Snapshot ARP que pueden existir en un volumen en un momento determinado. Las copias más antiguas se eliminan para garantizar que la cantidad total de copias de Snapshot ARP se encuentre dentro del límite especificado. La `-option-value` el parámetro acepta enteros entre 3 y 8, inclusive. El valor predeterminado es 6.
`arw.snap.create.interval.hours`	Especifica el intervalo *in hours* entre las copias snapshot ARP. Una nueva copia Snapshot de ARP se crea cuando se sospecha de un ataque basado en entropía de datos y la copia Snapshot de ARP creada más recientemente es más antigua que el intervalo especificado. La `-option-value` el parámetro acepta enteros entre 1 y 48, inclusive. El valor predeterminado es 4.
`arw.snap.normal.retain.interval.hours`	Especifica la duración *en horas* durante el cual se conserva una copia Snapshot ARP. Cuando una copia Snapshot de ARP alcanza el umbral de retención, cualquier otra copia de Snapshot de ARP creada antes de eliminarla. No se puede haber más de una copia Snapshot de ARP más antigua que el umbral de retención. La `-option-value` el parámetro acepta enteros entre 4 y 96, inclusive. El valor predeterminado es 48.
`arw.snap.max.retain.interval.days`	Especifica la duración máxima *en días* durante el cual se puede conservar una copia Snapshot ARP. Cualquier copia Snapshot de ARP anterior a esta duración se elimina cuando no se notifica ningún ataque en el volumen. El intervalo de retención máximo para las copias snapshot ARP se ignora si se detecta una amenaza moderada. La copia snapshot de ARP creada en respuesta a la amenaza se retiene hasta que haya respondido a la amenaza. Marcar una amenaza como falso positivo Elimina las copias snapshot de ARP en el volumen. La `-option-value` el parámetro acepta enteros entre 1 y 365, inclusive. El valor predeterminado es 5.

Ajuste ARW	Descripción
`arw.snap.create.interval.hours.post.max.count`	Especifica el intervalo *en horas* entre las copias Snapshot de ARP cuando el volumen ya contiene el número máximo de copias Snapshot de ARP. Cuando se alcanza el número máximo, se elimina una copia snapshot ARP para dar espacio a una nueva copia. La nueva velocidad de creación de copias Snapshot ARP puede reducirse para conservar la copia más antigua con esta opción. Si el volumen ya contiene el número máximo de copias Snapshot de ARP, el intervalo especificado en esta opción se utiliza para la siguiente creación de copia Snapshot de ARP, en lugar de `arw.snap.create.interval.hours`. La `-option-value` el parámetro acepta enteros entre 4 y 48, inclusive. El valor predeterminado es 8.
`arw.surge.snap.interval.days`	Especifica el intervalo *en días* entre las copias Snapshot de ARP creadas en respuesta a los aumentos de I/O. ONTAP crea una copia de exceso de Snapshot de ARP cuando hay un aumento en el tráfico de I/O y la última copia Snapshot de ARP creada es más antigua que este intervalo especificado. Esta opción también especifica el período de retención *in day* para copias Snapshot de sobrecarga ARP. La `-option-value` el parámetro acepta enteros entre 1 y 365, inclusive. El valor predeterminado es 5.
`arw.snap.new.extns.interval.hours`	Esta opción especifica el intervalo *in hours* entre las copias snapshot de ARP creadas cuando se detecta una nueva extensión de archivo. Se crea una nueva copia snapshot de ARP cuando Se observa una nueva extensión de archivo; la instantánea anterior creada al observar una nueva extensión de archivo es más antigua que este intervalo especificado. En una carga de trabajo que crea con frecuencia nuevas extensiones de archivos, este intervalo ayuda a controlar la frecuencia de las copias snapshot de ARP. Esta opción existe independientemente de `arw.snap.create.interval.hours`, Que especifica el intervalo para las copias snapshot ARP basadas en entropía de datos. La `-option-value` el parámetro acepta enteros entre 24 y 8760. El valor predeterminado es 48.

Información de copyright

Información de la marca comercial