Protección autónoma de ransomware

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Protección autónoma de ransomware

Obtenga más información sobre la protección autónoma frente a ransomware de ONTAP

A partir de ONTAP 9.10.1, los administradores de ONTAP pueden habilitar la Protección Autónoma contra Ransomware (ARP) para realizar análisis de carga de trabajo en entornos NAS (NFS y SMB) con el fin de detectar y advertir proactivamente sobre actividad anormal que podría indicar un ataque de ransomware. A partir de ONTAP 9.17.1, ARP también admite volúmenes de dispositivos de bloque, incluidos volúmenes SAN que contienen LUN o espacios de nombres NVMe, o volúmenes NAS que contienen discos virtuales de hipervisores como VMware.

ARP está integrado directamente en ONTAP, lo que garantiza un control y una coordinación integrados con las demás funciones de ONTAP. ARP opera en tiempo real, procesando datos a medida que se escriben o leen en el sistema de archivos, y detectando y respondiendo rápidamente a posibles ataques de ransomware.

ARP crea instantáneas bloqueadas a intervalos regulares junto con las programadas para mayor protección. Administra de forma inteligente el tiempo que se conservan las instantáneas. Si no se detecta ninguna actividad inusual, las instantáneas se reciclan rápidamente. Sin embargo, si se detecta un ataque, se conserva una instantánea creada antes del inicio del ataque durante un período prolongado. Para obtener más información, incluidos los cambios agregados por la versión de ONTAP , consulte Instantáneas de ARP.

Licencias y habilitación

Necesitas una licencia para usar ARP. Decide si quieres habilitar ARP por defecto en los nuevos volúmenes o habilitarlo manualmente por volumen.

Opciones de licencia para ARP

El soporte ARP está incluido con el"Licencia ONTAP One" . Si no tiene la licencia de ONTAP One, hay otras licencias disponibles para el uso de ARP que varían según su versión de ONTAP

Lanzamientos de ONTAP	Licencia
ONTAP 9.11.1 y versiones posteriores	`Anti_ransomware`
ONTAP 9.10.1	`MT_EK_MGMT` (Gestión de claves multiinquilino)

- Si está actualizando de ONTAP 9.10.1 a ONTAP 9.11.1 o posterior y ARP ya está configurado en su sistema, no necesita instalar el nuevo `Anti-ransomware` Licencia. Para nuevas configuraciones de ARP, se requiere la nueva licencia.
- Si está volviendo de ONTAP 9.11.1 o posterior a ONTAP 9.10.1 y ha habilitado ARP con la licencia Anti_ransomware, verá un mensaje de advertencia y es posible que deba reconfigurar ARP. "Aprenda sobre cómo revertir ARP" .

Opciones de habilitación para ARP

ARP proporciona opciones flexibles de habilitación a nivel de clúster, SVM y volumen, lo que te permite configurar la habilitación automática predeterminada para nuevos volúmenes o habilitar ARP manualmente en volúmenes existentes según lo necesites.

Activación automática predeterminada en nuevos volúmenes

A partir de ONTAP 9.18.1, ARP se habilita automáticamente por defecto en todos los volúmenes nuevos para AFF serie A y AFF serie C, ASA y ASA r2. Esta habilitación automática de ARP por defecto no se aplica a "volúmenes o configuraciones no compatibles".

La habilitación predeterminada de ARP en volúmenes nuevos entra en vigor después de un periodo de gracia de 12 horas tras una actualización o inmediatamente para una nueva instalación de ONTAP 9.18.1, siempre que se haya instalado una licencia de ARP en cualquiera de los casos. Debes habilitar ARP manualmente en los volúmenes existentes.

Durante el periodo de gracia, puedes "desactivar la activación por defecto para nuevos volúmenes a nivel de clúster usando System Manager o la ONTAP CLI". Si no te excluyes, ARP se habilita automáticamente para todos los nuevos volúmenes creados después del final del periodo de gracia. Si las necesidades cambian después del periodo de gracia, también tienes la flexibilidad de activar o desactivar la habilitación por defecto en cualquier momento.

Activación manual predeterminada en nuevos volúmenes

Si desactivaste la activación automática por defecto de ARP a nivel de clúster, también puedes elegir "habilitar manualmente ARP de forma predeterminada en todos los volúmenes nuevos" a nivel de SVM. Para ONTAP 9.17.1 y versiones anteriores, esta es la única forma de configurar ARP para que se active por defecto en los nuevos volúmenes.

Habilitación de ARP en todos o en volúmenes existentes específicos

A partir de 9.18.1, puedes habilitar manualmente ARP en todos los volúmenes existentes desde el nivel de clúster (selecciona **Cluster > Security** y ⋮ en la sección **Anti-ransomware**, luego selecciona **Enable on all existing volumes**).

Si prefieres limitar la activación de ARP a un volumen específico, puedes "habilitar ARP por volumen".

Estrategia de protección contra ransomware ONTAP

La protección eficaz contra el ransomware requiere muchas capas de protección que trabajen juntas.

Mientras que ONTAP incluye funciones como FPolicy, snapshots, SnapLock, y Active IQ Digital Advisor (también conocido como Digital Advisor) para ayudar a proteger frente al ransomware, ARP proporciona una capa adicional de defensa.

Para obtener más información sobre otras funciones en el portafolio de NetApp que protegen contra el ransomware, consulta:

- "La cartera de protección de NetApp y ransomware"
- "Fortalecimiento de la bóveda cibernética de ONTAP con PowerShell"

Lo que ARP detecta

ONTAP ARP está diseñado para proteger contra ataques de denegación de servicio donde el atacante retiene datos hasta que se paga un rescate. ARP ofrece detección de ransomware en tiempo real basándose en lo siguiente:

- Identificación de datos entrantes como texto cifrado o simple.
- Análisis que detectan:
  - **Entropía**: (Utilizada en NAS y SAN) Una evaluación de la aleatoriedad de los datos en un archivo
  - **Tipos de extensión de archivo**: (Se usa solo en NAS) Una extensión de archivo que no se ajusta a los tipos de extensión esperados
  - **IOPS de archivo**: (Se utiliza solo en NAS a partir de ONTAP 9.11.1) Un aumento en la actividad de volumen anormal con cifrado de datos

ARP detecta la propagación de la mayoría de los ataques de ransomware después de que solo se cifra una pequeña cantidad de archivos, responde automáticamente para proteger los datos y le alerta de que está ocurriendo un ataque sospechoso.

Ningún sistema de detección de ransomware puede garantizar una seguridad completa. ARP proporciona una capa adicional de defensa si el software antivirus no detecta una intrusión.

Conozca los modos ARP

Una vez que se habilita ARP para un volumen, este ingresa en un período de aprendizaje para establecer una línea de base. ARP analiza las métricas del sistema para desarrollar un perfil de alerta antes de pasar al modo de detección activa. En el modo activo, ARP monitorea la actividad anormal, tomando acciones de protección y generando alertas si detecta un comportamiento anormal.

Para ARP, los comportamientos del modo de aprendizaje y del modo activo difieren según la versión de ONTAP , el tipo de volumen y el protocolo (NAS o SAN).

Entornos NAS y tipos de modos

La siguiente tabla resume las diferencias entre ONTAP 9.10.1 y versiones posteriores para entornos NAS.

En las versiones con el modelo ARP anterior, se recomienda un período de aprendizaje antes de que comience la monitorización activa. Para entornos NAS que admitenARP/IA No hay período de aprendizaje y el monitoreo activo comienza de inmediato.

Modo	Descripción	Tipos y versiones de volúmenes
Aprendiendo	Para ciertas versiones de ONTAP y ciertos tipos de volumen, ARP se configura automáticamente en modo de aprendizaje cuando se habilita ARP. En este modo, el sistema ONTAP genera un perfil de alerta basado en las áreas analíticas: entropía, tipos de extensión de archivo e IOPS de archivo. Se recomienda dejar ARP en modo de aprendizaje durante 30 días. A partir de ONTAP 9.13.1, ARP determina automáticamente el intervalo de aprendizaje óptimo y automatiza el cambio, que podría ocurrir antes de los 30 días. Para versiones anteriores a ONTAP 9.13.1, puede realizar el cambio manualmente. A partir de ONTAP 9.16.1 para volúmenes FlexVol , solo existe el modo activo y el modo de aprendizaje se cambia automáticamente al modo activo para cualquier volumen FlexVol actualizado a esta versión o posterior. Para ONTAP 9.16.1 a 9.17.1, los volúmenes FlexGroup aún no son compatibles con ARP/AI y continúan ejecutando el modelo ARP anterior. Por este motivo, se sigue recomendando un período de aprendizaje para estas versiones con volúmenes FlexGroup . A partir de ONTAP 9.18.1, solo existe el modo activo para los volúmenes FlexVol y FlexGroup . Los volúmenes actualizados pasan automáticamente al modo activo. "Obtenga más información sobre cómo cambiar del modo de aprendizaje al modo activo" . 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 moverse al modo activo, ya que ONTAP sigue recopilando otras métricas. Obtenga más información sobre `security anti-ransomware volume workload-behavior show` en el "Referencia de comandos del ONTAP".	• Volúmenes FlexVol con ONTAP 9.10.1 a 9.15.1 • Volúmenes FlexGroup con ONTAP 9.13.1 a ONTAP 9.17.1
Activo	En el modo activo, si una extensión de archivo se marca como anormal, debe evaluar la alerta. Puede actuar en consecuencia para proteger sus datos o marcarla como falso positivo. Al marcar una alerta como falso positivo, se actualiza el perfil de alertas. Por ejemplo, si la alerta se activa por una nueva extensión de archivo y la marca como falso positivo, no recibirá una alerta la próxima vez que se detecte la extensión de archivo.	Todas las versiones de ONTAP compatibles y los volúmenes FlexVol y FlexGroup

Entornos SAN y tipos de modos

Los entornos SAN utilizan periodos de evaluación (similares a los modos de aprendizaje en entornos NAS) antes de pasar automáticamente a la detección activa. La siguiente tabla resume los modos de evaluación y activo.

Modo	Descripción	Tipos y versiones de volúmenes
Evaluación	Se realiza un período de evaluación de dos a cuatro semanas para determinar el comportamiento de cifrado de referencia, mientras que ARP/AI proporciona protección activa inmediata para los volúmenes SAN durante el período de evaluación. La detección y las alertas pueden producirse mientras se establecen los umbrales de referencia. Puedes determinar si el período de evaluación ha finalizado ejecutando la siguiente fórmula: `security anti-ransomware volume show` comando y verificación `Block device detection status`. "Obtenga más información sobre los volúmenes SAN y el período de evaluación de entropía" .	• Volúmenes FlexVol con ONTAP 9.17.1 y versiones posteriores
Activo	Después del período de evaluación, puede determinar si la protección ARP SAN está activa ejecutando el `security anti-ransomware volume show` comando y comprobación `Block device detection status`. Un estado de `Active_suitable_workload` Indica que la cantidad de entropía evaluada se puede monitorear correctamente. ARP ajusta automáticamente el umbral adaptativo según los datos revisados durante la evaluación.	• Volúmenes FlexVol con ONTAP 9.17.1 y versiones posteriores

Evaluación de amenazas e instantáneas ARP

ARP evalúa la probabilidad de amenaza basándose en los datos entrantes medidos según los análisis aprendidos. Cuando ARP detecta una anomalía, se asigna una medida. ARP podría asignar una instantánea en el momento de la detección o a intervalos regulares.

Umbrales ARP

- **Bajo**: La detección más temprana de una anormalidad en el volumen (por ejemplo, se observa una nueva extensión de archivo en el volumen). Este nivel de detección solo está disponible en versiones anteriores a ONTAP 9.16,1 que no tienen ARP/AI.
  - A partir de ONTAP 9.11.1, puede "Personalizar los parámetros de detección para ARP" .
  - En ONTAP 9.10.1, el umbral para escalar a moderado es de 100 archivos o más.
- **Moderado**: Se detecta alta entropía o se observan varios archivos con la misma extensión nunca antes vista. Este es el nivel de detección base en ONTAP 9.16.1 y versiones posteriores con ARP/AI.

La amenaza se intensifica a moderada después de que ONTAP genere un informe analítico que determina si la anomalía coincide con un perfil de ransomware. 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, puede… "modificar la configuración de alerta predeterminada" .

Para obtener más información, consulte "Responda a actividades anormales" .

Puede ver información sobre amenazas moderadas en la sección **Eventos** de System Manager o con `security anti-ransomware volume show` el comando. Los eventos de amenaza baja también se pueden ver con el `security anti-ransomware volume show` comando en versiones anteriores a ONTAP 9.16.1 que no tienen ARP/AI. Obtenga más información sobre `security anti-ransomware volume show` en el "Referencia de comandos del ONTAP".

Instantáneas de ARP

ARP crea una instantánea cuando se detectan los primeros signos de un ataque. Posteriormente, se realiza un análisis detallado para confirmar o descartar el posible ataque. Dado que las instantáneas ARP se crean de forma proactiva incluso antes de que se confirme por completo un ataque, también podrían generarse a intervalos regulares para ciertas aplicaciones legítimas. La presencia de estas instantáneas no debe considerarse una anomalía. Si se confirma un ataque, la probabilidad del ataque se incrementa a `Moderate` y se genera una notificación de ataque.

A partir de ONTAP 9.17.1, se generan instantáneas de ARP a intervalos regulares para los volúmenes NAS y SAN, así como en respuesta a anomalías detectadas. ONTAP antepone un nombre a la instantánea ARP para facilitar su identificación.

A partir de ONTAP 9.11.1, puede modificar la configuración de retención. Para obtener más información, consulte "Modifique las opciones de snapshots" .

La siguiente tabla resume las diferencias de instantáneas ARP por versión.

Función	ONTAP 9.17.1 y posteriores	ONTAP 9.16.1 y anteriores
Desencadenante de creación	• Las instantáneas se crean a intervalos fijos de 4 horas, independientemente de cualquier desencadenante específico. • Confirmación de un ataque Se crea una instantánea "periódica" o "de ataque" según el tipo de disparador.	• Se detecta alta entropía • Se detectó una nueva extensión de archivo (9.15.1 y anteriores) • Se detecta un aumento repentino de operaciones de archivos (9.15.1 y anteriores) El intervalo de creación de instantáneas se basa en el tipo de disparador.
Convención de nombres prefijados	Copia de seguridad periódica anti-ransomware	Copia de seguridad anti-ransomware
Comportamiento de eliminación	La instantánea ARP está bloqueada y el administrador no puede eliminarla	La instantánea ARP está bloqueada y el administrador no puede eliminarla
Número máximo de instantáneas	"Límite configurable de seis instantáneas"	"Límite configurable de seis instantáneas"

Función	ONTAP 9.17.1 y posteriores	ONTAP 9.16.1 y anteriores
Periodo de conservación	Las instantáneas normalmente se conservan durante 12 horas. • Volúmenes NAS: si se confirma un ataque mediante el análisis de archivos, se conservan las instantáneas creadas antes del ataque hasta que el administrador marque el ataque como verdadero o falso positivo (sospechoso claro). • Almacenes de datos de volumen SAN o de máquina virtual: si se confirma un ataque mediante un análisis de entropía de bloques, las instantáneas creadas antes del ataque se conservan durante 10 días (configurable).	• Determinado en función de las condiciones de activación (no fijo) • Las instantáneas creadas antes del ataque se conservan hasta que el administrador marca el ataque como verdadero o falso positivo (sospechoso claro).
Acción claramente sospechosa	Los administradores pueden realizar una acción de sospecha clara que establece la retención en función de la confirmación: • 24 horas para retención de falsos positivos • 7 días para una retención verdaderamente positiva	Los administradores pueden realizar una acción de sospecha clara que establece la retención en función de la confirmación: • 24 horas para retención de falsos positivos • 7 días para una retención verdaderamente positiva Este comportamiento de retención preventiva no existía antes de ONTAP 9.16.1
Tiempo de expiración	Se establece un tiempo de expiración para todas las instantáneas	Ninguno

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

ARP se basa en la tecnología probada de protección de datos y recuperación ante desastres de ONTAP para responder a ataques de ransomware. ARP crea instantáneas bloqueadas cuando se detectan los primeros signos de un ataque. Primero deberá confirmar si el ataque es real o un falso positivo. Si confirma el ataque, el volumen se puede restaurar mediante la instantánea de ARP.

Las instantáneas bloqueadas no se pueden eliminar por medios normales. Sin embargo, si más tarde decide marcar el ataque como un falso positivo, ONTAP elimina la copia bloqueada.

Puede recuperar archivos afectados desde instantáneas seleccionadas en lugar de revertir todo el volumen.

Consulte los siguientes temas para obtener más información sobre cómo responder a un ataque y recuperar datos:

- "Responda a actividades anormales"
- "Recuperar datos de instantáneas ARP"
- "Recuperarse de las instantáneas de ONTAP"

- "Recuperación inteligente de ransomware"

Protección con verificación multiadministrador para ARP

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".

Protección autónoma frente a ransomware con inteligencia artificial (ARP/AI)

A partir de ONTAP 9.16.1, ARP mejora la ciberresiliencia mediante la adopción de un modelo de aprendizaje automático para el análisis antiransomware que detecta formas de ransomware en constante evolución con una precisión del 99 % en entornos NAS. El modelo de aprendizaje automático de ARP se entrena previamente con un gran conjunto de datos de archivos, tanto antes como después de un ataque simulado de ransomware. Este entrenamiento, que requiere muchos recursos, se realiza fuera de ONTAP utilizando conjuntos de datos de investigación forense de código abierto para entrenar el modelo. Los datos del cliente no se utilizan en todo el proceso de modelado y no existen problemas de privacidad. El modelo preentrenado resultante de este entrenamiento se incluye en ONTAP . Este modelo no es accesible ni modificable a través de la CLI ni la API de ONTAP .

Transición inmediata a la protección activa para ARP/AI

Con ARP/AI, no hayperíodo de aprendizaje . ARP/AI se activa inmediatamente después de la instalación o actualización para los siguientes tipos de volúmenes compatibles:

- Volúmenes NAS FlexVol con ONTAP 9.16.1 y versiones posteriores
- Volúmenes NAS FlexGroup con ONTAP 9.18.1 y versiones posteriores
- Volúmenes SAN con ONTAP 9.17.1 y versiones posteriores (activos inmediatamente, incluso durante el"período de evaluación")

Para los volúmenes existentes y nuevos con funcionalidad ARP ya habilitada, la protección ARP/AI se activará automáticamente después de actualizar su clúster a una versión de ONTAP compatible con ARP/AI.

Actualizaciones automáticas ARP/AI

Para mantener la protección actualizada contra las últimas amenazas de ransomware, ARP/AI ofrece actualizaciones automáticas frecuentes que se realizan fuera de los plazos habituales de actualización y lanzamiento de ONTAP . Si tiene "actualizaciones automáticas activadas" También podrá empezar a recibir actualizaciones de seguridad automáticas de ARP/AI tras seleccionar las actualizaciones automáticas para los archivos de seguridad. También puede optar por… "realizar estas actualizaciones manualmente" y controlar cuándo se producen las actualizaciones.

A partir de ONTAP 9.16,1, las actualizaciones de seguridad para ARP/AI están disponibles con System Manager, además de las actualizaciones del sistema y del firmware.

"Obtenga más información sobre las actualizaciones ARP/AI"

Diferencias entre los modelos ARP/AI y ARP de un vistazo

Función	ARP	ARP/IA
Versiones de ONTAP	ONTAP 9.10.1-9.15.1	ONTAP 9.16.1 y posteriores; 9.15.1 (tech preview)

Función	ARP	ARP/IA
Método de detección	Analiza la actividad de archivos, la entropía de datos y los tipos de extensión de archivos	Modelo de IA/aprendizaje automático entrenado en grandes conjuntos de datos forenses; analiza la entropía y el comportamiento de los archivos
Período de aprendizaje	Requiere un modo de aprendizaje de 30 días para volúmenes NAS FlexVol (conmutación automática disponible en 9.13.1 y versiones posteriores)	Sin periodo de aprendizaje; activo inmediatamente al habilitarlo
Compatibilidad con tipos de volumen	• FlexVol: 9.10.1 y posteriores • FlexGroup: 9.13.1 y posteriores • SAN: no compatible	• FlexVol: 9.16.1 y posteriores • FlexGroup: 9.18.1 y posteriores • SAN: 9.17.1 y posteriores (con periodo de evaluación)
Creación de instantánea	Desencadenado por alta entropía, nuevas extensiones de archivo o aumentos en las operaciones de archivos	Creado a intervalos fijos de 4 horas y al confirmarse el ataque
Retención de instantáneas	Retenido hasta que el administrador elimine la actividad sospechosa	12 horas por defecto; ampliado según la confirmación del ataque (24 horas para falso positivo, 7 días para positivo confirmado)
Actualizaciones	Lógica de detección estática (actualizada solo con las actualizaciones de ONTAP)	Actualizaciones de seguridad automáticas independientes de las versiones de ONTAP
Despliegue	Activación manual por volumen o configuración predeterminada a nivel de SVM	Habilitación manual por volumen o configuración predeterminada a nivel de SVM; habilitación predeterminada en todos los volúmenes nuevos a nivel de clúster para sistemas compatibles en 9.18.1 y versiones posteriores
Periodo de evaluación	No aplicable	Necesario para volúmenes SAN (2-4 semanas) para establecer umbrales de cifrado de referencia

Información relacionada

- "Referencia de comandos del ONTAP"

Casos de uso y consideraciones de la protección autónoma frente a ransomware de ONTAP

La Protección Autónoma contra Ransomware (ARP) está disponible para cargas de trabajo NAS a partir de ONTAP 9.10.1 y SAN a partir de ONTAP 9.17.1. Antes de

implementar ARP, debe conocer 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 estos tipos de cargas de trabajo:

- Bases de datos en almacenamiento NFS o SAN
- Directorios iniciales Windows o Linux

  En entornos sin ARP/AI, los usuarios podrían crear archivos con extensiones que no se detectan durante el periodo de aprendizaje. Por ello, existe una mayor probabilidad 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 estos tipos de cargas de trabajo:

- Cargas de trabajo con una alta frecuencia de operaciones 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 las operaciones de creación, renombrado o eliminación de archivos. Si la propia aplicación es la fuente de la actividad del archivo, no se puede distinguir con eficacia de la actividad de ransomware.
- Cargas de trabajo donde la aplicación o el host cifran los datos.

  ARP depende de distinguir los datos entrantes como cifrados o no cifrados. Si la propia aplicación cifra los datos, la eficacia de la función se reduce. Sin embargo, ARP puede seguir funcionando según la actividad del archivo (eliminar, sobrescribir, crear, o crear o renombrar con una nueva extensión) y el tipo de archivo.

Configuraciones admitidas

ARP está disponible para volúmenes NAS NFS y SMB FlexVol a partir de ONTAP 9.10.1. A partir de la versión 9.17.1, ARP está disponible para volúmenes SAN FlexVol para iSCSI, FC y NVMe con almacenamiento SAN.

ARP es compatible para las configuraciones de MetroCluster a partir de ONTAP 9.10.1.

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

	ONTAP 9.18.1	ONTAP 9.17.1	ONTAP 9.16.1	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 protegidos con SnapMirror asíncrono (recuperación ante desastres de SVM)	✓	✓	✓	✓	✓	✓	✓		
Movilidad de datos de SVM (`vserver migrate`)	✓	✓	✓	✓	✓	✓	✓		
Volúmenes de FlexGroup [1]	✓	✓	✓	✓	✓	✓			
Verificación de varios administradores	✓	✓	✓	✓	✓				
ARP/AI con actualizaciones automáticas	✓	✓							
Habilitación predeterminada de ARP/AI[2]	✓								

[1] ONTAP 9.16.1 y 9.17.1 no proporcionan soporte ARP/AI para volúmenes FlexGroup . Tras una actualización a estas versiones, los volúmenes FlexGroup habilitados para ARP continúan funcionando con el mismo

modelo ARP utilizado antes de ARP/AI. A partir de ONTAP 9.18.1, los volúmenes FlexGroup utilizan el modelo ARP/AI.

[2] A partir de ONTAP 9.18.1, el comportamiento de habilitación predeterminada de ARP/AI está disponible para los sistemas AFF A-series y AFF C-series, ASA y ASA r2. Este comportamiento habilita automáticamente ARP/AI en todos los volúmenes nuevos después de un periodo de gracia de 12 horas tras una actualización o de inmediato para las nuevas instalaciones de ONTAP 9.18.1. Tendrás que habilitar ARP manualmente en "volúmenes existentes".

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 síncrono ni con SnapMirror Active Sync.

Si un volumen de origen de SnapMirror está habilitado para ARP, el volumen de destino de SnapMirror adquiere automáticamente el estado de configuración de ARP (como `dry-run` o `enabled`), datos de entrenamiento de ARP y una instantánea del volumen de origen creada por ARP. No se requiere habilitación explícita.

Aunque el volumen de destino consta de instantáneas de solo lectura (RO), no se realiza procesamiento ARP en sus datos. Sin embargo, cuando el volumen de destino de SnapMirror se convierte a lectura-escritura (RW), ARP se habilita automáticamente en el volumen de destino convertido a RW. El volumen de destino no requiere ningún procedimiento de aprendizaje adicional aparte del ya 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 entrenamiento ni las instantáneas de los volúmenes de origen a los de destino. Por ello, cuando el volumen de destino de SnapMirror se convierte a 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) en VMware. La detección de ARP se comporta de forma diferente para los cambios dentro y fuera de la VM. No se recomienda para cargas de trabajo que impliquen una gran cantidad de archivos muy comprimidos (como 7z y ZIP) o archivos cifrados (como PDF, DOC o ZIP protegidos con contraseña) dentro de la VM.

Realizar cambios fuera de la máquina virtual

ARP puede detectar cambios en la extensión de archivo en un volumen NFS fuera de la VM si una nueva extensión ingresa al volumen en un estado cifrado o si cambia una extensión de archivo.

Cambios dentro de la VM

Si un ataque de ransomware modifica archivos dentro de la máquina virtual sin realizar cambios externos, ARP detecta la amenaza si la entropía predeterminada de la máquina virtual es baja (por ejemplo, archivos .txt, .docx o .mp4). Para ONTAP 9.16.1 y versiones anteriores, ARP crea una instantánea de protección en este escenario, pero no genera una alerta de amenaza porque las extensiones de archivo externas a la máquina virtual no se han alterado. A partir de la compatibilidad con SAN en ONTAP 9.17.1, ARP genera una alerta de amenaza adicional si detecta una anomalía de entropía dentro de la máquina virtual.

Si, por defecto, los archivos tienen alta entropía (por ejemplo, archivos .gzip o protegidos con contraseña), la capacidad de detección de ARP es limitada. En este caso, ARP puede tomar instantáneas proactivas; sin embargo, no se activarán alertas si las extensiones de archivo no han sido alteradas externamente.

Para SAN, ARP analiza las estadísticas de entropía a nivel de volumen y activa detecciones cuando se encuentra una anomalía de entropía.

La detección de ataques que ocurren dentro de una máquina virtual solo está disponible para volúmenes FlexVol y no está disponible si el almacén de datos de la máquina virtual está configurado en un volumen FlexGroup en ONTAP 9.18.1 y versiones posteriores.

Configuraciones no admitidas

ARP no es compatible con entornos ONTAP S3.

ARP no admite las siguientes configuraciones de volumen:

- Volúmenes FlexGroup (en ONTAP 9.10.1 a 9.12.1).

  Desde ONTAP 9.13.1 hasta ONTAP 9.17.1, se admiten volúmenes FlexGroup , pero están limitados al modelo ARP utilizado antes de ARP/AI. Los volúmenes FlexGroup son compatibles con ARP/AI a partir de ONTAP 9.18.1.

- Volúmenes FlexCache (ARP es compatible con los volúmenes FlexVol de origen, pero no con los volúmenes de caché)
- Volúmenes sin conexión
- Volúmenes de SnapLock
- SnapMirror síncrono activo
- SnapMirror síncrono
- SnapMirror asíncrono (en ONTAP 9.10.1 y 9.11.1). SnapMirror asíncrono es compatible a partir de ONTAP 9.12.1. Para 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, medido en rendimiento e IOPS máximos. El impacto de la función ARP depende de la carga de trabajo específica del volumen. 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 excede el límite de volumen por nodo [1]
Lectura intensiva o los datos se pueden comprimir	150	4 % de IOPS máximo

Características de las cargas de trabajo	Límite de volúmenes recomendado por nodo	Degradación del rendimiento cuando se excede el límite de volumen por nodo [1]
Escritura intensiva y los datos no se pueden comprimir	60	• NAS: 10 % del IOPS máximo para ONTAP 9.15.1 y versiones anteriores • NAS: 5% del máximo de IOPS para ONTAP 9.16.1 y versiones posteriores • SAN: 5 % del IOPS máximo para ONTAP 9.17.1 y versiones posteriores

[1] El rendimiento del sistema no se degrada más allá de estos porcentajes, independientemente de la cantidad de volúmenes agregados que excedan los límites recomendados.

Debido a que los análisis de ARP se ejecutan en una secuencia priorizada, los análisis se ejecutan en cada volumen con menor frecuencia a medida que aumenta la cantidad de volúmenes protegidos.

Habilitar ARP por defecto en un gran número de nuevos volúmenes puede incrementar el uso de recursos del sistema. Considera las demandas de espacio para procesos competidores como las instantáneas cuando habilites ARP en volúmenes.

Límites de volumen para ARP por plataforma

A partir de ONTAP 9.18.1, ARP admite límites de volumen aumentados según el tipo de plataforma y la cantidad de núcleos de CPU.

Tipo de plataforma	Máximo de volúmenes con ARP habilitado por nodo
Gama baja (sistemas con hasta 20 CPU cores)	250
Mediana (sistemas con hasta 64 núcleos de CPU)	500
Gama alta (sistemas con más de 64 núcleos de CPU)	1000

El recuento de núcleos de CPU se aplica a cada nodo individual en un par de HA de 2 nodos.

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 a "Habilite MAV para volúmenes protegidos por ARP".

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

Obtenga más información acerca de `security anti-ransomware volume disable`, `security anti-ransomware volume pause` y `security anti-ransomware volume attack clear-suspect` en el "Referencia de comandos del ONTAP".

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

Obtenga más información sobre `security anti-ransomware vserver event-log modify` y `security anti-ransomware volume event-log modify` en el "Referencia de comandos del ONTAP".

Siguientes pasos

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

Activar ARP

Habilita ONTAP Autonomous Ransomware Protection en un volumen

A partir de ONTAP 9.10,1, puede habilitar la protección autónoma frente a ransomware (ARP) en un volumen existente o crear un volumen nuevo y habilitar ARP desde el principio.

Acerca de esta tarea

Para habilitar ARP, siga el procedimiento que corresponda a su entorno después deusted se asegura de que su entorno cumpla con ciertos requisitos :

- NAS con volúmenes FlexVol
- NAS con volúmenes FlexGroup
- Volúmenes SAN

Después de habilitar ARP, es posible que ARP entre en un período de transición dependiendo de su entorno y versión de ONTAP :

Tipo de volumen	Versión de ONTAP	Comportamiento tras la habilitación
NAS FlexGroup	ONTAP 9.18.1 y posteriores	ARP/IA se activa inmediatamente sin necesidad de periodo de aprendizaje.
	ONTAP 9.13.1 a 9.17.1	ARP inicia en modo de aprendizaje durante 30 días
NAS FlexVol	ONTAP 9.16.1 y versiones posteriores	ARP/IA se activa inmediatamente sin necesidad de periodo de aprendizaje.
	ONTAP 9.10.1 a 9.15.1	ARP inicia en modo de aprendizaje durante 30 días
Volúmenes SAN	ONTAP 9.17.1 y posteriores	ARP/AI se activa de inmediato, iniciando un período de evaluación para establecer un umbral de alerta adecuado antes de pasar de un umbral conservador inicial.

Antes de empezar

Antes de habilitar ARP, asegúrese de que su entorno tenga lo siguiente:

Requisitos específicos de NAS

- Una máquina virtual de almacenamiento (SVM) con el protocolo NFS o SMB (o ambos) habilitado.
- Carga de trabajo NAS con clientes configurados.
- Un activo"ruta de unión" para el volumen.

Requisitos específicos de SAN

- Una máquina virtual de almacenamiento (SVM) con protocolo iSCSI, FC o NVMe habilitado.
- Carga de trabajo SAN con clientes configurados.

Requisitos generales

- El"licencia correcta" para su versión de ONTAP .
- (Recomendado) Verificación multiadministrador (MAV) habilitada (ONTAP 9.13.1 y posterior). Ver"Habilite la verificación multiadministradora" .

Habilitar ARP en volúmenes NAS FlexVol

Puede habilitar ARP en volúmenes NAS FlexVol utilizando System Manager o la CLI de ONTAP . El proceso varía según la versión de ONTAP .

ONTAP 9.16.1 y versiones posteriores

A partir de ONTAP 9.16.1, ARP/AI se activa inmediatamente sin necesidad de un período de aprendizaje.

System Manager

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 Deshabilitado a Activado.
3. Verifique el estado ARP del volumen en la casilla **Antiransomware**.

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

CLI

Habilitar ARP en un volumen existente:

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

Crea un nuevo volumen con ARP habilitado:

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state enabled -junction-path
</path_name>
```

Verificar el estado de ARP:

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

Obtenga más información sobre `security anti-ransomware volume show` en el "Referencia de comandos del ONTAP".

ONTAP 9.10.1 a 9.15.1

Para ONTAP 9.10.1 a 9.15.1, debe habilitar ARP inicialmente en"modo de aprendizaje" (o estado de "prueba en seco"). El sistema analiza la carga de trabajo para caracterizar el comportamiento normal. Comenzar en modo activo puede generar un exceso de informes de falsos positivos.

Se recomienda dejar 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 periodo de aprendizaje y automatiza el cambio, que podría ocurrir antes de los 30 días.

System Manager

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

Deshabilitado a Activado.

3. Seleccione **Habilitado en modo de aprendizaje** en la casilla **Antiransomware**.

> Puede"Deshabilitar el aprendizaje automático a transiciones de modos activos en la máquina virtual de almacenamiento asociada." Si desea controlar manualmente la transición del modo de aprendizaje al modo activo.

> 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.

4. Verifique el estado ARP del volumen en la casilla **Antiransomware**.

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

CLI

Habilitar ARP en un volumen existente:

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

Obtenga más información sobre `security anti-ransomware volume dry-run` en el "Referencia de comandos del ONTAP".

Crea un nuevo volumen con ARP habilitado:

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

Desactivar el cambio automático (opcional):

Si actualizó a ONTAP 9.13.1 a través de ONTAP 9.15.1 y desea controlar manualmente el cambio del modo de aprendizaje al modo activo para todos los volúmenes asociados, puede hacerlo desde la SVM:

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

Verificar el estado de ARP:

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

Habilitar ARP en volúmenes NAS FlexGroup

Puede habilitar ARP en volúmenes NAS FlexGroup mediante System Manager o la CLI de ONTAP . El proceso varía según su versión de ONTAP .

ONTAP 9.18.1 y posteriores

A partir de ONTAP 9.18.1, ARP/AI se activa inmediatamente para los volúmenes FlexGroup sin necesidad de un período de aprendizaje.

System Manager

1. Seleccione **Almacenamiento > Volúmenes** y, a continuación, seleccione el volumen de FlexGroup que desea proteger.
2. En la pestaña **Seguridad** de la vista general **Volúmenes**, selecciona **Estado** para cambiar de Deshabilitado a Activado.
3. Verifique el estado ARP del volumen en la casilla **Antiransomware**.

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

CLI

Habilitar ARP en un volumen FlexGroup existente:

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

Crea un nuevo volumen FlexGroup con ARP habilitado:

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state enabled -junction-path </path_name>
```

Verificar el estado de ARP:

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

ONTAP 9.13.1 a 9.17.1

Para ONTAP 9.13.1 a 9.17.1, los volúmenes FlexGroup comienzan en"modo de aprendizaje" . El sistema analiza la carga de trabajo para caracterizar el comportamiento normal.

Se recomienda dejar que ARP se ejecute en modo de aprendizaje durante un mínimo de 30 días. ARP determina automáticamente el intervalo óptimo del período de aprendizaje y automatiza el cambio, que podría ocurrir antes de 30 días.

System Manager

1. Seleccione **Almacenamiento > Volúmenes** y, a continuación, seleccione el volumen de FlexGroup que desea proteger.
2. En la pestaña **Seguridad** de la vista general **Volúmenes**, selecciona **Estado** para cambiar de Deshabilitado a Activado.
3. Seleccione **Habilitado en modo de aprendizaje** en la casilla **Antiransomware**.

Puede"Deshabilitar el aprendizaje automático a transiciones de modos activos" Si desea controlar manualmente la transición del modo de aprendizaje al modo activo.

4. Verifique el estado ARP del volumen en la casilla **Antiransomware**.

CLI

Habilitar ARP en un volumen FlexGroup existente:

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

Crea un nuevo volumen FlexGroup con ARP habilitado:

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state dry-run -junction-path </path_name>
```

Desactivar el cambio automático (opcional):

Si desea controlar manualmente el cambio del modo de aprendizaje al modo activo:

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

Verificar el estado de ARP:

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

Habilitar ARP en volúmenes SAN

A partir de ONTAP 9.17.1, puede habilitar ARP en volúmenes SAN. La funcionalidad ARP/AI se habilita automáticamente e inmediatamente comienza a supervisar y proteger activamente los volúmenes SAN durante el proceso."período de evaluación" al mismo tiempo que determina si las cargas de trabajo son adecuadas para ARP y establece un umbral de cifrado óptimo para la detección.

Puede habilitar ARP en volúmenes SAN utilizando System Manager o la CLI de ONTAP .

System Manager

Pasos

1. Seleccione **Almacenamiento > Volúmenes** y, a continuación, seleccione el volumen SAN que desea proteger.
2. En la pestaña **Seguridad** de la vista general **Volúmenes**, selecciona **Estado** para cambiar de Deshabilitado a Activado.
3. ARP/AI entra automáticamente en el período de evaluación.
4. Verifique el estado de ARP y el estado de evaluación en la casilla **Antiransomware**.

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

CLI

Habilitar ARP en un volumen SAN existente:

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

Crear un nuevo volumen SAN con ARP habilitado:

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state enabled
```

Verifique el estado y la evaluación del ARP:

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

Comprueba el `Block device detection status` campo para monitorear el progreso del período de evaluación.

Obtenga más información sobre `security anti-ransomware volume show` en el "Referencia de comandos del ONTAP".

Información relacionada

- "Cambia al modo activo después de un periodo de aprendizaje"

Habilita la protección autónoma frente a ransomware de ONTAP de forma predeterminada en nuevos volúmenes

A partir de ONTAP 9.10.1, puedes configurar las máquinas virtuales de almacenamiento (SVM) para que los nuevos volúmenes se habiliten por defecto con Autonomous Ransomware Protection (ARP). Puedes modificar esta configuración usando System

Manager o con la ONTAP CLI.

A partir de ONTAP 9.18.1, ARP se habilita de forma predeterminada en todos los volúmenes nuevos a nivel de clúster para "sistemas compatibles" después de un periodo de gracia de 12 horas tras una actualización de clúster o una nueva instalación. Si desactivas la habilitación automática predeterminada de ARP a nivel de clúster, igual puedes elegir habilitar manualmente ARP de forma predeterminada en todos los volúmenes nuevos a nivel de SVM.

Para ONTAP 9.17.1 y versiones anteriores, la configuración a nivel de SVM es la única forma de habilitar ARP por defecto en los nuevos volúmenes.

Acerca de esta tarea

Por defecto, los nuevos volúmenes se crean con la funcionalidad ARP desactivada. Deberá habilitar la funcionalidad ARP y configurarla para que esté habilitada de forma predeterminada en los nuevos volúmenes creados en la SVM.

Los volúmenes existentes sin ARP habilitado no cambiarán automáticamente su estado de habilitación de ARP cuando cambie el valor predeterminado para la SVM. Los cambios en la configuración de SVM descritos en este procedimiento solo afectan a los volúmenes nuevos. Aprende cómo"Habilite ARP para los volúmenes existentes" .

Después de habilitar ARP, es posible que ARP entre en un período de transición dependiendo de su entorno y versión de ONTAP :

Tipo de volumen	Versión de ONTAP	Comportamiento tras la habilitación
NAS FlexGroup	ONTAP 9.18.1 y posteriores	ARP/IA se activa inmediatamente sin necesidad de periodo de aprendizaje.
	ONTAP 9.13.1 a 9.17.1	ARP inicia en modo de aprendizaje durante 30 días
NAS FlexVol	ONTAP 9.16.1 y versiones posteriores	ARP/IA se activa inmediatamente sin necesidad de periodo de aprendizaje.
	ONTAP 9.10.1 a 9.15.1	ARP inicia en modo de aprendizaje durante 30 días
Volúmenes SAN	ONTAP 9.17.1 y posteriores	ARP/AI se activa de inmediato, iniciando un período de evaluación para establecer un umbral de alerta adecuado antes de pasar de un umbral conservador inicial.

Antes de empezar

Antes de habilitar ARP, asegúrese de que su entorno tenga lo siguiente:

Requisitos específicos de NAS

- Una máquina virtual de almacenamiento (SVM) con el protocolo NFS o SMB (o ambos) habilitado.
- Un activo"ruta de unión" para el volumen.

Requisitos específicos de SAN

- Una máquina virtual de almacenamiento (SVM) con protocolo iSCSI, FC o NVMe habilitado.

Requisitos generales

- El"licencia correcta" para su versión de ONTAP .
- (Recomendado) Verificación multiadministrador (MAV) habilitada (ONTAP 9.13.1+). Ver"Habilite la

verificación multiadministradora" .

Pasos

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

System Manager

1. Seleccione **Almacenamiento** o **Clúster** (según su entorno), seleccione **Máquinas virtuales de almacenamiento** y seleccione la máquina virtual de almacenamiento que contendrá los volúmenes que desea proteger con ARP.
2. Vaya a la pestaña **Configuración**. En **Seguridad**, localice la opción **Anti-ransomware** y seleccione  .
3. Marque la casilla para habilitar el antiransomware (ARP). Marque la casilla adicional para habilitar ARP en todos los volúmenes elegibles de la máquina virtual de almacenamiento.
4. Para las versiones de ONTAP con un período de aprendizaje recomendado, seleccione **Cambiar automáticamente del modo de aprendizaje al modo activo después de un aprendizaje suficiente**. Esto permite que ARP determine el intervalo óptimo del periodo de aprendizaje y automatice el cambio al modo activo.

CLI

Modificar una SVM existente para habilitar ARP de forma predeterminada en los nuevos volúmenes.

Seleccionar `dry-run` si su versión de ARP requiere unperíodo de aprendizaje . De lo contrario, seleccione `enabled` .

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume
-state <dry-run|enabled>
```

Cree una nueva SVM con ARP habilitado de forma predeterminada para los nuevos volúmenes.

Seleccionar `dry-run` si su versión de ARP requiere unperíodo de aprendizaje . De lo contrario, seleccione `enabled` .

```
vserver create -vserver <svm_name> -anti-ransomware-default-volume
-state <dry-run|enabled>
```

Modificar la SVM existente para deshabilitar la transición automática del aprendizaje al modo activo

Si actualizó a ONTAP 9.13.1 a través de ONTAP 9.15.1 y el estado predeterminado es `dry-run` (modo de aprendizaje), el aprendizaje adaptativo está habilitado para que el cambio a `enabled` El estado (modo activo) se realiza automáticamente. Puede desactivar este interruptor automático para controlar manualmente el cambio del modo de aprendizaje al modo activo para todos los volúmenes asociados:

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

Verifique el estado ARP

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

Información relacionada

- "Cambia al modo activo después de un periodo de aprendizaje"
- "Visualización de volumen de seguridad antiransomware"

Excluye la activación por defecto de ONTAP Autonomous Ransomware Protection

A partir de ONTAP 9.18.1, Autonomous Ransomware Protection (ARP) se habilita automáticamente de forma predeterminada en todos los volúmenes nuevos para AFF A-series y AFF C-series, ASA y ASA r2 después de un periodo de calentamiento de 12 horas tras una actualización o una instalación nueva, siempre que se haya instalado una licencia de ARP. Puedes optar por no activar esta habilitación predeterminada durante o después del periodo de gracia de 12 horas usando System Manager o la CLI de ONTAP.

Los volúmenes existentes deben ser "activado manualmente" para ARP.

Acerca de esta tarea

La configuración que elijas para este procedimiento se puede cambiar más adelante. Después del periodo de gracia, siempre tienes la flexibilidad de activar o desactivar la activación por defecto en cualquier momento:

```
security anti-ransomware auto-enable modify -new-volume-auto-enable
false|true
```

Pasos

Puedes usar System Manager o la CLI de ONTAP para gestionar las opciones de activación predeterminada de ARP.

System Manager

1. Seleccione **Cluster > Settings**.
2. Debe realizar una de las siguientes acciones:
   - Desactivar durante el periodo de gracia activo:
     i. En la sección **Anti-ransomware**, verás un mensaje que indica las horas que faltan antes de que se habilite ARP. Selecciona **Don't enable**.
     ii. Selecciona **Desactivar** en el siguiente cuadro de diálogo para confirmar que la activación predeterminada de ARP está desactivada para los nuevos volúmenes.
   - Desactivar después del periodo de gracia:
     i. En la sección **Anti-ransomware**, selecciona  .
     ii. Selecciona la casilla y luego **Guardar** para desactivar la habilitación predeterminada de ARP para nuevos volúmenes.

CLI

1. Verifica el estado de habilitación predeterminado:

```
security anti-ransomware auto-enable show
```

2. Desactiva la activación por defecto para nuevos volúmenes:

```
security anti-ransomware auto-enable modify -new-volume-auto-enable
false
```

Información relacionada

- "Habilita ONTAP Autonomous Ransomware Protection en un volumen individual"

Cambia al modo activo en ONTAP ARP después de un período de aprendizaje

En entornos NAS, cambie manual o automáticamente un volumen con ARP habilitado del modo de aprendizaje al modo activo. Deberá cambiar de modo si está utilizando ARP con ONTAP 9.15.1 o anterior, o si ARP se está ejecutando en volúmenes FlexGroup con ONTAP 9.17.1 o anterior.

Una vez que ARP haya completado el modo de aprendizaje durante un mínimo recomendado de 30 días, puede cambiar manualmente al modo activo. A partir de ONTAP 9.13.1, ARP determina automáticamente el intervalo óptimo del período de aprendizaje y automatiza el cambio, que podría ocurrir antes de los 30 días.

Si está utilizando ARP con protección ARP/AI, ARP se activará automáticamente. No se requiere un periodo de aprendizaje.

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.

Cambie manualmente al modo activo después del periodo de aprendizaje

Para ONTAP 9.10.1 a 9.15.1 (ONTAP 9.17.1 y anteriores con volúmenes FlexGroup), puede realizar manualmente la transición del modo de aprendizaje ARP al modo activo mediante System Manager o la CLI de ONTAP una vez finalizado el período de aprendizaje.

Acerca de esta tarea

La transición manual al modo activo después de un período de aprendizaje descrito en este procedimiento es específica de los entornos NAS.

Pasos

Puede utilizar el Administrador del sistema o la CLI de ONTAP para cambiar del modo de aprendizaje al modo activo.

System Manager

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

CLI

1. Modifique el volumen protegido para cambiar al modo activo si aún no lo hace 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 enabled
   ```

2. Verifique el estado ARP del volumen.

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

Cambio automático del modo de aprendizaje al modo activo

A partir de ONTAP 9.13.1, se ha añadido el aprendizaje adaptativo a las analíticas de ARP, y 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 la 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
```

Si el cambio automático está habilitado, el volumen pasará automáticamente al modo activo después de un máximo de 30 días, incluso si no se cumplen todas las condiciones. Este límite de 30 días es fijo y no se puede modificar.

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

Información relacionada

- "volumen de seguridad anti-ransomware"

Obtenga más información sobre el período de evaluación de ONTAP ARP para volúmenes SAN

A partir de ONTAP 9.17.1, ARP requiere un período de evaluación para determinar si los niveles de entropía de las cargas de trabajo de volúmenes SAN son adecuados para la protección contra ransomware. Una vez habilitado ARP en un volumen SAN, ARP/AI supervisa y protege activamente el volumen durante el período de evaluación, al tiempo que determina un umbral de cifrado óptimo. La detección y las alertas pueden producirse durante el período de evaluación utilizando un umbral conservador mientras se establecen los umbrales de referencia. ARP distingue entre cargas de trabajo adecuadas e inadecuadas en el volumen SAN evaluado y, si se determina que son adecuadas para la protección, establece automáticamente un umbral de cifrado basado en las estadísticas del período de evaluación.

Comprender la evaluación de la entropía

El sistema recopila estadísticas de cifrado continuas en intervalos de 10 minutos. Durante la evaluación, también se crean continuamente instantáneas periódicas de ARP cada cuatro horas. Si el porcentaje de cifrado dentro de un intervalo excede el umbral de cifrado óptimo identificado para este volumen, se activa una alerta. `Anti_ransomware_attack_backup` Se crea una instantánea y el tiempo de retención de la misma aumenta en cualquier instantánea ARP periódica.

Confirmar que el periodo de evaluación está activo

Puede confirmar que la evaluación está activa ejecutando el siguiente comando y confirmando un estado de `evaluation_period`. Si un volumen no es elegible para evaluación, no se mostrará el estado de

evaluación.

```
security anti-ransomware volume show -vserver <svm_name> -volume
<volume_name>
```

Ejemplo de respuesta:

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : evaluation_period
```

Recopilación de datos del período de evaluación del monitor

Puede supervisar la detección de cifrado en tiempo real ejecutando el siguiente comando. Este comando devuelve un histograma que muestra la cantidad de datos en cada rango de porcentaje de cifrado. El histograma se actualiza cada 10 minutos.

```
security anti-ransomware volume entropy-stat show-encryption-percentage-
histogram -vserver <svm_name> -name <lun_name> -duration real_time
```

Ejemplo de respuesta:

```
Vserver     Name              Entropy Range   Seen N Time     Data Written
----------  ----------------  --------------- --------------
-------------
vs0         lun1              0-5%            4               100MB
vs0         lun1              6-10%           10              900MB
vs0         lun1              11-15%          20              40MB
vs0         lun1              16-20%          10              70MB
vs0         lun1              21-25%          60              450MB
vs0         lun1              26-30%          4               100MB
vs0         lun1              31-35%          10              900MB
vs0         lun1              36-40%          20              40MB
vs0         lun1              41-45%          0               0
vs0         lun1              46-50%          0               0
vs0         lun1              51-55%          0               0
vs0         lun1              56-60%          0               0
vs0         lun1              61-65%          0               0
vs0         lun1              66-70%          0               0
vs0         lun1              71-75%          0               0
vs0         lun1              76-80%          0               0
vs0         lun1              81-85%          0               0
vs0         lun1              86-90%          0               0
vs0         lun1              91-95%          0               0
vs0         lun1              96-100%         0               0

20 entries were displayed.
```

Cargas de trabajo adecuadas y umbrales adaptativos

La evaluación finaliza con uno de los siguientes resultados:

- **La carga de trabajo es adecuada para ARP**. ARP establece automáticamente el umbral adaptativo por encima del 10 % del porcentaje máximo de cifrado observado durante el período de evaluación. ARP también continúa recopilando estadísticas y crea instantáneas periódicas de ARP.
- **La carga de trabajo no es adecuada para ARP**. ARP establece automáticamente el umbral adaptativo al porcentaje máximo de cifrado observado durante el período de evaluación. ARP también continúa recopilando estadísticas y crea instantáneas periódicas de ARP, pero el sistema finalmente recomienda deshabilitar ARP en el volumen.

Determinar los resultados de la evaluación

Una vez finalizado el período de evaluación, ARP establece automáticamente el umbral adaptativo en función de los resultados de la evaluación.

Puede determinar los resultados de la evaluación ejecutando el siguiente comando. La idoneidad del volumen se indica en el `Block device detection status` campo:

```
security anti-ransomware volume show  -vserver <svm_name> -volume
<volume_name>
```

Ejemplo de respuesta:

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : Active_suitable_workload

Block device evaluation start time :  5/16/2025 01:49:01
```

También puedes mostrar el valor umbral adoptado como resultado de la evaluación:

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

Ejemplo de respuesta:

```
                                  Vserver Name : vs_1

                                   Volume Name : vm_2

Block Device Auto Learned Encryption Threshold : 10
...
```

Pausa la protección autónoma frente a ransomware de ONTAP para excluir los eventos de cargas 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.

"Más información acerca de MAV".

Acerca de esta tarea

Durante una pausa ARP, ONTAP no registra eventos ni acciones para nuevas escrituras; sin embargo, el análisis continúa en segundo plano para los registros anteriores.

> 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 descripción general de Volúmenes, seleccione **Pausar anti-ransomware** en el cuadro **Anti-ransomware**.

   A partir de ONTAP 9.13.1, si utiliza MAV para proteger la configuración ARP, la operación de pausa le solicita que obtenga la aprobación de uno o más administradores adicionales. "La aprobación debe recibirse de todos los administradores" asociado con el grupo de aprobación MAV o la operación fracasará.

3. Para reanudar la monitorización, seleccione **Reanudar anti-ransomware**.

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` el comando:

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

   Obtenga más información sobre `security anti-ransomware volume` en el "Referencia de comandos del ONTAP".

3. Si está utilizando MAV (disponible con ARP a partir de ONTAP 9.13.1) para proteger la configuración de ARP, la operación de pausa le solicita que obtenga la aprobación de uno o más administradores adicionales. Se debe obtener la aprobación de todos los administradores asociados con el 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>]
```

+
Obtenga más información sobre `security multi-admin-verify request` en el "Referencia de comandos del ONTAP".

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

A partir de ONTAP 9.11.1, se pueden modificar los parámetros de detección de ransomware en un volumen específico con la protección autónoma contra ransomware habilitada y notificar 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 o evaluación, desarrolla valores de referencia para el comportamiento del volumen. Estos incluyen la entropía, las extensiones de archivo y, a partir de ONTAP 9.11.1, las IOPS. Estos valores de referencia se utilizan para evaluar las amenazas de ransomware. Para obtener más información sobre estos criterios, consulte "Lo que ARP detecta" .

Ciertos volúmenes y cargas de trabajo requieren parámetros de detección diferentes. Por ejemplo, el volumen habilitado para ARP podría albergar numerosos tipos de extensiones de archivo, en cuyo caso es posible que desee modificar el recuento de umbral para extensiones de archivo nunca antes vistas a un número mayor que el valor predeterminado de 20 o deshabilitar las advertencias basadas en extensiones de archivo nunca antes vistas. A partir de ONTAP 9.11.1, puede modificar los parámetros de detección de ataques para que se adapten mejor a sus cargas de trabajo específicas.

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

Detección de ataques en entornos NAS

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 24 horas y 20 archivo son los valores predeterminados, que se pueden modificar.

> Para reducir el número de alertas de falsos positivos, vaya a **Almacenamiento > Volúmenes > Seguridad > Configurar características de la carga de trabajo** y desactive **Monitorear nuevos tipos de archivos**. Esta opción está deshabilitada de forma predeterminada en ONTAP 9.14.1 P7, 9.15.1 P1, 9.16.1 y versiones posteriores.

Detección de ataques en entornos SAN

A partir de ONTAP 9.17.1, ARP emite una advertencia si detecta tasas de cifrado altas que superan un umbral aprendido automáticamente. Este umbral se establece después de un "período de evaluación" pero puede modificarse.

Modificar los parámetros de detección de ataques

Dependiendo del comportamiento esperado del 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
          Block Device Auto Learned Encryption Threshold : 10
           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 : 5
       Never Seen before File Extensions Duration in Hour : 48
```

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

   Obtenga más información sobre `security anti-ransomware volume attack-detection-`

`parameters modify` en el "Referencia de comandos del ONTAP".

Informe de sobretensiones conocidas

ARP continúa modificando los valores de línea base para los parámetros de detección incluso cuando está activo. Si conoce aumentos en su actividad de volumen, ya sea un aumento puntual o un aumento característico de una nueva normalidad, debe informarlos como seguros. 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>
   ```

   Obtenga más información sobre `security anti-ransomware volume workload-behavior clear-surge` en el "Referencia de comandos del ONTAP".

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>
   ```

   Obtenga más información sobre `security anti-ransomware volume workload-behavior update-baseline-from-surge` en el "Referencia de comandos del ONTAP" .

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 la verificación multiadministrador. Para más información, consulte "Verificación multi-admin con volúmenes protegidos con ARP" .

Pasos

Puede utilizar el Administrador del sistema o la CLI de ONTAP para configurar alertas para eventos ARP.

System Manager

Configure alertas para un volumen

1. Vaya a **Volúmenes**. Seleccione el volumen cuya configuración desea modificar.
2. Seleccione la pestaña **Seguridad** y luego **Configuración de gravedad del evento**.
3. Para recibir alertas de **Nueva extensión de archivo detectada** y **Instantánea de ransomware creada**, seleccione el menú desplegable bajo el encabezado **Gravedad**. Cambie la configuración de **No generar evento** a **Aviso**.
4. Seleccione **Guardar**.

Configure alertas para una SVM

1. Vaya a **Storage VM** y luego seleccione la SVM para la cual desea habilitar la configuración.
2. En el encabezado **Seguridad**, localice la tarjeta **Anti-ransomware**. Seleccione ⋮ Luego, **Editar gravedad del 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**. Cambie la configuración de **No generar evento** a **Aviso**.
4. Seleccione **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>
-volume <volume_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>
-volume <volume_name> -is-enabled-on-snapshot-copy-creation true
```

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

Obtenga más información sobre `security anti-ransomware vserver event-log` comandos en el "Referencia de comandos del ONTAP" .

Información relacionada

- "Comprende los ataques autónomos de protección frente a ransomware y el snapshot autónomo de protección frente a ransomware".
- "Referencia de comandos del ONTAP"

Responder a la actividad anormal detectada por ONTAP ARP

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. Después de categorizar el ataque, puede borrar la advertencia y los avisos sobre archivos sospechosos.

Cuando se categoriza un ataque, las instantáneas de ARP se conservan durante un período abreviado iniciado por la operación de categorización (ONTAP 9.16.1 y posteriores) o se eliminan instantáneamente (ONTAP 9.15.1 y anteriores).

A partir de ONTAP 9.11.1, puede modificar el "configuración de retención" para instantáneas ARP.

Acerca de esta tarea

ARP muestra una lista de archivos sospechosos al detectar cualquier combinación de alta entropía de datos, actividad anormal de volumen con cifrado de datos y extensiones de archivo inusuales. A partir de ONTAP 9.17.1, tanto para entornos NAS como SAN, los detalles de los picos de entropía también se informan en la página Antiransomware del Administrador del Sistema.

Cuando se emite una notificación de advertencia de ARP, responda designando la actividad de una de dos maneras:

- **Falso positivo**

  Se espera que el tipo de archivo identificado o el pico de entropía se produzcan en su carga de trabajo y se pueden ignorar.

- * Potencial ataque de ransomware*

  El tipo de archivo identificado o el pico de entropía es inesperado en su carga de trabajo y debe tratarse como un ataque potencial.

La supervisión normal se reanuda después de actualizar su decisión y borrar las notificaciones de ARP. ARP registra su evaluación en el perfil de evaluación de amenazas y utiliza su decisión para supervisar las actividades posteriores de los archivos.

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 protegiendo activamente un volumen y no en modo de aprendizaje o evaluación.

Pasos

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

System Manager

1. Cuando reciba una notificación de "actividad anormal", siga el enlace. También puede ir a la pestaña **Seguridad** de la vista general de **Volúmenes**.

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

2. En la pestaña **Seguridad**, revise los tipos de archivos sospechosos o el informe de picos de entropía.
   - Para los archivos sospechosos, examine cada tipo de archivo en el cuadro de diálogo **Tipos de archivos sospechosos** y marque cada uno individualmente.
   - Para picos de entropía, examine el informe de entropía.
3. Graba tu respuesta:

Si selecciona este valor…	Realice esta acción…
Falso positivo	a. Debe realizar una de las siguientes acciones: ◦ Para obtener advertencias sobre el tipo de archivo, seleccione **Actualizar y borrar tipos de archivos sospechosos**. ◦ Para picos de entropía, seleccione **Marcar como falso positivo**. Estas acciones borran las advertencias sobre archivos o actividad sospechosos. ARP reanuda la supervisión normal del volumen. En ONTAP 9.16.1 y versiones posteriores, las instantáneas de ARP se eliminan automáticamente tras un periodo de retención abreviado activado por la operación de categorización. En ONTAP 9.15.1 y versiones anteriores, las instantáneas de ARP relacionadas se eliminan automáticamente tras borrar los tipos de archivo sospechosos. A partir de ONTAP 9.13.1, si utiliza MAV para proteger la configuración ARP, la operación clear-suspect le solicita que obtenga la aprobación de uno o más administradores adicionales. "La aprobación debe recibirse de todos los administradores" asociado con el grupo de aprobación MAV o la operación fracasará.

Posible ataque de ransomware	a. Responder al ataque: ◦ Para las advertencias sobre el tipo de archivo, marque los archivos seleccionados como **Posible ataque de ransomware** y "restaure los datos protegidos" . ◦ Para los picos de entropía que indican un ataque, seleccione **Marcar como posible ataque de ransomware** y "restaure los datos protegidos" . b. Una vez completada la restauración de datos, registre su decisión y reanude la supervisión normal de ARP: ◦ Para obtener advertencias sobre el tipo de archivo, seleccione **Actualizar y borrar tipos de archivos sospechosos**. ◦ Para picos de entropía, seleccione **Marcar como posible ataque de ransomware** y seleccione **Guardar y descartar**. No hay avisos de tipos de archivos sospechosos que borrar si ha restaurado un volumen completo. Al registrar su decisión, se borra el informe de ataque. En ONTAP 9.16.1 y versiones posteriores, las instantáneas de ARP se eliminan automáticamente tras un periodo de retención abreviado activado por la operación de categorización. En ONTAP 9.15.1 y versiones anteriores, tras restaurar un volumen, las instantáneas de ARP se eliminan automáticamente.

CLI

Verificar el ataque

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: 5/12/2025 01:03:23
Number of Attacks: 1
Attack Detected By: encryption_percentage_analysis
```

También puede comprobar los mensajes de EMS:

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

2. Genere un informe de ataque y especifique dónde guardarlo:

```
security anti-ransomware volume attack generate-report -vserver
<svm_name> -volume <vol_name> -dest-path
<[svm_name]:[junction_path/sub_dir_name]>
```

Comando de ejemplo:

```
security anti-ransomware volume attack generate-report -vserver vs0
-volume vol1 -dest-path vs0:vol1
```

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:

```
cat report_file_vs0_vol1_14-09-2021_01-21-08
```

Tomar medidas

1. Realice una de las siguientes acciones según su evaluación de las extensiones de archivo o los picos de entropía:

   - Falso positivo

     Ejecute uno de los siguientes comandos para registrar su decisión y reanudar la supervisión normal de Autonomous Ransomware Protection:

     - Para extensiones de archivo:

       ```
       anti-ransomware volume attack clear-suspect -vserver
       <svm_name> -volume <vol_name> [<extension_identifiers>] -false
       -positive true
       ```

       Utilice el siguiente parámetro opcional para identificar sólo extensiones específicas como falsos positivos:

       - `[-extension <text>, … ]`: Extensiones de archivo

- Para picos de entropía:

```
security anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive true
```

◦ Ataque potencial de ransomware

Responder al ataque y "Recupere los datos de la instantánea de backup creada por ARP". Una vez recuperados los datos, ejecute uno de los siguientes comandos para registrar su decisión y reanudar la monitorización normal de ARP

- Para extensiones de archivo:

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

Utilice el siguiente parámetro opcional para identificar solo extensiones específicas como posible ransomware:

- `[-extension <text>, … ]`: Extensión de archivo

- Para picos de entropía:

```
security anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive
false
```

Este `clear-suspect` Esta operación borra el informe de ataque. No hay avisos de tipo de archivo sospechoso que borrar si se restauró un volumen completo. En ONTAP 9.16.1 y versiones posteriores, las instantáneas de ARP se eliminan automáticamente tras un periodo de retención abreviado activado por la operación de categorización. En ONTAP 9.15.1 y versiones anteriores, las instantáneas de ARP se eliminan automáticamente tras restaurar un volumen o borrar un evento sospechoso.

2. A partir de la versión 9.18.1, puede determinar el estado de `clear-suspect` operación:

```
security anti-ransomware volume show -clear-suspect-status -volume
<vol_name> -vserver <svm_name>
```

Opciones de MAV

1. Si utiliza MAV y una `clear-suspect` operación esperada necesita aprobaciones adicionales, cada aprobador de 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.

2. 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>]
```

Información relacionada

- "Base de conocimientos de NetApp : Comprensión de los ataques de Autonomous Ransomware Protection y la instantánea de Autonomous Ransomware Protection"
- "Modificar las opciones de instantáneas automáticas"
- "volumen de seguridad anti-ransomware"
- "Solicitud de verificación de seguridad multiadministrador"

Restaura los datos de las instantáneas ARP de ONTAP después de un ataque de ransomware

La Protección Autónoma contra Ransomware (ARP) crea instantáneas para protegerse contra una posible amenaza de ransomware. Puede usar una de estas instantáneas de ARP u otra instantánea de su volumen para restaurar los datos.

Acerca de esta tarea

El ARP crea instantáneas con uno de los siguientes nombres antepuestos:

- `Anti_ransomware_periodic_backup` : Se utiliza en ONTAP 9.17.1 y versiones posteriores para instantáneas creadas a intervalos regulares. Por ejemplo, `Anti_ransomware_periodic_backup.2025-06-01_1248` .
- `Anti_ransomware_attack_backup`:Se utiliza en ONTAP 9.17.1 y versiones posteriores para instantáneas creadas en respuesta a anomalías. Por ejemplo, `Anti_ransomware_attack_backup.2025-08-25_1248` .
- `Anti_ransomware_backup` : Se utiliza en ONTAP 9.16.1 y versiones anteriores con instantáneas

creadas en respuesta a anomalías. Por ejemplo, `Anti_ransomware_backup.2022-12-20_1248` .

Para restaurar desde una instantánea distinta a la `Anti_ransomware` Instantánea después de identificar un ataque al sistema, primero debe publicar la instantánea ARP.

Si no se informa de ningún ataque al sistema, primero debe restaurar desde el `Anti_ransomware` instantánea y luego complete una restauración posterior del volumen a partir de la instantánea que elija.

> Si el volumen protegido por ARP forma parte de una relación SnapMirror , deberá actualizar manualmente todas las copias reflejadas del volumen después de restaurarlo desde una instantánea. Si omite este paso, las copias reflejadas podrían quedar inutilizables y será necesario eliminarlas y volver a crearlas.

Antes de empezar

"Debes marcar el ataque como un posible ataque de ransomware" antes de restaurar datos desde una instantánea.

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 instantánea 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 «posible ataque de ransomware».
   d. Seleccione **Actualizar** y **Borrar tipos de archivos sospechosos**.
2. Mostrar las instantáneas en los volúmenes:

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

Restaurar si no se identificó un ataque del sistema

1. Mostrar las instantáneas en los volúmenes:

   Selecciona **Almacenamiento > Volúmenes** y, a continuación, selecciona el volumen y **Copias instantáneas**.
2. Seleccionar ⋮ Luego elige el `Anti_ransomware` instantánea.
3. Seleccione **Restaurar**.
4. Vuelva al menú **Copias de instantánea** y, a continuación, elija la instantánea que desea utilizar. Seleccione **Restaurar**.

CLI

Restaurar después de un ataque al sistema

Para restaurar desde la instantánea ARP, vaya al paso dos. Para restaurar datos de instantáneas anteriores, debe liberar el bloqueo en la instantánea ARP.

> ⓘ Solo es necesario liberar el SnapLock anti-ransomware antes de restaurar desde snapshots anteriores si utiliza `volume snapshot restore` el comando como se describe a continuación. Si va a restaurar datos utilizando FlexClone, SnapRestore de archivo único u otros métodos, esto no es necesario.

1. Marcar el ataque como un posible ataque de ransomware (`-false-positive false`) y borrar archivos sospechosos (`clear-suspect`):

   ```
   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, … `*`]` : Extensiones de archivo

- `[-start-time date_time -end-time date_time]` :Horas de inicio y finalización para el rango de archivos que se borrarán, en el formato "MM/DD/AAAA HH:MM:SS".

2. Enumere las snapshots en un volumen:

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

El siguiente ejemplo muestra la 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 a partir de una copia de Snapshot:

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

El siguiente ejemplo 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 snapshots en un volumen:

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

El siguiente ejemplo muestra la 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 a partir de una copia de Snapshot:

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

El siguiente ejemplo restaura el contenido de `vol1` :

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

Obtenga más información sobre `volume snapshot` en el "Referencia de comandos del ONTAP".

Información relacionada

- "Base de conocimientos de NetApp : Prevención y recuperación de ransomware en ONTAP"
- "Referencia de comandos del ONTAP"

Ajustar la configuración para las instantáneas ARP generadas automáticamente

A partir de ONTAP 9.11,1, puede usar la interfaz de línea de comandos para controlar la configuración de retención de las copias Snapshot de protección autónoma frente a ransomware (ARP) que se generan automáticamente en respuesta a ataques sospechosos de ransomware.

Antes de empezar

Solo puedes modificar las opciones de instantáneas ARP en un "nodo SVM" y no en otros tipos de SVM.

Pasos

1. Mostrar todos los valores actuales de la instantánea ARP:

```
options -option-name arw*
```

2. Mostrar la configuración actual de la instantánea ARP seleccionada:

```
options -option-name <arw_setting_name>
```

3. Modificar la configuración de la instantánea ARP:

```
options -option-name <arw_setting_name> -option-value
<arw_setting_value>
```

Puedes modificar los siguientes ajustes:

> Algunos de los comandos descritos están obsoletos a partir de ONTAP 9.17.1. Los comandos introducidos en ONTAP 9.17.1 son compatibles con entornos NAS y SAN.

Ajuste	Descripción	Versiones compatibles
`arw.snap.max.count`	Especifica el número máximo de instantáneas ARP que pueden existir en un volumen en un momento dado. Las copias antiguas se eliminan para garantizar que el número total de instantáneas ARP se mantenga dentro del límite especificado.	ONTAP 9.11.1 y versiones posteriores
`arw.snap.create.interval.hours`	Especifica el intervalo en horas entre instantáneas de ARP. Se crea una nueva instantánea de ARP cuando se sospecha un ataque basado en la entropía de datos y la instantánea de ARP creada más recientemente es anterior al intervalo especificado.	ONTAP 9.11.1 y versiones posteriores
`arw.snap.normal.retain.interval.hours`	Especifica la duración, en horas, de la conservación de una instantánea de ARP. Cuando una instantánea de ARP alcanza el umbral de conservación, se elimina.	• ONTAP 9.11.1 a ONTAP 9.16.1 • Obsoleto en ONTAP 9.17.1 y versiones posteriores

Ajuste	Descripción	Versiones compatibles
`arw.snap.max.retain.interval.days`	Especifica la duración máxima *en días* para la que se puede conservar una instantánea ARP. Cualquier instantánea de ARP anterior a esta duración se elimina cuando no se notifica ningún ataque en el volumen. El intervalo de retención máximo para las instantáneas ARP se ignora si se detecta una amenaza moderada. La instantánea de ARP creada en respuesta a la amenaza se retiene hasta que haya respondido a la amenaza. Cuando se marca una amenaza como falso positivo, ONTAP eliminará las instantáneas ARP del volumen.	• ONTAP 9.11.1 a ONTAP 9.16.1 • Obsoleto en ONTAP 9.17.1 y versiones posteriores
`arw.snap.create.interval.hours.post.max.count`	Especifica el intervalo *en horas* entre instantáneas ARP cuando el volumen ya contiene el número máximo de instantáneas ARP. Al alcanzar el número máximo, se elimina una instantánea ARP para dejar espacio para una nueva copia. Con esta opción, se puede reducir la velocidad de creación de la nueva instantánea ARP para conservar la copia anterior. Si el volumen ya contiene el número máximo de instantáneas ARP, se utiliza el intervalo especificado en esta opción para la siguiente creación de la instantánea ARP, en lugar de... `arw.snap.create.interval.hours` .	• ONTAP 9.11.1 a 9.16.1 • Obsoleto en ONTAP 9.17.1 y versiones posteriores
`arw.snap.low.encryption.retain.duration.hours`	Especifica la duración de retención *en horas* para las instantáneas de ARP creadas durante períodos de baja actividad de cifrado.	• ONTAP 9.17.1 y posteriores
`arw.snap.new.extns.interval.hours`	Especifica el intervalo *en horas* entre las instantáneas ARP creadas al detectar una nueva extensión de archivo. Se crea una nueva instantánea ARP al detectar una nueva extensión de archivo; la instantánea anterior creada al detectar una nueva extensión de archivo es anterior a este intervalo especificado. En una carga de trabajo que crea nuevas extensiones de archivo con frecuencia, este intervalo ayuda a controlar la frecuencia de las instantáneas ARP. Esta opción existe independientemente de `arw.snap.create.interval.hours` , que especifica el intervalo para las instantáneas ARP basadas en la entropía de datos.	• ONTAP 9.11.1 a ONTAP 9.16.1 • Obsoleto en ONTAP 9.17.1 y versiones posteriores

Ajuste	Descripción	Versiones compatibles
`arw.snap.retain.hours.after.clear.suspect.false.alert`	Especifica el intervalo *en horas* en que se conserva una instantánea de ARP como medida de precaución después de que el administrador marque un incidente de ataque como falso positivo. Una vez transcurrido este periodo de retención preventiva, la instantánea puede eliminarse según la duración de retención estándar definida en las opciones. `arw.snap.normal.retain.interval.hours` y `arw.snap.max.retain.interval.days` .	• ONTAP 9.16.1 y versiones posteriores
`arw.snap.retain.hours.after.clear.suspect.real.attack`	Especifica el intervalo *en horas* en que se conserva una instantánea de ARP como medida de precaución después de que el administrador marque un incidente de ataque como un ataque real. Una vez transcurrido este periodo de retención preventiva, la instantánea puede eliminarse según la duración de retención estándar definida en las opciones. `arw.snap.normal.retain.interval.hours` y `arw.snap.max.retain.interval.days` .	• ONTAP 9.16.1 y versiones posteriores
`arw.snap.surge.interval.days`	Especifica el intervalo *in days* entre las instantáneas ARP creadas en respuesta a los picos de E/S. ONTAP crea una copia de exceso de snapshots de ARP cuando hay un aumento en el tráfico de E/S y la última instantánea de ARP creada es más antigua que este intervalo especificado. Esta opción también especifica el período de retención *in day* para una instantánea de sobrecarga ARP.	ONTAP 9.11.1 y versiones posteriores
`arw.high.encryption.alert.enabled`	Habilita alertas para niveles altos de cifrado. Cuando esta opción está configurada en `on` (predeterminado), ONTAP envía una alerta cuando el porcentaje de cifrado excede el umbral especificado en `arw.high.encryption.percentage.threshold` .	ONTAP 9.17.1 y posteriores
`arw.high.encryption.percentage.threshold`	Especifica el porcentaje máximo de cifrado para un volumen. Si el porcentaje de cifrado supera este umbral, ONTAP considera el aumento como un ataque y crea una instantánea ARP. `arw.high.encryption.alert.enabled` debe configurarse en `on` para que esta opción tenga efecto.	ONTAP 9.17.1 y posteriores
`arw.snap.high.encryption.retain.duration.hours`	Especifica el intervalo de duración de retención *en horas* para las instantáneas creadas durante un evento de umbral de cifrado alto.	ONTAP 9.17.1 y posteriores

4. Si utiliza ARP con un entorno SAN, también puede modificar las siguientes configuraciones del período de evaluación:

Ajuste	Descripción	Versiones compatibles
`arw.block_device.auto.learn.threshold.min_value`	Especifica el valor porcentual del umbral de cifrado mínimo durante la fase de aprendizaje automático de la evaluación para dispositivos de bloque.	ONTAP 9.17.1 y posteriores
`arw.block_device.auto.learn.threshold.max_value`	Especifica el valor porcentual del umbral de cifrado máximo durante la fase de aprendizaje automático de la evaluación para dispositivos de bloque.	ONTAP 9.17.1 y posteriores
`arw.block_device.evaluation.phase.min_hours`	Especifica el intervalo mínimo *en horas* que debe ejecutarse la fase de evaluación antes de que se establezca el umbral de cifrado.	ONTAP 9.17.1 y posteriores
`arw.block_device.evaluation.phase.max_hours`	Especifica el intervalo máximo *en horas* que debe ejecutarse la fase de evaluación antes de que se establezca el umbral de cifrado.	ONTAP 9.17.1 y posteriores
`arw.block_device.evaluation.phase.min_data_ingest_size_GB`	Especifica la cantidad mínima de datos *en GB* que se deben ingerir durante la fase de evaluación antes de que se establezca el umbral de cifrado.	ONTAP 9.17.1 y posteriores
`arw.block_device.evaluation.phase.alert.enabled`	Especifica si se habilitan las alertas para la fase de evaluación de ARP en dispositivos de bloque. El valor predeterminado es `True`.	ONTAP 9.17.1 y posteriores
`arw.block_device.evaluation.phase.alert.threshold`	Especifica el porcentaje de umbral durante la fase de evaluación de ARP en dispositivos de bloque. Si el porcentaje de cifrado supera este umbral, se activa una alerta.	ONTAP 9.17.1 y posteriores

Información relacionada

- "Evaluación de amenazas e instantáneas ARP"
- "Período de evaluación de la entropía de SAN"

Actualizar la protección autónoma frente a ransomware de ONTAP con IA (ARP/AI)

Para mantener la protección actualizada frente a las últimas amenazas de ransomware, ARP/AI ofrece actualizaciones automáticas que se producen fuera de las cadencias habituales de las versiones de ONTAP.

A partir de ONTAP 9.16.1, las actualizaciones de seguridad para ARP/AI están disponibles en las descargas del software System Manager, además de las actualizaciones del sistema y del firmware. Si su clúster de ONTAP ya está registrado en "actualizaciones automáticas del sistema y firmware" Recibirá una notificación automática cuando haya actualizaciones de seguridad de ARP/AI disponibles. También puede cambiar sus preferencias de actualización para que ONTAP instale actualizaciones de seguridad automáticamente.

Si Actualice manualmente ARP/AIdesea , puede descargar actualizaciones del sitio de soporte de NetApp e instalarlas mediante System Manager.

Acerca de esta tarea

Solo puedes actualizar ARP/AI mediante el Administrador del sistema.

Seleccione una preferencia de actualización para ARP/AI

En el Administrador del sistema, la configuración en la página Habilitar actualizaciones automáticas para archivos de seguridad está establecida en `Show notifications` Si ya está inscrito en las actualizaciones automáticas de firmware y del sistema, puede cambiar la configuración de actualización a `Automatically update` Si prefiere que ONTAP aplique las últimas actualizaciones automáticamente. Si usa un sitio oscuro o prefiere realizar las actualizaciones manualmente, puede mostrar notificaciones o descartar automáticamente las actualizaciones de seguridad.

Antes de empezar

Para actualizaciones de seguridad automáticas, "AutoSupport y AutoSupport OnDemand deben estar habilitados y el protocolo de transporte se debe establecer con HTTPS".

Pasos

1. En System Manager, haga clic en **Clúster > Configuración > Actualizaciones de software**.
2. En la sección **Actualizaciones de software**, seleccione →.
3. En la página **Actualizaciones de software**, selecciona la pestaña **Todas las demás actualizaciones**.
4. Seleccione la pestaña **Todas las demás actualizaciones** y haga clic en **Más**.
5. Selecciona **Editar ajustes de actualización automática**.
6. En la página Configuración de actualización automática, selecciona **Archivos de seguridad**.
7. Especifique la acción que se debe realizar para los archivos de seguridad (actualizaciones ARP/AI).

   Puede elegir actualizar automáticamente, mostrar notificaciones o descartar actualizaciones automáticamente.

   > ⓘ Para que las actualizaciones de seguridad se actualicen automáticamente, AutoSupport y AutoSupport OnDemand deben estar habilitados y el protocolo de transporte se debe establecer en HTTPS.

8. Acepte los términos y condiciones y seleccione **Guardar**.

Actualice manualmente ARP/AI con el paquete de seguridad más reciente

Siga el procedimiento adecuado en función de si está registrado en Active IQ Unified Manager.

> ⓘ Asegúrese de instalar solo una actualización ARP más reciente que la versión actual para evitar cualquier degradación ARP no intencionada.

ONTAP 9.16,1 y versiones posteriores con asesor digital

1. En System Manager, vaya a **Dashboard**.

   En la sección **Salud**, se muestra un mensaje si hay alguna actualización de seguridad recomendada para el clúster.

2. Haga clic en el mensaje de alerta.
3. Junto a las actualizaciones de seguridad en la lista de actualizaciones recomendadas, selecciona **Acciones**.
4. Haga clic en **Actualizar** para instalar la actualización inmediatamente o en **Programar** para programarla para más tarde.

   Si la actualización ya está programada, puedes **Editar** o **Cancelar**.

ONTAP 9.16,1 y posterior sin Asesor Digital

1. Vaya a "Sitio de soporte de NetApp"e inicie sesión.
2. Complete las solicitudes y descargue el paquete de seguridad que desee utilizar para actualizar su ARP/AI de clúster.
3. Copie los archivos en un servidor HTTP o FTP de su red o en una carpeta local a la que pueda acceder el clúster con ARP/AI.
4. En System Manager, haga clic en **Clúster > Configuración > Actualizaciones de software**.
5. En **Actualizaciones de software**, selecciona la pestaña **Todas las demás actualizaciones**.
6. En el panel **Actualizaciones manuales**, haz clic en **Agregar archivos de seguridad** y agrega los archivos usando una de estas preferencias:
   - **Descargar desde el servidor**: Introduzca la URL del paquete de archivos de seguridad.
   - **Subir desde el cliente local**: Navega hasta el archivo TGZ descargado.

   > Asegúrese de que el nombre del archivo comience por `ontap_security_file_arpai_` y tenga `.tgz` como extensión de archivo.

7. Haga clic en **Agregar** para aplicar las actualizaciones.

Verifique las actualizaciones ARP/AI

Para ver un historial de actualizaciones automáticas que se han descartado o no se han podido instalar, haga lo siguiente:

1. En System Manager, haga clic en **Clúster > Configuración > Actualizaciones de software**.
2. En la sección **Actualizaciones de software**, seleccione →.
3. En la página **Actualizaciones de software**, selecciona la pestaña **Todas las demás actualizaciones** y haz clic en **Más**.
4. Selecciona **Ver todas las actualizaciones automáticas**.

Información relacionada

- "Aprende sobre ARP/IA"
- "Suscripciones de correo electrónico para actualizaciones de software"