



Seguridad y cifrado de datos

Cloud Volumes ONTAP

NetApp

February 21, 2023

This PDF was generated from <https://docs.netapp.com/es-es/cloud-manager-cloud-volumes-ontap/gcp/task-encrypting-volumes.html> on February 21, 2023. Always check docs.netapp.com for the latest.

Tabla de Contenido

- Seguridad y cifrado de datos 1
 - Cifrar volúmenes con soluciones de cifrado de NetApp 1
 - Gestione las claves con el Servicio de administración de claves en la nube de Google..... 1
 - Mejorar la protección contra el ransomware 3

Seguridad y cifrado de datos

Cifrar volúmenes con soluciones de cifrado de NetApp

Cloud Volumes ONTAP admite el cifrado de volúmenes de NetApp (NVE) y el cifrado de agregados de NetApp (NAE). NVE y NAE son soluciones basadas en software que permiten el cifrado de volúmenes para datos en reposo conforme a la normativa FIPS 140-2. ["Obtenga más información sobre estas soluciones de cifrado"](#).

Tanto NVE como NAE son compatibles con un gestor de claves externo.

Los nuevos agregados tendrán NAE habilitado de forma predeterminada después de configurar un gestor de claves externo. Los volúmenes nuevos que no forman parte de un agregado de NAE tendrán el valor de NVE habilitado de forma predeterminada (por ejemplo, si tiene agregados existentes que se crearon antes de configurar un gestor de claves externo).

Cloud Volumes ONTAP no admite la gestión de claves incorporada.

Lo que necesitará

Su sistema Cloud Volumes ONTAP debe registrarse con el soporte de NetApp. Una licencia de cifrado de volúmenes de NetApp se instala automáticamente en cada sistema Cloud Volumes ONTAP registrado en el soporte de NetApp.

- ["Adición de cuentas del sitio de soporte de NetApp a BlueXP"](#)
- ["Registro de sistemas de pago por uso"](#)



BlueXP no instala la licencia NVE en sistemas que residen en la región China.

Pasos

1. Revise la lista de administradores de claves compatibles en la ["Herramienta de matriz de interoperabilidad de NetApp"](#).



Busque la solución **Key Managers**.

2. ["Conéctese a la CLI de Cloud Volumes ONTAP"](#).
3. Configure la gestión de claves externas.
 - Google Cloud: ["Servicio de gestión de claves de Google Cloud"](#)

Gestione las claves con el Servicio de administración de claves en la nube de Google

Puede utilizar ["Servicio de gestión de claves de Google Cloud Platform \(Cloud KMS\)"](#) Para proteger sus claves de cifrado de ONTAP en una aplicación puesta en marcha de Google Cloud Platform.

La gestión de claves con Cloud KMS se puede habilitar con la CLI o la API DE REST de ONTAP.

Cuando utilice Cloud KMS, tenga en cuenta que, de forma predeterminada, se utiliza una LIF de SVM de datos para comunicarse con el extremo de gestión de claves de cloud. Una red de gestión de nodos se usa

para comunicarse con los servicios de autenticación del proveedor de cloud (oauth2.googleapis.com). Si la red de clúster no está configurada correctamente, el clúster no utilizará correctamente el servicio de gestión de claves.

Requisitos previos

- Cloud Volumes ONTAP debe ejecutar la versión 9.10.1 de o posterior
- Licencia de Volume Encryption (ve) instalada
- Debe ser un administrador de clústeres o SVM
- Una suscripción activa a Google Cloud Platform

Limitaciones

- Cloud KMS solo puede configurarse en una SVM de datos

Configuración

Google Cloud

1. En su entorno de Google Cloud, "[Cree una clave y un anillo de clave de GCP simétrico](#)".
2. Cree una función personalizada para su cuenta de servicio de Cloud Volumes ONTAP.

```
gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

  --permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

3. Asigne el rol personalizado a la clave de Cloud KMS y a la cuenta de servicio de Cloud Volumes ONTAP:

```
gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
--location key_location --member serviceAccount:_service_account_Name_ --role
projects/customer_project_id/roles/kmsCustomRole
```

4. Descargue la clave JSON de la cuenta de servicio:

```
gcloud iam service-accounts keys create key-file --iam-account=sa-name
@project-id.iam.gserviceaccount.com
```

Cloud Volumes ONTAP

1. Conéctese a la LIF de gestión de clústeres con el cliente SSH preferido.
2. Cambie al nivel de privilegio avanzado:
`set -privilege advanced`
3. Cree un DNS para la SVM de datos.
`dns create -domains c.<project>.internal -name-servers server_address -vserver SVM_name`

4. Crear entrada CMEK:

```
security key-manager external gcp enable -vserver SVM_name -project-id project  
-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name  
key_name
```

5. Cuando se le solicite, introduzca la clave JSON de la cuenta de servicio desde su cuenta de GCP.

6. Confirme que el proceso activado se ha realizado correctamente:

```
security key-manager external gcp check -vserver svm_name
```

7. OPCIONAL: Cree un volumen para probar el cifrado `vol create volume_name -aggregate aggregate -vserver vservice_name -size 10G`

Solucionar problemas

Si necesita solucionar problemas, puede cola los registros de la API DE REST sin configurar en los dos últimos pasos que se indican a continuación:

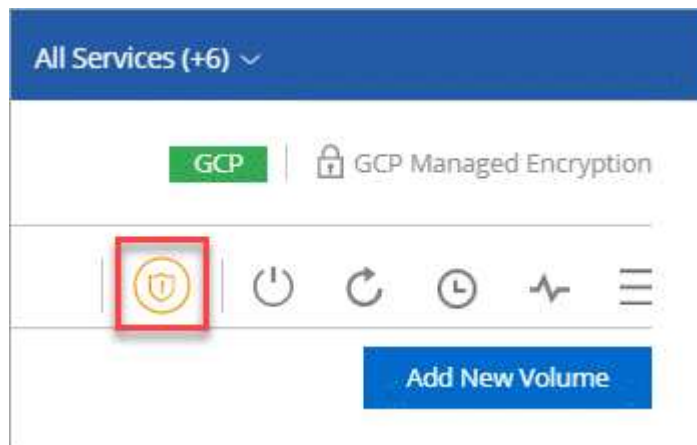
1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Mejorar la protección contra el ransomware

Los ataques de ransomware pueden suponer un coste comercial, recursos y reputación. BlueXP le permite implementar la solución de NetApp para el ransomware, que proporciona herramientas eficaces para la visibilidad, la detección y la corrección.

Pasos

1. En el entorno de trabajo, haga clic en el icono **Ransomware**.



2. Implemente la solución de NetApp para ransomware:

- a. Haga clic en **Activar política de instantánea** si tiene volúmenes que no tienen activada una directiva de instantánea.

La tecnología Snapshot de NetApp proporciona la mejor solución del sector para la reparación de ransomware. La clave para una recuperación correcta es restaurar a partir de backups no infectados. Las copias Snapshot son de solo lectura, lo que evita que se dañen el ransomware. También pueden proporcionar granularidad para crear imágenes de una sola copia de archivos o una solución completa

de recuperación tras desastres.

- b. Haga clic en **Activar FPolicy** para habilitar la solución FPolicy de ONTAP, que puede bloquear las operaciones de archivos según la extensión de un archivo.

Esta solución preventiva mejora la protección contra ataques de ransomware bloqueando tipos de archivos comunes de ransomware.

El alcance predeterminado de FPolicy bloquea los archivos que tienen las siguientes extensiones:

micro, cifrado, bloqueado, cifrado, cifrado, Crinf, r5a, XRNT, XTBL, R16M01D05, Pzdc, bueno, LOL!, OMG!, RDM, RK, encryptedRS, crjoker, encephed, LeChiffre



BlueXP crea este alcance al activar FPolicy en Cloud Volumes ONTAP. La lista se basa en tipos de archivos comunes de ransomware. Puede personalizar las extensiones de archivos bloqueados mediante los comandos `vserver fpolicy Scope` de la CLI de Cloud Volumes ONTAP.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection ⓘ

50 %
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes ⓘ

Activate Snapshot Policy

2 Block Ransomware File Extensions ⓘ

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names ⓘ](#)

Activate FPolicy

Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.