



Seguridad y cifrado de datos

Cloud Volumes ONTAP

NetApp

February 13, 2026

Tabla de contenidos

- Seguridad y cifrado de datos 1
 - Cifre volúmenes en Cloud Volumes ONTAP con soluciones de cifrado de NetApp 1
 - Administre las claves de cifrado de Cloud Volumes ONTAP con AWS Key Management Service 1
 - Configuración 1
 - Administrar claves de cifrado de Cloud Volumes ONTAP con Azure Key Vault 2
 - Proceso de configuración 3
 - Administrar claves de cifrado de Cloud Volumes ONTAP con Google Cloud KMS 10
 - Configuración 11
 - Solución de problemas 12
 - Habilite las soluciones de protección contra ransomware de NetApp para Cloud Volumes ONTAP 12
 - Protección contra extensiones de archivos de ransomware comunes 12
 - Protección autónoma contra ransomware 14
 - Cree copias instantáneas a prueba de manipulaciones de archivos WORM en Cloud Volumes ONTAP. . . 15

Seguridad y cifrado de datos

Cifre volúmenes en Cloud Volumes ONTAP con soluciones de cifrado de NetApp

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

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

```
] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[] ifdef::aws[] endif::aws[] ifdef::azure[]  
endif::azure[] ifdef::gcp[] endif::gcp[]
```

Administre las claves de cifrado de Cloud Volumes ONTAP con AWS Key Management Service

Puedes utilizar ["Servicio de administración de claves \(KMS\) de AWS"](#) para proteger sus claves de cifrado ONTAP en una aplicación implementada por AWS.

La administración de claves con AWS KMS se puede habilitar con la CLI o la API REST de ONTAP .

Al utilizar el KMS, tenga en cuenta que, de forma predeterminada, se utiliza el LIF de una SVM de datos para comunicarse con el punto final de administración de claves en la nube. Se utiliza una red de administración de nodos para comunicarse con los servicios de autenticación de AWS. Si la red del clúster no está configurada correctamente, el clúster no utilizará adecuadamente el servicio de administración de claves.

Antes de empezar

- Cloud Volumes ONTAP debe ejecutar la versión 9.12.0 o posterior
- Debe tener instalada la licencia de Volume Encryption (VE) y
- Debe tener instalada la licencia de Administración de claves de cifrado de múltiples inquilinos (MTEKM).
- Debe ser un administrador de clúster o SVM
- Debe tener una suscripción activa a AWS



Sólo se pueden configurar claves para un SVM de datos.

Configuración

AWS

1. Debes crear un ["conceder"](#) para la clave AWS KMS que utilizará la función IAM que administra el cifrado. El rol de IAM debe incluir una política que permita las siguientes operaciones:
 - DescribeKey
 - Encrypt
 - Decrypt Para crear una subvención, consulte ["Documentación de AWS"](#) .

2. "Agregue una política al rol de IAM apropiado." La política debe apoyar la `DescribeKey`, `Encrypt`, y `Decrypt` operaciones.

Cloud Volumes ONTAP

1. Cambie a su entorno de Cloud Volumes ONTAP .
2. Cambiar al nivel de privilegio avanzado:
`set -privilege advanced`
3. Habilite el administrador de claves de AWS:
`security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. Cuando se le solicite, ingrese la clave secreta.
5. Confirme que AWS KMS se configuró correctamente:
`security key-manager external aws show -vserver svm_name`

Administrar claves de cifrado de Cloud Volumes ONTAP con Azure Key Vault

Puede usar Azure Key Vault (AKV) para proteger sus claves de cifrado de ONTAP en una aplicación implementada en Azure. Consulte la ["Documentación de Microsoft"](#) .

AKV se puede utilizar para proteger claves de NetApp Volume Encryption (NVE) solo para SVM de datos. Para obtener más información, consulte la ["Documentación de ONTAP"](#) .

La administración de claves con AKV se puede habilitar con la CLI o la API REST de ONTAP .

Al utilizar AKV, tenga en cuenta que, de forma predeterminada, se utiliza un LIF SVM de datos para comunicarse con el punto final de administración de claves en la nube. Se utiliza una red de administración de nodos para comunicarse con los servicios de autenticación del proveedor de la nube (`login.microsoftonline.com`). Si la red del clúster no está configurada correctamente, el clúster no utilizará adecuadamente el servicio de administración de claves.

Antes de empezar

- Cloud Volumes ONTAP debe ejecutar la versión 9.10.1 o posterior
- Licencia de Volume Encryption (VE) instalada (la licencia de Volume Encryption de NetApp se instala automáticamente en cada sistema Cloud Volumes ONTAP registrado en el soporte de NetApp)
- Debe tener una licencia de administración de claves de cifrado multiinquilino (`MT_EK_MGMT`)
- Debe ser un administrador de clúster o SVM
- Una suscripción activa de Azure

Limitaciones

- AKV solo se puede configurar en un SVM de datos
- NAE no se puede utilizar con AKV. NAE requiere un servidor KMIP con soporte externo.
- Los nodos de Cloud Volumes ONTAP sondean AKV cada 15 minutos para confirmar la accesibilidad y la disponibilidad de la clave. Este período de sondeo no es configurable y, después de cuatro fallas consecutivas en el intento de sondeo (que suman un total de 1 hora), los volúmenes se colocan fuera de línea.

Proceso de configuración

Los pasos descritos capturan cómo registrar su configuración de Cloud Volumes ONTAP con Azure y cómo crear un Azure Key Vault y claves. Si ya ha completado estos pasos, asegúrese de tener la configuración correcta, especialmente en [Crear un almacén de claves de Azure](#) , y luego proceder a [Configuración de Cloud Volumes ONTAP](#) .

- [Registro de aplicaciones de Azure](#)
- [Crear un secreto de cliente de Azure](#)
- [Crear un almacén de claves de Azure](#)
- [Crear una clave de cifrado](#)
- [Crear un punto de conexión de Azure Active Directory \(solo HA\)](#)
- [Configuración de Cloud Volumes ONTAP](#)

Registro de aplicaciones de Azure

1. Primero debe registrar su aplicación en la suscripción de Azure que desea que Cloud Volumes ONTAP use para acceder a Azure Key Vault. Dentro del portal de Azure, seleccione **Registros de aplicaciones**.
2. Seleccione **Nuevo registro**.
3. Proporcione un nombre para su aplicación y seleccione un tipo de aplicación compatible. El inquilino único predeterminado es suficiente para el uso de Azure Key Vault. Seleccione **Registrarse**.
4. En la ventana Descripción general de Azure, seleccione la aplicación que ha registrado. Copie el **ID de la aplicación (cliente)** y el **ID del directorio (inquilino)** en una ubicación segura. Serán necesarios más adelante en el proceso de registro.

Crear un secreto de cliente de Azure

1. En el portal de Azure para el registro de su aplicación Azure Key Vault, seleccione el panel **Certificados y secretos**.
2. Seleccione **Nuevo secreto de cliente**. Ingrese un nombre significativo para su secreto de cliente. NetApp recomienda un período de vencimiento de 24 meses; sin embargo, sus políticas de gobernanza de la nube específicas pueden requerir una configuración diferente.
3. Haga clic en **Agregar** para crear el secreto del cliente. Copie la cadena secreta que aparece en la columna **Valor** y guárdela en una ubicación segura para usarla más adelante. [Configuración de Cloud Volumes ONTAP](#) . El valor secreto no se mostrará nuevamente después de que salga de la página.

Crear un almacén de claves de Azure

1. Si tiene un Azure Key Vault existente, puede conectarlo a su configuración de Cloud Volumes ONTAP ; sin embargo, debe adaptar las políticas de acceso a la configuración en este proceso.
2. En el portal de Azure, navegue hasta la sección **Key Vaults**.
3. Haga clic en **+Crear** e ingrese la información requerida, incluido el grupo de recursos, la región y el nivel de precios. Además, ingrese la cantidad de días que desea conservar las bóvedas eliminadas y seleccione **Habilitar protección de purga** en la bóveda de claves.
4. Seleccione **Siguiente** para elegir una política de acceso.
5. Seleccione las siguientes opciones:
 - a. En **Configuración de acceso**, seleccione la **Política de acceso a la bóveda**.
 - b. En **Acceso a recursos**, seleccione **Azure Disk Encryption para cifrado de volumen**.
6. Seleccione **+Crear** para agregar una política de acceso.

7. En **Configurar desde una plantilla**, haga clic en el menú desplegable y luego seleccione la plantilla **Administración de claves, secretos y certificados**.
8. Elija cada uno de los menús desplegables de permisos (clave, secreto, certificado) y luego **Seleccionar todo** en la parte superior de la lista del menú para seleccionar todos los permisos disponibles. Deberías tener:
 - **Permisos clave:** 20 seleccionados
 - **Permisos secretos:** 8 seleccionados
 - **Permisos de certificado:** 16 seleccionados

Create an access policy



- 1 Permissions 2 Principal 3 Application (optional) 4 Review + create

Configure from a template

Key, Secret, & Certificate Management

Key permissions

Key Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Update
- ☒ Create
- ☒ Import
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore

Cryptographic Operations

- ☒ Select all
- ☒ Decrypt
- ☒ Encrypt
- ☒ Unwrap Key
- ☒ Wrap Key
- ☒ Verify
- ☒ Sign

Privileged Key Operations

- ☒ Select all
- ☒ Purge
- ☒ Release

Rotation Policy Operations

- ☒ Select all
- ☒ Rotate
- ☒ Get Rotation Policy
- ☒ Set Rotation Policy

Secret permissions

Secret Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Set
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore

Privileged Secret Operations

- ☒ Select all
- ☒ Purge

Certificate permissions

Certificate Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Update
- ☒ Create
- ☒ Import
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore
- ☒ Manage Contacts
- ☒ Manage Certificate Authorities
- ☒ Get Certificate Authorities
- ☒ List Certificate Authorities
- ☒ Set Certificate Authorities
- ☒ Delete Certificate Authorities

Privileged Certificate Operations

- ☒ Select all
- ☒ Purge

Previous

Next

9. Haga clic en **Siguiente** para seleccionar la **Aplicación principal** registrada en Azure que creó en [Registro de aplicaciones de Azure](#) . Seleccione **Siguiente**.



Sólo se puede asignar un director por póliza.

Select a principal'. Below this is a search bar with the placeholder text 'Search by object ID, name, or email address'. Underneath the search bar is a section titled 'Selected item' which currently says 'No item selected'. At the bottom are two buttons: 'Previous' and 'Next'."/>

10. Haga clic en **Siguiente** dos veces hasta llegar a **Revisar y crear**. Luego, haga clic en **Crear**.
11. Seleccione **Siguiente** para avanzar a las opciones de **Redes**.
12. Elija el método de acceso a la red adecuado o seleccione **Todas las redes** y **Revisar + Crear** para crear la bóveda de claves. (El método de acceso a la red puede estar prescrito por una política de gobernanza o por su equipo de seguridad en la nube corporativa).
13. Registre la URI de la bóveda de claves: en la bóveda de claves que creó, navegue hasta el menú Descripción general y copie la **URI de la bóveda** de la columna de la derecha. Necesitarás esto para un paso posterior.

Crear una clave de cifrado

1. En el menú del Key Vault que ha creado para Cloud Volumes ONTAP, navegue hasta la opción **Claves**.
2. Seleccione **Generar/importar** para crear una nueva clave.
3. Deje la opción predeterminada establecida en **Generar**.
4. Proporcione la siguiente información:

- Nombre de la clave de cifrado
- Tipo de clave: RSA
- Tamaño de clave RSA: 2048
- Habilitado: Sí

5. Seleccione **Crear** para crear la clave de cifrado.
6. Regrese al menú **Teclas** y seleccione la clave que acaba de crear.
7. Seleccione el ID de la clave en **Versión actual** para ver las propiedades de la clave.
8. Localice el campo **Identificador de clave**. Copie la URI hasta la cadena hexadecimal, pero sin incluirla.

Crear un punto de conexión de Azure Active Directory (solo HA)

1. Este proceso solo es necesario si está configurando Azure Key Vault para un sistema HA Cloud Volumes ONTAP .
2. En el portal de Azure, navegue a **Redes virtuales**.
3. Seleccione la red virtual donde implementó el sistema Cloud Volumes ONTAP y seleccione el menú **Subredes** en el lado izquierdo de la página.
4. Seleccione el nombre de subred para su implementación de Cloud Volumes ONTAP de la lista.
5. Vaya al encabezado **Puntos finales de servicio**. En el menú desplegable, seleccione lo siguiente:
 - **Microsoft.AzureActiveDirectory**
 - **Microsoft.KeyVault**
 - **Microsoft.Storage** (opcional)

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

Save

Cancel

6. Seleccione **Guardar** para capturar su configuración.

Configuración de Cloud Volumes ONTAP

1. Conéctese al LIF de administración del clúster con su cliente SSH preferido.
2. Ingrese al modo de privilegios avanzados en ONTAP:

```
set advanced -con off
```

3. Identifique el SVM de datos deseado y verifique su configuración DNS:

```
vserver services name-service dns show
```

- a. Si existe una entrada DNS para el SVM de datos deseado y contiene una entrada para el DNS de Azure, no se requiere ninguna acción. Si no es así, agregue una entrada de servidor DNS para el SVM de datos que apunta al DNS de Azure, al DNS privado o al servidor local. Esto debería coincidir con la entrada para el SVM de administración del clúster:

```
vserver services name-service dns create -vserver SVM_name -domains domain  
-name-servers IP_address
```

- b. Verifique que se haya creado el servicio DNS para los datos SVM:

```
vserver services name-service dns show
```

4. Habilite Azure Key Vault usando el ID de cliente y el ID de inquilino guardados después del registro de la aplicación:

```
security key-manager external azure enable -vserver SVM_name -client-id  
Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id  
full_key_URI
```



El `full_key_URI` El valor debe utilizar el `<https:// <key vault host name>/keys/<key label>` formato.

5. Tras la habilitación exitosa de Azure Key Vault, ingrese el `client secret value` cuando se le solicite.

6. Compruebe el estado del administrador de claves:

`security key-manager external azure check` La salida se verá así:

```
::*> security key-manager external azure check
```

```
Vserver: data_svm_name
```

```
Node: akvlab01-01
```

```
Category: service_reachability
```

```
Status: OK
```

```
Category: ekvip_server
```

```
Status: OK
```

```
Category: kms_wrapped_key_status
```

```
Status: UNKNOWN
```

```
Details: No volumes created yet for the vserver. Wrapped KEK status  
will be available after creating encrypted volumes.
```

```
3 entries were displayed.
```

Si el `service_reachability` el estado no es OK, la SVM no puede acceder al servicio Azure Key Vault con toda la conectividad y los permisos necesarios. Asegúrese de que las políticas y el enrutamiento de la red de Azure no impidan que su red virtual privada llegue al punto de conexión público de Azure Key Vault. Si es así, considere usar un punto de conexión privado de Azure para acceder al almacén de claves desde

dentro de la red virtual. Es posible que también necesite agregar una entrada de hosts estáticos en su SVM para resolver la dirección IP privada de su punto final.

El `kms_wrapped_key_status` informará UNKNOWN en la configuración inicial. Su estatus cambiará a OK después de cifrar el primer volumen.

7. OPCIONAL: Cree un volumen de prueba para verificar la funcionalidad de NVE.

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size  
-state online -policy default
```

Si se configura correctamente, Cloud Volumes ONTAP creará automáticamente el volumen y habilitará el cifrado del volumen.

8. Confirme que el volumen se creó y se cifró correctamente. Si es así, el `-is-encrypted` El parámetro se mostrará como `true`.

```
vol show -vserver SVM_name -fields is-encrypted
```

9. Opcional: si desea actualizar las credenciales en el certificado de autenticación de Azure Key Vault, use el siguiente comando:

```
security key-manager external azure update-credentials -vserver v1  
-authentication-method certificate
```

Enlaces relacionados

- ["Configurar Cloud Volumes ONTAP para usar una clave administrada por el cliente en Azure"](#)
- ["Documentación de Microsoft Azure: Acerca de Azure Key Vault"](#)
- ["Guía de referencia de comandos de ONTAP"](#)

Administrar claves de cifrado de Cloud Volumes ONTAP con Google Cloud KMS

Puedes utilizar ["Servicio de administración de claves de Google Cloud Platform \(Cloud KMS\)"](#) para proteger sus claves de cifrado de Cloud Volumes ONTAP en una aplicación implementada en Google Cloud Platform.

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

Al utilizar Cloud KMS, tenga en cuenta que, de forma predeterminada, se utiliza el LIF de una SVM de datos para comunicarse con el punto final de administración de claves en la nube. Se utiliza una red de administración de nodos para comunicarse con los servicios de autenticación del proveedor de la nube (`oauth2.googleapis.com`). Si la red del clúster no está configurada correctamente, el clúster no utilizará adecuadamente el servicio de administración de claves.

Antes de empezar

- Su sistema debe ejecutar Cloud Volumes ONTAP 9.10.1 o posterior
- Debe utilizar un SVM de datos. Cloud KMS solo se puede configurar en un SVM de datos.
- Debe ser un administrador de clúster o SVM
- La licencia de cifrado de volumen (VE) debe estar instalada en el SVM
- A partir de Cloud Volumes ONTAP 9.12.1 GA, también se debe instalar la licencia de administración de

claves de cifrado multiinquilino (MTEKM)

- Se requiere una suscripción activa a Google Cloud Platform

Configuración

Google Cloud

1. En su entorno de Google Cloud, "[crear un llavero y una clave GCP simétricos](#)".
2. Asigne una función personalizada a la clave Cloud KMS y a la cuenta de servicio Cloud Volumes ONTAP.
 - a. Crear el rol personalizado:

```
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.locations.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

- b. Asigna el rol personalizado que creaste:

```
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
```



Si utiliza Cloud Volumes ONTAP 9.13.0 o posterior, no necesita crear una función personalizada. Puede asignar los valores predefinidos[cloudkms.cryptoKeyEncrypterDecrypter ^] papel.

3. Descargar 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 al LIF de administración del clúster con su cliente SSH preferido.
2. Cambiar al nivel de privilegio avanzado:

```
set -privilege advanced
```
3. Cree un DNS para los datos SVM.

```
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, ingrese la clave JSON de la cuenta de servicio de su cuenta de GCP.
6. Confirme que el proceso habilitado se realizó 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 vserver_name -size 10G`

Solución de problemas

Si necesita solucionar problemas, puede seguir los registros de la API REST sin procesar en los dos últimos pasos anteriores:

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

Habilite las soluciones de protección contra ransomware de NetApp para Cloud Volumes ONTAP

Los ataques de ransomware pueden costarle a una empresa tiempo, recursos y reputación. La NetApp Console le permite implementar dos soluciones de NetApp contra ransomware: protección contra extensiones de archivos de ransomware comunes y protección autónoma contra ransomware (ARP). Estas soluciones proporcionan herramientas eficaces para la visibilidad, la detección y la remediación.

Protección contra extensiones de archivos de ransomware comunes

Disponible en la consola, la configuración de protección contra ransomware le permite utilizar la funcionalidad ONTAP FPolicy para protegerse contra los tipos de extensiones de archivos de ransomware más comunes.

Pasos

1. En la página **Sistemas**, haga doble clic en el nombre del sistema Cloud Volumes ONTAP que configure para usar protección contra ransomware.
2. En la pestaña Descripción general, haga clic en el panel Características y luego haga clic en el ícono de lápiz junto a **Protección contra ransomware**.

Information	Features
System Tags	3 Tags 
Scheduled Downtime	Off 
Blob Access Tiering	Hot 
Instance Type	Standard_E8ds_v4 
Charging Method	Capacity-based 
Write Speed	<i>Not Supported</i> 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

3. Implementar la solución NetApp para ransomware:

- Haga clic en **Activar política de instantáneas**, si tiene volúmenes que no tienen una política de instantáneas habilitada.

La tecnología Snapshot de NetApp proporciona la mejor solución de la industria para la remediación de ransomware. La clave para una recuperación exitosa es restaurar desde copias de seguridad no infectadas. Las copias instantáneas son de solo lectura, lo que evita la corrupción por ransomware. También pueden proporcionar la granularidad necesaria para crear imágenes de una única copia de archivo o una solución completa de recuperación ante desastres.

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

Esta solución preventiva mejora la protección contra ataques de ransomware al bloquear los tipos de archivos de ransomware más comunes.

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

micro, encriptado, bloqueado, cripto, crypt, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, bueno, ¡LOL!, ¡Dios mío!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre



Este alcance se crea cuando se activa FPolicy en Cloud Volumes ONTAP. La lista se basa en los tipos de archivos de ransomware más comunes. Puede personalizar las extensiones de archivos bloqueadas mediante los comandos `vserver fpolicy policy 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

Protección autónoma contra ransomware

Cloud Volumes ONTAP admite la función de protección autónoma contra ransomware (ARP), que realiza análisis en las cargas de trabajo para detectar y advertir de forma proactiva sobre actividades anormales que podrían indicar un ataque de ransomware.

Independientemente de las protecciones de extensión de archivo proporcionadas a través de "[configuración de protección contra ransomware](#)". La función ARP utiliza el análisis de la carga de trabajo para alertar al usuario sobre posibles ataques en función de la "actividad anormal" detectada. Tanto la configuración de protección contra ransomware como la función ARP se pueden utilizar en conjunto para lograr una protección integral contra ransomware.

La función ARP está disponible para su uso con su propia licencia (BYOL) y suscripciones de mercado para sus licencias sin costo adicional.

Los volúmenes habilitados para ARP tienen un estado designado de "Modo de aprendizaje" o "Activo".

La configuración de ARP para volúmenes se realiza a través de ONTAP System Manager y ONTAP CLI.

Para obtener más información sobre cómo habilitar ARP con ONTAP System Manager y la CLI de ONTAP , consulte "[Documentación de ONTAP : Habilitar la protección autónoma contra ransomware](#)".

Autonomous Ransomware Protection

0 TiB

Protected Capacity

100 TiB

Precommitted capacity

0 TiB

PAYGO

BYOL

100 TiB

Marketplace Contracts

0 TiB

Cree copias instantáneas a prueba de manipulaciones de archivos WORM en Cloud Volumes ONTAP

Puede crear copias instantáneas a prueba de manipulaciones de archivos de una sola escritura y múltiples lecturas (WORM) en un sistema Cloud Volumes ONTAP y conservar las instantáneas sin modificaciones durante un período de retención específico. Esta funcionalidad está impulsada por la tecnología SnapLock y proporciona una capa adicional de protección y cumplimiento de datos.

Antes de empezar

Asegúrese de que el volumen que utiliza para crear copias instantáneas sea un volumen SnapLock . Para obtener información sobre cómo habilitar la protección SnapLock en volúmenes, consulte la "[Documentación de ONTAP : Configurar SnapLock](#)" .

Pasos

1. Cree copias instantáneas desde el volumen SnapLock . Para obtener información sobre cómo crear copias de instantáneas mediante la CLI o el Administrador del sistema, consulte la "[Documentación de ONTAP : Descripción general de la administración de copias de instantáneas locales](#)" .

Las copias instantáneas heredan las propiedades WORM del volumen, lo que las hace a prueba de manipulaciones. La tecnología SnapLock subyacente garantiza que una instantánea permanezca protegida contra edición y eliminación hasta que transcurra el período de retención especificado.

2. Puede modificar el período de retención si es necesario editar estas instantáneas. Para obtener más información, consulte la "[Documentación de ONTAP : Establecer el tiempo de retención](#)" .



Si bien una copia Snapshot está protegida por un período de retención específico, el administrador del clúster puede eliminar el volumen de origen, ya que el almacenamiento WORM en Cloud Volumes ONTAP funciona bajo un modelo de "administrador de almacenamiento confiable". Además, un administrador de nube confiable puede eliminar los datos WORM operando en los recursos de almacenamiento en la nube.

Enlaces relacionados

- Para obtener más información sobre WORM, consulte ["Obtenga más información sobre el almacenamiento WORM en Cloud Volumes ONTAP"](#) .
- Para obtener información sobre la carga de los volúmenes SnapLock , consulte ["Licencias y tarificación en Cloud Volumes ONTAP"](#) .

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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