



Seguridad y cifrado de datos

Cloud Volumes ONTAP

NetApp

February 27, 2023

This PDF was generated from <https://docs.netapp.com/es-es/cloud-manager-cloud-volumes-ontap/azure/task-encrypting-volumes.html> on February 27, 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 claves con Azure Key Vault 1
 - Mejorar la protección contra el ransomware 9

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.
 - Azure: ["Azure Key Vault \(AKV\)"](#)

Gestione claves con Azure Key Vault

Puede utilizar ["Azure Key Vault \(AKV\)"](#) Para proteger sus claves de cifrado de ONTAP en una aplicación puesta en marcha de Azure.

AKV puede utilizarse para proteger ["Claves de cifrado de volúmenes de NetApp \(NVE\)"](#) Solo para SVM de datos.

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

Cuando se utiliza AKV, tenga en cuenta que, de forma predeterminada, se utiliza una LIF de SVM de datos

para comunicarse con el extremo de gestión de claves cloud. Una red de gestión de nodos se usa para comunicarse con los servicios de autenticación del proveedor de cloud (login.microsoftonline.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 cifrado de volúmenes (ve) instalada (la licencia de cifrado de volúmenes de NetApp se instala automáticamente en todos los sistemas Cloud Volumes ONTAP que se registran con el soporte de NetApp)
- Debe tener una licencia Multi-tenant Encryption Key Management (MT_EK_MGMT)
- Debe ser un administrador de clústeres o SVM
- Una suscripción a Active Azure

Limitaciones

- AKV solo se puede configurar en una SVM de datos

Proceso de configuración

Los pasos descritos capturan cómo registrar su configuración de Cloud Volumes ONTAP con Azure y cómo crear un almacén de claves y un almacén de claves de Azure. Si ya ha completado estos pasos, asegúrese de tener los valores de configuración correctos, especialmente en [Cree un almacén de claves de Azure](#), y luego continúe a [Configuración de Cloud Volumes ONTAP](#).

- [Registro de aplicaciones de Azure](#)
- [Cree el secreto del cliente de Azure](#)
- [Cree un almacén de claves de Azure](#)
- [Cree la clave de cifrado](#)
- [Crear un extremo de Azure Active Directory \(solo alta disponibilidad\)](#)
- [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 utilice para acceder al almacén de claves de Azure. En el portal de Azure, seleccione **App registrs**.
2. Seleccione **Nuevo registro**.
3. Proporcione un nombre para la aplicación y seleccione un tipo de aplicación compatible. El único inquilino predeterminado es suficiente para el uso del almacén de claves de Azure. Seleccione **Registrar**.
4. En la ventana de resumen de Azure, seleccione la aplicación que ha registrado. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)** en una ubicación segura. Serán necesarios más adelante en el proceso de inscripción.

Cree el secreto del cliente de Azure

1. En el portal de Azure para registrar su aplicación de almacén de claves de Azure, seleccione el panel **certificados y secretos**.
2. Seleccione **Nuevo secreto de cliente**. Introduzca un nombre significativo para el secreto de cliente. NetApp recomienda un período de vencimiento de 24 meses; sin embargo, sus políticas específicas de gobernanza del cloud pueden requerir un ajuste diferente.

3. Haga clic en **Agregar** para crear el secreto de cliente. Copie la cadena secreta que aparece en la columna **value** y guárdela en una ubicación segura para su uso posterior en [Configuración de Cloud Volumes ONTAP](#). El valor secreto no se volverá a mostrar después de salir de la página.

Cree un almacén de claves de Azure

1. Si ya tiene un almacén de claves de Azure, puede conectarlo a la configuración de Cloud Volumes ONTAP; no obstante, debe adaptar las políticas de acceso a los ajustes de este proceso.
2. En el portal de Azure, desplácese hasta la sección **Key Vaults**.
3. Haga clic en **+Crear** e introduzca la información necesaria, incluidos el grupo de recursos, la región y el nivel de precios. Además, introduzca el número de días que desea retener los almacenes eliminados y seleccione **Activar protección de purga** en el almacén 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 al almacén**.
 - b. En **acceso a recursos**, seleccione **cifrado de disco de Azure para cifrado de volúmenes**.
6. Seleccione **+Crear** para agregar una directiva de acceso.
7. En **Configurar de una plantilla**, haga clic en el menú desplegable y, a continuación, seleccione la plantilla **Key, Secret y Certificate Management**.
8. Elija cada uno de los menús de permisos desplegables (clave, secreto, certificado) y, a continuación, **Seleccione todos** en la parte superior de la lista de menús para seleccionar todos los permisos disponibles. Debe tener:
 - **Permisos de clave**: 20 seleccionado
 - **Permisos secretos**: 8 seleccionado
 - **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 registrada **Principal** de Azure creada en [Registro de aplicaciones de Azure](#). Seleccione **Siguiente**.



Sólo se puede asignar un principal por póliza.

Create an access policy

Permissions **Principal** Application (optional) Review + create

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Selected item

No item selected

Previous **Next**

10. Haga clic en **Siguiente** dos veces hasta llegar a **revisar y crear**. A continuación, haga clic en **Crear**.
11. Seleccione **Siguiente** para avanzar a las opciones de **redes**.
12. Elija el método de acceso a la red apropiado o seleccione **todas las redes** y **Revisión + Crear** para crear el almacén de claves. (El método de acceso a la red puede ser prescrito por una política de gobierno o su equipo de seguridad cloud de la empresa).
13. Registre el URI del almacén de claves: En el almacén de claves que ha creado, desplácese al menú Descripción general y copie el URI **Vault** de la columna de la derecha. Se necesita esto para un paso más adelante.

Cree la clave de cifrado

1. En el menú del almacén de claves creado para Cloud Volumes ONTAP, desplácese a la opción **Keys**.
2. Seleccione **generar/importar** para crear una nueva clave.
3. Deje la opción predeterminada establecida en **generar**.
4. Proporcione la siguiente información:

- Nombre de clave de cifrado
- Tipo de clave: RSA
- Tamaño de clave RSA: 2048
- Activado: Sí

5. Seleccione **Crear** para crear la clave de cifrado.
6. Vuelva al menú **Keys** y seleccione la tecla que acaba de crear.
7. Seleccione el ID de clave en **Versión actual** para ver las propiedades clave.
8. Busque el campo **Identificador de clave**. Copie el URI hasta pero no incluyendo la cadena hexadecimal.

Crear un extremo de Azure Active Directory (solo alta disponibilidad)

1. Este proceso solo es necesario si se configura el almacén clave de Azure para un entorno de trabajo Cloud Volumes ONTAP de alta disponibilidad.
2. En el portal de Azure, navegue hasta **Virtual Networks**.
3. Seleccione la red virtual en la que ha desplegado el entorno de trabajo de Cloud Volumes ONTAP y seleccione el menú **subredes** en el lado izquierdo de la página.
4. Seleccione en la lista el nombre de subred para la implementación de Cloud Volumes ONTAP.
5. Desplácese hasta el 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 la configuración.

Configuración de Cloud Volumes ONTAP

1. Conéctese a la LIF de gestión de clústeres con el cliente SSH preferido.
2. Introduzca el modo de privilegio avanzado en ONTAP:

```
set advanced -con off
```

3. Identifique la SVM de datos deseada y verifique su configuración de DNS:

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

- a. Si existe una entrada DNS para la SVM de datos deseada y contiene una entrada para el DNS de Azure, no es necesario hacer nada. Si no lo hace, añada una entrada del servidor DNS para la SVM de datos que apunte al DNS de Azure, al DNS privado o al servidor local. Esto debe coincidir con la entrada de la SVM de administrador del clúster:

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

- b. Compruebe que el servicio DNS se haya creado para la SVM de datos:

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

4. Habilite el almacén de claves de Azure mediante el ID de cliente e ID de inquilino guardados después del registro de aplicación:

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

5. Compruebe el estado del gestor de claves:

`security key-manager external azure check`La salida tendrá el aspecto siguiente:

```
::*> 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 la `service_reachability` el estado no es OK, La SVM no puede acceder al servicio Azure Key Vault con todos los permisos y conectividad necesarios. Asegúrese de que sus políticas y enrutamiento de red de Azure no bloquee su vNet privado y no alcance el extremo público de Azure KeyVault. En caso afirmativo, considere utilizar un extremo privado de Azure para acceder al almacén de claves desde vNet. También es posible que deba añadir una entrada de hosts estática a la SVM para resolver la dirección IP privada para el extremo.

La `kms_wrapped_key_status` reportará UNKNOWN en la configuración inicial. Su estado cambiará a OK una vez que se cifra el primer volumen.

6. 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 activará el cifrado de volúmenes.

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

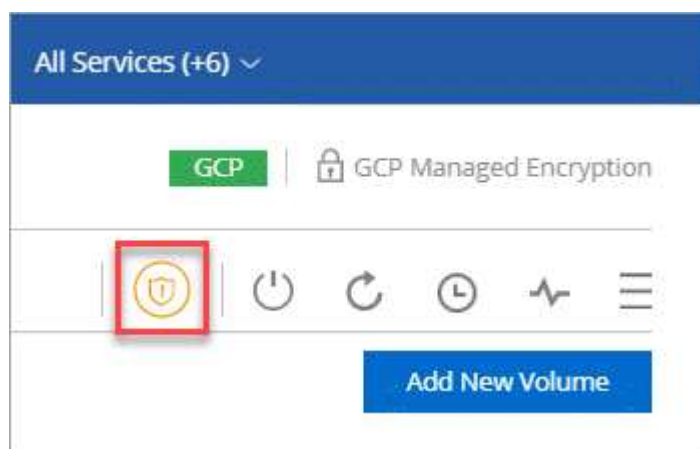
```
vol show -vserver SVM_name -fields is-encrypted
```

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 ⓘ



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 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.