Seguridad y cifrado de datos

Cloud Volumes ONTAP

NetApp
April 23, 2024

Tabla de contenidos

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.

Gestione claves con el servicio de gestión de claves de AWS

Puede utilizar "Servicio de gestión de claves (KMS) de AWS" Para proteger sus claves de cifrado de ONTAP en una aplicación implementada por AWS.

La gestión de claves con el KMS de AWS se puede habilitar con la interfaz de línea de comandos o la API DE REST de ONTAP.

Al usar KMS, tenga en cuenta que, de forma predeterminada, se usa LIF de una SVM de datos para comunicarse con el punto final de la gestión de claves de cloud. Una red de gestión de nodos se usa para comunicarse con los servicios de autenticación de AWS. Si la red de clúster no está configurada correctamente, el clúster no utilizará correctamente el servicio de gestión de claves.

Antes de empezar

- Cloud Volumes ONTAP debe ejecutar la versión 9.12.0 de o posterior
- Debe haber instalado la licencia de cifrado de volúmenes (VE) y.
- Debe haber instalado la licencia Multi-tenant Encryption Key Management (MTEKM).
- Debe ser un administrador de clústeres o SVM
- Debe tener una suscripción activa a AWS

Solo puede configurar claves para una SVM de datos.

Configuración

AWS

1. Debe crear un "otorgar" Para la clave KMS de AWS que utilizará el rol de gestión de cifrado de IAM. El rol de IAM debe incluir una política que permita las siguientes operaciones:
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`
     Para crear un permiso, consulte "Documentación de AWS".
2. "Agregue una política al rol de IAM adecuado." La política debe apoyar el `DescribeKey`, `Encrypt`, y. `Decrypt` operaciones.

Cloud Volumes ONTAP

1. Cambie al entorno de Cloud Volumes ONTAP.
2. Cambie 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, introduzca la clave secreta.
5. Confirme que el KMS de AWS se ha configurado correctamente:
   `security key-manager external aws show -vserver` *`svm_name`*

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.

Antes de empezar

- 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
- NAE no se puede utilizar con AKV. NAE requiere un servidor KMIP externo compatible.

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

- [x] Select all
- [x] Get
- [x] List
- [x] Update
- [x] Create
- [x] Import
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore

Cryptographic Operations

- [x] Select all
- [x] Decrypt
- [x] Encrypt
- [x] Unwrap Key
- [x] Wrap Key
- [x] Verify
- [x] Sign

Privileged Key Operations

- [x] Select all
- [x] Purge
- [x] Release

Rotation Policy Operations

- [x] Select all
- [x] Rotate
- [x] Get Rotation Policy
- [x] Set Rotation Policy

Secret permissions

Secret Management Operations

- [x] Select all
- [x] Get
- [x] List
- [x] Set
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore

Privileged Secret Operations

- [x] Select all
- [x] Purge

Certificate permissions

Certificate Management Operations

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

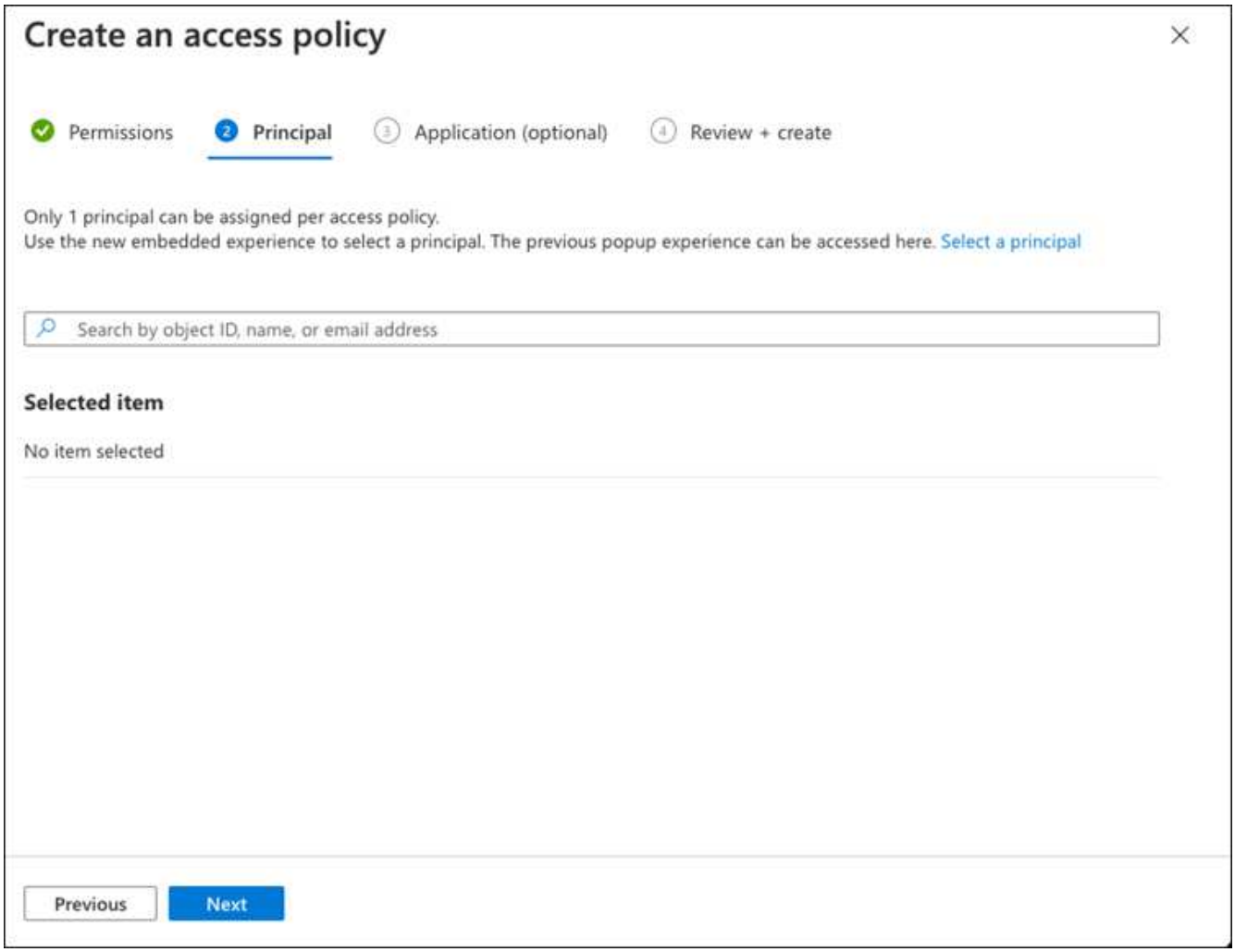
Privileged Certificate Operations

- [x] Select all
- [x] 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.



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

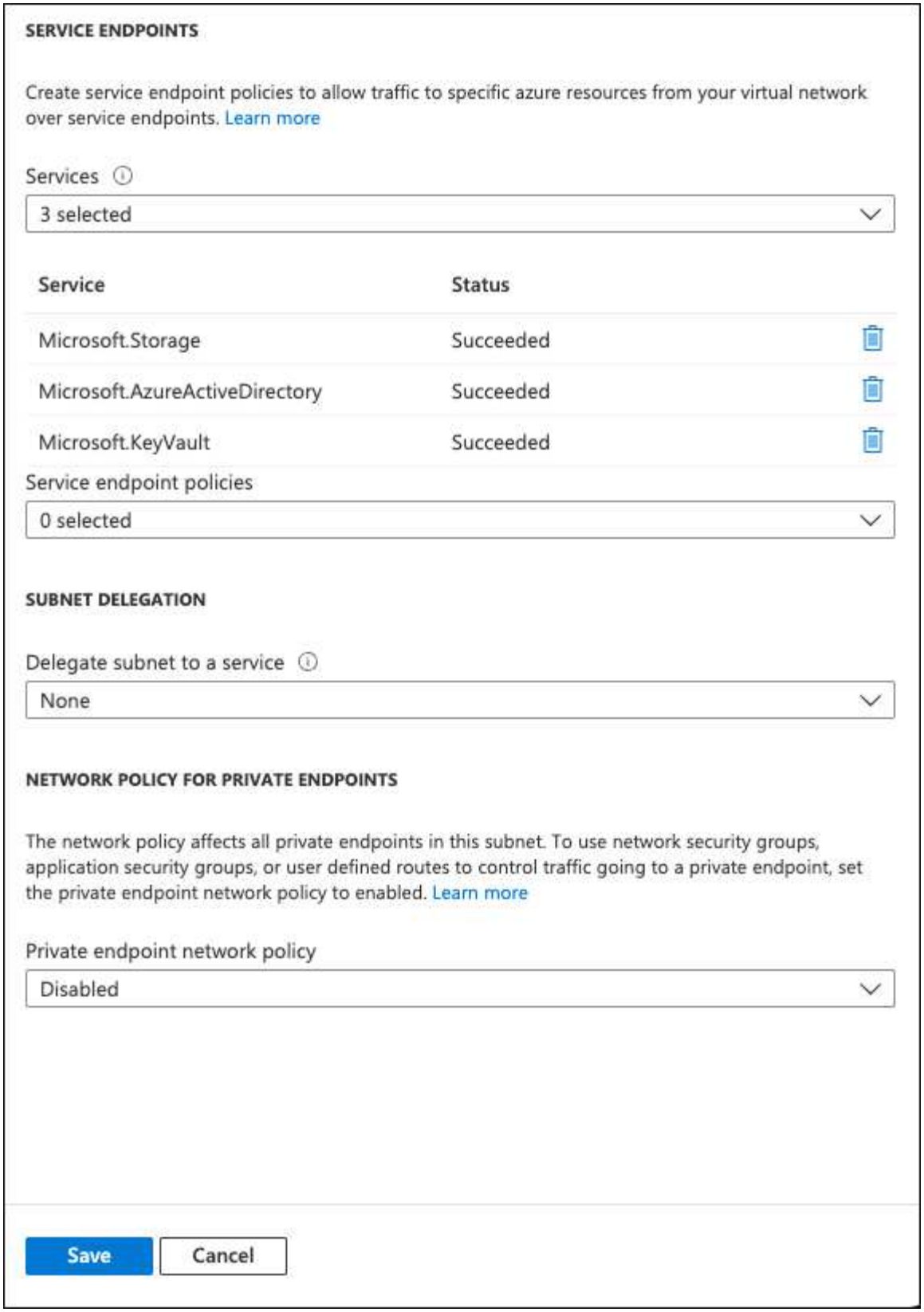
1. En el menú del almacén de claves creado para Cloud Volumes ONTAP, desplácese a la opción **Keys**.
2. Seleccione **generar/importar** para crear una nueva clave.
3. Deje la opción predeterminada establecida en **generar**.
4. Proporcione la siguiente información:

- 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)



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 key_vault_URI -key-id full_key_URI`

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

5. Una vez que se haya habilitado correctamente el almacén de claves de Azure, introduzca `client secret value` cuando se le solicite.
6. 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: ekmip_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.

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 activará el cifrado de volúmenes.

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
   ```

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.

Al usar Cloud KMS, tenga en cuenta que, de forma predeterminada, se usa LIF de una SVM de datos para comunicarse con el punto final de la 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.

Antes de empezar

- Cloud Volumes ONTAP debe ejecutar la versión 9.10.1 de o posterior
- Licencia de Volume Encryption (ve) instalada
- Licencia de administración de claves de cifrado multi-tenant (MTEKM) instalada, a partir de Cloud Volumes ONTAP 9.12.1 GA.
- 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` *`vserver_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

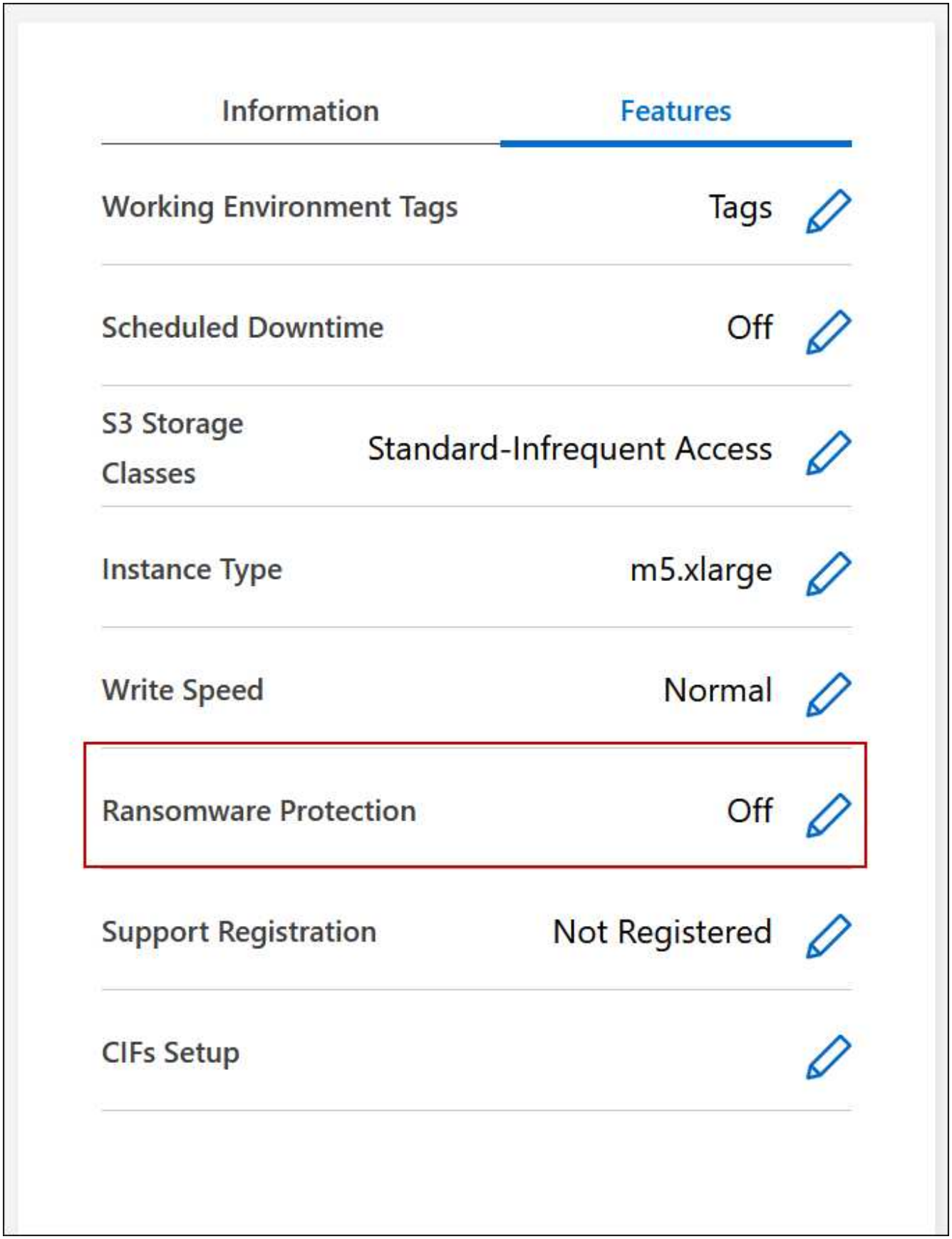
Los ataques de ransomware pueden suponer un coste comercial, recursos y reputación. BlueXP te permite implementar dos soluciones de NetApp para el ransomware: Protección desde extensiones de archivos comunes contra ransomware y protección autónoma contra ransomware (ARP). Estas soluciones proporcionan herramientas eficaces para la visibilidad, la detección y la corrección.

Protección contra extensiones de archivos de ransomware comunes

La configuración de protección frente a ransomware, disponible a través de BlueXP, le permite utilizar la funcionalidad de FPolicy de ONTAP para protegerse frente a los tipos de extensión comunes de archivo frente al ransomware.

Pasos

1. En la página Canvas, haga doble clic en el nombre del sistema que configure para la protección contra ransomware.
2. En la ficha Descripción general, haga clic en el panel Características y, a continuación, haga clic en el icono de lápiz situado junto a **Protección contra ransomware**.



3. 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.

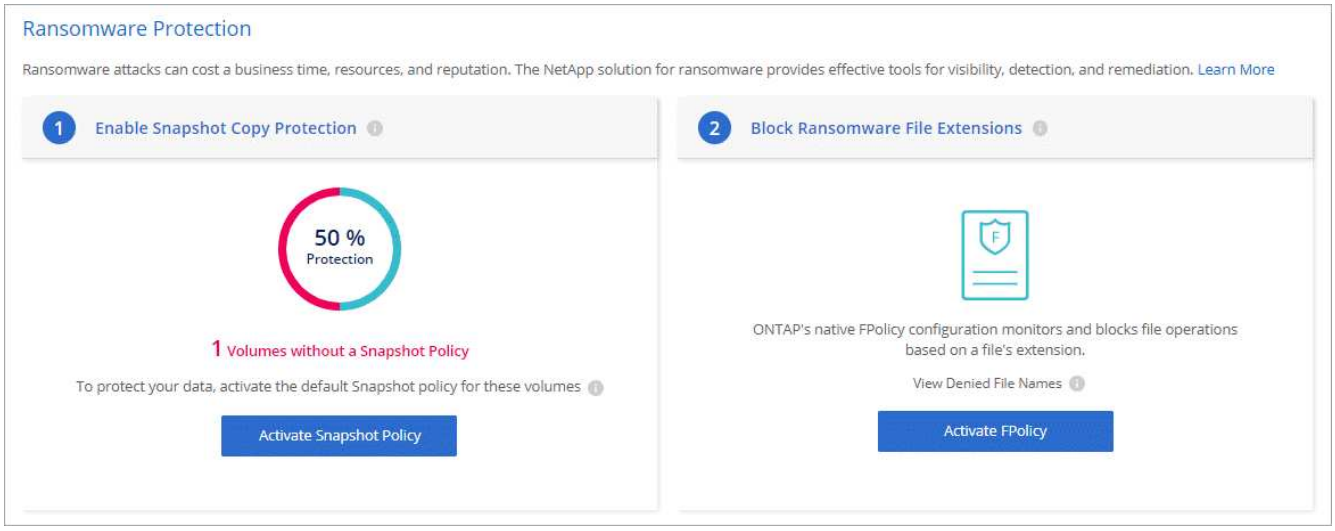
b. Haga clic en **Activar FPolicy** para habilitar la solución FPolicy de ONTAP, que puede bloquear las operaciones de archivos según la extensión de un archivo.

   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.



Protección autónoma de ransomware

Cloud Volumes ONTAP admite la función autónoma de protección frente a ransomware (ARP), que realiza análisis de cargas de trabajo para detectar y advertir de forma proactiva sobre actividad anormal que podría indicar un ataque de ransomware.

Separe de las protecciones de extensión de archivo proporcionadas a través del "configuración de protección contra ransomware", La función ARP utiliza el análisis de la carga de trabajo para alertar al usuario sobre posibles ataques basados en la “actividad anormal” detectada. Tanto la configuración de protección contra ransomware como la función ARP se pueden usar conjuntamente para una protección integral contra ransomware.

La función ARP está disponible para su uso solo con licencias BYOL (términos de 1 a 36 meses) tanto en modelos de licencia basados en nodos como en capacidad. Debe ponerse en contacto con su representante

de ventas de NetApp para adquirir una nueva licencia adicional independiente para usar con la función ARP de Cloud Volumes ONTAP.

La licencia ARP se considera una licencia «flotante», lo que significa que no está vinculada a una única instancia de Cloud Volumes ONTAP y se puede aplicar a varios entornos de Cloud Volumes ONTAP.

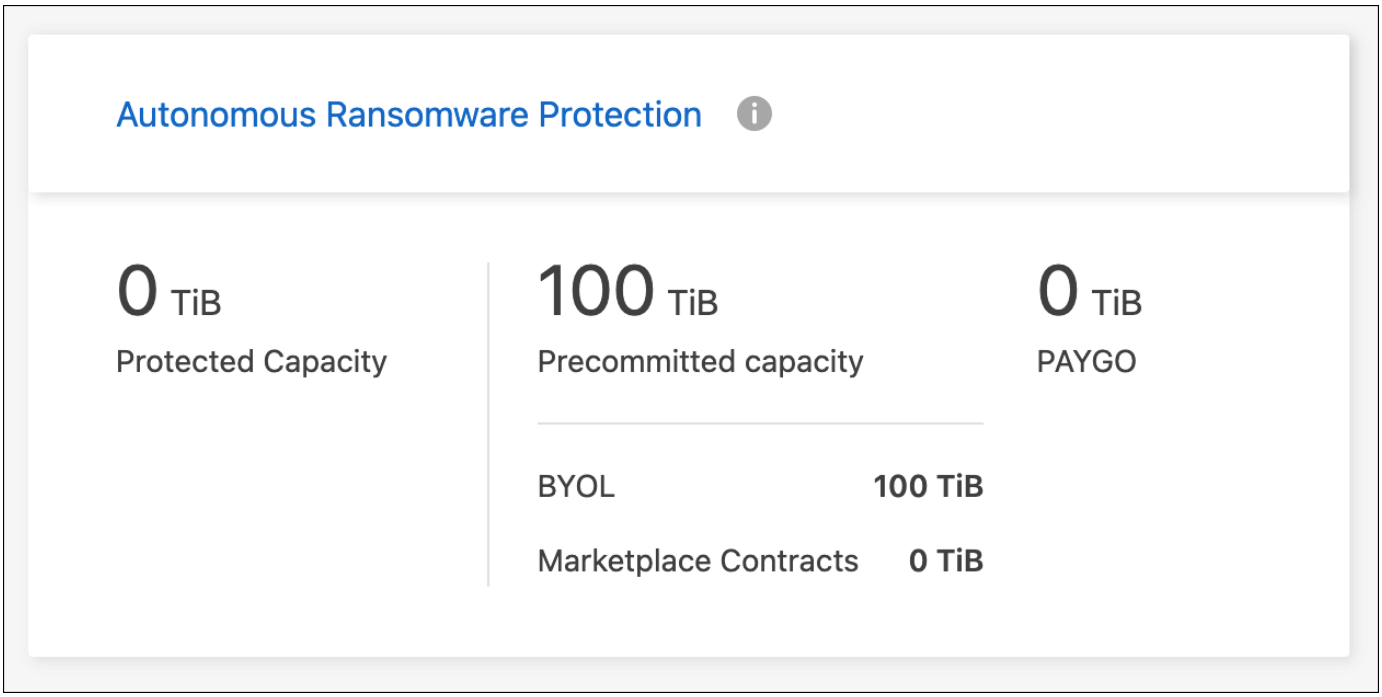
> El uso de la función ARP con licencias Cloud Volumes ONTAP basadas en nodos no se refleja actualmente en la cartera digital. La capacidad de ver el uso de ARP basado en nodos estará disponible en Digital Wallet en una versión futura.

Tras la compra de una licencia complementaria y añadirla a la cartera digital, puedes habilitar ARP por volumen con Cloud Volumes ONTAP. La carga de ARP se mide a un nivel de volumen, según la capacidad total aprovisionada de los volúmenes con la función ARP habilitada. La capacidad mínima de la licencia es 1TB. Sin embargo, no hay carga de capacidad mínima para la función ARP.

Los volúmenes habilitados para ARP tienen un estado designado de “Modo de aprendizaje” o “Activo”. Cualquier volumen con un estado ARP desactivado se excluye de la carga. Por ejemplo, un entorno Cloud Volumes ONTAP con 30 TiB de capacidad aprovisionada puede elegir que solo un subconjunto de volúmenes de 15 TiB que tengan ARP habilitado.

La configuración de ARP para volúmenes se realiza mediante System Manager de ONTAP y la CLI de ONTAP.

Para obtener más información sobre cómo habilitar ARP con ONTAP System Manager y CLI, consulte "Habilite la protección de ransomware autónoma".



> No hay soporte disponible para el uso de funciones con licencia sin una licencia.