Seguridad

Astra Trident

NetApp
January 14, 2026

This PDF was generated from https://docs.netapp.com/es-es/trident-2310/trident-reco/security-reco.html on January 14, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Seguridad . . . 1
- Seguridad . . . 1
  - Ejecute Astra Trident en su propio espacio de nombres . . . 1
  - Utilice la autenticación CHAP con los back-ends DE SAN de ONTAP . . . 1
  - Utilice la autenticación CHAP con NetApp HCI y back-ends de SolidFire . . . 1
  - Utilice Astra Trident con NVE y NAE . . . 1
- Configuración de clave unificada de Linux (LUKS) . . . 2
  - Active el cifrado LUKS . . . 2
  - Configuración de backend para importar volúmenes LUKS . . . 4
  - Gire una frase de paso LUKS . . . 4
  - Habilite la expansión de volumen . . . 6

Seguridad

Seguridad

Utilice las recomendaciones que se enumeran aquí para asegurarse de que su instalación de Astra Trident es segura.

Ejecute Astra Trident en su propio espacio de nombres

Es importante evitar que las aplicaciones, los administradores de aplicaciones, los usuarios y las aplicaciones de gestión accedan a las definiciones de objetos de Astra Trident o a los pods para garantizar un almacenamiento fiable y bloquear la potencial actividad maliciosa.

Para separar el resto de aplicaciones y usuarios de Astra Trident, instale siempre Astra Trident en su propio espacio de nombres Kubernetes (`trident`). Si coloca Astra Trident en su propio espacio de nombres, solo el personal administrativo de Kubernetes tiene acceso al pod de la Astra Trident y los artefactos (como los secretos CHAP y de back-end, si corresponde) almacenados en los objetos de CRD named.
Debe asegurarse de permitir que solo los administradores tengan acceso al espacio de nombres de Astra Trident y, por lo tanto, tengan acceso a `tridentctl` cliente más.

Utilice la autenticación CHAP con los back-ends DE SAN de ONTAP

Astra Trident admite la autenticación basada en CHAP para las cargas de trabajo SAN de ONTAP (mediante el `ontap-san` y.. `ontap-san-economy` de windows). NetApp recomienda utilizar CHAP bidireccional con Astra Trident para la autenticación entre un host y el back-end de almacenamiento.

En el caso de los back-ends de ONTAP que utilizan controladores de almacenamiento SAN, Astra Trident puede configurar CHAP bidireccional y gestionar los nombres de usuario y los secretos CHAP a través de `tridentctl`.
Consulte "aquí" Para comprender cómo Astra Trident configura CHAP en los back-ends de ONTAP.

Utilice la autenticación CHAP con NetApp HCI y back-ends de SolidFire

NetApp recomienda poner en marcha CHAP bidireccional para garantizar la autenticación entre un host y los back-ends de NetApp HCI y SolidFire. Astra Trident utiliza un objeto secreto que incluye dos contraseñas CHAP por inquilino. Cuando se instala Astra Trident, gestiona los secretos CHAP y los almacena en `tridentvolume` Objeto CR para el PV correspondiente. Al crear un VP, Astra Trident utiliza los secretos de CHAP para iniciar una sesión iSCSI y comunicarse con el sistema NetApp HCI y SolidFire a través de CHAP.

> Los volúmenes que crea Astra Trident no están asociados con ningún grupo de acceso de volumen.

Utilice Astra Trident con NVE y NAE

ONTAP de NetApp proporciona cifrado de datos en reposo para proteger los datos confidenciales en el caso de robo, devolución o reasignación de un disco. Para obtener más información, consulte "Configure la información general de cifrado de volúmenes de NetApp".

- Si NAE está habilitado en el back-end, cualquier volumen aprovisionado en Astra Trident se habilitará para NAE.

- Si NAE no está habilitado en el back-end, todos los volúmenes aprovisionados en Astra Trident tendrán el cifrado NVE habilitado a menos que establezca el indicador NVE en `false` en la configuración de back-end.

> Los volúmenes que se crean en Astra Trident en un back-end con la NAE habilitada deben ser NVE o NAE cifrados.
>
> - Puede establecer el indicador NVE Encryption como `true` En la configuración del back-end de Trident, con el fin de anular el cifrado NAE y utilizar una clave de cifrado específica por volumen.
> - Establecer la Marca NVE Encryption como `false` En un back-end habilitado para NAE se creará un volumen habilitado para NAE. No puede deshabilitar el cifrado NAE mediante la Marca NVE Encryption a. `false`.

- Es posible crear manualmente un volumen NVE en Astra Trident mediante la definición explícita de la Marca NVE a. `true`.

Para obtener más información sobre las opciones de configuración del back-end, consulte:

- "Opciones de configuración DE SAN de ONTAP"
- "Opciones de configuración de NAS de ONTAP"

Configuración de clave unificada de Linux (LUKS)

Puede habilitar Unified Key Setup (LUKS) de Linux para cifrar los volúmenes DE ECONOMÍA SAN de ONTAP y SAN DE ONTAP en Astra Trident. Astra Trident admite la rotación de claves de acceso y la expansión de volumen para volúmenes cifrados con LUKS.

En Astra Trident, los volúmenes cifrados por LUKS utilizan el cifer y el modo AES-xts-Capellanía, como recomienda "NIST".

Antes de empezar

- Los nodos de trabajo deben tener instalado cryptsetup 2.1 o superior (pero inferior a 3.0). Si desea más información, visite "Gitlab: Cryptsetup".
- Por motivos de rendimiento, recomendamos que los nodos de trabajo admitan las nuevas instrucciones estándar de cifrado avanzado (AES-ni). Para verificar el soporte de AES-ni, ejecute el siguiente comando:

```
grep "aes" /proc/cpuinfo
```

Si no se devuelve nada, su procesador no admite AES-ni. Para obtener más información sobre AES-ni, visite: "Intel: Instrucciones estándar de cifrado avanzado (AES-ni)".

Active el cifrado LUKS

Puede habilitar el cifrado por volumen en el lado del host usando la configuración de clave unificada de Linux (LUKS) para SAN de ONTAP y volúmenes DE ECONOMÍA SAN de ONTAP.

Pasos

1. Defina los atributos de cifrado LUKS en la configuración de backend. Para obtener más información sobre las opciones de configuración del back-end para SAN de ONTAP, consulte "Opciones de configuración DE SAN de ONTAP".

```
"storage": [
    {
        "labels":{"luks": "true"},
        "zone":"us_east_1a",
        "defaults": {
            "luksEncryption": "true"
        }
    },
    {
        "labels":{"luks": "false"},
        "zone":"us_east_1a",
        "defaults": {
            "luksEncryption": "false"
        }
    },
]
```

2. Uso `parameters.selector` Para definir los pools de almacenamiento mediante el cifrado LUKS. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

3. Cree un secreto que contenga la frase de paso LUKS. Por ejemplo:

```
kubectl -n trident create -f luks-pvc1.yaml
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: A
  luks-passphrase: secretA
```

Limitaciones

Los volúmenes cifrados LUKS no pueden aprovechar la deduplicación y la compresión de ONTAP.

Configuración de backend para importar volúmenes LUKS

Para importar un volumen LUKS, debe establecer `luksEncryption` para(`true` en el backend. La `luksEncryption` La opción indica a Astra Trident si el volumen cumple con la normativa LUKS (`true`) O no cumple con LUKS (`false`) como se muestra en el siguiente ejemplo.

```
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: trident_svm
username: admin
password: password
defaults:
  luksEncryption: 'true'
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'
```

Gire una frase de paso LUKS

Puede girar la frase de paso de LUKS y confirmar la rotación.

> No olvide una clave de acceso hasta que haya verificado que ya no hace referencia a ningún volumen, snapshot o secreto. Si se pierde una clave de acceso de referencia, es posible que no se pueda montar el volumen y los datos seguirán estando cifrados e inaccesibles.

Acerca de esta tarea

LA rotación DE la frase de paso LUKS se produce cuando se crea un pod que monta el volumen después de especificar una nueva frase de paso LUKS. Cuando se crea un nuevo pod, Astra Trident compara la frase de paso de LUKS del volumen con la frase de paso activa en el secreto.

- Si la clave de acceso del volumen no coincide con la clave de acceso activa en el secreto, se produce la rotación.
- Si la clave de acceso del volumen coincide con la clave de acceso activa en el secreto, el `previous-luks-passphrase` se ignora el parámetro.

Pasos

1. Añada el `node-publish-secret-name` y.. `node-publish-secret-namespace` Parámetros de StorageClass. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-san
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/backendType: "ontap-san"
  csi.storage.k8s.io/node-stage-secret-name: luks
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-publish-secret-name: luks
  csi.storage.k8s.io/node-publish-secret-namespace: ${pvc.namespace}
```

2. Identifique las bases de datos passhrases existentes en el volumen o la snapshot.

Volumen

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["A"]
```

Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames:["A"]
```

3. Actualice el secreto LUKS del volumen para especificar las passphrases nuevas y anteriores. Asegúrese `previous-luke-passphrase-name` y.. `previous-luks-passphrase` coincidir con la frase de contraseña anterior.

```
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA
```

4. Cree un nuevo pod montando el volumen. Esto es necesario para iniciar la rotación.
5. Compruebe que se ha girado la frase de paso.

Volumen

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["B"]
```

Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames:["B"]
```

Resultados

La frase de contraseña se giró cuando solo se devuelve la nueva frase de contraseña en el volumen y la instantánea.

> Si se devuelven dos passphrasas, por ejemplo `luksPassphraseNames: ["B", "A"]`, la rotación está incompleta. Puede activar un nuevo pod para intentar completar la rotación.

Habilite la expansión de volumen

Es posible habilitar la ampliación de volumen en un volumen cifrado LUKS.

Pasos

1. Habilite el `CSINodeExpandSecret` puerta de características (beta 1.25+). Consulte "Kubernetes 1.25: Use Secrets for Node-Driven Expansion of CSI Volumes" para obtener más detalles.
2. Añada el `node-expand-secret-name` y.. `node-expand-secret-namespace` Parámetros de StorageClass. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-expand-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-expand-secret-namespace: ${pvc.namespace}
allowVolumeExpansion: true
```

Resultados

Al iniciar la ampliación de almacenamiento en línea, el kubelet pasa las credenciales adecuadas al controlador.

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.