Proteja sus datos

ASA r2

NetApp
September 26, 2024

Tabla de contenidos

Proteja sus datos

Cifrado de datos estáticos en sistemas de almacenamiento R2 de ASA

Al cifrar datos en reposo, no se podrán leer si un medio de almacenamiento se reasigna, devuelve, se pierde o es robado. Puede usar System Manager de ONTAP para cifrar sus datos a nivel de hardware y software para lograr una protección de doble capa.

El cifrado en almacenamiento de NetApp (NSE) admite el cifrado de hardware mediante unidades de cifrado automático (SED). SEDS cifra los datos a medida que se escriben. Cada SED contiene una clave de cifrado única. Los datos cifrados almacenados en el SED no se pueden leer sin la clave de cifrado del SED. Los nodos que intentan leer desde un SED se deben autenticar para acceder a la clave de cifrado del SED. Los nodos se autentican obteniendo una clave de autenticación de un administrador de claves y, a continuación, presentando la clave de autenticación al SED. Si la clave de autenticación es válida, el SED le dará al nodo su clave de cifrado para acceder a los datos que contiene.

Use el administrador de claves incorporado o un gestor de claves externo de ASA R2 para servir claves de autenticación a los nodos.

Además de NSE, también puede habilitar el cifrado del software para añadir otra capa de seguridad a sus datos.

Pasos

1. En el Administrador del sistema, selecciona **Clúster > Configuración**.
2. En la sección **Seguridad**, en **Cifrado**, selecciona **Configurar**.
3. Configure el gestor de claves.

Opción	Pasos
Configure el gestor de claves incorporado	a. Seleccione **Onboard Key Manager** para agregar los servidores de claves. b. Introduzca una frase de contraseña.
Configure un gestor de claves externo	a. Seleccione **Administrador de claves externo** para agregar los servidores de claves. b. + Add Seleccione para agregar los servidores de claves. c. Añada los certificados de CA del servidor KMIP. d. Añada los certificados de cliente KMIP.

4. Seleccione **Cifrado de doble capa** para habilitar el cifrado de software.
5. Seleccione **Guardar**.

El futuro

Ahora que ha cifrado sus datos en reposo, si utiliza el protocolo NVMe/TCP, puede hacerlo "cifrar todos los datos enviados a través de la red" entre su host NVMe/TCP y su sistema ASA R2.

Protéjase contra ataques de ransomware en sistemas de almacenamiento ASA R2

Para obtener una mejor protección contra ataques de ransomware, replica snapshots en un clúster remoto y, a continuación, bloquea las snapshots de destino para que estén a prueba de manipulaciones. Las instantáneas bloqueadas no se pueden eliminar accidentalmente ni de forma malintencionada. Puede utilizar snapshots bloqueados para recuperar datos si una unidad de almacenamiento se ve afectada por un ataque de ransomware.

Inicialice el reloj de SnapLock Compliance

Para poder crear copias Snapshot a prueba de manipulaciones, debe inicializar el reloj de SnapLock Compliance en los clústeres locales y de destino.

Pasos

1. Seleccione **Cluster > Overview**.
2. En la sección **Nodos**, selecciona **Inicializar reloj SnapLock Compliance**.
3. Selecciona **Inicializar**.
4. Compruebe que se ha inicializado el reloj de conformidad.
   a. Seleccione **Cluster > Overview**.
   b. En la sección **Nodos**, seleccione ; y luego seleccione **Reloj SnapLock Compliance**.

¿Cuál es el siguiente?

Después de inicializar el reloj de SnapLock Compliance en los clústeres locales y de destino, está listo para "crear una relación de replicación con snapshots bloqueadas".

Proteja las conexiones NVMe en sus sistemas de almacenamiento ASA R2

Si utiliza el protocolo NVMe, puede configurar la autenticación en banda para mejorar la seguridad de sus datos. La autenticación en banda permite una autenticación bidireccional y unidireccional segura entre sus hosts NVMe y su sistema ASA R2. La autenticación en banda está disponible para todos los hosts NVMe. Si utiliza el protocolo NVMe/TCP, puede mejorar aún más la seguridad de datos configurando la seguridad de la capa de transporte (TLS) para cifrar todos los datos enviados a través de la red entre los hosts NVMe/TCP y el sistema ASA R2.

Pasos

1. Seleccione **HOSTS**; luego seleccione **NVMe**.
2. Seleccione + Add .
3. Introduzca el nombre de host y, a continuación, seleccione el sistema operativo del host.
4. Introduzca la descripción de un host y, a continuación, seleccione la máquina virtual de almacenamiento para conectarse al host.

5. Seleccione junto al nombre de host.
6. Seleccione **Autenticación en banda**.
7. Si está utilizando el protocolo NVMe/TCP, seleccione **Requerir seguridad de la capa de transporte (TLS)**.
8. Seleccione **Agregar**.

Resultado

La seguridad de sus datos se mejora con la autenticación en banda y/o TLS.

Información de copyright

Información de la marca comercial