Daten auf einem FIPS-Laufwerk oder SED unzugänglich machen

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/encryption-at-rest/data-seds-inaccessible-concept.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

Daten auf einem FIPS-Laufwerk oder SED unzugänglich machen 1
Datenträgerbereinigung und -vernichtung in ONTAP 1
Ein FIPS-Laufwerk oder SED in ONTAP bereinigen 1
Ein FIPS-Laufwerk oder eine SED in ONTAP zerstören 3
Daten auf einem FIPS-Laufwerk oder SED im Notfall in ONTAP vernichten 5

Daten auf einem FIPS-Laufwerk oder SED unzugänglich machen

Datenträgerbereinigung und -vernichtung in ONTAP

Wenn Sie Daten auf einem FIPS-Laufwerk oder Self-Encrypting Drive dauerhaft unzugänglich machen möchten, der ungenutzte Speicherplatz jedoch für neue Daten verfügbar bleiben soll, kann das Laufwerk bereinigt werden. Wenn Daten dauerhaft unzugänglich gemacht werden sollen und eine Wiederverwendung des Laufwerks nicht erforderlich ist, kann es zerstört werden.

- Datenträgerbereinigung

  Beim Bereinigen eines Self-Encrypting Drives ändert das System den Verschlüsselungsschlüssel auf einen neuen Zufallswert, setzt den Sperrzustand beim Einschalten auf „false“ und setzt die Schlüssel-ID auf einen Standardwert, entweder die Hersteller Secure ID 0x0 (SAS-Laufwerke) oder einen Null-Schlüssel (NVMe-Laufwerke). Dadurch sind die Daten auf dem Laufwerk unzugänglich und können nicht wiederhergestellt werden. Bereinigte Laufwerke können als nicht mit Nullen überschriebene Ersatzlaufwerke wiederverwendet werden.

- Datenträger zerstören

  Wenn Sie ein FIPS-Laufwerk oder ein Self-Encrypting Drive zerstören, setzt das System den Festplattenverschlüsselungsschlüssel auf einen unbekannten Zufallswert und sperrt die Festplatte unwiderruflich. Dadurch wird die Festplatte dauerhaft unbrauchbar und die darauf befindlichen Daten sind dauerhaft unzugänglich.

Es besteht die Möglichkeit, einzelne Self-Encrypting Drives zu bereinigen oder zu zerstören oder alle Self-Encrypting Drives eines Knotens zu zerstören.

Ein FIPS-Laufwerk oder SED in ONTAP bereinigen

Wenn Daten auf einem FIPS-Laufwerk oder Self-Encrypting Drive dauerhaft unzugänglich gemacht werden sollen und das Laufwerk für neue Daten verwendet werden soll, kann der `storage encryption disk sanitize` Befehl zum Bereinigen des Laufwerks verwendet werden.

Über diese Aufgabe

Beim Bereinigen eines Self-Encrypting Drives ändert das System den Verschlüsselungsschlüssel auf einen neuen Zufallswert, setzt den Sperrzustand beim Einschalten auf „false“ und setzt die Schlüssel-ID auf einen Standardwert, entweder die Hersteller Secure ID 0x0 (SAS-Laufwerke) oder einen Null-Schlüssel (NVMe-Laufwerke). Dadurch sind die Daten auf dem Laufwerk unzugänglich und können nicht wiederhergestellt werden. Bereinigte Laufwerke können als nicht mit Nullen überschriebene Ersatzlaufwerke wiederverwendet werden.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Alle Daten, die erhalten bleiben müssen, zu einem Aggregat auf einer anderen Festplatte migrieren.
2. Das Aggregat auf dem FIPS-Laufwerk oder dem zu bereinigenden SED löschen:

   `storage aggregate delete -aggregate aggregate_name`

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

   Weitere Informationen zu `storage aggregate delete` finden sich in der "ONTAP-Befehlsreferenz".

3. Die Datenträger-ID für das zu bereinigende FIPS-Laufwerk oder die Self-Encrypting Drives (SED) identifizieren:

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   1.10.2  data <id_value>
   [...]
   ```

4. Wenn ein FIPS-Laufwerk im FIPS-Konformitätsmodus betrieben wird, wird die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf den Standardwert MSID 0x0 gesetzt:

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   Mit dem `security key-manager query` Befehl lassen sich die Schlüssel-IDs anzeigen.

   ```
   cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

   Info: Starting modify on 1 disk.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

5. Das Laufwerk bereinigen:

   `storage encryption disk sanitize -disk disk_id`

   Mit diesem Befehl können nur Hot Spare- oder defekte Festplatten bereinigt werden. Um alle Festplatten unabhängig vom Typ zu bereinigen, ist die Option `-force-all-state` zu verwenden. Weitere Informationen zu `storage encryption disk sanitize` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP fordert Sie auf, vor dem Fortfahren eine Bestätigungsphrase einzugeben. Die Phrase muss exakt so eingegeben werden, wie sie auf dem Bildschirm angezeigt wird.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. Die bereinigte Festplatte wiederherstellen: `storage disk unfail -spare true -disk disk_id`
7. Es ist zu prüfen, ob die Festplatte einen Besitzer hat: `storage disk show -disk disk_id` + Falls die Festplatte keinen Besitzer hat, ist einer zuzuweisen. `storage disk assign -owner node -disk disk_id`
8. Öffnen Sie die Nodeshell für den Node, dem die Festplatten gehören, die Sie bereinigen möchten:

   `system node run -node node_name`

   Führe den `disk sanitize release` Befehl aus.

9. Beenden Sie die Nodeshell. Die Festplatte wird erneut in den betriebsbereiten Zustand versetzt: `storage disk unfail -spare true -disk disk_id`
10. Es sollte überprüft werden, dass die Festplatte nun als Ersatzfestplatte verfügbar ist und zur Wiederverwendung in einem Aggregat bereitsteht: `storage disk show -disk disk_id`

Verwandte Informationen

- "Speicherdatenträger zuweisen"
- "Speicherdatenträger anzeigen"
- "Speicherfestplatte wiederherstellen"
- "Speicherverschlüsselung Festplatte ändern"
- "Speicherverschlüsselung Festplattenbereinigung"
- "storage encryption disk show-status"

Ein FIPS-Laufwerk oder eine SED in ONTAP zerstören

Wenn Daten auf einem FIPS-Laufwerk oder Self-Encrypting Drive dauerhaft unzugänglich gemacht werden sollen und das Laufwerk nicht wiederverwendet werden muss, kann der `storage encryption disk destroy` Befehl verwendet werden, um die Festplatte zu zerstören.

Über diese Aufgabe

Wenn Sie ein FIPS-Laufwerk oder eine Self-Encrypting Drive zerstören, setzt das System den Festplattenverschlüsselungsschlüssel auf einen unbekannten Zufallswert und sperrt das Laufwerk unwiderruflich. Dadurch wird die Festplatte praktisch unbrauchbar und die darauf befindlichen Daten dauerhaft unzugänglich. Es besteht jedoch die Möglichkeit, die Festplatte mithilfe der auf dem Etikett aufgedruckten physischen Secure ID (PSID) auf die werkseitig konfigurierten Einstellungen zurückzusetzen. Weitere Informationen finden sich unter "Wiederinbetriebnahme eines FIPS-Laufwerks oder SED, wenn Authentifizierungsschlüssel verloren gegangen sind".

> Ein FIPS-Laufwerk oder Self-Encrypting Drive sollte nur zerstört werden, wenn der Non-Returnable Disk Plus Service (NRD Plus) vorhanden ist. Durch das Zerstören eines Datenträgers erlischt die Garantie.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Alle Daten, die erhalten bleiben müssen, werden in ein Aggregat auf einer anderen Festplatte migriert.
2. Das Aggregat auf dem FIPS-Laufwerk oder dem zu zerstörenden SED löschen:

   `storage aggregate delete -aggregate aggregate_name`

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

   Weitere Informationen zu `storage aggregate delete` finden sich in der "ONTAP-Befehlsreferenz".

3. Die Datenträger-ID für das FIPS-Laufwerk oder den zu zerstörenden Self-Encrypting Drive (SED) identifizieren:

   `storage encryption disk show`

   Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   1.10.2  data <id_value>
   [...]
   ```

4. Zerstören der Festplatte:

   `storage encryption disk destroy -disk disk_id`

   Weitere Informationen zu `storage encryption disk destroy` finden sich in der "ONTAP-Befehlsreferenz".

Sie werden aufgefordert, vor dem Fortfahren eine Bestätigungsphrase einzugeben. Die Phrase muss exakt so eingegeben werden, wie sie auf dem Bildschirm angezeigt wird.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

Verwandte Informationen

- "Speicherverschlüsselungsfestplatte zerstören"
- "storage encryption Disk anzeigen"
- "storage encryption disk show-status"

Daten auf einem FIPS-Laufwerk oder SED im Notfall in ONTAP vernichten

Im Falle eines Sicherheitsnotfalls kann der Zugriff auf ein FIPS-Laufwerk oder eine SED sofort verhindert werden, selbst wenn das Speichersystem oder der KMIP-Server nicht mit Strom versorgt wird.

Bevor Sie beginnen

- Wenn ein KMIP-Server ohne verfügbare Stromversorgung verwendet wird, muss der KMIP-Server mit einem leicht zu zerstörenden Authentifizierungsobjekt (zum Beispiel einer Smartcard oder einem USB-Laufwerk) konfiguriert werden.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Notfallvernichtung von Daten auf einem FIPS-Laufwerk oder SED durchführen:

Wenn…	Dann…

Die Stromversorgung des Speichersystems ist gewährleistet und es besteht ausreichend Zeit, das Speichersystem ordnungsgemäß offline zu nehmen.	a. Wenn das Speichersystem als HA-Paar konfiguriert ist, sollte die Übernahme deaktiviert werden. b. Alle Aggregate offline nehmen und löschen. c. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced` d. Wenn sich das Laufwerk im FIPS-Konformitätsmodus befindet, wird die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID gesetzt: `storage encryption disk modify -disk * -fips-key-id 0x0` e. Das Speichersystem anhalten. f. Im Wartungsmodus starten. g. Datenträger bereinigen oder zerstören: ◦ Wenn die Daten auf den Festplatten unzugänglich gemacht werden sollen und die Festplatten dennoch wiederverwendet werden können, empfiehlt sich eine Bereinigung der Festplatten: `disk encrypt sanitize -all` ◦ Wenn die Daten auf den Datenträgern unzugänglich gemacht werden sollen und die Datenträger nicht aufbewahrt werden müssen, zerstören Sie die Datenträger: `disk encrypt destroy disk_id1 disk_id2 …` Die `disk encrypt sanitize` und	Die Stromversorgung des Speichersystems ist gewährleistet, und die Daten müssen sofort vernichtet werden.

a. **Wenn Sie die Daten auf den Festplatten unzugänglich machen und die Festplatten dennoch wiederverwenden möchten, bereinigen Sie die Festplatten:**
b. Wenn das Speichersystem als HA-Paar konfiguriert ist, sollte die Übernahme deaktiviert werden.
c. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:
`set -privilege advanced`
d. Wenn sich das Laufwerk im FIPS-Konformitätsmodus befindet, wird die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID gesetzt:
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Festplatte bereinigen:
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Wenn die Daten auf den Datenträgern unzugänglich gemacht werden sollen und die Datenträger nicht aufbewahrt werden müssen, die Datenträger zerstören:**
	b. Wenn das Speichersystem als HA-Paar konfiguriert ist, sollte die Übernahme deaktiviert werden.
	c. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:
	`set -privilege advanced`
	d. Zerstören Sie die Festplatten:
	`storage encryption disk destroy -disk * -force-all-states true`
		Das Speichersystem stürzt ab und befindet sich dadurch in einem dauerhaft deaktivierten Zustand, wobei alle Daten gelöscht werden. Um das System erneut zu verwenden, ist eine Neukonfiguration erforderlich.

Strom ist für den KMIP-Server verfügbar, jedoch nicht für das Speichersystem.	a. Melden Sie sich beim KMIP Server an. b. Alle Schlüssel, die mit den FIPS-Laufwerken oder Self-Encrypting Drives verknüpft sind und die Daten enthalten, auf die kein Zugriff mehr möglich sein soll, werden zerstört. Dadurch wird der Zugriff des Speichersystems auf die Festplattenverschlüsselungsschlüssel verhindert.	Strom ist für den KMIP-Server oder das Speichersystem nicht verfügbar.

Verwandte Informationen

- "Speicherverschlüsselungsfestplatte zerstören"
- "Speicherverschlüsselung Festplatte ändern"

- "Speicherverschlüsselung Festplattenbereinigung"

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.