



# 使FIPS磁碟機或SED上的資料無法存取 ONTAP 9

NetApp  
February 12, 2026

# 目錄

使FIPS磁碟機或SED上的資料無法存取 .....	1
了解如何使 FIPS 驅動器或 SED 上的ONTAP資料無法存取 .....	1
在 ONTAP 中清理 FIPS 磁碟機或 SED .....	1
在 ONTAP 中銷毀 FIPS 磁碟機或 SED .....	3
ONTAP 中的 FIPS 磁碟機或 SED 上的緊急資料會被粉碎 .....	5

# 使FIPS磁碟機或SED上的資料無法存取

## 了解如何使 FIPS 驅動器或 SED 上的ONTAP資料無法存取

如果您想要使FIPS磁碟機或SED上的資料永久無法存取、但要保留磁碟機未使用的空間以供新資料使用、您可以清理磁碟。如果您想要永久無法存取資料、而且不需要重複使用磁碟機、可以將其銷毀。

- 磁碟資料抹除

當您清理自我加密磁碟機時、系統會將磁碟加密金鑰變更為新的隨機值、將開機鎖定狀態重設為假、並將金鑰ID設為預設值、例如製造商安全ID 0x0 (SAS磁碟機) 或null金鑰 (NVMe磁碟機)。這樣做會使磁碟上的資料無法存取、而且無法擷取。您可以將已消毒的磁碟重複使用為非零備援磁碟。

- 磁碟銷毀

當您銷毀FIPS磁碟機或SED時、系統會將磁碟加密金鑰設為未知的隨機值、並以不可扭轉的方式鎖定磁碟。這樣做會使磁碟永遠無法使用、且上的資料永遠無法存取。

您可以清除或銷毀個別自我加密磁碟機、或是節點的所有自我加密磁碟機。

## 在 ONTAP 中清理 FIPS 磁碟機或 SED

如果您想讓 FIPS 磁碟機或 SED 上的資料永遠無法存取、並將磁碟機用於新資料、您可以使用 `storage encryption disk sanitize` 用於清理磁碟機的命令。

### 關於這項工作

當您清理自我加密磁碟機時、系統會將磁碟加密金鑰變更為新的隨機值、將開機鎖定狀態重設為假、並將金鑰ID設為預設值、例如製造商安全ID 0x0 (SAS磁碟機) 或null金鑰 (NVMe磁碟機)。這樣做會使磁碟上的資料無法存取、而且無法擷取。您可以將已消毒的磁碟重複使用為非零備援磁碟。

### 開始之前

您必須是叢集管理員才能執行此工作。

### 步驟

1. 將任何需要保留的資料移轉到另一個磁碟上的集合體。
2. 刪除FIPS磁碟機或SED上要消毒的Aggregate：

```
storage aggregate delete -aggregate aggregate_name
```

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

如"[指令參考資料ONTAP](#)"需詳細 `storage aggregate delete` 資訊，請參閱。

3. 識別要消毒的FIPS磁碟機或SED的磁碟ID：

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

如"指令參考資料ONTAP"需詳細 `storage encryption disk show` 資訊，請參閱。

```
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. 如果FIPS磁碟機以FIPS相容模式執行、請將節點的FIPS驗證金鑰ID設回預設的MSID 0x0：

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

您可以使用 `security key-manager query` 檢視金鑰ID的命令。

```
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. 為磁碟機消毒：

```
storage encryption disk sanitize -disk disk_id
```

您只能使用此命令來清除熱備援磁碟或中斷的磁碟。若要清理所有磁碟，無論其類型為何，請使用 ``-force-all-state`` 選項。如"指令參考資料ONTAP"需詳細 `storage encryption disk sanitize` 資訊，請參閱。



ONTAP 會提示您輸入確認片語、然後再繼續。輸入完全如畫面所示的詞彙。

```
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.
```



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

如"[指令參考資料ONTAP](#)"需詳細 `storage aggregate delete` 資訊，請參閱。

### 3. 識別要銷毀的FIPS磁碟機或SED的磁碟ID：

```
storage encryption disk show
```

如"[指令參考資料ONTAP](#)"需詳細 `storage encryption disk show` 資訊，請參閱。

```
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. 銷毀磁碟：

```
storage encryption disk destroy -disk disk_id
```

如"[指令參考資料ONTAP](#)"需詳細 `storage encryption disk destroy` 資訊，請參閱。



系統會提示您輸入確認短句、然後再繼續。輸入完全如畫面所示的詞彙。

```
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.
```

## 相關資訊

- ["儲存加密磁碟銷毀"](#)

- "儲存加密磁碟顯示"
- "儲存加密磁碟顯示狀態"

## ONTAP 中的 FIPS 磁碟機或 SED 上的緊急資料會被粉碎

發生安全性緊急情況時、即使儲存系統或KMIP伺服器無法使用電源、您仍可立即防止存取FIPS磁碟機或SED。

### 開始之前

- 如果您使用的KMIP伺服器沒有可用的電源、則KMIP伺服器必須設定容易銷毀的驗證項目（例如智慧卡或USB磁碟機）。
- 您必須是叢集管理員才能執行此工作。

### 步驟

1. 緊急銷毀FIPS磁碟機或SED上的資料：

如果...	然後...
-------	-------

儲存系統可提供電力、您也有時間讓儲存系統正常離線

a. 如果儲存系統設定為HA配對、請停用接管功能。

b. 使所有集合體離線並加以刪除。

c. 將權限層級設為進階：  
`set -privilege advanced`

d. 如果磁碟機處於FIPS相容模式、請將節點的FIPS驗證金鑰ID設回預設MSID：  
`storage encryption disk modify -disk * -fips-key-id 0x0`

e. 停止儲存系統。

f. 開機進入維護模式。

g. 清理或銷毀磁碟：

◦ 如果您想讓磁碟上的資料無法存取、但仍能重複使用磁碟、請清理磁碟：

```
disk encrypt  
sanitize -all
```

◦ 如果您想讓磁碟上的資料無法存取、而且不需要儲存磁碟、請銷毀磁碟：

```
disk encrypt  
destroy disk_id1  
disk_id2 ...
```



◦ `disk encrypt sanitize` 和 `disk encrypt destroy` 命令僅保留用於維護模式。這些命令必須在每個HA節點上執行、而且無法用於中斷的磁碟。

h. 針對合作夥伴節點重複這些步驟。如此一來、儲存系統就會處於永久停用狀態、並清除所有資料。若要再次使用系統、您必須重新設定。

儲存系統可提供電力、您必須立即切斷資料

<p>a. 如果您想要使磁碟上的資料無法存取且仍能重複使用磁碟、請清理磁碟：</p> <p>b. 如果儲存系統設定為HA配對、請停用接管功能。</p> <p>c. 將權限層級設為進階：</p> <pre>set -privilege advanced</pre> <p>d. 如果磁碟機處於FIPS相容模式、請將節點的FIPS驗證金鑰ID設回預設MSID：</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. 清理磁碟：</p> <pre>storage encryption disk sanitize -disk * -force-all-states true</pre>	<p>a. 如果您想要使磁碟上的資料無法存取、而且不需要儲存磁碟、請銷毀磁碟：</p> <p>b. 如果儲存系統設定為HA配對、請停用接管功能。</p> <p>c. 將權限層級設為進階：</p> <pre>set -privilege advanced</pre> <p>d. 銷毀磁碟： storage encryption disk destroy -disk * -force -all-states true</p>	<p>儲存系統會出現問題、使系統處於永久停用狀態、並清除所有資料。若要再次使用系統、您必須重新設定。</p>
<p>KMIP伺服器可供電、但儲存系統無法供電</p>	<p>a. 登入 KMIP 伺服器。</p> <p>b. 銷毀與FIPS磁碟機或SED相關的所有金鑰、這些金鑰包含您要防止存取的資料。如此可防止儲存系統存取磁碟加密金鑰。</p>	<p>KMIP伺服器或儲存系統無法使用電源</p>

相關資訊

- ["儲存加密磁碟銷毀"](#)
- ["儲存加密磁碟修改"](#)
- ["儲存加密磁碟清理"](#)

## 版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

## 商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。