



使 **FIPS** 驱动器或 **SED** 上的数据无法访问 ONTAP 9

NetApp
April 24, 2024

目录

- 使 FIPS 驱动器或 SED 上的数据无法访问 1
 - 使 FIPS 驱动器或 SED 上的数据无法访问概述 1
 - 清理 FIPS 驱动器或 SED 1
 - 销毁 FIPS 驱动器或 SED 3
 - 紧急粉碎FIPS驱动器或SED上的数据 4

使 FIPS 驱动器或 SED 上的数据无法访问

使 FIPS 驱动器或 SED 上的数据无法访问概述

如果要使 FIPS 驱动器或 SED 上的数据永久不可访问，但要为新数据保留驱动器的未用空间，则可以对磁盘进行清理。如果要使数据永久不可访问且无需重复使用驱动器，可以将其销毁。

- 磁盘清理

清理自加密驱动器时，系统会将磁盘加密密钥更改为新的随机值，将开机锁定状态重置为 `false`，并将密钥 ID 设置为默认值，即制造商安全 ID 0x0（SAS 驱动器）或空密钥（NVMe 驱动器）。这样做会使磁盘上的数据无法访问且无法检索。您可以将已清理的磁盘重复用作未置零的备用磁盘。

- 磁盘销毁

销毁 FIPS 驱动器或 SED 后，系统会将磁盘加密密钥设置为未知的随机值，并永久锁定磁盘。这样做会使磁盘永久不可用，并且磁盘上的数据永久不可访问。

您可以清理或销毁节点的单个自加密驱动器或所有自加密驱动器。

清理 FIPS 驱动器或 SED

如果要使 FIPS 驱动器或 SED 上的数据永久不可访问、并使用该驱动器存储新数据、则可以使用 `storage encryption disk sanitize` 命令以对驱动器进行磁盘管理。

关于此任务

清理自加密驱动器时，系统会将磁盘加密密钥更改为新的随机值，将开机锁定状态重置为 `false`，并将密钥 ID 设置为默认值，即制造商安全 ID 0x0（SAS 驱动器）或空密钥（NVMe 驱动器）。这样做会使磁盘上的数据无法访问且无法检索。您可以将已清理的磁盘重复用作未置零的备用磁盘。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 将需要保留的所有数据迁移到另一个磁盘上的聚合。
2. 删除要清理的 FIPS 驱动器或 SED 上的聚合：

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

有关完整的命令语法，请参见手册页。

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

3. 确定要清理的 FIPS 驱动器或 SED 的磁盘 ID：

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

有关完整的命令语法，请参见手册页。

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. 如果 FIPS 驱动器以 FIPS 兼容模式运行，请将节点的 FIPS 身份验证密钥 ID 设置回默认 MSID 0x0：

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

您可以使用 `security key-manager query` 用于查看密钥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. 清理驱动器：

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

您只能使用此命令清理热备用磁盘或损坏的磁盘。要清理所有磁盘、而不管其类型如何、请使用 `-force -all-state` 选项有关完整的命令语法，请参见手册页。



ONTAP将提示您输入确认短语、然后再继续。输入屏幕上所示的短语。

```
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.

销毁 FIPS 驱动器或 SED

如果要使FIPS驱动器或SED上的数据永久不可访问、并且不需要重复使用该驱动器、则可以使用 `storage encryption disk destroy` 命令销毁磁盘。

关于此任务

销毁 FIPS 驱动器或 SED 后，系统会将磁盘加密密钥设置为未知的随机值，并永久锁定该驱动器。这样做会使磁盘几乎不可用，并且磁盘上的数据永远不可访问。但是，您可以使用磁盘标签上印有的物理安全 ID （PSID）将磁盘重置为出厂配置的设置。有关详细信息，请参见 ["丢失身份验证密钥后，使 FIPS 驱动器或 SED 恢复正常运行"](#)。



除非您拥有不可退回的磁盘加载服务（NRD Plus），否则不应销毁 FIPS 驱动器或 SED。销毁磁盘将使其保修失效。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 将需要保留的所有数据迁移到另一个磁盘上的聚合。
2. 删除要销毁的 FIPS 驱动器或 SED 上的聚合：

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

有关完整的命令语法，请参见手册页。

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

3. 确定要销毁的 FIPS 驱动器或 SED 的磁盘 ID：

```
storage encryption disk show
```

有关完整的命令语法，请参见手册页。

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. 销毁磁盘：

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

有关完整的命令语法，请参见手册页。



系统将提示您输入确认短语，然后再继续。输入屏幕上所示的短语。

```
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.
```

紧急粉碎FIPS驱动器或SED上的数据

在发生安全紧急情况时，您可以立即阻止访问 FIPS 驱动器或 SED ，即使存储系统或 KMIP 服务器没有电源也是如此。

开始之前

- 如果您使用的 KMIP 服务器没有电源，则必须为 KMIP 服务器配置一个易于销毁的身份验证项（例如，智能卡或 USB 驱动器）。
- 您必须是集群管理员才能执行此任务。

步骤

- 1. 对 FIPS 驱动器或 SED 上的数据执行紧急粉碎：

条件	那么 ...
----	--------

<p>存储系统已通电，您有时间使存储系统正常脱机</p>	<ol style="list-style-type: none"> 如果存储系统配置为 HA 对，请禁用接管。 使所有聚合脱机并将其删除。 将权限级别设置为高级： <pre>set -privilege advanced</pre> 如果驱动器处于 FIPS 兼容模式，请将节点的 FIPS 身份验证密钥 ID 重新设置为默认 MSID： <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> 暂停存储系统。 启动至维护模式： 清理或销毁磁盘： <ul style="list-style-type: none"> 如果要使磁盘上的数据无法访问、并且仍然能够重复使用这些磁盘、请清理这些磁盘： <pre>disk encrypt sanitize -all</pre> 如果要使磁盘上的数据无法访问、并且不需要保存磁盘、请销毁磁盘： <pre>disk encrypt destroy disk_id1 disk_id2 ...</pre> <div data-bbox="699 1472 756 1528">  </div> <div data-bbox="818 1297 1016 1709"> <p>。 disk encrypt sanitize 和 disk encrypt destroy 命令仅保留用于维护模式。这些命令必须在每个 HA 节点上运行，并且不适用于损坏的磁盘。</p> </div> 对配对节点重复上述步骤。这会使存储系统处于永久禁用状态，并擦除所有数据。要再次使用系统，必须重新配置它。	<p>存储系统已通电，您必须立即粉碎数据</p>
------------------------------	--	--------------------------

<p>a. * 如果要使磁盘上的数据无法访问且仍能重复使用这些磁盘，请清理磁盘： *</p> <p>b. 如果存储系统配置为 HA 对，请禁用接管。</p> <p>c. 将权限级别设置为高级：</p> <pre>set -privilege advanced</pre> <p>d. 如果驱动器处于 FIPS 兼容模式，请将节点的 FIPS 身份验证密钥 ID 重新设置为默认 MSID：</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. 清理磁盘：</p> <pre>storage encryption disk sanitize -disk * -force-all-states true</pre>	<p>a. * 如果要使磁盘上的数据无法访问，并且不需要保存磁盘，请销毁磁盘： *</p> <p>b. 如果存储系统配置为 HA 对，请禁用接管。</p> <p>c. 将权限级别设置为高级：</p> <pre>set -privilege advanced</pre> <p>d. 销毁磁盘： storage encryption disk destroy -disk * -force -all-states true</p>	<p>存储系统崩溃，使系统处于永久禁用状态，并擦除所有数据。要再次使用系统，必须重新配置它。</p>
<p>KMIP 服务器可以通电，但存储系统不能通电</p>	<p>a. 登录到KMIP服务器。</p> <p>b. 销毁与包含要阻止访问的数据的 FIPS 驱动器或 SED 关联的所有密钥。这样会阻止存储系统访问磁盘加密密钥。</p>	<p>KMIP 服务器或存储系统不能通电</p>

有关完整的命令语法，请参见手册页。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。