



FIPSドライブまたは**SED**のデータにアクセス できないようにする ONTAP 9

NetApp
December 20, 2024

目次

FIPSドライブまたはSEDのデータにアクセスできないようにする	1
FIPSドライブまたはSEDのデータにアクセスできない概要	1
FIPSドライブまたはSEDの完全消去	1
FIPSドライブまたはSEDの破棄	3
FIPSドライブまたはSEDの緊急時のシュレッドデータ	5

FIPSドライブまたはSEDのデータにアクセスできないようにする

FIPSドライブまたはSEDのデータにアクセスできない概要

FIPSドライブまたはSEDのデータに永久にアクセスできない状態にし、ドライブの未使用スペースを新しいデータに使用できるようにしておく場合は、ディスクを完全消去できます。データに永久にアクセスできない状態にし、ドライブを再利用する必要もない場合は、ディスクを破棄できます。

- ディスク完全消去

自己暗号化ドライブを完全消去すると、ディスク暗号化キーが新しいランダムな値に変更され、電源オンロックの状態がfalseにリセットされ、キーIDがデフォルト値のManufacturer Secure ID 0x0（SASドライブ）またはnullキー（NVMeドライブ）に設定されます。これにより、ディスクのデータにアクセスできない状態になり、データを取得できなくなります。完全消去したディスクは、初期化されていないスペアディスクとして再利用できます。

- ディスクの破棄

FIPSドライブまたはSEDを破棄すると、ディスク暗号化キーが不明なランダム値に設定され、ディスクが完全にロックされます。これにより、ディスクが永続的に使用できない状態になり、ディスクのデータに永久にアクセスできなくなります。

完全消去と破棄は、個々の自己暗号化ドライブまたはノードのすべての自己暗号化ドライブに対して実行できます。

FIPSドライブまたはSEDの完全消去

FIPSドライブまたはSEDのデータに永久にアクセスできない状態にし、そのドライブを新しいデータに使用する場合は、コマンドを使用してドライブを完全消去できます

```
storage encryption disk sanitize。
```

タスクの内容

自己暗号化ドライブを完全消去すると、ディスク暗号化キーが新しいランダムな値に変更され、電源オンロックの状態がfalseにリセットされ、キーIDがデフォルト値のManufacturer Secure ID 0x0（SASドライブ）またはnullキー（NVMeドライブ）に設定されます。これにより、ディスクのデータにアクセスできない状態になり、データを取得できなくなります。完全消去したディスクは、初期化されていないスペアディスクとして再利用できます。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 保持する必要があるデータを別のディスク上のアグリゲートに移行します。
2. 完全消去するFIPSドライブまたはSEDのアグリゲートを削除します。

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

コマンド構文全体については、マニュアルページを参照してください。

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

3. 完全消去するFIPSドライブまたはSEDのディスクIDを確認します。

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

コマンド構文全体については、マニュアルページを参照してください。

```
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. FIPSドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDである0x0に戻します。

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

キーIDは、コマンドを使用して表示できます `security key-manager query`。

```
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. ドライブを完全消去します。

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

このコマンドを使用して完全消去できるのは、ホットスペアディスクまたは破損ディスクのみです。タイプに関係なくすべてのディスクを完全消去するには、オプションを使用し `-force-all-state` ます。コマンド構文全体については、マニュアルページを参照してください。



続行する前に、確認フレーズの入力を求めるプロンプトがONTAPに表示されます。画面に表示されたフレーズを正確に入力します。

```
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. 完全消去したディスクの障害状態を解除します。 `storage disk unfailed -spare true -disk disk_id`
7. ディスクに所有者があるかどうかを確認します `storage disk show -disk disk_id`。 +ディスクに所有者がない場合は、所有者を割り当てます。 `storage disk assign -owner node -disk disk_id`
8. 完全消去するディスクを所有するノードのノードシェルに切り替えます。

```
system node run -node node_name
```

コマンドを実行します `disk sanitize release`。

9. ノードシェルを終了します。ディスクの障害状態を再度解除します。 `storage disk unfailed -spare true -disk disk_id`
10. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。 `storage disk show -disk disk_id`

FIPSドライブまたはSEDの破棄

FIPSドライブまたはSEDのデータに永久にアクセスできない状態にし、ドライブを再利用する必要もない場合は、コマンドを使用してディスクを破棄できます `storage encryption disk destroy`。

タスクの内容

FIPSドライブまたはSEDを破棄すると、ディスク暗号化キーが不明なランダム値に設定され、ドライブが完全にロックされます。これにより、ディスクが実質的に使用できない状態になり、ディスクのデータに永久にアクセスできなくなります。ただし、ディスクのラベルに印刷されているPhysical Secure ID (PSID; 物理的なセキュアID) を使用して、ディスクを工場出荷時の設定にリセットすることができます。詳細については、を参照してください ["認証キーが失われた場合にFIPSドライブまたはSEDを使用可能な状態に戻す"](#)。



障害ディスク返却不要サービス (NRD Plus) を利用している場合を除き、FIPSドライブまたはSEDは破棄しないでください。ディスクを破棄すると保証が無効になります。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 保持する必要があるデータを別のディスク上のアグリゲートに移行します。
2. 破棄する FIPS ドライブまたは SED のアグリゲートを削除します。

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

コマンド構文全体については、マニュアルページを参照してください。

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

3. 破棄する FIPS ドライブまたは SED のディスク ID を確認します。

```
storage encryption disk show
```

コマンド構文全体については、マニュアルページを参照してください。

```
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. ディスクを破棄します。

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

コマンド構文全体については、マニュアルページを参照してください。



続行する前に確認のフレーズを入力するように求められます。画面に表示されたフレーズを正確に入力します。

```
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.
```

FIPSドライブまたはSEDの緊急時のシュレッドデータ

セキュリティに関する緊急事態が発生した場合は、ストレージシステムまたはKMIPサーバへの給電が遮断されていても、FIPSドライブまたはSEDへのアクセスを即座に禁止できます。

開始する前に

- 使用可能な電力が供給されていないKMIPサーバを使用している場合は、破棄しやすい認証アイテム（スマートカードやUSBドライブなど）を使用してKMIPサーバを設定する必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. FIPSドライブまたはSEDのデータの緊急時のシュレディングを実行します。

状況	そしたら...
----	---------

<p>ストレージシステムに給電されており、ストレージシステムを正常にオフラインにする時間がある</p>	<ol style="list-style-type: none"> a. ストレージシステムがHAペアとして構成されている場合は、テイクオーバーを無効にします。 b. すべてのアグリゲートをオフラインにしてから削除します。 c. 権限レベルをadvancedに設定します。 + set -privilege advanced d. ドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDに戻します。 + storage encryption disk modify -disk * -fips-key-id 0x0 e. ストレージシステムを停止します。 f. メンテナンスモードでブートします。 g. ディスクを完全消去するか破棄します。 <ul style="list-style-type: none"> ◦ ディスクのデータにアクセスできない状態にしてディスクを再利用する場合は、ディスクを完全消去します。 + disk encrypt sanitize -all ◦ ディスクのデータにアクセスできない状態にし、ディスクを保存する必要もない場合は、ディスクを破棄します。 + disk encrypt destroy disk_id1 disk_id2 ... 	<p>ストレージシステムに給電されており、データをただちにシュレツディングする必要がある</p>
---	---	--

<p>a. * ディスク上のデータにアクセスできない状態にし、ディスクを再利用する場合は、ディスクを完全消去します。 *</p> <p>b. ストレージシステムがHAペアとして構成されている場合は、テイクオーバーを無効にします。</p> <p>c. 権限レベルをadvancedに設定します。</p> <pre>set -privilege advanced</pre> <p>d. ドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDに戻します。</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. ディスクを完全消去します。</p> <pre>storage encryption disk sanitize -disk * -force-all-states true</pre>	<p>a. * ディスク上のデータにアクセスできない状態にし、ディスクを保存する必要もない場合は、ディスクを破棄してください： *</p> <p>b. ストレージシステムがHAペアとして構成されている場合は、テイクオーバーを無効にします。</p> <p>c. 権限レベルをadvancedに設定します。</p> <pre>set -privilege advanced</pre> <p>d. ディスクを破棄します。</p> <pre>storage encryption disk destroy -disk * -force-all-states true</pre>	<p>ストレージシステムがパニック状態になり、システムは永続的に無効な状態になり、すべてのデータが消去されます。システムを再度使用するには、再設定する必要があります。</p>
<p>KMIPサーバに給電されているが、ストレージシステムには給電されていない</p>	<p>a. KMIPサーバにログインします。</p> <p>b. アクセスを禁止するデータを含むFIPSドライブまたはSEDに関連付けられているすべてのキーを破棄します。これにより、ストレージシステムからディスク暗号化キーにアクセスできなくなります。</p>	<p>KMIPサーバまたはストレージシステムに給電されていない</p>

コマンド構文全体については、マニュアルページを参照してください。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。