FIPS ドライブまたは SED のデータにアクセスできない状態にします

ONTAP 9

NetApp
April 24, 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状態にします

FIPS ドライブまたは SED のデータにアクセスできない概要を確認します

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は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 （ SAS ；メーカーのセキュア ID ） 0x0 （ SAS ドライブ）または null （ 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。完全消去されたディスクは、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 を完全消去します

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て、そのドライブを新しいデータに使用する場合は、を使用できます `storage encryption disk sanitize` コマンドを使用してドライブを完全消去します。

このタスクについて

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 （ SAS ；メーカーのセキュア ID ） 0x0 （ SAS ドライブ）または null （ 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。完全消去されたディスクは、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。

作業を開始する前に

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. 保持する必要のあるデータを別のディスク上のアグリゲートにすべて移行します。

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
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

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`

   を使用できます `security key-manager query` キーIDを表示するコマンド。

   ```
   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`

   このコマンドで完全消去できるのは、ホットスペアディスクと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、を使用します `-force-all-state` オプションコマンド構文全体

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.
```

FIPS ドライブまたは SED を破棄します

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、を使用できます `storage encryption disk destroy` コマンドを使用してディスクを破棄します。

このタスクについて

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はできます。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"。

> （故障）ディスク返却不要サービス（ NRD Plus ）を契約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。

作業を開始する前に

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. 保持しておく必要のあるデータを別のディスク上のアグリゲートにすべて移行します。
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
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

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 へのアクセスをただちに禁止できます。

作業を開始する前に

- 使用可能な電力がない KMIP サーバを使用している場合は、 KMIP サーバで簡単に破棄できる認証アイテム（スマートカードや USB ドライブなど）が設定されている必要があります。
- 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ッディングを実行します。

状況	作業

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適切な手順でオフラインにする時間があります	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。 ◦ ディスクのデータにアクセスできない状態にし、ディスクを再利用できるようにするには、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 …`	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ッディングする必要があります

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。 *
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。
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. ディスクを完全消去します。
`storage encryption disk sanitize -disk * -force-all-states true`
	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： *
	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。
	c. 権限レベルを advanced に設定します。
	`set -privilege advanced`
	d. ディスクを破棄します。
	`storage encryption disk destroy -disk * -force-all-states true`
		ストレージシステムがパニック状態になります。これで、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。

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	a. KMIPサーバにログインします。 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。	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

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。