使用 Sedutil 设置 TCG Ruby

摘要

本文档介绍了如何通过名为 sedutil 的工具设置符合 Ultrastar® DC SN640 或 DC SN840 NVMe™ TCG Ruby 标准的 SSD。本文将介绍 TCG Ruby 规范的基础知识、Western Digital 的实施以及一些关键的范围操作。本文档还将介绍“sedutil”工具，并使用 sedutil 识别 TCG Ruby 驱动器、设置密码、设置频段以及锁定和解锁驱动器。

本文档不讨论 TCG Ruby 加密细节。更多信息可从可信计算组网站下载。请参阅文档末尾的注释。

TCG Ruby

TCG Ruby 的目的是提供最新的企业安全子系统类 (SSC)，以支持 NVMe 数据中心驱动器，并简化实施和集成。

它是更广泛的 Opal SSC（如 Pyrite 和 Opalite）的一部分，并与 Opal 系列具有协议兼容性。然而，TCG Ruby 所支持的功能略有限制，因为某些功能不被认为与企业级驱动器相关。例如，预启动身份验证支持是可选的。

Western Digital 对 TCG Ruby 规范的特定实现（参见下面 Opal v2.01 和 TCG Ruby 的比较）使其与 Opal 非常相似，但不支持 预启动身份验证。1、2

|  |  |  |
| --- | --- | --- |
| **功能** | **Opal V2.01** | **TCG Ruby** |
| **激活与生命周期** | 是 | 是 |
| **管理员、用户数量** | 4 名管理员、8 名用户 | 1 名管理员、2 名用户 |
| **所需逻辑块寻址 (LBA) 范围的最小数量** | 全局范围 +8 | 全局范围（Western Digital 驱动器上为 +8） |
| **最小 数据存储 大小** | 10MB | 128 KB |
| **最小 MBR 表大小** | 128MB | 可选：如果支持，则为 128MB |
| **可配置访问控制** | 是 | 是 |
| **PSID** | 是 | 是 |
| **介质加密** | 必需 | 必需 |
| **加密擦除** | Revert、Revert SP、GenKey 用于设备和锁定范围级别擦除粒度的方法 | 与 Opal 相同 |

逻辑块寻址 (LBA) 范围是 LBA 的跨度，驱动器可以将其划分为多个部分，这些部分共享相同的加密详细信息。适用一些规则：

1. 范围不能重叠，除非是范围 0，根据定义，它是一个包含驱动器全部容量的全局范围。

2. 一旦通过定义起始 LBA 和 LBA 计数设置了范围，就可以将其锁定为写入或读/写。

3. 任何锁定都必须在锁定设置生效之前启用：“锁定启用”禁用后，锁定功能将失效，尽管范围仍保持不变。

4. 范围可以通过重新加密来加密擦除，这将更改该范围的加密密钥。

SID 是可用于向驱动器进行身份验证并最初冻结或移除其他实体的实体。

Admin1 是所有范围的管理员：它可以操作任何范围并执行任何更改。User1 和 User2 是访问权限可配置的实体。例如，它们可能被允许仅在某些特定范围内操作，或者不被允许擦除数据，而只能锁定这些范围上的读写操作。

下载并编译 Sedutil 工具

第一步是从 GitHub 下载工具并编译它们。本文档中的测试是在 Linux® Ubuntu 18.04.03 上执行的（它需要在启动时设置内核开关 *libata\_tpm* ），但特定工具版本也应该在 Windows 和 FreeBSD 上工作。Windows 编译需要 VSC 2015 或更高版本。

下载和编译命令如下：请注意，git 将在运行它的任何目录中创建一个名为 sedutil 的目录。如果需要不同的目录，请查阅 git 手册以获取帮助。

*git clone*

*autoreconf -i*

*./configure*

*make*

*(make install) // 如果您不想在系统范围内安装该工具，则不需要*

在流程结束时，工具将被编译，源目录中将有一个名为 *sedutil-cli*  的可执行文件。可执行文件 *sedutil-cli*  可能会在执行最后一条命令时在系统范围内安装。

控制驱动器

下一步是扫描系统中的驱动器并检查兼容驱动器。在此示例中，驱动器符合 TCG Ruby 标准，这通过驱动器旁边的一个小写字母 r 表示，如图 1 所示。

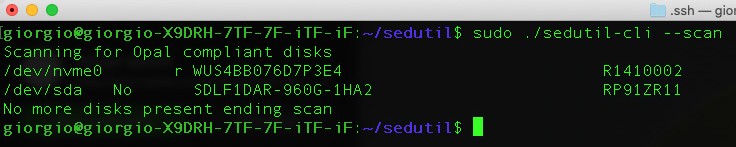


图 1.扫描系统中的驱动器

可以查询驱动器支持的功能，请参见下面的图 2：请注意，对于带有 TCG Ruby 的 Ultrastar DC SN640 或 DC SN840，逻辑块大小为 512 字节。

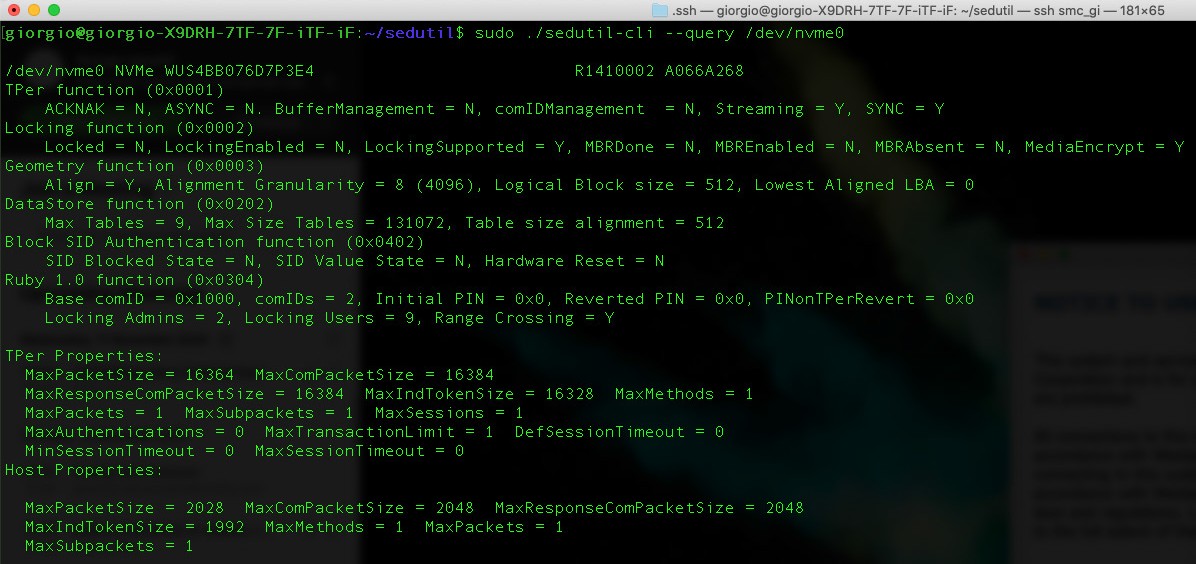


图 2。Ultrastar DC SN640 驱动器型号查询

控制驱动器的过程称为“获取所有权”。这将把最初设置为电子可读值（称为 MSID）的默认密码（SID 和 admin1）更改为您的密码。

使用 sedutil，这涉及发出图 3 中的命令，将密码（在此示例中）更改为“test”：



图 3.获取所有权

图 3 中显示的错误消息是由于 TCG Ruby 实现不支持 MBR 引导，可以安全地忽略。请注意，admin1 和 SID 密码都已更改。以下所有命令均使用admin1密码，最终SID和admin1可以逐一更改。

此时加密已初始化，密码现在与其默认值不同。初始设置后将 SID 和 Admin1 密码更改为不同的值是一种很好的做法。这可以通过以下方式实现：

*--setSIDPassword <SIDPassword> <newSIDPassword> <设备>*

*--setPassword <旧密码> admin1 <新密码> <设备>*

请注意，除了 *revertTPer*  命令（将驱动器恢复为默认值）和 *PSIDrevert*  命令（使用驱动器标签上打印的 PSID）外，任何命令都使用 admin1 密码。

设置频段和锁定

TCG Ruby 兼容设备至少有一个全局频段（称为 band0），也可以有更多。在西部数据的实施中，最多支持 8 个频段。您可以使用以下命令列出波段及其状态

*--listlockingranges*，如图4所示。

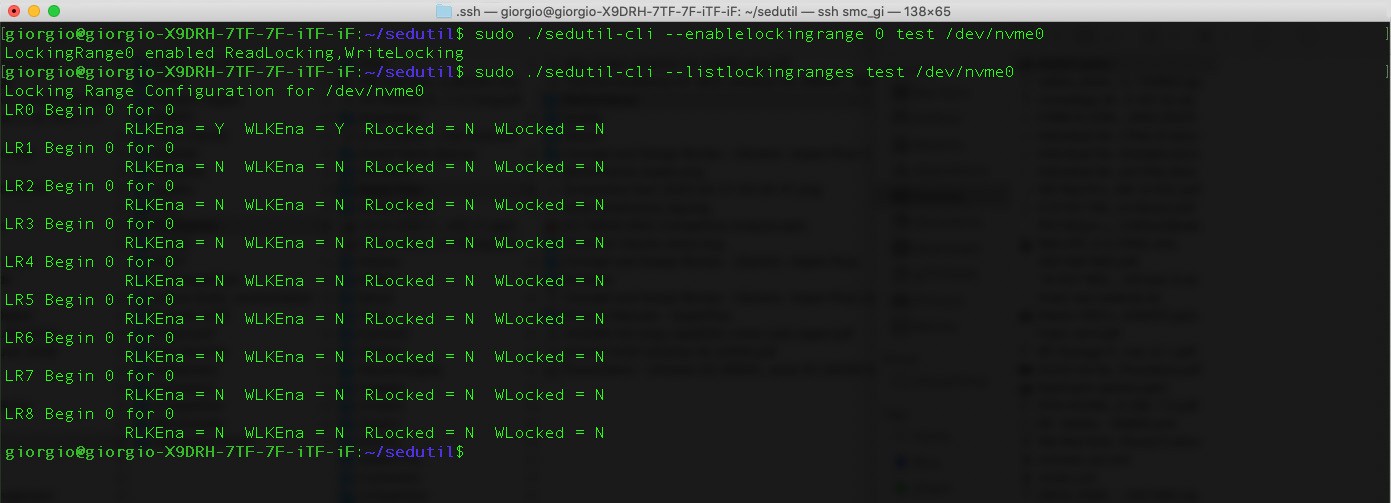


图 4.列出并启用全局范围

锁定频带包含两个步骤：读取或读写操作需要锁定（体现在 *RLocked*、*WLocked* 中），同时需要启用写入和读取锁定（体现在 *RLKEna*  和 *WLKEna* 中）。设置锁定但不启用 将导致无法锁定。

图 4 演示了如何启用全局范围（使用选项 *--enablelockingrange*  并使用我们的密码“test”），然后列出频段的状态。

在这种情况下，8 个频段未定义，并且全局频段已启用。

接下来是设置一个频段的示例，具体来说是频段 1。

带定义为从一个块号（在我们的例子中为 512 字节，请参阅开头的查询以了解每种驱动器类型的具体值）开始，并从该块延伸一定数量的块。除了全局频带（根据定义，其覆盖整个容量）之外，其他频带不能重叠。

图 5 演示了如何使用选项 *-- setuplockingrange <band#> <from block #> <to block #> 设置从区块 0 开始的 2000 个区块的 band1。*图 5 中的密码为“test”：

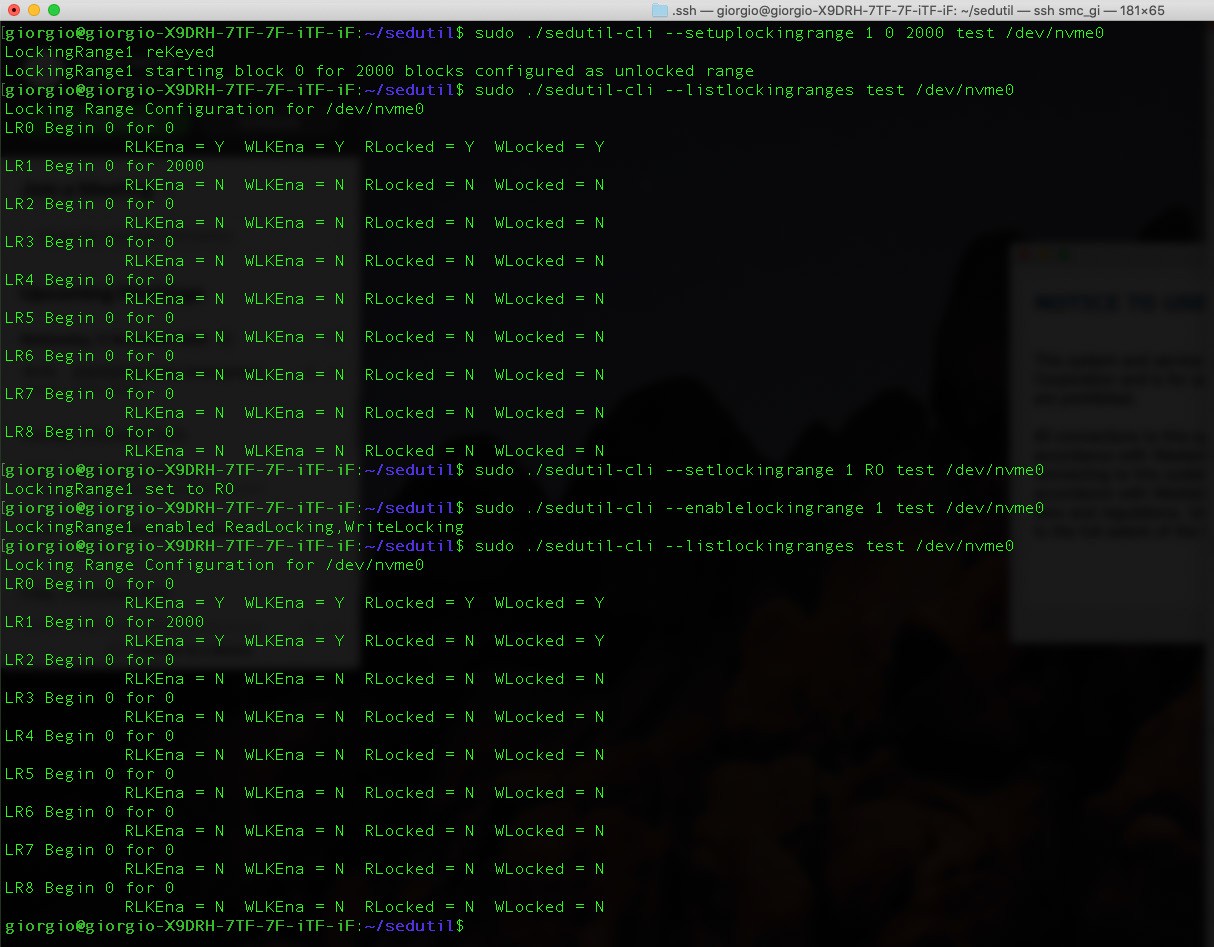


图 5. 设置 band1

此时，波段 1（或锁定范围）已设置并写入锁定（*WLocked=Y*）。–此示例使用带有 RO（只读）开关的 *--setlockingrange*  选项。如果需要，还可以使用 LK 开关启用完整锁定，使用 RW 将其删除。

测试锁定的驱动器

可以测试锁定的驱动器，并且只有当锁被禁用时才可以写入。图 6 证明了这一点。



图 6.启用和禁用锁定

执行的操作列表如下：

1.启用锁定（尽管使用此命令仅选择了写锁，但我们同时启用锁定并设置锁定）。

2.尝试使用 dd 写入驱动器。命令失败。

3.禁用锁定。

4.写入设备，成功。

最后，可以重新设置锁定范围，这将改变该特定频段的加密密钥。这将正确擦除乐队，因为原始密钥已被更改并且无法恢复。

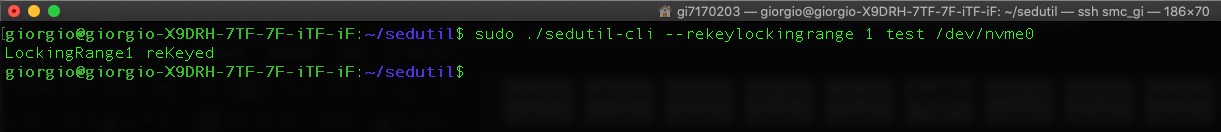


图 7.重新锁定范围 1

恢复默认设置

您可以使用 *--revertNoErase* 恢复默认设置而不擦除驱动器，如图 8 所示。

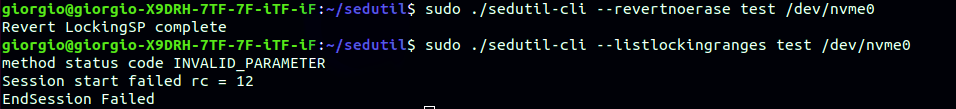


图 8.Revertnoerase 命令

SID 密码丢失时恢复默认设置

如果您忘记了密码，则可以随时将驱动器重置为默认值，尽管会通过 PSID 密码丢失所有数据，该密码写在磁盘的标签上（图 8），并且无法从驱动器中以电子方式读取。



PSID 位置

图9.标签上的PSID位置

该命令明确警告您有关删除数据（图 9）。

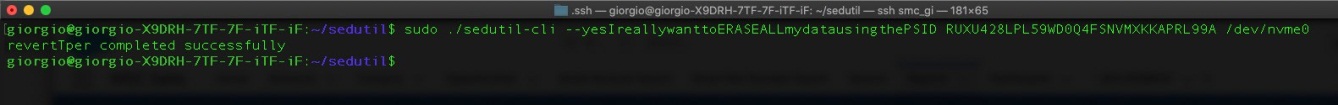


图 10.使用 PSID 恢复默认设置

结论

本文介绍了一个开源sedutil工具，该工具允许用户在Ultrastar DC SN640 或 DC SN840 NVMe SSD TCG Ruby 兼容 SSD 上配置加密。已经讨论了基本概念和命令，展示了如何控制驱动器、加密数据、擦除驱动器以及将驱动器恢复为默认值。

参考

1https://trustedcomputinggroup.org/wp-content/uploads/TCG\_Storage\_SSC\_Ruby\_v1\_r1\_pub.pdf

2https://trustedcomputinggroup.org/wp-content/uploads/TCG\_Storage-Opal\_SSC\_v2.01\_rev1.00.pdf

3https://

4https://trustedcomputinggroup.org/wp-content/uploads/Storage-Ruby-SSC-v1.0-Specification-FAQ \_20182811\_Final.pdf

5https://nvmexpress.org/wp-content/uploads/TCGandNVMe\_Joint\_White\_Paper-TCG\_Storage\_Opal\_and\_NVMe\_FINAL.pdf

|  |  |
| --- | --- |
| **西部数据。** |  |
|  |  |
|  |  |
| 大橡树大道 5601 号  美国加利福尼亚州圣何塞 95119  www.westerndigital.com | © 2021 西部数据公司或其附属公司。版权所有。  Western Digital、Western Digital 徽标和 Ultrastar 是 Western Digital Corporation 或其附属公司在美国和/或其他国家/地区的注册商标或商标。NVMe 文字商标和 NVMe 徽标商标是 NVM Express, Inc. 的商标。所有其他商标均属于其各自所有者的财产。所有其他商标均属于其各自所有者的财产。 |