White Paper

Verification of TCG Opal SSC

TCG Opal SSC

Verification for SSD Drives

Written By:

Haiyan Lin
Sr. Software Engineer

Table of Contents

List of Figures

1. Introduction

SANBlaze has announced the availability of TCG Opal SSC verification capability that allows customers to quickly and effectively test and validate the Opal SSC implementation of their SSDs. This white paper introduces the TCG Opal SSC implementation and describes how to verify that your SSDs implemented the Opal SSC specification correctly using the SANBlaze platform.

2. Understanding TCG Opal SSC

TCG (Trusted Computing Group) Storage Work Group (SWG) developed the Core Specification, officially known as *TCG Storage Architecture Core Specification*, which provides a comprehensive definition of TCG-related functions for a TCG storage device. The Core Specification can be further broken down into multiple subsets of functionality called Security Subsystem Classes (SSCs). SSCs explicitly define the minimum acceptable Core Specification capabilities of a storage device in a specific “class” and potentially expands functionality beyond what is defined in the Core Specification.

The *Opal SSC specification,* predicated on ease of implementation and integration, is also called “Opal SSC” or “Opal” for short, and is a security management protocol for storage devices. The Opal family of SSCs include Opal, Opalite, Pyrite, and Ruby and define the functionality for implementing the Core Specification on storage devices such as file management on storage devices. The Opal family of SSCs also defines class level permissions for the storage and retrieval of files, thus protecting user data. Devices conforming to Opal SSC specifications may be referred to as TCG Opal devices.

The Opal Storage specification is a set of security specifications used for applying hardware-based encryption to storage devices. In other words, it is a specification for self-encrypting drives (SEDs) such that all data on the drive is always encrypted, without the use of third-party encryption solutions. Some NVMe SSDs may implement a slimmed-down Opal, either Opalite or Pyrite.

2.1 Why TCG Opal for SSDs?

Data security for solid state drives (SSDs) remains a hot issue because most electronic storage devices are made to store data directly into flash memory spaces and they are made to do it faster, more efficiently, and in demanding environments. However, SSD devices are not born with resistance to external data threats. Some software utility application programs designed to prevent potential theft are available for use on the host computer system, but software encryption programs will slow access time to the data and overall bandwidth to the storage device due to consumption of compute resources.

As SSDs become more popular for storing sensitive data, there is a growing need for strong data encryption to mitigate the risk of data theft. One of the most recommended methods is to implement encryption within the drive. Realizing that data security is fast becoming one of the most pressing issues facing the information technology industry, most SSD manufacturers bring hardware-based full drive encryption (FDE) capability in the form of Opal Security Subsystem Class (SSC) to solid state drives as self-encrypting drives (SEDs).

Self-encrypting drives automatically encrypt data without any user interaction, and therefore have an enormous and positive impact on the protection of sensitive and confidential information in the event that a data breach should occur. In this white paper, we will look into the SED basics, advantages of SEDs and hardware encryption, and the features of Opal-compliant storage devices.

2.2 SED Basics

A Self-Encrypting Drive (SED) is a Storage Device that integrates encryption of user data at rest (DAR). All user data written to the storage device is encrypted by specialized hardware implemented inside the Storage Device controller. The data is decrypted as it is read. The encryption and decryption are performed using a Media Encryption Key (MEK) generated internally in the Storage Device.

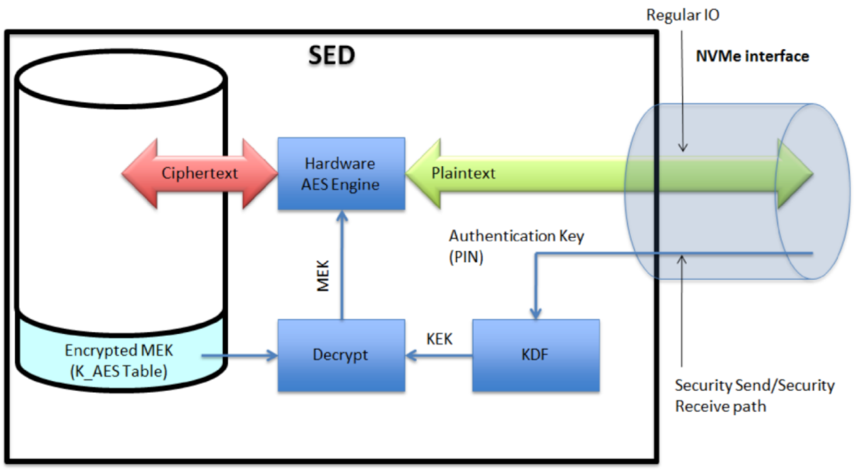


Figure 1: Self-Encrypting Drive (SED)

When an Authentication Credential has been set and the device is locked, it is not possible to access User Data. Once the correct Authentication Credential has been supplied to the Storage Device by the host, and the Storage Device is unlocked, data can be read from and written to the device.

The Authentication Credential is a value derived from the user's password, passphrase, or some other authentication mechanism. The storage device uses a value derived from the Authentication Credential as a "Key Encryption Key" or KEK. Once the Authentication Credential is set, the KEK is used to encrypt the MEK prior to MEK's storage on the media. The MEK is only stored persistently in encrypted form. Any instances of a plaintext MEK are only held internally to the Storage Device controller, and only temporarily while the Storage Device has power. When the Storage Device loses power, the plaintext MEK is lost.

After a storage device power cycle, since the plaintext MEK has been "forgotten" by the storage device, it is no longer possible to read or write data via the storage interface. The storage device is "locked". In order to gain access to user data in plaintext, it is necessary for the user to supply the correct unlock password or passphrase. The host application accepts a password as input from the user, generates an Authentication Credential from the supplied password, and sends the Authentication Credential to the storage device to attempt to unlock access to the data. If the supplied Authentication Credential is correct, the Opal firmware in the storage device will be able to successfully decrypt the encrypted MEK, which can be used to encrypt/decrypt data. If the Authentication Credential is incorrect, the Opal firmware will not be able to successfully decrypt the encrypted MEK, and data will remain inaccessible.

2.3 Advantages of SEDs and Hardware Encryption

As previously mentioned, Opal is a set of specifications developed for self-encrypting drives (SEDs) which is a special form of full drive encryption (FDE) that is always hardware-based. An SED has a hardware based encryption engine on board, often integrated into the drive's controller. It boosts better performance, security, and manageability compared to software-based FDE implementations, which commonly suffer performance degradation as a result of the encryption overhead. The Opal SSC specifications for hardware-encrypted storage devices offer distinguished advantages over a software FDE implementation as follows:

- **Performance**: Software encryption mechanisms mostly rely on CPU and memory resources in the host system. Therefore, software encryption often causes a significant and noticeable reduction in data throughput performance. On the contrary, hardware encryption does not incur the CPU and memory overhead because it transfers the computational load of the encryption process to dedicated processors and, therefore, maximizes performance. Dedicated hardware can outperform software running on a general-purpose OS-based platforms**.**

- **Data Security**: SSDs complying with Opal specifications are self-encryption devices. Therefore, cold-boot attacks do not work because the encryption key is stored in the hard drive controller instead of the system's memory where the encryption key for software-based solutions is kept. Software runs under an operating system that is vulnerable to viruses and other attacks. This exposes software-encrypted devices to attacks through the memory device, OS and BIOS. In addition, hardware-based encryption is performed in the hardware. That is, user authentication is performed by the drive before it is unlocked, independent of the OS. Hence, hardware-based encryption and user authentication offer superior protection against data breaches, loss and theft.

- **Management**: Unlike software encryption, hardware-encrypted SSDs are encrypted automatically without any user management. This provides an additional layer of security as the encryption key is generated internally and never exposed to intrusion. Since the key is self-generated and stays with the drive, encryption key management is not required**.**

2.4 Features of Opal-compliant Storage Devices

The Opal protocol associated with encryption management is developed to protect the confidentiality of user data against unauthorized access. The specifications include data structures and mechanisms for password protection and storage management. The Opal-compliant storage devices have the following features:

- **Self-encrypting devices:** Self-encrypting devices automatically and continuously encrypt the data on the devices without any user interaction. That is, data encryption is performed on the device, totally independent from the host operating system. Plus, the encryption key exists inside the device itself.

- **Pre-boot authentication:** When the drive is being accessed, the shadow MBR (Master Boot Record), or shadow disk, will request the drive password at boot. The KEK (Key Encryption Key) is used to encrypt or decrypt the MEK (Media Encryption Key), and can be supplied by the user as a password to access the drive. The software in the shadow disk requires the KEK from the user to unlock the real disk for use and to decrypt the MEK so the real disk can be read and written to. Once the correct KEK is given to the drive, the user can be authorized to access the stored data and the operating system boots normally. Pre-boot authentication provides an additional layer of security for devices compliant with TCG Opal specifications.

- **LBA-specific permissions:** Users are assigned different permissions for LBA ranges (for example namespaces) created by the device administrator. Each LBA range is password-protected and can only be accessed by users with the correct key to perform permitted actions (read/write /erase) as follows:
    - Enable/Disable additional users
    - Create and configure multiple LBA ranges
    - Assign access control of users to LBA ranges
    - Lock/Unlock LBA ranges
    - Erase LBA ranges using cryptographic erase
    - MBR shadowing

3. TCG Opal SSC Verification: SANBlaze Application Support

The SANBlaze engineering team has incorporated TCG Opal SSC testing into our platform for our customers. SANBlaze Application Support for TCG Opal SSC includes Certified by SANBlaze pre-developed test cases that allow users to start validating TCG Opal SSC support and capability right out of the box. Test cases support the following functionality:

- Locking and Encryption information display
- Factory-reset with PSID
- Password setup
- Lock with password
- Unlock with password
- Password revert
- Negative testing through scripts to check out all TCG Opal SSC features

3.1 TCG Opal SSC Verification Examples with the SANBlaze Platform

3.1.1 Locking and Encryption Information Display

The commands below will check if the target drive supports locking or not, and display encryption information:

```
[root@vlun-111 ~]# sed-util /iport0/target112 scan
/iport0/target112lun1: Locking supported, not enabled
[root@vlun-111 ~]# sed-util /iport0/target112 show -brief
Locking Feature:
 Locking Supported: 1
 Locking Enabled: 0
 Locked: 0
 Encryption Supported: 1
 MBR Enabled: 0
 MBR Done: 0
[root@vlun-111 ~]# sed-util /iport0/target112 show
Supported Security Protocol:
 Protocol 00: Security Protocol Information
 Protocol 01: TCG (Management Layer)
 Protocol 02: TCG (Communication Layer)
 Protocol ef: ATA Device Server Password
Level 0 Discovery:
 Feature 0001: Trusted Peripheral
  Sync Supported: 1
  Async Supported: 0
  ACK/NAK Supported: 0
  Buffer Mgmt Supported: 0
  Streaming Supported: 1
  ComID Mgmt Supported: 0
 Feature 0002: Locking
  Locking Supported: 1
  Locking Enabled: 0
  Locked: 0
  Encryption Supported: 1
  MBR Enabled: 0
  MBR Done: 0
 Feature 0003: Geometry
  Logical Block Size: 512
  Alignment Granularity: 16
  Lowest Aligned LBA: 0
 Feature 0201: Single User
  Number of Locking Objects Supported: 9
  Any Object in Single User Mode: 0
  All Objects in Single User Mode: 0
  Policy (Admin vs. User): 1
 Feature 0202: DataStore Tables
  Number of Tables: 9
  Size of Tables: 10485760
  Table Size Alignment: 1
 Feature 0203: Opal V2
  Base ComID: 1004
  Number of ComIDs: 2
  Range Crossing: 0
  Number of Locking SP Admins: 4
  Number of Locking SP Users: 9
  Initial C_PIN_SID PIN Indicator: 0
  Behavior of C_PIN_SID PIN after Revert: 0
 Feature 0403: Configurable Namespace Locking
  Range_P: 0
  Range_C: 0
  Maximum Key Count: 32
  Unused Key Count: 31
  Maximum Ranges Per Namespace: 0

Properties:
 MaxComPacketSize: 66048
 MaxResponseComPacketSize: 66048
 MaxPacketSize: 66028
 MaxIndTokenSize: 65540
 MaxPackets: 1
 MaxSubpackets: 1
 MaxMethods: 1
 MaxAuthentications: 5
 MaxSessions: 1
 MaxTransactionLimit: 1
 DefSessionTimeout: 0
 MaxComPacketSize: 2048
 MaxResponseComPacketSize: 2048
 MaxPacketSize: 2028
 MaxIndTokenSize: 1992
 MaxPackets: 1
 MaxSubpackets: 1
 MaxMethods: 1
MSID PIN:
 0x03: 20SZYFBYA7ZTKU6LCDJDY2L4C30NSECL
```

3.1.2 Factory-reset with PSID

The command below will perform the factory-reset with the specified PSID. It failed in the following example because we did not provide the correct PSID.

```
[root@vlun-111 ~]# PSID=0
[root@vlun-111 ~]# sed-util /iport0/target112 factory-reset -password $PSID
sed-opal sed-reverttper /iport0/target112lun1 --password 0 --psid
Not Authorized
failed with 256
```

3.1.3 Password Setup

The command below will setup the password as “123456” for lock, unlock and revert.

```
[root@vlun-111 ~]# sed-util /iport0/target112 setup -password 123456
sed-opal sed-ownership /iport0/target112lun1 --password 123456
Success
sed-opal sed-activatelsp /iport0/target112lun1 --password 123456
Success
sed-opal sed-setuplr /iport0/target112lun1 --password 123456 --user admin1 --rangeStart 0 --
rangeLength 0 --readLockEnabled --writeLockEnabled
Success
sed-opal sed-save /iport0/target112lun1 --password 123456 --user admin1 --locktype RW
Success
echo SEDPassword=123456 > /iport0/target112lun1
```

3.1.4 Lock with Password

After locking the drive with the specified password then the drive cannot be accessed, as shown below.

```
[root@vlun-111 ~]# sed-util /iport0/target112 lock -password 123456
sed-opal sed-lock-state /iport0/target112lun1 --password 123456 --user admin1 --locktype LK
Success
[root@vlun-111 ~]# io /iport0/target112lun1 Read
NVMe command Read failed, NVMe Status=286h (ACCESS_DENIED, SCT=2h, SC=86h) (96 usec)
Read failed
```

3.1.5 Unlock with Password

The user can access the drive after unlocking with the specified password.

```
[root@vlun-111 ~]# sed-util /iport0/target112 unlock -password 123456
sed-opal sed-lock-state /iport0/target112lun1 --password 123456 --user admin1 --locktype RW
Success
[root@vlun-111 ~]# io /iport0/target112lun1 Read -v
Derived additional arguments: -bs 1000 -ms 0
Allocate read buffer of 1000h bytes
Issuing CDB: 02 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00
Received CQE: 00 00 00 00 00 00 00 00 03 00 01 00 24 07 01 00
Data (showing 4096 bytes)...
00000000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
. . .
00000fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
NVMe command Read succeeded, 4096 bytes, NVMe Status=0h (SUCCESS) (122 usec)
Successful Read
```

3.1.6 Password Revert

After reverting the original password, then you cannot lock/unlock/revert with the original password.

```
[root@vlun-111 ~]# sed-util /iport0/target112 revert -password 123456
```

```
sed-opal sed-reverttper /iport0/target112lun1 --password 123456
Success
sed-opal sed-save /iport0/target112lun1 --password "" --user admin1 --locktype RW
Success
echo SEDPassword= > /iport0/target112lun1
[root@vlun-111 ~]# sed-util /iport0/target112 lock -password 123456
sed-opal sed-lock-state /iport0/target112lun1 --password 123456 --user admin1 --locktype LK
Invalid Parameter
failed with 3072
[root@vlun-111 ~]# sed-util /iport0/target112 unlock -password 123456
sed-opal sed-lock-state /iport0/target112lun1 --password 123456 --user admin1 --locktype RW
Invalid Parameter
failed with 3072
[root@vlun-111 ~]# sed-util /iport0/target112 revert -password 123456
sed-opal sed-reverttper /iport0/target112lun1 --password 123456
Not Authorized
failed with 256
```

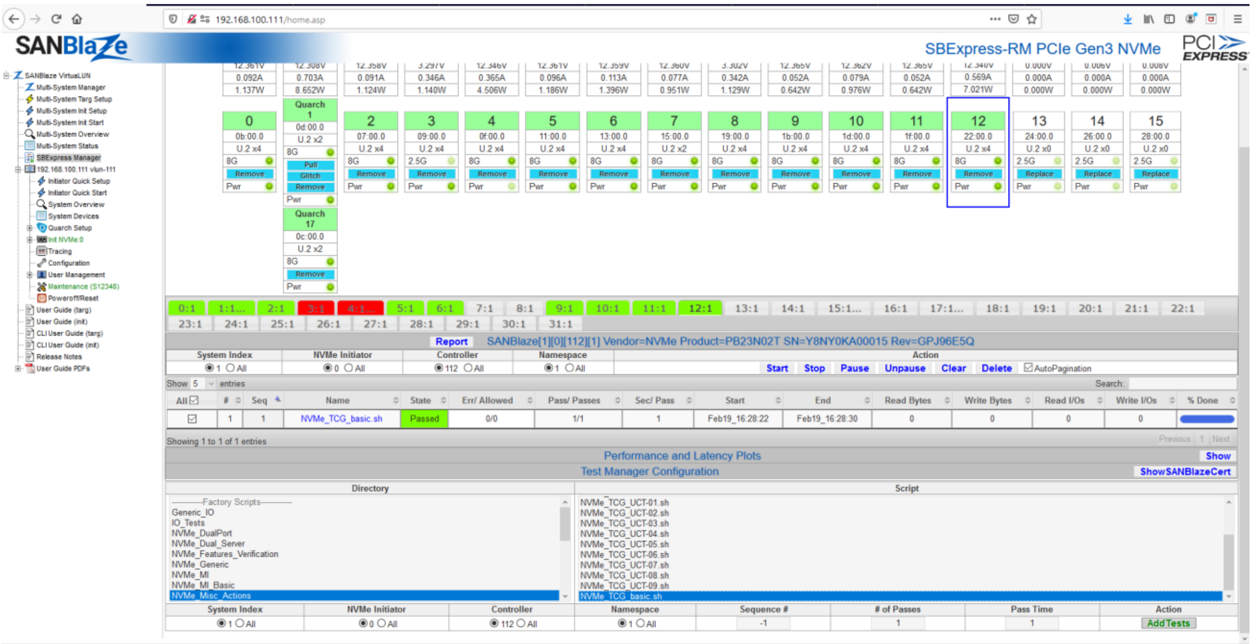
If the drive was locked before with the original password, after reverting the password the drive can now be accessed although we did not unlock it:

```
[root@vlun-111 ~]# sed-util /iport0/target112 lock -password 123456

sed-opal sed-lock-state /iport0/target112lun1 --password 123456 --user admin1 --locktype LK
Success
[root@vlun-111 ~]# io /iport0/target112lun1 Read -v
Derived additional arguments: -bs 1000 -ms 0
Allocate read buffer of 1000h bytes
Issuing CDB: 02 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00
Received CQE: 00 00 00 00 00 00 00 00 05 00 01 00 3a 07 0d 05
NVMe command Read failed, NVMe Status=286h (ACCESS_DENIED, SCT=2h, SC=86h) (96 usec)
Read failed
[root@vlun-111 ~]# sed-util /iport0/target112 revert -password 123456
sed-opal sed-reverttper /iport0/target112lun1 --password 123456
Success
sed-opal sed-save /iport0/target112lun1 --password "" --user admin1 --locktype RW
Success
echo SEDPassword= > /iport0/target112lun1
[root@vlun-111 ~]# io /iport0/target112lun1 Read -v
Derived additional arguments: -bs 1000 -ms 0
Allocate read buffer of 1000h bytes
Issuing CDB: 02 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00
Received CQE: 00 00 00 00 00 00 00 00 06 00 01 00 df 07 01 00
Data (showing 4096 bytes)...
00000000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
. . .
00000fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
NVMe command Read succeeded, 4096 bytes, NVMe Status=0h (SUCCESS) (162 usec)
Successful Read
```

3.2 TCG Opal SSC Verification Scripts Running on the SANBlaze Platform

We designed the scripts to do negative testing to check out all TCG Opal SSC features as follows. The user can select and add the test scripts to start testing.



Report SANBlaze[1][0][112][1] Vendor=NVMe Product=PB23N02T SN=Y8NY0KA00015 Rev=GPJ96E5Q

System Index	NVMe Initiator	Controller	Namespace	Action
● 1 ○ All	● 0 ○ All	● 112 ○ All	● 1 ○ All	Start Stop Pause Unpause Clear Delete ☑ AutoPagination

Show 5 entries Search:

All ☑	#	Seq	Name	State	Err/ Allowed	Pass/ Passes	Sec/ Pass	Start	End	Read Bytes	Write Bytes	Read I/Os	Write I/Os	% Done
☑	1	1	NVMe_TCG_basic.sh	Passed	0/0	1/1	1	Feb19_16:28:22	Feb19_16:28:30	0	0	0	0	

Showing 1 to 1 of 1 entries

Performance and Latency Plots Show

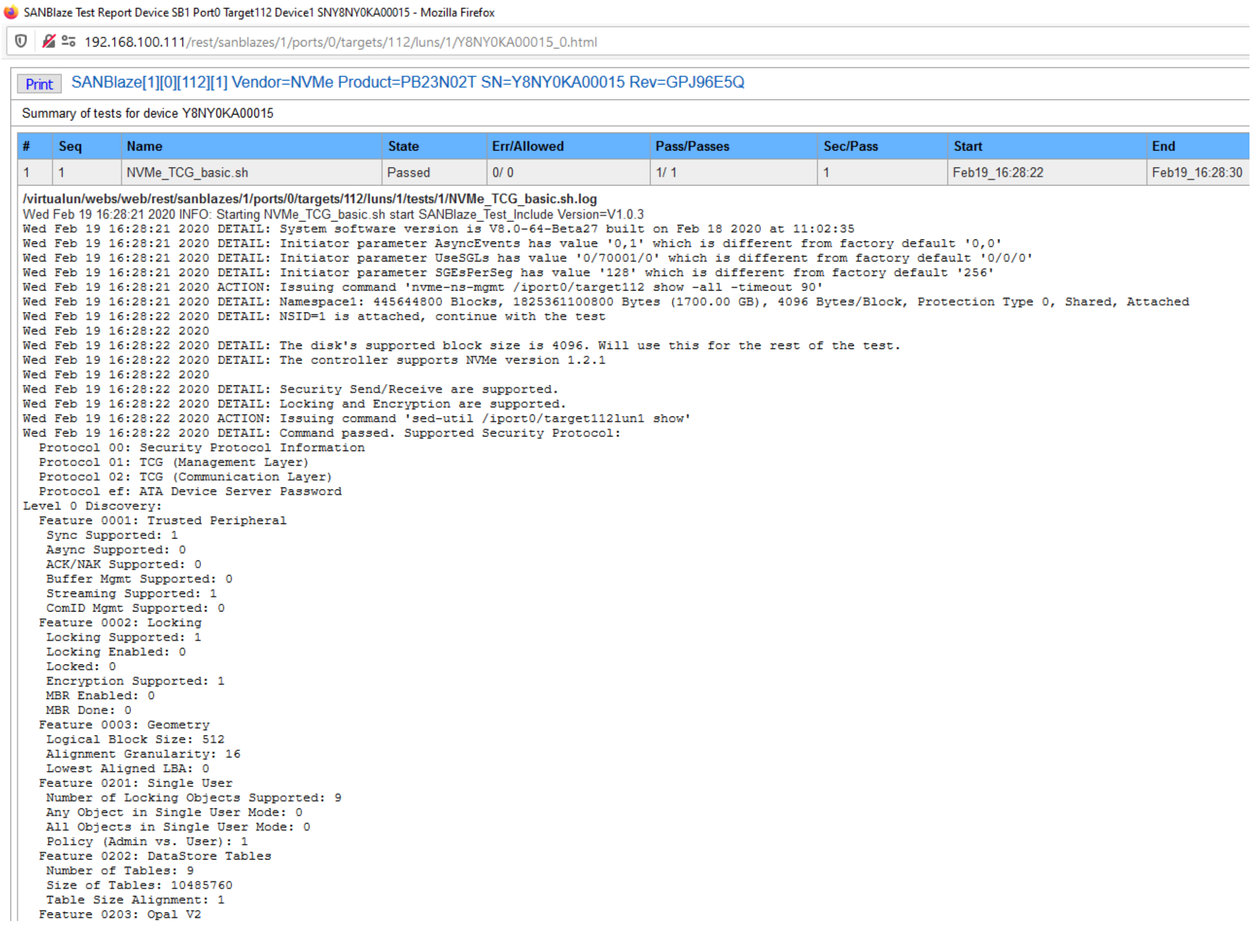
Test Manager Configuration ShowSANBlazeCert

Directory	Script
------------Factory Scripts------------ Generic_IO IO_Tests NVMe_DualPort NVMe_Dual_Server NVMe_Features_Verification NVMe_Generic NVMe_MI NVMe_MI_Basic NVMe_Misc_Actions	NVMe_TCG_UCT-01.sh NVMe_TCG_UCT-02.sh NVMe_TCG_UCT-03.sh NVMe_TCG_UCT-04.sh NVMe_TCG_UCT-05.sh NVMe_TCG_UCT-06.sh NVMe_TCG_UCT-07.sh NVMe_TCG_UCT-08.sh NVMe_TCG_UCT-09.sh NVMe_TCG_basic.sh

System Index	NVMe Initiator	Controller	Namespace	Sequence #	# of Passes	Pass Time	Action
● 1 ○ All	● 0 ○ All	● 112 ○ All	● 1 ○ All	-1	1	1	AddTests

Figure 2: Running Opal Test Scripts on the SANBlaze SBExpress Platform

The test results can be viewed “on the fly” in the web browser as follows:


SANBlaze Test Report Device SB1 Port0 Target112 Device1 SNY8NY0KA00015 - Mozilla Firefox
192.168.100.111/rest/sanblazes/1/ports/0/targets/112/luns/1/Y8NY0KA00015_0.html
Print

SANBlaze[1][0][112][1] Vendor=NVMe Product=PB23N02T SN=Y8NY0KA00015 Rev=GPJ96E5Q

Summary of tests for device Y8NY0KA00015

#	Seq	Name	State	Err/Allowed	Pass/Passes	Sec/Pass	Start	End
1	1	NVMe_TCG_basic.sh	Passed	0/ 0	1/ 1	1	Feb19_16:28:22	Feb19_16:28:30

/virtualun/webs/web/rest/sanblazes/1/ports/0/targets/112/luns/1/tests/1/NVMe_TCG_basic.sh.log

```
Wed Feb 19 16:28:21 2020 INFO: Starting NVMe_TCG_basic.sh start SANBlaze_Test_Include Version=V1.0.3
Wed Feb 19 16:28:21 2020 DETAIL: System software version is V8.0-64-Beta27 built on Feb 18 2020 at 11:02:35
Wed Feb 19 16:28:21 2020 DETAIL: Initiator parameter AsyncEvents has value '0,1' which is different from factory default '0,0'
Wed Feb 19 16:28:21 2020 DETAIL: Initiator parameter UseSGLs has value '0/70001/0' which is different from factory default '0/0/0'
Wed Feb 19 16:28:21 2020 DETAIL: Initiator parameter SGEsPerSeg has value '128' which is different from factory default '256'
Wed Feb 19 16:28:21 2020 ACTION: Issuing command 'nvme-ns-mgmt /iport0/target112 show -all -timeout 90'
Wed Feb 19 16:28:21 2020 DETAIL: Namespace1: 445644800 Blocks, 1825361100800 Bytes (1700.00 GB), 4096 Bytes/Block, Protection Type 0, Shared, Attached
Wed Feb 19 16:28:22 2020 DETAIL: NSID=1 is attached, continue with the test
Wed Feb 19 16:28:22 2020
Wed Feb 19 16:28:22 2020 DETAIL: The disk's supported block size is 4096. Will use this for the rest of the test.
Wed Feb 19 16:28:22 2020 DETAIL: The controller supports NVMe version 1.2.1
Wed Feb 19 16:28:22 2020
Wed Feb 19 16:28:22 2020 DETAIL: Security Send/Receive are supported.
Wed Feb 19 16:28:22 2020 DETAIL: Locking and Encryption are supported.
Wed Feb 19 16:28:22 2020 ACTION: Issuing command 'sed-util /iport0/target112lun1 show'
Wed Feb 19 16:28:22 2020 DETAIL: Command passed. Supported Security Protocol:
  Protocol 00: Security Protocol Information
  Protocol 01: TCG (Management Layer)
  Protocol 02: TCG (Communication Layer)
  Protocol ef: ATA Device Server Password
Level 0 Discovery:
  Feature 0001: Trusted Peripheral
   Sync Supported: 1
   Async Supported: 0
   ACK/NAK Supported: 0
   Buffer Mgmt Supported: 0
   Streaming Supported: 1
   ComID Mgmt Supported: 0
  Feature 0002: Locking
   Locking Supported: 1
   Locking Enabled: 0
   Locked: 0
   Encryption Supported: 1
   MBR Enabled: 0
   MBR Done: 0
  Feature 0003: Geometry
   Logical Block Size: 512
   Alignment Granularity: 16
   Lowest Aligned LBA: 0
  Feature 0201: Single User
   Number of Locking Objects Supported: 9
   Any Object in Single User Mode: 0
   All Objects in Single User Mode: 0
   Policy (Admin vs. User): 1
  Feature 0202: DataStore Tables
   Number of Tables: 9
   Size of Tables: 10485760
   Table Size Alignment: 1
  Feature 0203: Opal V2
```

Figure 3: Viewing Test Results

For more information on SANBlaze's TCG Opal SSC Verification for SSDs, contact SANBlaze.

SANBlaze Technology, Inc.
One Monarch Drive, Suite 204
Littleton, MA 01460
(978) 679-1400

Help Center
Storage Testing Sales
Storage Testing Support
Embedded Computing Sales
Embedded Computing Support

For General Inquiries:

Email Sales   Email Support