STORAGE DEVELOPER CONFERENCE
SDC 22
Fremont, CA
September 12-15, 2022
BY Developers FOR Developers
A SNIA Event

Accelerate Your SNIA Swordfish™ Implementation Through Open-source Tools, the SMI Lab, and the Swordfish CTP Program

Chris Lionetti, HPE
SNIA Board Secretary, SMI Governing Board

Abstract

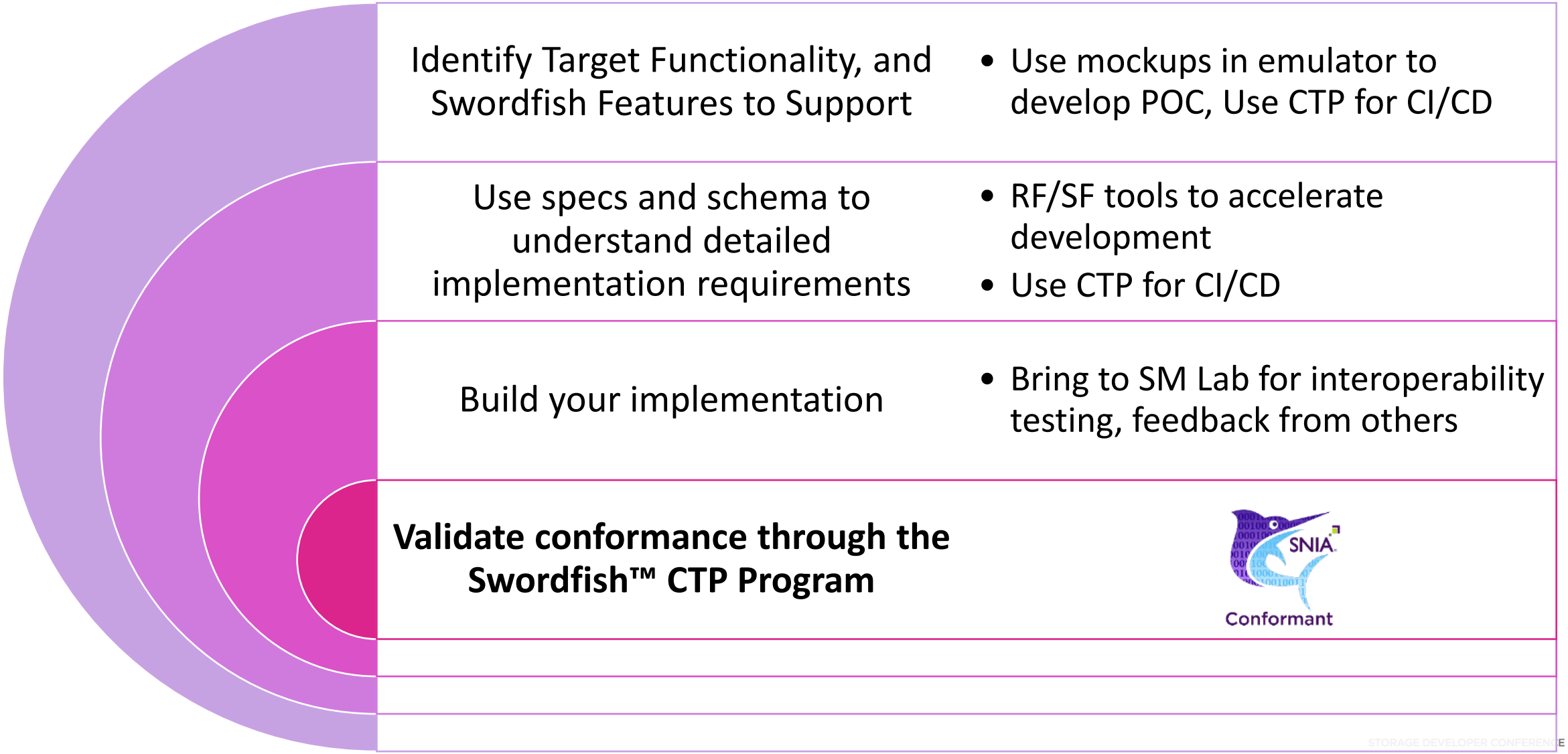
- The SNIA Swordfish™ ecosystem is broader than just the specification. This session will provide an overview an overview of the various tools and programs to help developers accelerate both implementation and adoption of Swordfish.

- This includes demonstrating the interactive nature of tools, schema, and development, by leveraging the testing done by other tools, such as schema validation, implementation conformance testing throughout the development cycle. The presentation will also cover the of use the SMI Lab as test bed for CI/CD, what functionality implementations and base requirements are needed for implementations to pass Swordfish CTP.

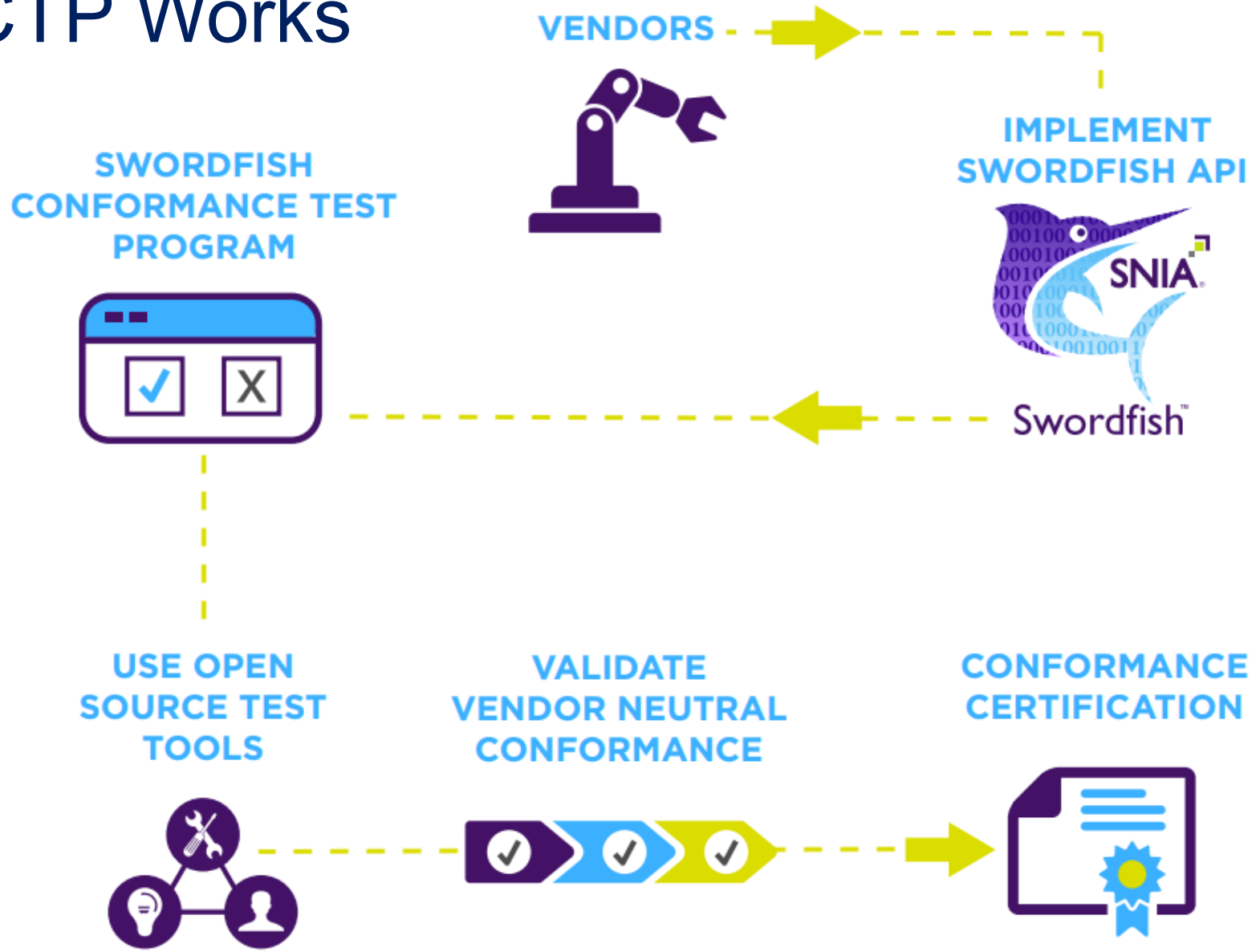
- Learning Objectives:

1. Educate attendees on Swordfish development
2. Teach participations how to use the latest Swordfish open source tools to speed their Swordfish implementation.
3. Discuss how to deploy a Swordfish mockup or implementation in the SM Lab for ongoing interoperability testing
4. Discuss how to engage with the Swordfish CTP program for validation, and to accelerate development.

Solve the Puzzle: Developing a Conformant Swordfish Service



How CTP Works



What is Swordfish CTP?

- Swordfish CTP:
  - A vendor-neutral test suite to validate conformance to the SNIA Swordfish Specification as well as conformance to the DMTF Redfish Specification
  - Uses the Redfish specification, Swordfish Specification and published Swordfish Profiles to determine compliance
    - Profiles define required subsets of functionality that implementations can advertise as customer “Features”
    - Each Feature corresponds to key customer functionality and is advertised to clients
  - Built using open-source tools
    - Leverage pre-built tools: Redfish test framework; Redfish-URI-Validator; Redfish-Service-Validator; Redfish-Protocol-Validator; Redfish-interop-validator
    - Custom tools built to extend, verifying Swordfish-specific requirements: Swordfish Features test; Swordfish Capacity Source test
  - Targeting a completely automated test submission, validation and publication process

Why Do SNIA Swordfish CTP?

INCREASES INTEROPERABILITY

MEETS NEED OF STANDARDS-BASED SOLUTIONS

CONFORMS TO INDUSTRY STANDARDS

ENABLES VENDOR CHOICE FREEDOM

REDUCES INTEGRATION COSTS

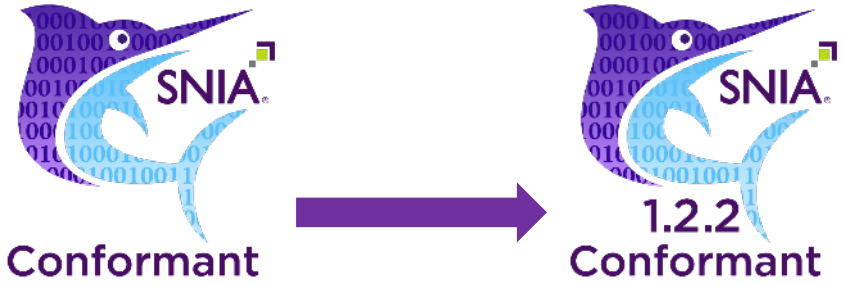
LOWERS COST OF OWNERSHIP

Test Submission Model

- Self-test and validation
  - Participants run tests against their own equipment / software, submit test results to SNIA / SMI to validate and post on the Swordfish site as certified results
  - Current process: “Testing the tests” – companies working directly with CTP lead and testers to simplify process, debug issues
    - Process will be completely automated (with audit process) – results submitted through online portal, processed through automatic validation process, then automatic results created for review before publishing

CTP Logo and Version

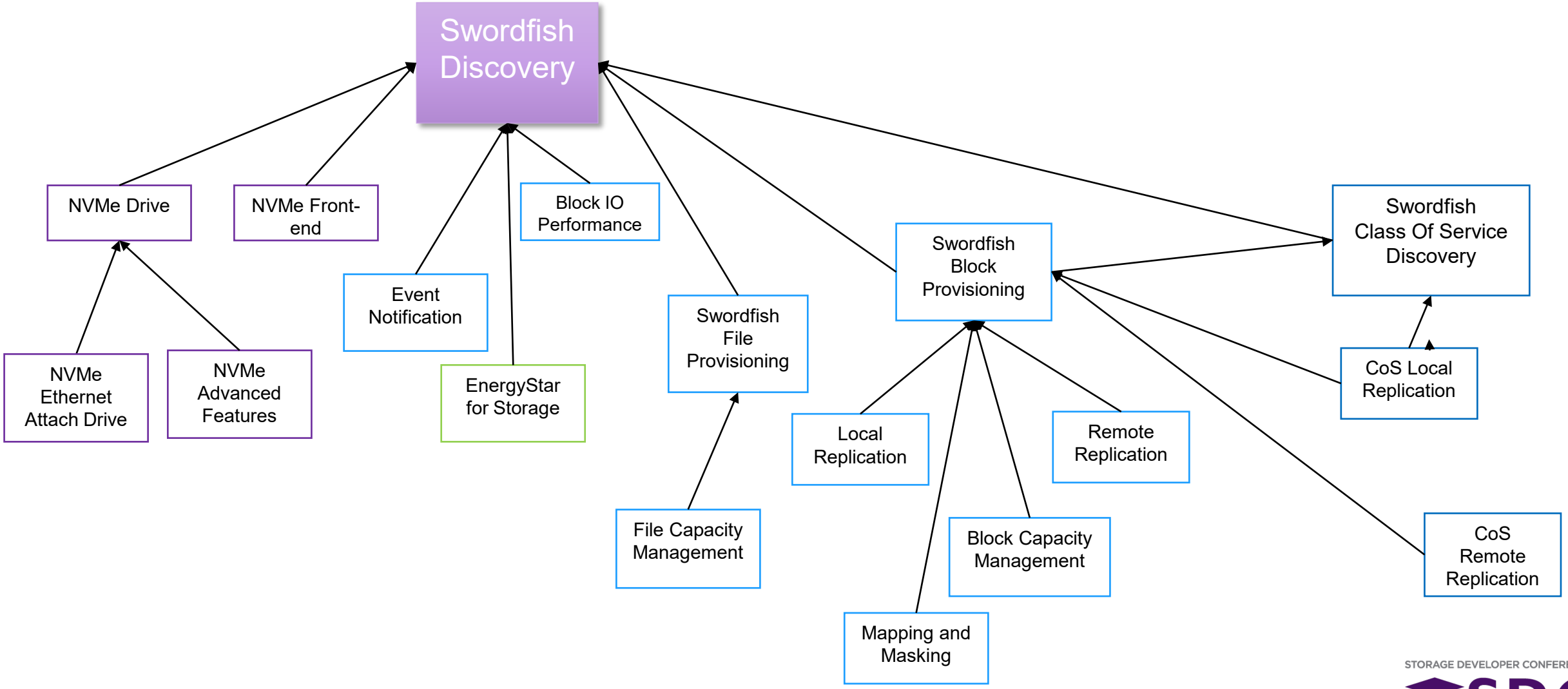
- The CTP Program logos are numbered to correspond to the versions of Swordfish that the SSM TWG chooses to release as SNIA Standards
  - Easy for clients to match your implementations with specifications
  - Identifiable logos to use in marketing materials



What is Covered by tests?

- Conformance to Redfish (and Swordfish) specifications
  - Base required functionality
    - $metadata, odata enumerations
    - Required properties in schema
  - Check all URIs are valid (per RF/SF schema)
  - Limited functionality validation – e.g., sessions for authentication
- Conformance to requirements in Swordfish profiles
  - Each Profile contains only requirements for that feature

Swordfish Profiles Inheritance Hierarchy



Framework and Test Overview

Test Framework

- The test framework leverages the “Redfish-Test-Framework”, an open source framework from the Redfish Forum
  - No need to learn complex setup: Framework is bundled with simple command-line interface specific to Swordfish
- Test early and often
  - CTP supports checking compliance level using mockups
  - Or, use an emulator as a test / development tool: Swordfish API Emulator and DEM both being enhanced to support CTP compliance
- Enhancements (some work in progress, some TBD):
  - SNIA authenticated self-run test result mechanism (e.g., certificate based authentication for CTP members for submitted test results)

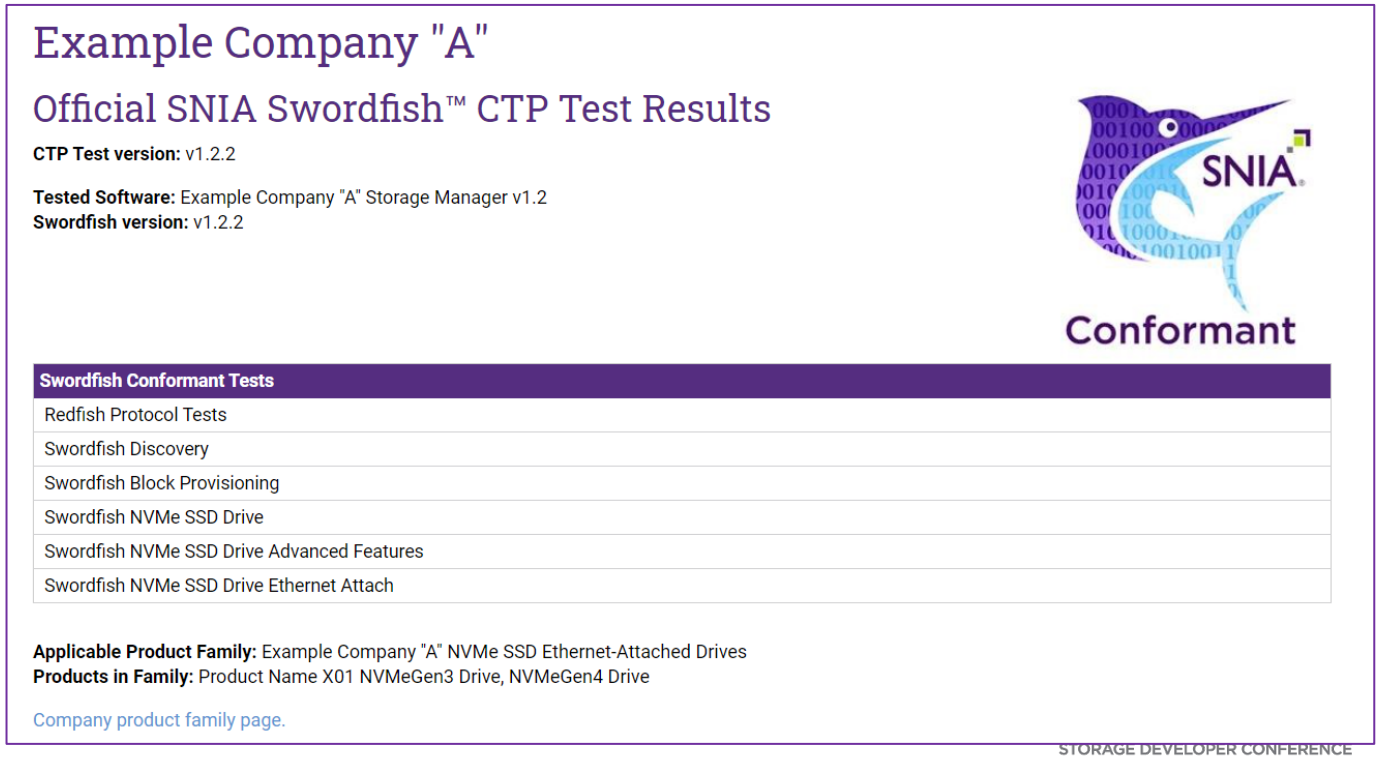
```
(.venv) [root@e7f161f18cda swordfish-ctp-tests]# python ./run_snia_test.py -h
usage: run_snia_test.py [-h] [--user USER] [--password PASSWORD]
                        [--secure SECURE] [--authtype AUTHTYPE]
                        [--profiles PROFILES [PROFILES ...]]
                        [--profile_version PROFILE_VERSION]
                        host level

Python Script for the official Swordfish CTP Testing Suite.
       The hostname provided should be a full URI, as example `https://example.com:8000".

       The hostname may also be provided as a mockup directory as formatted for the Redfish-Moc
kup-Server or Redfish-Protocol-Validator

       The following test levels are available:  serviceroottest, servicetest, officialtest

       After performing the run, your test directory will be output into your Swordfish-CTP-Tes
ts folder as "test_dir_currentdate".

positional arguments:
  host                  Full URL of System being tested (or directory of mockup)
  level                 Level of testing

optional arguments:
  -h, --help            show this help message and exit
  --user USER, -u USER  Username for server
  --password PASSWORD, -p PASSWORD
                        Password of server
  --secure SECURE, -s SECURE
                        Ensures certificate checking on https servers
  --authtype AUTHTYPE   Specify that we are using redfish session or not
  --profiles PROFILES [PROFILES ...]
                        Specify profiles to test against service
  --profile_version PROFILE_VERSION
                        Default version of profiles to test against
(.venv) [root@e7f161f18cda swordfish-ctp-tests]#
```


Test Results: Summary results available from individual test runs

- Each run shows results of each test run
- Submit results when desired tests are passing
  - Redfish service-level tests required
  - Swordfish Discovery feature required
- From final / validated test results, these results will be transformed into results posted online at snia.org/ctp
  - Results will be categorized as Base Redfish, and by Swordfish Feature – only “passed” features published

Test Results: Published Results

- Final / validated test results will be posted online at snia.org/swordfish-ctp
  - Results will be categorized as Base Redfish, and by Swordfish Feature
  - Only “passed” features published



Example Company "A"

Official SNIA Swordfish™ CTP Test Results

CTP Test version: v1.2.2

Tested Software: Example Company "A" Storage Manager v1.2
Swordfish version: v1.2.2

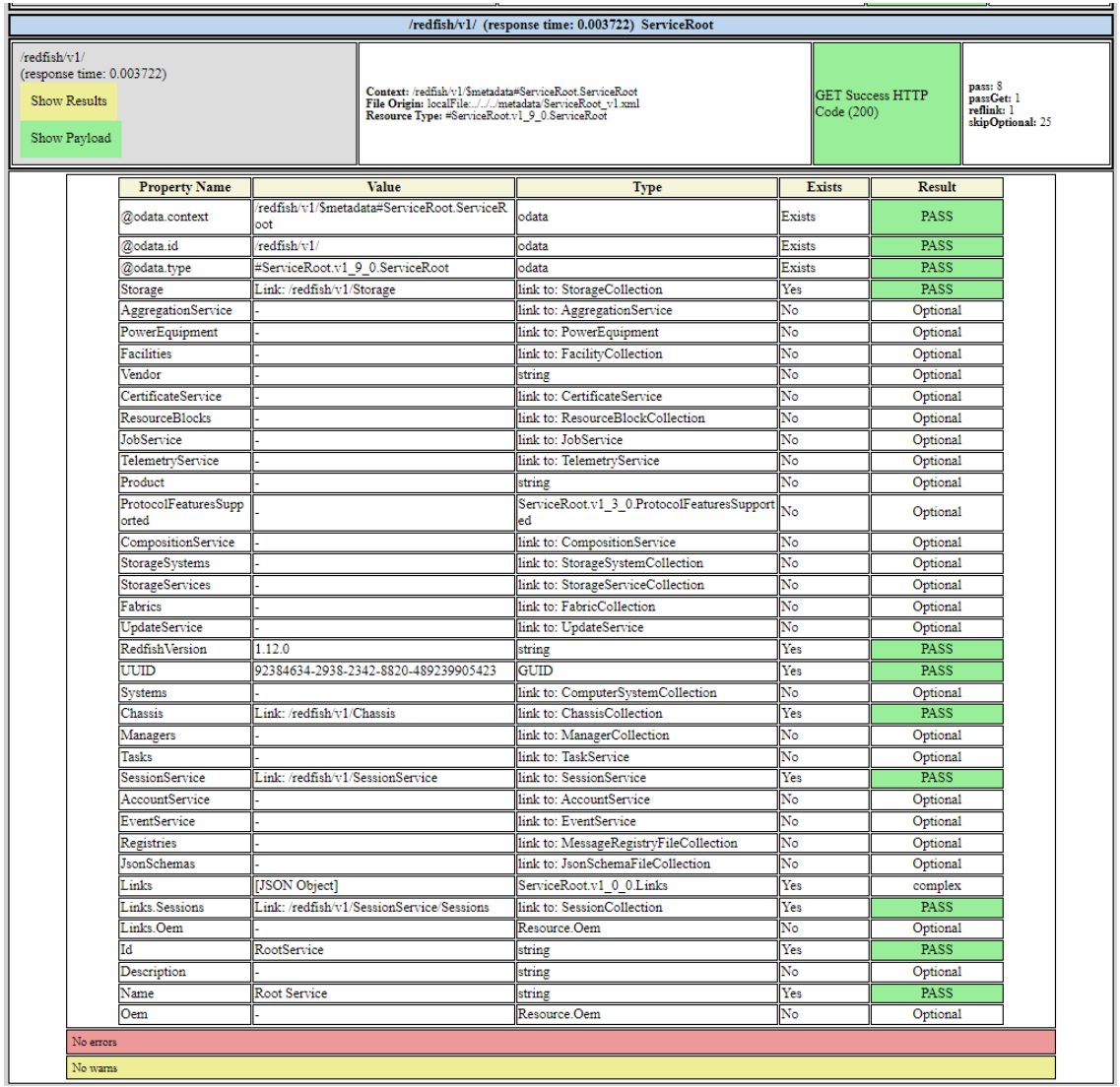
SNIA Conformant

Swordfish Conformant Tests
Redfish Protocol Tests
Swordfish Discovery
Swordfish Block Provisioning
Swordfish NVMe SSD Drive
Swordfish NVMe SSD Drive Advanced Features
Swordfish NVMe SSD Drive Ethernet Attach

Applicable Product Family: Example Company "A" NVMe SSD Ethernet-Attached Drives
Products in Family: Product Name X01 NVMeGen3 Drive, NVMeGen4 Drive

Company product family page.

Redfish Service Tests



/redfish/v1/ (response time: 0.003722) ServiceRoot

/redfish/v1/
(response time: 0.003722)
Show Results
Show Payload

Context: /redfish/v1/$metadata#ServiceRoot.ServiceRoot
File Origin: localFile:../../../metadata/ServiceRoot_v1.xml
Resource Type: #ServiceRoot.v1_9_0.ServiceRoot

GET Success HTTP Code (200)

pass: 8
passGet: 1
reflink: 1
skipOptional: 25

Property Name	Value	Type	Exists	Result
@odata.context	/redfish/v1/$metadata#ServiceRoot.ServiceRoot	odata	Exists	PASS
@odata.id	/redfish/v1/	odata	Exists	PASS
@odata.type	#ServiceRoot.v1_9_0.ServiceRoot	odata	Exists	PASS
Storage	Link: /redfish/v1/Storage	link to: StorageCollection	Yes	PASS
AggregationService	-	link to: AggregationService	No	Optional
PowerEquipment	-	link to: PowerEquipment	No	Optional
Facilities	-	link to: FacilityCollection	No	Optional
Vendor	-	string	No	Optional
CertificateService	-	link to: CertificateService	No	Optional
ResourceBlocks	-	link to: ResourceBlockCollection	No	Optional
JobService	-	link to: JobService	No	Optional
TelemetryService	-	link to: TelemetryService	No	Optional
Product	-	string	No	Optional
ProtocolFeaturesSupported	-	ServiceRoot.v1_3_0.ProtocolFeaturesSupported	No	Optional
CompositionService	-	link to: CompositionService	No	Optional
StorageSystems	-	link to: StorageSystemCollection	No	Optional
StorageServices	-	link to: StorageServiceCollection	No	Optional
Fabrics	-	link to: FabricCollection	No	Optional
UpdateService	-	link to: UpdateService	No	Optional
RedfishVersion	1.12.0	string	Yes	PASS
UUID	92384634-2938-2342-8820-489239905423	GUID	Yes	PASS
Systems	-	link to: ComputerSystemCollection	No	Optional
Chassis	Link: /redfish/v1/Chassis	link to: ChassisCollection	Yes	PASS
Managers	-	link to: ManagerCollection	No	Optional
Tasks	-	link to: TaskService	No	Optional
SessionService	Link: /redfish/v1/SessionService	link to: SessionService	Yes	PASS
AccountService	-	link to: AccountService	No	Optional
EventService	-	link to: EventService	No	Optional
Registries	-	link to: MessageRegistryFileCollection	No	Optional
JsonSchemas	-	link to: JsonSchemaFileCollection	No	Optional
Links	[JSON Object]	ServiceRoot.v1_0_0.Links	Yes	complex
Links.Sessions	Link: /redfish/v1/SessionService/Sessions	link to: SessionCollection	Yes	PASS
Links.Oem	-	Resource.Oem	No	Optional
Id	RootService	string	Yes	PASS
Description	-	string	No	Optional
Name	Root Service	string	Yes	PASS
Oem	-	Resource.Oem	No	Optional

No errors

No warns

Service validator checks general conformance to schema

Troubleshooting from test results

PhysicalPortAssignment	-	link to: NetworkPort	No	Optional
BootMode	Disabled	string (enum)	Yes	PASS
VirtualFunctionsEnabled	True	boolean	Yes	PASS
MaxVirtualFunctions	16	number	Yes	PASS
Links	[JSON Object]	NetworkDeviceFunction.v1_0_0.Links	Yes	complex
Links.EthernetInterfaces	Array (size: 1)	array of: EthernetInterface	Yes	...
Links.EthernetInterfaces[0]	Link: /redfish/v1/Chassis/EBOFEnclosure/NetworkAdapters/8fd725a1/NetworkDeviceFunctions/11100/EthernetInterfaces	EthernetInterface	Yes	FAIL
Links.OffloadSystem	-	link to: ComputerSystem	No	Optional
Links.OffloadProcessors	-	Processor	No	Optional
Links.PhysicalNetworkPortAssignment	-	link to: Port	No	Optional
Links.EthernetInterface	-	link to: EthernetInterface	No	Optional
Links.PhysicalPortAssignment	-	link to: NetworkPort	No	Optional
Links.Endpoints	-	Endpoint	No	Optional
Links.PCIeFunction	-	link to: PCIeFunction	No	Optional
Links.Oem	-	Resource.Oem	No	Optional
Id	11100	string	Yes	PASS
Description	-	string	No	Optional
Name	Network Device Function View	string	Yes	PASS
Oem	-	Resource.Oem	No	Optional

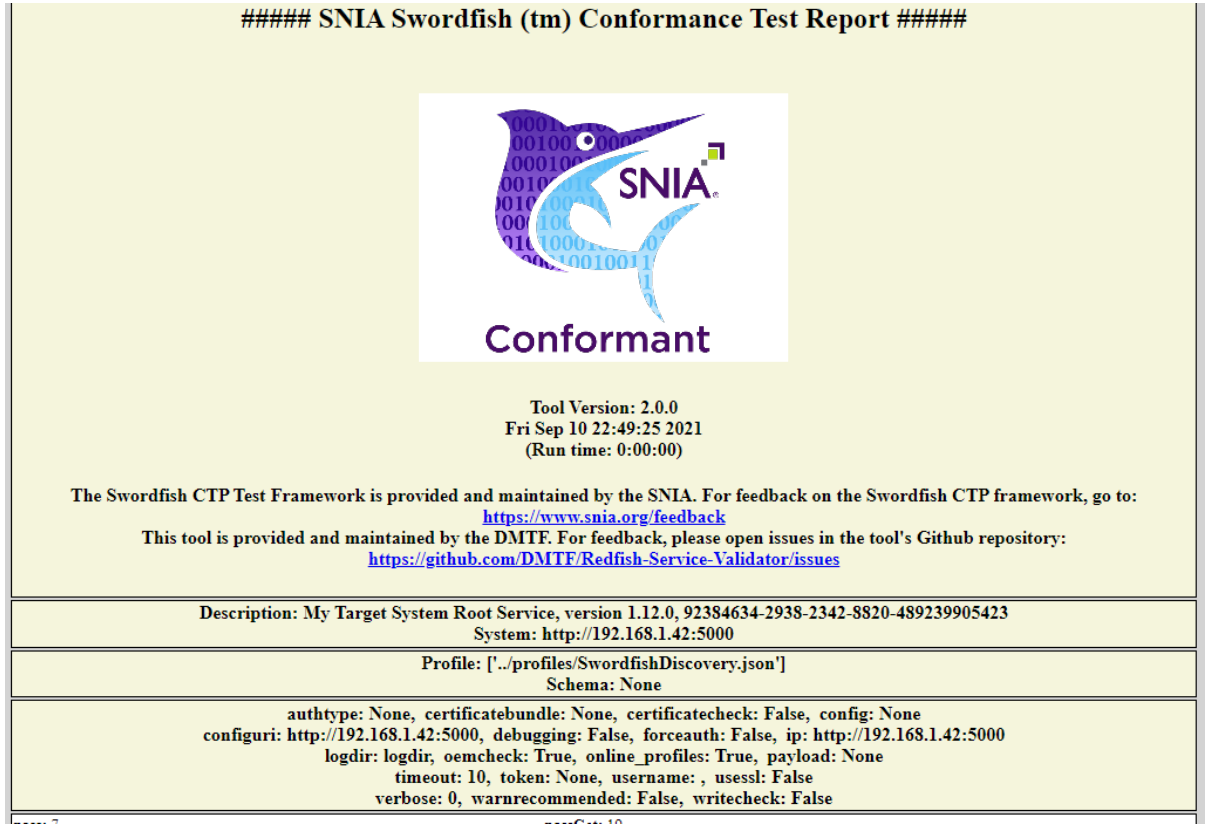
ERROR - Links.EthernetInterfaces[0]: Linked resource reports schema version (or namespace): EthernetInterface.EthernetInterface not found in typechain

WARNING - /redfish/v1/Chassis/EBOFEnclosure/NetworkAdapters/8fd725a1/NetworkDeviceFunctions/11101 @odata.id: Expected @odata.id to match URI link /redfish/v1/Chassis/EBOFEnclosure/NetworkAdapters/8fd725a1/NetworkDeviceFunctions/11100

- Descriptive messages show issues with any failures or warnings
- Additional log files available for more detailed reporting

Individual Features Tests

Each test run has parameters, system info



SNIA Swordfish (tm) Conformance Test Report

Conformant

Tool Version: 2.0.0
Fri Sep 10 22:49:25 2021
(Run time: 0:00:00)

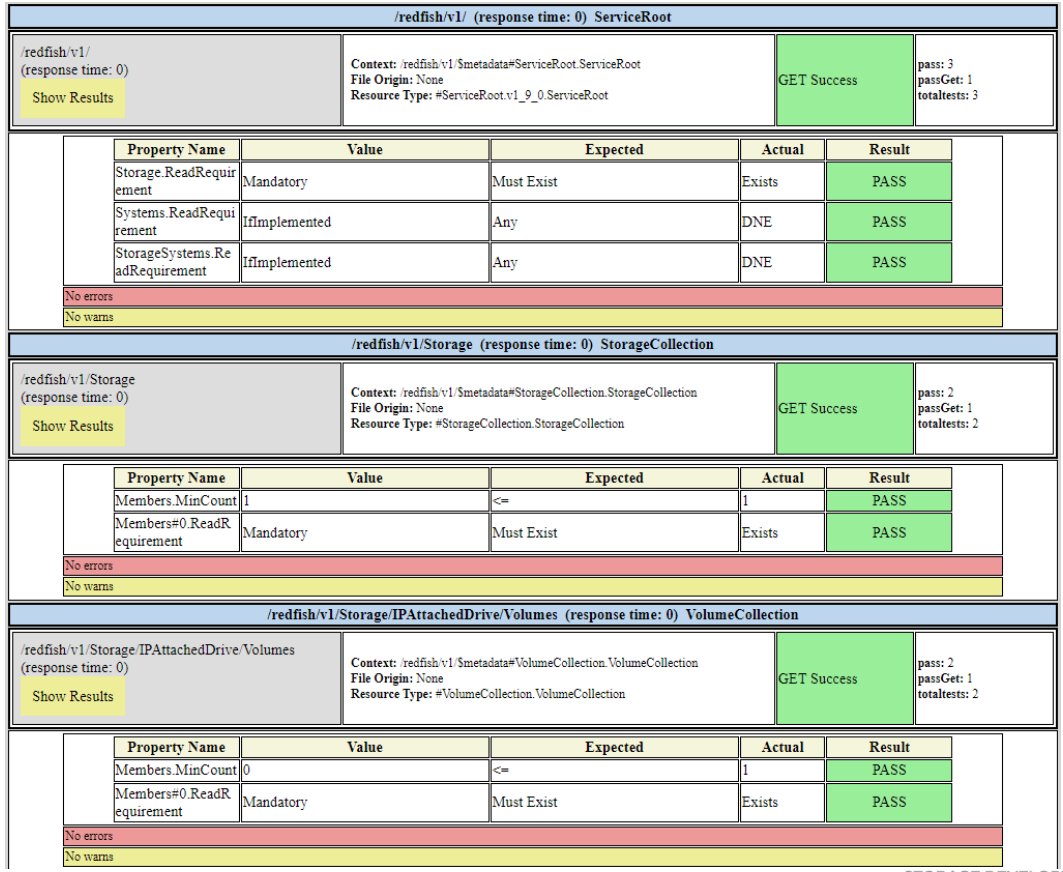
The Swordfish CTP Test Framework is provided and maintained by the SNIA. For feedback on the Swordfish CTP framework, go to:
https://www.snia.org/feedback
This tool is provided and maintained by the DMTF. For feedback, please open issues in the tool's Github repository:
https://github.com/DMTF/Redfish-Service-Validator/issues

Description: My Target System Root Service, version 1.12.0, 92384634-2938-2342-8820-489239905423
System: http://192.168.1.42:5000

Profile: ['../profiles/SwordfishDiscovery.json']
Schema: None

authtype: None, certificatebundle: None, certificatecheck: False, config: None
configuri: http://192.168.1.42:5000, debugging: False, forceauth: False, ip: http://192.168.1.42:5000
logdir: logdir, oemcheck: True, online_profiles: True, payload: None
timeout: 10, token: None, username: , usessl: False
verbose: 0, warnrecommended: False, writecheck: False

Results show PASS/FAIL for each item



/redfish/v1/ (response time: 0) ServiceRoot

/redfish/v1/
(response time: 0)
Show Results

Context: /redfish/v1/$metadata#ServiceRoot.ServiceRoot
File Origin: None
Resource Type: #ServiceRoot.v1_9_0.ServiceRoot

GET Success

pass: 3
passGet: 1
totaltests: 3

Property Name	Value	Expected	Actual	Result
Storage.ReadRequirement	Mandatory	Must Exist	Exists	PASS
Systems.ReadRequirement	IfImplemented	Any	DNE	PASS
StorageSystems.ReadRequirement	IfImplemented	Any	DNE	PASS

No errors
No warns

/redfish/v1/Storage (response time: 0) StorageCollection

/redfish/v1/Storage
(response time: 0)
Show Results

Context: /redfish/v1/$metadata#StorageCollection.StorageCollection
File Origin: None
Resource Type: #StorageCollection.StorageCollection

GET Success

pass: 2
passGet: 1
totaltests: 2

Property Name	Value	Expected	Actual	Result
Members.MinCount	1	<=	1	PASS
Members#0.ReadRequirement	Mandatory	Must Exist	Exists	PASS

No errors
No warns

/redfish/v1/Storage/IPAttachedDrive/Volumes (response time: 0) VolumeCollection

/redfish/v1/Storage/IPAttachedDrive/Volumes
(response time: 0)
Show Results

Context: /redfish/v1/$metadata#VolumeCollection.VolumeCollection
File Origin: None
Resource Type: #VolumeCollection.VolumeCollection

GET Success

pass: 2
passGet: 1
totaltests: 2

Property Name	Value	Expected	Actual	Result
Members.MinCount	0	<=	1	PASS
Members#0.ReadRequirement	Mandatory	Must Exist	Exists	PASS

No errors
No warns

Ready to Participate?

- We are working with companies now to “test the tests”.
  - Please contact us at storagemanagement@snia.org if you are interested in joining the SNIA Swordfish CTP Program

Relationship to SM Lab

- Swordfish SM Lab has a symbiotic relationship with the Swordfish Conformance program
  - Participants can use the SM Lab to test their own products as well as interoperability with the latest and greatest versions of other companies' products.
  - Regular automated results reporting of available infrastructure
- Multiple virtual participation options (e.g., virtual plugfests)
- Free access to CTP for SM Lab members

Where to Find More Info…

SNIA Swordfish™

- Swordfish Standards
  - Schemas, Specs, Mockups, User and Practical Guide`s, … https://www.snia.org/swordfish
  - **NVMe Mapping Guide**
- Swordfish Specification Forum
  - Ask and answer questions about Swordfish
  - http://swordfishforum.com/
- Scalable Storage Management (SSM) TWG
  - Technical Work Group that defines Swordfish
  - Influence the next generation of the Swordfish standard
  - Join SNIA & participate: https://www.snia.org/member_com/join-SNIA
- Join the SNIA Storage Management Initiative
  - Unifies the storage industry to develop and standardize interoperable storage management technologies
  - https://www.snia.org/forums/smi/about/join

DMTF Redfish™

- Redfish Standards
  - Specifications, whitepapers, guides,… https://www.dmtf.org/standards/redfish

Open Fabric Management Framework

- OFMF Working Group (OFMFWG)
  - Description & Links https://www.openfabrics.org/working-groups/
- OFMFWG mailing list subscription
  - https://lists.openfabrics.org/mailman/listinfo/ofmfwg
- Join the Open Fabrics Alliance
  - https://www.openfabrics.org/membership-how-to-join/

NVM Express

- Specifications https://nvmexpress.org/developers/
- Join: https://nvmexpress.org/join-nvme/

Please take a moment to rate this session.

Your feedback is important to us.

