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

A SNIA Event

Redfish Ecosystem for Storage

Presented by Jeff Hilland
President, DMTF & Distinguished Technologist, HPE

Disclaimer

- The information in this presentation represents a snapshot of work in progress within DMTF & SNIA
- This information is subject to change without notice.
- For additional information, see the DMTF & SNIA websites: www.snia.org/swordfish, www.dmtf.org

Agenda

- DMTF Background
  - Who we are and what we do
- Redfish
  - Background
  - General Structure
  - Local Storage
  - Fabric Model for Networks
  - Security
  - RDE (Redfish Device Enablement)
  - The Complete Picture

DMTF – An Industry Standards Organization

WHO Led by innovative, industry-leading companies, DMTF has a global presence with members in multiple countries.

WHAT DMTF standards support diverse emerging and traditional IT infrastructures including cloud, virtualization, network, servers and storage. A complete list is available at **www.dmtf.org/standards.**

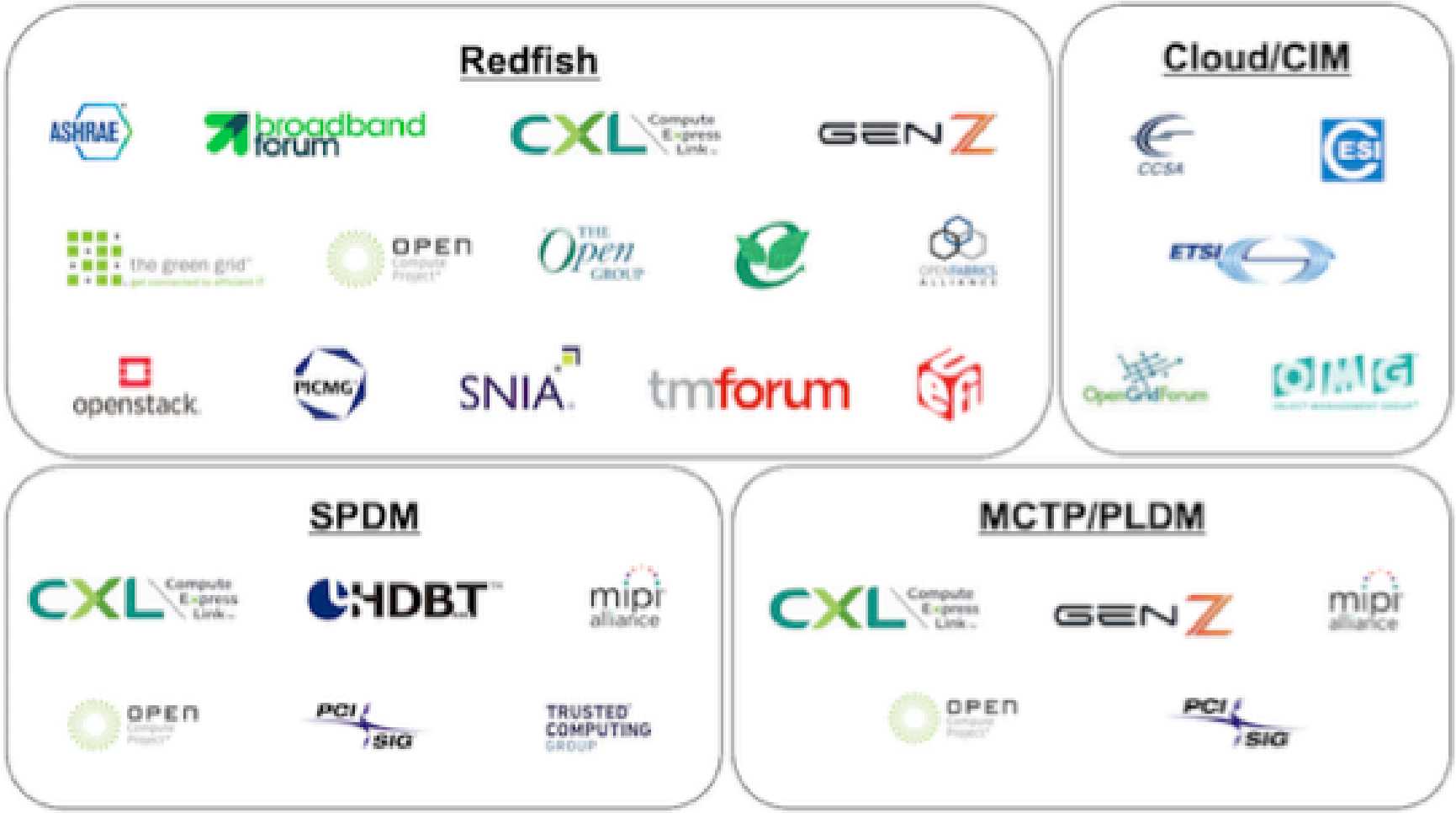
WHY Nationally and internationally recognized by ANSI and ISO, DMTF standards enable a **more integrated and cost-effective approach to management through interoperable solutions.**

HOW Simultaneous development of Open Source and Open Standards is made possible by DMTF, which has the support, tools and infrastructure for efficient development and collaboration.

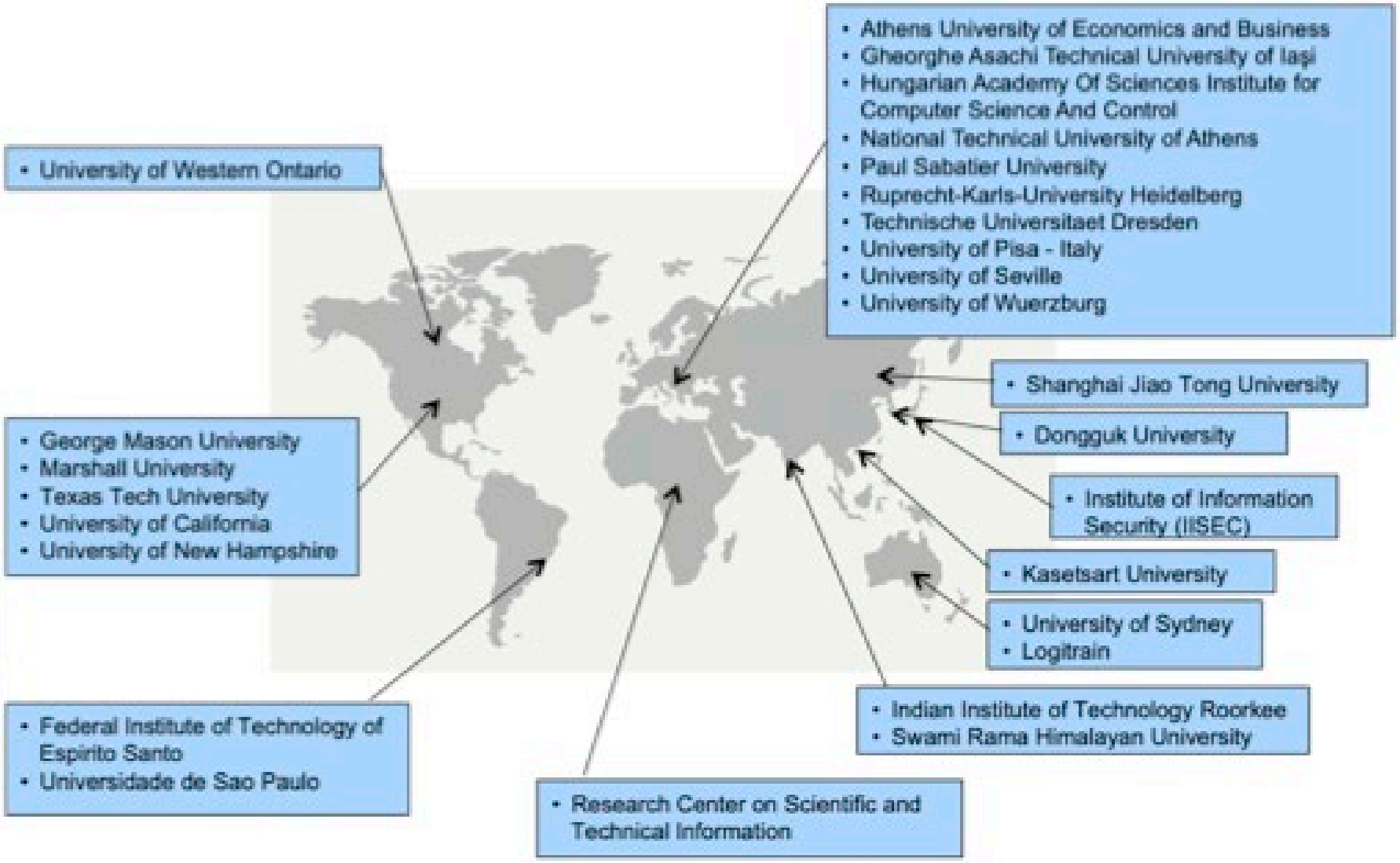
DMTF Board Member Companies

DMTF Alliance Partnership

DMTF and it's Alliance Partners develop a common dialogue and work together for the good of the industry, avoiding overlap and helping ensure interoperability



DMTF Academic Alliance Partnership



DMTF does more than Redfish

- SMBIOS is everywhere
- PMCI
  - MCTP & PLDM: FW Update, Monitoring & Control, FRU, RDE, PLDM, Mappings and Bindings, and NC-SI
  - PMCI Tools TF
- SPDM WG
    - Based on the USB Authentication Protocol (and then expanded)
    - Expected to be leveraged by PCIe, OCP, JEDEC, I3C, CXL, HDBaseT and others
    - Provides Authentication, Attestation and Encryption Key Exchange
    - Includes mapping for MCTP & encrypted MCTP
  - Security Code TF
- CIM
  - Consolidated efforts under a single CIM Forum

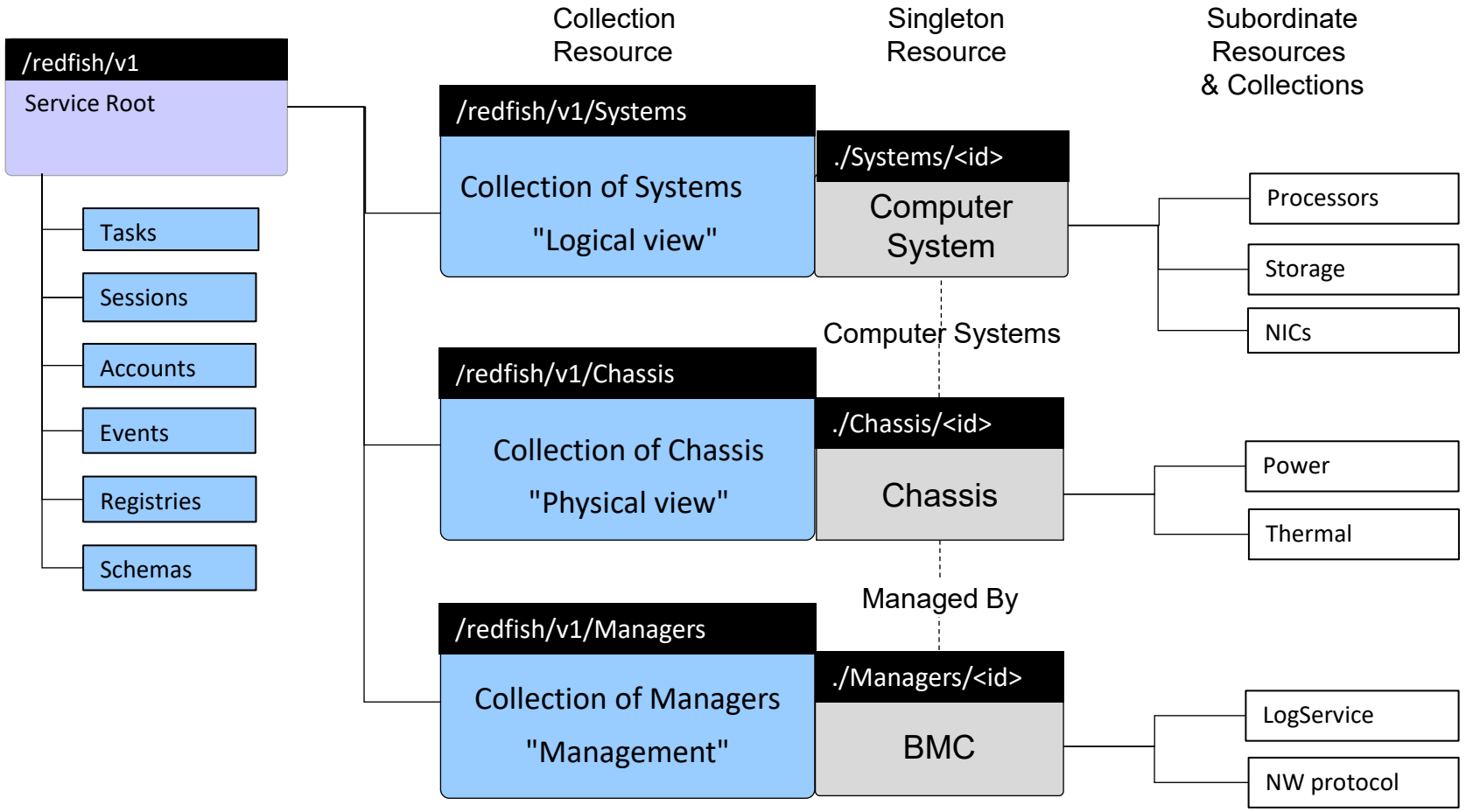
What is Redfish?

- **Industry Standard Software Defined Management for Converged, Hybrid IT defined by the DMTF**
  - RESTful interface using HTTPS in JSON format
  - Schema-backed but human-readable payload usable by GUIs, Scripts and browsers
  - Extensible, Secure, Interoperable
  - Accepted by ISO as ISO/IEC 30115:2018
  - Developer hub at redfish.dmtf.org
- **Initial release in 2015**
  - Additional features coming out approximately every 4 months
  - Started as secure, multi-node capable replacement for IPMI-over-LAN
  - Represent full server category: Rackmount, Blades, HPC, Racks, Future
  - Scope expanded to cover Storage, Networking, Fabrics, Datacenter Infrastructure
  - Shipping on almost every industry standard server shipped today
- **Current releases address the rest of IT infrastructure**
  - Alliances with multiple other standards bodies to define Redfish support
  - Working with SNIA to cover more advanced **Storage** (Swordfish)
  - Working with OCP & ASHRAE to cover **Facilities** (DCIM)
  - Adapt & translate YANG models to cover some level of Ethernet **Switching**
  - Work with Gen-Z & others to cover **Fabrics**
  - Work within the DMTF for internal support (MCTP/PLDM, RDE, SPDM etc.)
  - Host Interface – replacement for IPMI KCS
  - Profiles, Test Tools, Integrations and more

Timeline of Redfish® Specification

- **The DMTF Redfish technology**
  - Sep 2014: SPMF Formed in DMTF.
  - Aug 2015: Redfish Specification with base models (v1.0)
  - 2016: Models for BIOS, disk drives, memory, storage, volume, Models for endpoint, **fabric**, switch, PCIe device, zone, software/firmware inventory & update, Adv. communications devices (multi-function NICs), **host interface** (KCS replacement), privilege mapping
  - 2017: **Composability**, WIP for Telemetry, Location, errata, WIPs for Ethernet Switching, DCIM, OCP & Profiles, **Profiles**, Query parameters, errata
  - 2018: LDAP/AD, **SSE**, Assembly, minor enhancements & errata, **OpenAPI**, **Telemetry**, Jobs, **Schedule**, Compose II, Message II, Certificates, Sensor II (DCIM), FPGA
  - 2019: Spec Clean up; Additions to Certs, Telemetry, Console, Syslog, FW Update multipart, PCIe mods, Composition Registry, Ability to configure SNMP and SMTP services, **Aggregation** & **Ethernet Fabrics** (eBGP and Address Pools)
  - 2020: Adds Support for Network Device Registry, Secure Boot Database and Signatures, Adds Support for StorageDevice Message Registry, Additions of *Connection* and *StorageController* schemas, support for **Gen- Z & *NVMe-over-Fabrics*™**, Incorporates the migration to new resource definitions, **DCIM** starts
  - 2021: Extends the composability model adds multi-client support, **SmartNIC**, OAuth, cables, ***DCIM, Licenses***
  - 2022: ComponentIntegrity, SecurityPolicy, Registry Updates, tons of tweaks, CXL WIP

Redfish Resource Map (simplified system)



GET http://<ip-addr>/redfish/v1/Systems/{id}/Processors/{id}

Use the Redfish Resource Explorer (redfish.dmtf.org) to explore the resource map

Redfish Storage Model

also known as

Local Storage

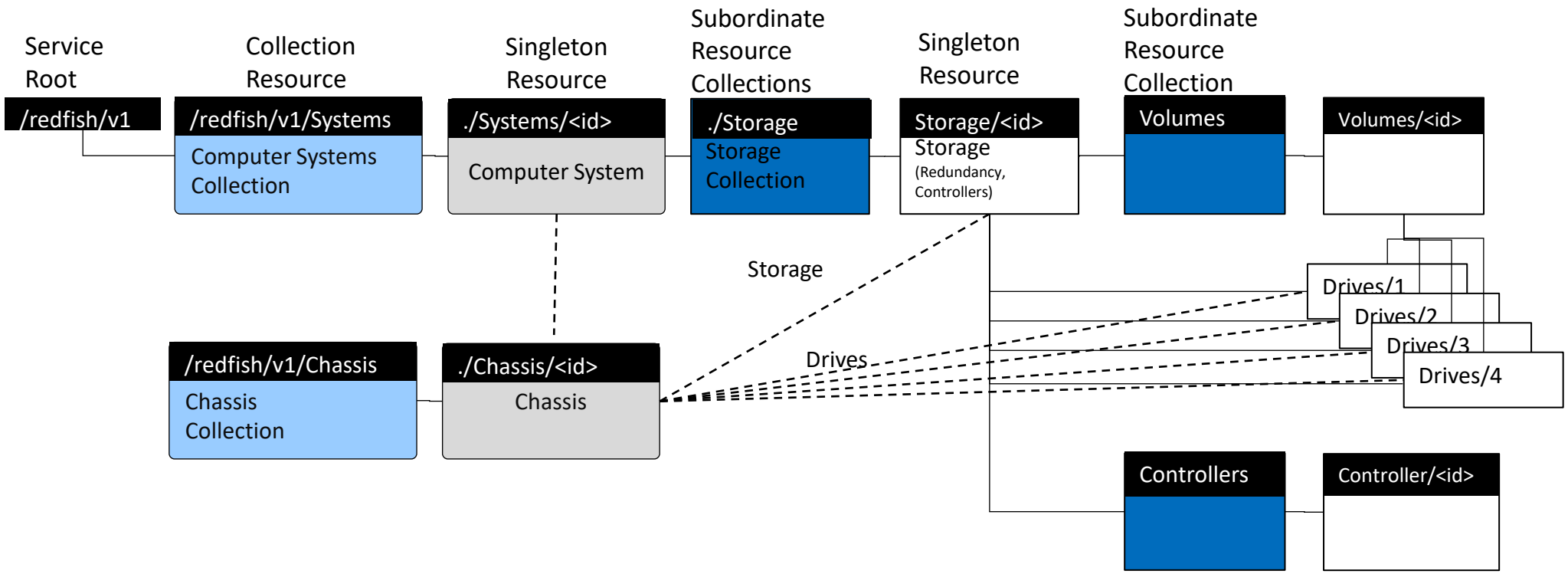
Server Storage

Redfish Storage

Storage Resource Overview

- Storage: A representation of a storage sub-system
  - Contains sets of Volumes, Drives, and Storage Controllers
  - Storage Controller information is an array of objects in the Storage resource
    - Describes the protocols supported by the controller, the speed of the controller interface, and manufacturer information about the controller
- Drive: The physical media for the data
  - Manufacturer information about the drive (part number, serial number, etc.)
  - Capability information about the drive (size, protocol, encryption, etc.)
  - Contains control aspects (secure erase and LED setting)
- Volume: The logical construct used by the OS/hypervisor
  - Contains status about a volume (what drives contribute to the volume, size information, identifier information, etc.)
  - Allows a client to control the volume (initialization, encryption settings, etc.)
- Controller: The physical or logical storage controller
  - Was an array inside of storage (deprecated)
  - Broken out as its own object now (needed for NVMe)

Storage in Redfish – pre 2020.3



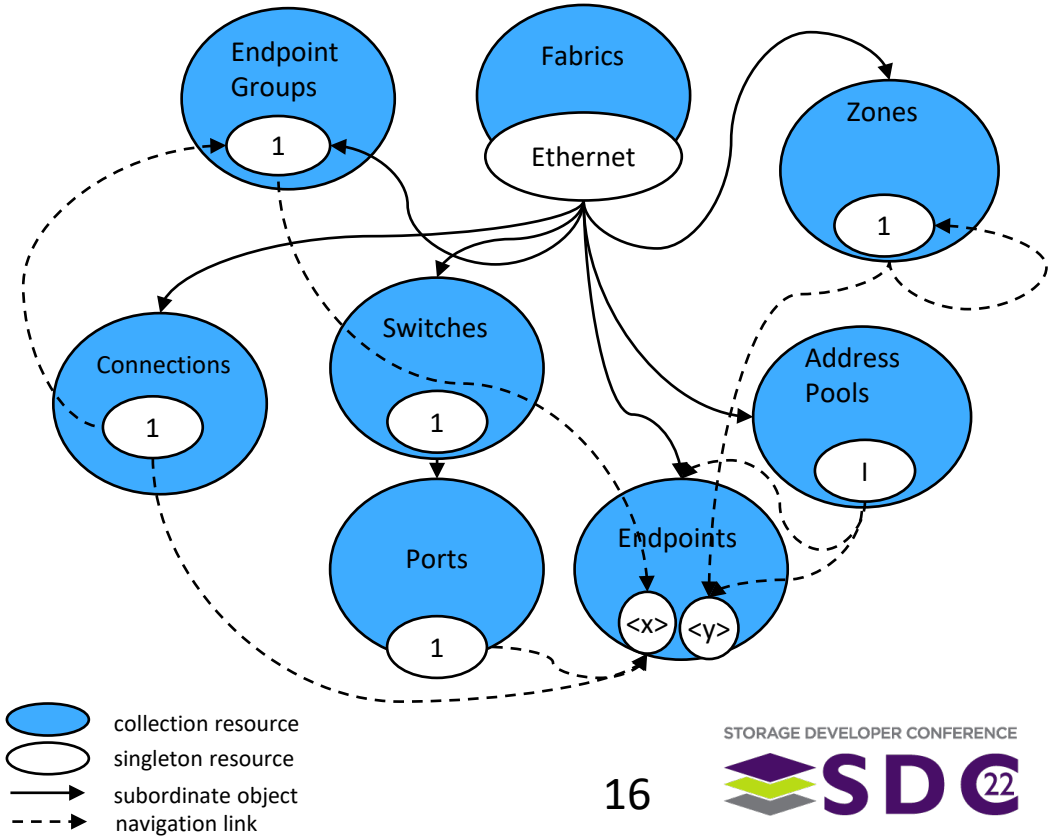
Note that the Volumes are in Collections off of the Storage resource, drives are in arrays off of the storage resource and optionally the Chassis.

Controllers can either be an object in Storage or their own object (like for NVMe)

Fabric Model

Redfish Common Fabric Model

- Goal is to unify the representation of Fabrics, regardless of fabric type
  - Then the rest of the resources in Redfish can show their relationship to the fabric.
  - Enable client to walk from the controller to the port to the switch port, on through the switches and ports to the target's port and controller.
  - DMTF, OFA & SNIA joint collaboration on the OFMF (Open Fabric Management Framework) in the OFA.
- Simple Representation
  - Collection of Fabrics off of the Service Root
  - Switch
    - Switches have Ports that represent the connection
  - Endpoint
    - Represent the "logical" endpoint, not where the cable ends.
      - Parts of the protocol stack/standard that determine source or destination
  - Zone
    - Represents routing & default behavior.
  - AddressPool
    - Show address allocation, eBGP, DNS and common endpoint settings
  - Connection
    - Which endpoints are allowed to communicate



Device Security Model

SPDM, TPMs & Security Policy

- SPDM & TPM Sessions are represented by ComponentIntegrity
  - This has the state of the SPDM session and/or TPM properties negotiated as well as a way to get the signed measurements
  - They will point to the Certificates off of the devices used for the session
- SPDM & TPM Policies are represented by SecurityPolicy off of Manager
  - This has the Trusted/Revoked Certificates list, policies on algorithms as well as TLS Policy (used for the session)
  - Subordinate to Manager (URI is /redfish/v1/Managers/{ManagerId}/SecurityPolicy

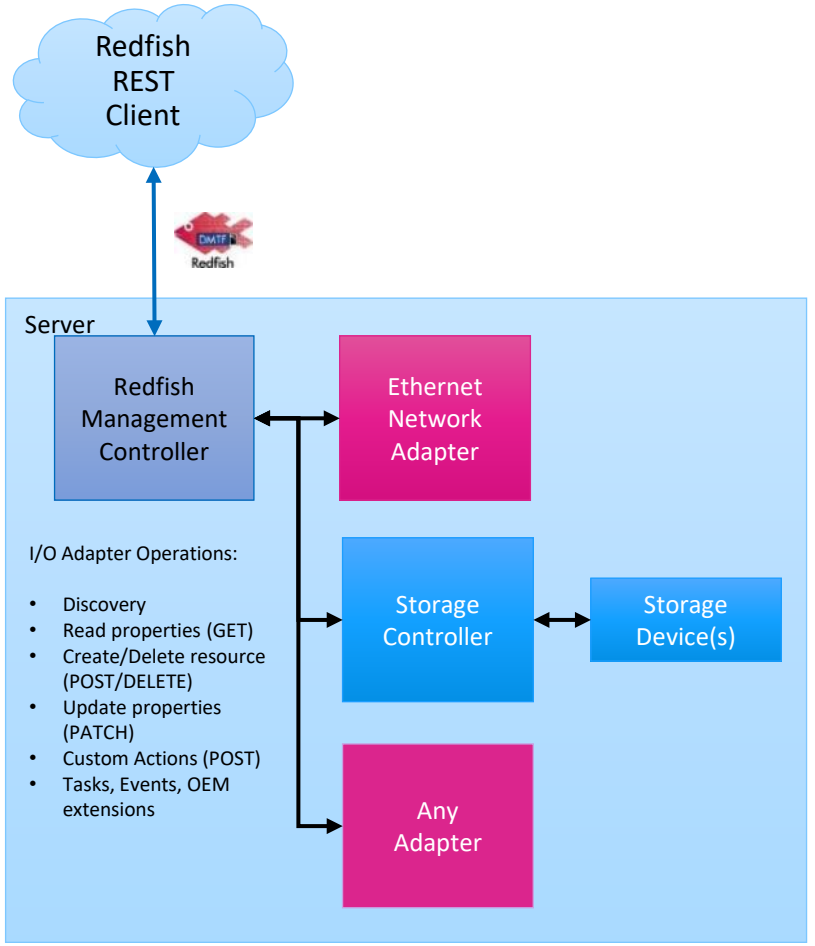
Redfish Device Enablement (RDE)

Or “How you can fill all that storage stuff out without creating a lock step firmware dependency between the management controller firmware and the storage firmware”

Redfish Device Enablement: PLDM Redfish Providers

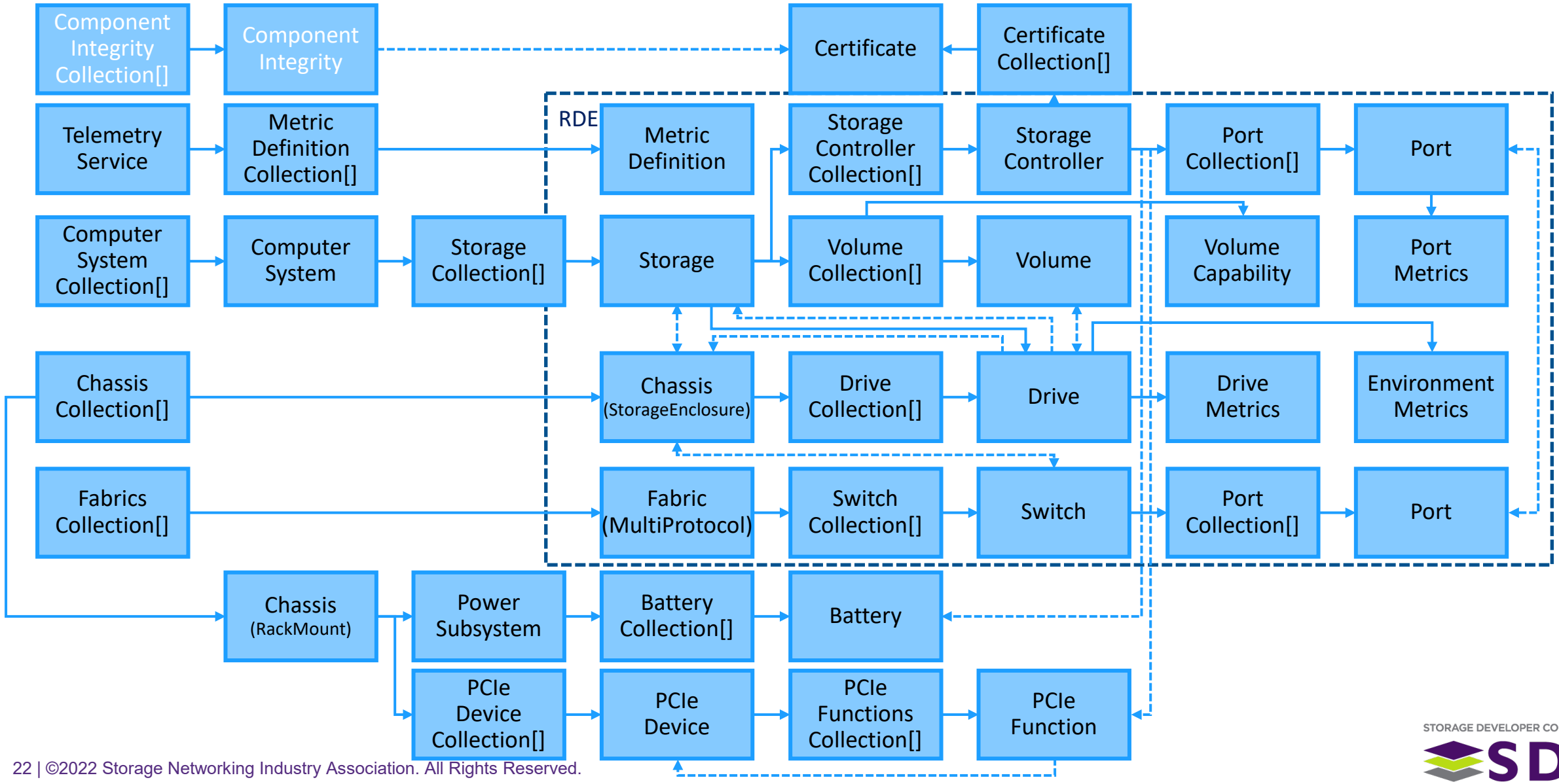
PMCI WG developing a standard to enable a server Management Controller to present a Redfish-conformant management of I/O Adapters without building in code specific to each adapter family/vendor/model.

- Support adapter “self-contained, self-describing” including value-add (OEM) properties
- New managed devices (and device classes) do not require Management Controller firmware updates
- Support a range of capabilities from primitive to advanced devices (lightweight/low bandwidth options)
- Leveraging PLDM, a provider architecture is being specified that can binary encode the data in a small enough format for devices to understand and support.
- MC acts as a broker to encode/decode the data to/from the provider
- PLDM works over I2C & PCIe VDM. Additional mappings under consideration.



What's it look like?

DMTF Redfish Storage Model



Redfish Developer Hub: redfish.dmtf.org

- Resources
  - Schema Index
  - Specifications
  - GitHub for Redfish Tools
  - Registries
  - Other Documentation
- Mockups
  - Simple Rack-mounted Server
  - Bladed System
  - Proposed OCP Redfish Profile
  - More being added
- Education/Community
  - Redfish User Forum
  - Whitepapers, Presentations
  - YouTube shorts & Webinars

In Summary

- Redfish, along with the other DMTF WGs and DMTF alliance partners like SNIA, is working to define interoperable software defined hybrid IT management for servers, storage, networking, power/cooling, fabrics and more
- And is solving problems from security attestation to key exchange, composition to resource managers, aggregation engines to fabric management
- As well as plumbing the mechanisms inside the box to be self contained and self describing
- And enabling a zero-trust model in the platform

Please take a moment to rate this session.

Your feedback is important to us.

