News from DMTF

View this email in your browser

August 2024

Issue Highlights
Redfish Releases 2024.2
SPDM Announces the Release of libspdm 3.4
DMTF Releases DASH Conformance Test Suite Update
Retirement News!
In Case You Missed It • YouTube • More!

Redfish Release 2024.2 Now Available

Redfish® Release 2024.2 is now available for public download. Designed to deliver simple and secure management for hybrid IT and the Software Defined Data Center (SDDC), the latest release of the Redfish standard includes 6 schema updates, additional support for NVM Express® (NVMe®) devices, and developer resources. This release is driven by industry needs to synchronize support for NVM Configuration Lock functionality.

Key highlights of the Redfish 2024.2 release are the additions of TargetConfigurationLockLevel support, *NVMe*, and *BlockSecurityIDEnabled* to **Drive**, and TargetConfigurationLockLevel support and SetControllerPassword to **Storage**.

The Redfish 2024.2 updates include:

- 2024.2 Redfish Schema Bundle – This .zip file contains the current versions of all Redfish schemas. The bundle includes 6 schema updates and developer resources.
  - **NEW** – *TargetConfigurationLockLevel* - Restricts the usage of **in-band** configurations of the drive or storage subsystems
  - For NVMe devices, the *ConfigurationLockState* property in both the **Drive** and **Storage** resources contains supplemental information
  - *ConfigurationLock* shows the current lock state and is used by clients to change the lock state
    - "Enabled" – In-band configurations are locked
    - "Disabled" – No locking applied
    - "Partial" – Only some of the desired locking configuration could be applied
      - This value is prohibited from PATCH/PUT operations and is only for reporting purposes
- Redfish Release 2024.2 Overview – This presentation provides detailed descriptions of each revision in Redfish 2024.2.
- Redfish Resource and Schema Guide – Updated for 2024.2 this human-readable guide to the Redfish Schema is designed to help educate users of Redfish. Application developers and DevOps personnel creating client-side software to communicate with a Redfish service, as well as other consumers of the standard, will benefit from the explanations in this resource.
- Redfish Publications Repository - Public GitHub repository contains an official read-only copy of the Redfish schemas and standard message registries
  - Creates public, durable locations for referencing specific schema or registry items in issue reports, forum postings, or other online references
  - Allows developers to automatically synchronize with new Redfish releases using normal GitHub tools and processes
  - Repository will be updated as each Redfish release become public
- Redfish Data Model Specification – Includes normative statements ("LongDescription") and informative description details from schema in a single document. Intended for both Redfish Service and client-side developers.
- Redfish Conformance Testing Tools - Open source tools for service developers to validate their conformance with the Redfish protocol, data model, and profiles. Tools include the Redfish Protocol Validator, Redfish Service Validator, Redfish Interop Validator.
- Redfish Property Guide – Intended primarily for schema authors, this newly revised reference helps with locating existing property definitions within the schema.
- Redfish Release History – Updated with each new release, this presentation offers a comprehensive view of each revision to Redfish since 2016.

To learn more about Redfish, click here. The Redfish Developer Hub is a one-stop, in-depth technical resource and provides all the files, tools, community support, tutorials and other advanced education you may need to help you use Redfish. Technical work on the Redfish standard takes place in DMTF's Redfish Forum. To find out how you can join and contribute to this standard, click here. To submit input via the DMTF Technology Submission and Feedback Portal click here.

UPCOMING WEBINAR

DMTF's Redfish Forum would like to invite anyone interested in learning about the **Redfish 2024.1 and 2024.2 releases to join a live webinar,** hosted via Zoom, on **Thursday, August 15, 2024, at 9:00 a.m. PT**. The Forum chairs will present the contents of the two releases followed by a round table discussion. For questions regarding the webinar, email webinars@dmtf.org. Don't delay, be sure to register today!

SPDM Announces the Release of libspdm 3.4

The Security Protocols and Data Models (SPDM) Code Task Force recently announced its latest open source release of libspdm, version 3.4. It is conformant with DSP0274 1.0, 1.1, 1.2 and part of 1.3, and is now available for download. In addition, there are three notable changes:

- Addition of MEL (GET_MEASUREMENT_EXTENSION_LOG)
- Support for Secured Messages using SPDM Specification DSP0277 1.2
- Support for MbedTLS 3.0. The 3.X version of MbedTLS is not compatible with the older 2.X versions; this will help with future versions and represents a considerable amount of work.

The SPDM and secured message libraries follow:

- DSP0274 SPDM Specification (version 1.0.2, version 1.1.3, version 1.2.2 and version 1.3.0)
- DSP0277 Secured Messages using SPDM Specification (version 1.1.0, version 1.2.0)
- DSP0275 SPDM over MCTP Binding Specification (version 1.0.2)
- DSP0276 Secured Messages using SPDM over MCTP Binding Specification (version 1.1.1)

You can find all of this in the group's readme here. In addition, details such as SPDM supported commands, cryptographic algorithm support, design, threat model, and users guide can be found in the readme in the repository.

Protocols defined by SPDM can be used for a wide range of security functionalities including authentication of hardware/firmware identities, delivering measurements, performing attestation, and establishing session keys for secure communication channels.

In addition to the core library, libspdm enables spdm-emu, which contains a full SPDM Requester and Responder; spdm-dump, which can parse SPDM messages; and the SPDM Responder Validator, which is still under development but can be used to test an SPDM Responder implementation for its conformance to the SPDM specification.

For more information about libspdm, please visit https://github.com/DMTF/libspdm.

DMTF Releases DASH Conformance Test Suite Update

DMTF continues its ongoing dedication to management interoperability with the release of the latest versions of the Conformance Test Suite (CTS) for its Desktop and mobile Architecture for System Hardware (DASH) standard. DASH CTS 2024 (Java versions 8 and 9) is available, and the DMTF Certification Registry is accepting submissions.

Providing secure out-of-band and remote management of desktop and mobile systems using the Web Services for Management (WS-Management) standard, DASH addresses current requirements for managing modern hardware in a networked environment. The DASH CTS serves to improve interoperability by validating conforming implementations.

In the DASH Conformance Program companies self-test their implementations and submit digitally signed results to the DASH Conformance Program Administrator (an independent third party) for validation. Once validated, participants can have their submission information included in the DMTF Certification Registry.

Please visit the DMTF website to learn more about DASH CTS. To learn more or to participate in the development of DMTF conformance programs for system management standards, please see DMTF's CIM Forum.

Retirement Congratulations are in Order!

We would like to extend our congratulations and sincere appreciation to Kimon Berlin and Mike Walker on their retirement.

Kimon recently retired from HP (after 30 years with the company!) and worked tirelessly on several releases of the SMBIOS specification and SMBIOS related CIM Schema development. He also co-chaired the SMBIOS working group for numerous years.

Mike, who has been retired from the corporate world for several years, leaves behind a legacy at DMTF. As a fellow since 2015, Mike has been a dedicated member and worked on countless specifications that have significantly impacted the industry, most notably CIM. His leadership as chair of the CIM Schema Task Force for many years is a testament to his commitment.

We can't thank them enough for their dedication and commitment to the organization. Congratulations, Kimon and Mike, on your retirement, and best wishes from all of us at DMTF!

In Case You Missed It

DMTF Seeks Industry Feedback on Support for Post Quantum Cryptography in Specifications

The Security Protocols and Data Models (SPDM) Working Group is requesting industry feedback on a proposal regarding support of the National Institute for Standards and Technology (NIST) selection of Post Quantum Cryptography (PQC) algorithms in future SPDM specification versions.

View the WIP presentation here. SPDM is looking for specific feedback regarding the following:

- Among NIST's selected PQC algorithms, which algorithms and which parameters sets is your company planning to support?
- Is your company considering support for Post-Quantum/Traditional (PQ/T) hybrid key and signature schemes? If yes, which combinations?
- What are your thoughts on the proposed plan for PQC and/or hybrid schemes in SPDM?
- When does your company need PQC and/or hybrid schemes in SPDM?

All feedback must be received by end of August 2024. Feedback may be submitted via a SPDM Working Group representative or through our website at https://www.dmtf.org/standards/feedback/.

Now Available - Authorization WIP Presentation released by SPDM Working Group

The Security Protocols and Data Models Working Group recently released an Authorization Work-in-Progress (WIP) presentation that previews a new Authorization Specification (DSP0289) slated for future release. This WIP presentation aims to help address authorization uniformity across SPDM and PMCI standards, DMTF alliance partners, and the industry.

Click here to view the presentation. SPDM is looking for feedback; feedback may be submitted via a SPDM Working Group representative or our website at https://www.dmtf.org/standards/feedback/.

Newsletter Feedback

We welcome your input on what you'd like to see included here – just Contact Us online and share your suggestions!

DMTF on YouTube

Check out our latest videos and be sure to subscribe to the DMTF YouTube Channel to stay up-to-date with our current and upcoming webinars.

Click Here to Get All the Latest News Delivered to Your Inbox!

Need a DMTF Logo for your Marketing Materials?

We've got you covered! Email press@dmtf.org for the DMTF and/or Redfish logo files as well as the most current Logo Usage Guidelines and Graphic Standards. We've recently updated the usage guidelines to include the use of the Redfish logo on a dark background.

Personalize your DMTF Meeting Schedule

Log into the members portal here where you can see your specific work group meetings.

Please note you will need to be logged in to the member portal in order to access this feature.

Upcoming Events

SDC 2024
September 16-18, 2024
Santa Clara, California

OCP Global Summit
October 15-17, 2024
San Jose, California

SC24
November 17-22, 2024
Atlanta, Georgia

Recent DMTF Specifications

DSP0277 1.2.0 (Secured Messages Using SPDM Specification)
DSP2058 1.3.0 (SPDM Architecture White Paper)
DSP2067 1.0.0 (PLDM CXL Memory Modeling White Paper)
DSP0274 1.3.1 (SPDM Specification)
DSP0249 1.2.0 (PLDM State Set Specification)
DSP8010 2024.2 (Redfish Schema Bundle)
DSP2058 2024.2 (Redfish Data Model Specification)
DSP2046 2024.2 (Redfish Resource and Schema Guide)
DSP2053 2024.2 (Redfish Property Guide)
DSP0218 1.2.0 (PLDM for Redfish Device Enablement)
DSP0240 1.2.0 (PLDM Base Specification)
DSP0242 1.0.0 (PLDM for File Transfer Specification)
DSP0248 1.3.0 (PLDM for Platform Monitoring and Control Specification)
DSP0134 3.8.0 (SMBIOS Specification)

Information about DMTF's leadership, technologies, and how to participate can be found at www.dmtf.org. Contact us online or reach us at http://www.dmtf.org/contact.

About DMTF

DMTF creates open manageability standards spanning diverse emerging and traditional IT infrastructures including cloud, virtualization, network, servers and storage. Member companies and alliance partners worldwide collaborate on standards to improve the interoperable management of information technologies. The organization is led by a diverse board of directors from Broadcom Inc., Cisco; Dell Technologies; Hewlett Packard Enterprise; Intel Corporation; Lenovo; Positivo Tecnologia S.A; and Verizon.

1050 SW 6th Avenue, #1100
Portland, OR 97204