Redfish 2019.1 Work in Progress

DMTF Redfish Forum

March 2019

Disclaimer

- The information in this presentation represents a snapshot of work in progress within the DMTF.

- This information is subject to change without notice. The standard specifications remain the normative reference for all information.

- For additional information, see the Distributed Management Task Force (DMTF) website.

Work in Progress for Redfish release 2019.1

- DMTF Redfish Forum working to complete 2019.1 release bundle.
  - Expect Forum to finalize in April 2019, with public availability in May 2019.
- Redfish Specification v1.7 (DSP0266)
  - A significant reformatting of the specification is underway for readability.
    - While the text is significantly changed, the protocol itself is not, and except for items explicitly mentioned, no normative changes were intended.
  - Some new functionality added as well
- Schema updates – details in following slides
- Registry updates – details in following slides
- Redfish Interoperability Profile Specification v1.1 (DSP0272)
- Host Interface Specification v1.1 (DSP0270)

Redfish Specification v1.7

- Normative clarifications to Protocol
  - Several (small) normative protocol clarifications will be added, which is primarily the reason for the minor version bump
    - Default "levels" for $expand query, if not specified by the client, is 1 level
    - Clarified PATCH behavior for arrays and handling of certain error conditions
    - More clarifications expected before release
  - Fixed missing statements in the Composability clause
    - Expandable resources were mentioned in white paper but not in Specification
- New functionality
  - Support for localization of schema files
    - File naming rules and schema annotations to indicate language support
  - Support for local schema repository
    - Allows for OpenAPI YAML files along with JSON schema and CSDL
    - Specifies a URI (folder) location – filenames are already specified

Certificates Schema additions

- An additional *CertificateCollection* is proposed in the *Boot* object within *ComputerSystem*

- This collection of Certificates is to be used with HTTPS booting, where a system will make a request to an HTTPS server for retrieving a boot image

Telemetry Schema additions

- Proposed updates to Triggers
  - Addition of *EventTriggers*, an array of *MessageIds* that specify when to create a trigger occurrence based on Events generated by the service
  - Addition of *MetricReportDefinitions* link to force a specified *MetricReport* (or set of *MetricReports*) to be updated when a trigger condition occurs

- Proposed updates to *MetricReportDefinition*
  - Addition of *SuppressRepeatedMetricValue* and *MetricReportHeartbeatInterval* to control how repeated metrics are transmitted
    - If *SuppressRepeatedMetricValue* is enabled, then repeated metrics are not transmitted
    - *MetricReportHeartbeatInterval* controls when to send the metrics regardless of the value being changed

"Password Change Required" support

- New ManagerAccount property "PasswordChangeRequired" (boolean)
  - When "True", user must change password before access is granted
  - Implementations that use default credentials should set this to "True"
  - Allows administrators to deploy systems and user accounts that require users to change their individual credentials before use
- Redfish with return HTTP 401 on any request using that account
  - Behavior continues until user changes password
  - POST to create a Redfish Session will succeed, but will return 401
  - PATCH to ManagerAccount to update "Password" property will succeed
- New Base Message to indicate "PasswordChangeRequired"
  - Returned in all 401 responses, including POST to create Session
  - Message includes the URI to the ManagerAccount where the PATCH is performed to change the password
  - Allows client software to locate ManagerAccount instance without GET

Serial Console discovery enhancements

- Existing "*SerialConsole*" support in Redfish *Manager* schema does not fully describe those features
  - Doesn't specify a *ComputerSystem* instance when multiple targets exist
  - Doesn't describe behavior of console – does it mimic the serial console output or a "text-mode" VGA display
  - No provision for SSH parameters/options if needed
  - No indication of shared BMC/Host console modes (hot key support)
- Intend to add support in *ComputerSystem* to fully describe this
  - New properties for all the above
  - Looking for industry feedback on any other information needed
  - Thread on http://www.RedfishForum.com asking for input

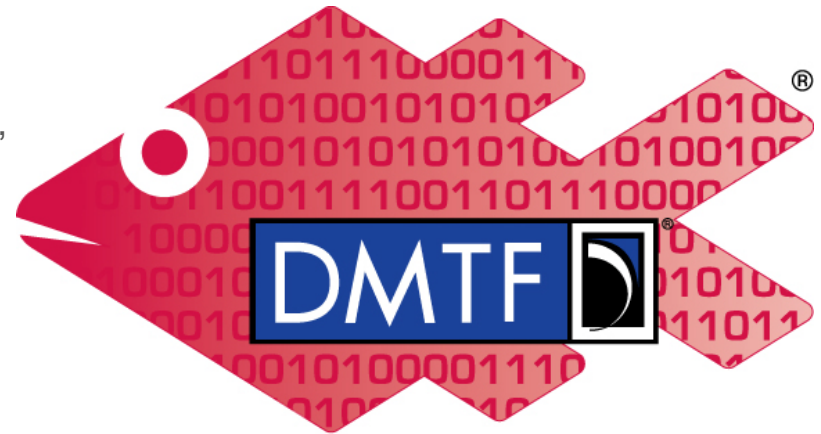# Syslog support (*ManagerNetworkProtocol* addition)

```
"Syslog": {
  "Port": 514,
  "ProtocolEnabled": true,
  "RemoteLoggingServers": [ {
      "Name": "System Errors Syslog Server",
      "LowestSyslogSeverity": "Warning",
      "SyslogProtocol": "UDP",
      "SyslogUri": "myserver.contoso.com:514",
    },
    {
      "Name": "Daemon Debugging Syslog Server",
      "LowestSyslogSeverity": "Debug",
      "SyslogProtocol": "TCP",
      "EnabledSyslogFacilities": [ "Daemon" ],
      "SyslogUri": "myotherserver.contoso.com:514"
    }
    ]
},
```

- Syslog is a de facto standard for message logging.
- Default value of the Port property should be 514 for compatibility with established client implementations
- Specify Severity level to log and syslog-specific protocol to use
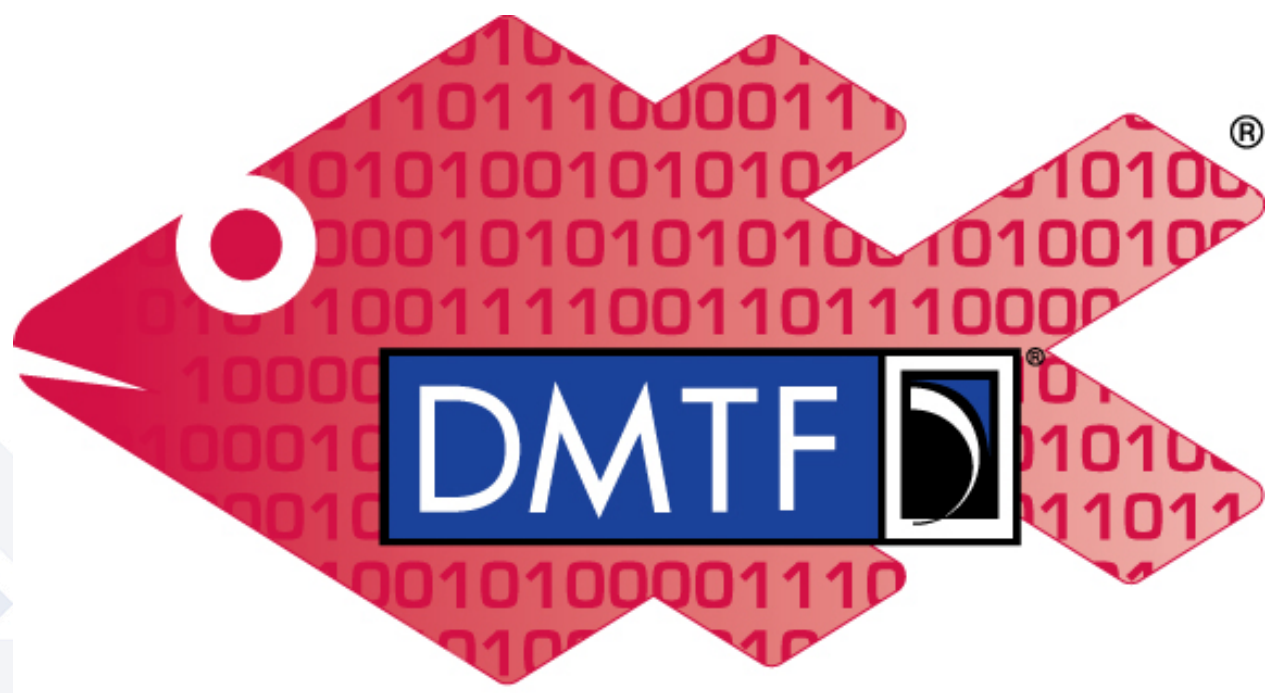- SyslogUri contains the hostname and port of a server that is listening for incoming syslog messages

Getting involved in Redfish

- Redfish Standards page
  - Schemas, Specs, Mockups, White Papers, FAQ, Educational Material & more
  - http://www.dmtf.org/standards/redfish

- Redfish Developer Portal
  - Redfish Interactive Resource Explorer
  - Educational material, Hosted Schema files, documentation & other links
  - http://redfish.dmtf.org

- Redfish User Forum
  - User forum for questions, suggestions and discussion of all Redfish topics
  - http://www.redfishforum.com

- DMTF Redfish Forum
  - Companies involved, Upcoming Schedules & Future work, Charter
  - Join the DMTF to get involved in future work
  - http://www.dmtf.org/standards/spmf

www.dmtf.org