Redfish IEC 62443 Enhancements

Mike Raineri, Dell Technologies

www.dmtf.org

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 DMTF website: www.dmtf.org

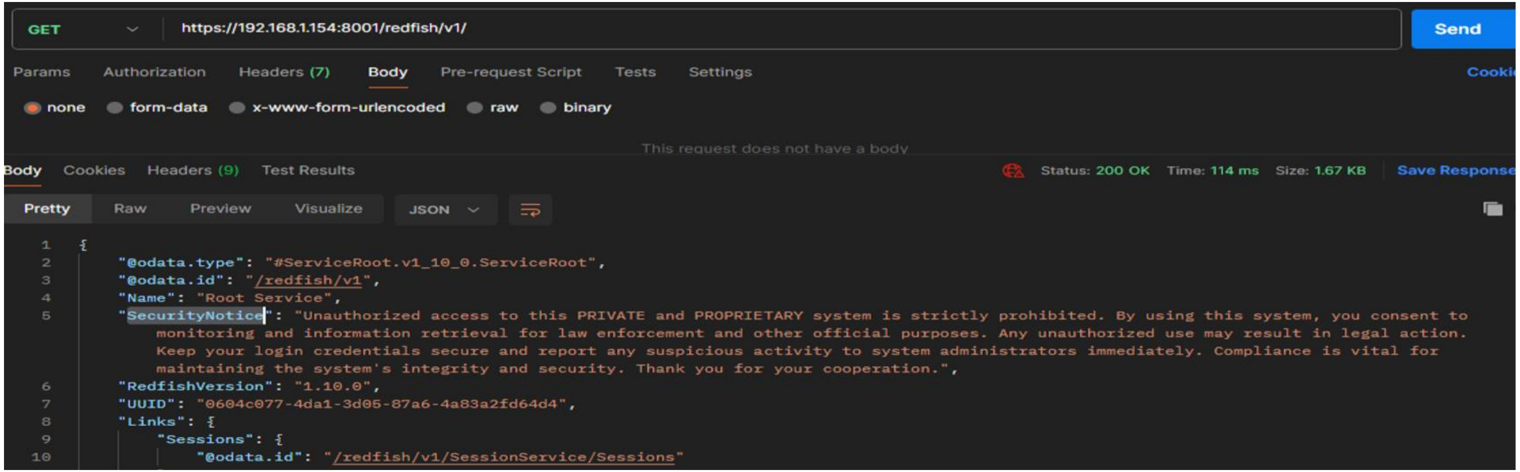
Overview

- OPAF (Open Process Automation Forum) provided feedback to the Redfish Forum to include new properties to enable IEC-62443-4-2 certification
- The following slides show the feedback requested and the Redfish Forum's responses

FSA-CR 1.12 System Use Notification

Requirement Id	**FSA-CR 1.12**
Requirement Name	System Use Notification
Description	When a component provides local human user access/HMI, it shall provide the capability to display a system **use notification message before authenticating**. The system use notification message **shall be configurable** by authorized personnel.
Recommended Solution	a property called “SecurityNotice” to the ServiceRoot and allowing it to be patched

Example



GET https://192.168.1.154:8001/redfish/v1/

Status: 200 OK Time: 114 ms Size: 1.67 KB

```
{
    "@odata.type": "#ServiceRoot.v1_10_0.ServiceRoot",
    "@odata.id": "/redfish/v1",
    "Name": "Root Service",
    "SecurityNotice": "Unauthorized access to this PRIVATE and PROPRIETARY system is strictly prohibited. By using this system, you consent to
        monitoring and information retrieval for law enforcement and other official purposes. Any unauthorized use may result in legal action.
        Keep your login credentials secure and report any suspicious activity to system administrators immediately. Compliance is vital for
        maintaining the system's integrity and security. Thank you for your cooperation.",
    "RedfishVersion": "1.10.0",
    "UUID": "0604c077-4da1-3d05-87a6-4a83a2fd64d4",
    "Links": {
        "Sessions": {
            "@odata.id": "/redfish/v1/SessionService/Sessions"
```

System Use Notification

- Propose to follow the same design pattern as *ServiceIdentification*
  - New property: *ServiceUseNotification*
- Administrators PATCH the property in the **Manager** resource that hosts the Redfish service
- The property is also shown in **ServiceRoot** in GET responses if there is a configured value for the property
  - Omit if not configured

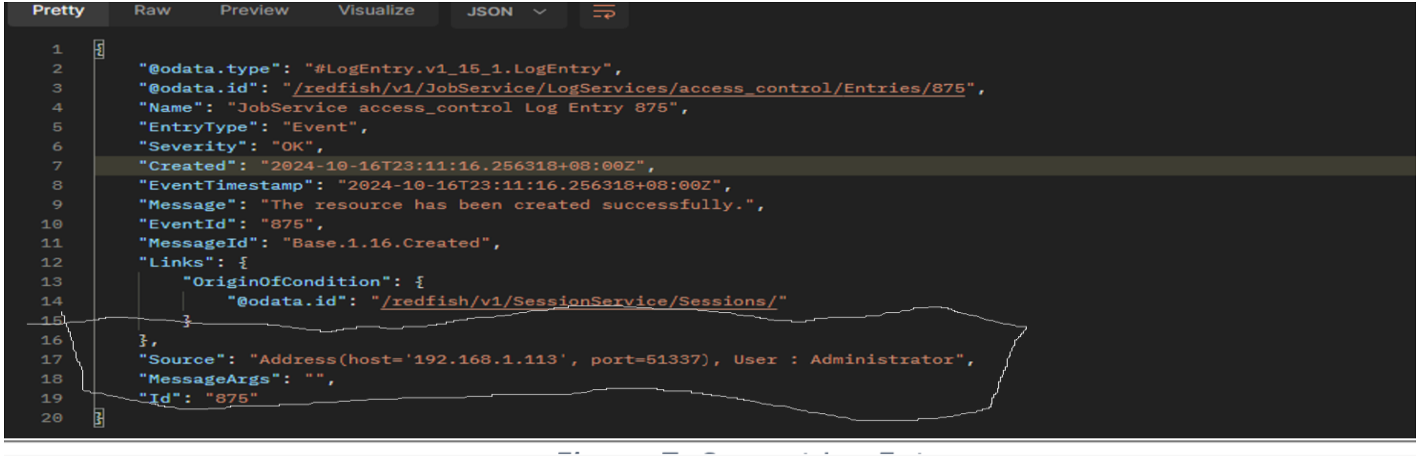
System Use Notification

```
PATCH /redfish/v1/Managers/BMC

{
    "ServiceUseNotification": "By using this service, you consent to Contoso's usage policy found at
                              contoso.org/policies"
}



GET /redfish/v1/

{
    "@odata.id": "/redfish/v1/",
    "Id": "ServiceRoot",
    "ServiceUseNotification": "By using this service, you consent to Contoso's usage policy found at
                              contoso.org/policies",
    ...
}
```

FSA-CR 1.12 Non-Repudiation

Requirement Id	**FSA-CR 2.12**
Requirement Name	Non-repudiation
Description	If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action. Control elements that are not able to support such capability shall be listed in component documents.
Recommended Solution	In the Log Entries: Add a property called “**source**” to the log entries that records the username and source of the action

Example



```
{
    "@odata.type": "#LogEntry.v1_15_1.LogEntry",
    "@odata.id": "/redfish/v1/JobService/LogServices/access_control/Entries/875",
    "Name": "JobService access_control Log Entry 875",
    "EntryType": "Event",
    "Severity": "OK",
    "Created": "2024-10-16T23:11:16.256318+08:00Z",
    "EventTimestamp": "2024-10-16T23:11:16.256318+08:00Z",
    "Message": "The resource has been created successfully.",
    "EventId": "875",
    "MessageId": "Base.1.16.Created",
    "Links": {
        "OriginOfCondition": {
            "@odata.id": "/redfish/v1/SessionService/Sessions/"
        }
    },
    "Source": "Address(host='192.168.1.113', port=51337), User : Administrator",
    "MessageArgs": "",
    "Id": "875"
}
```

Non-Repudiation

- Propose to leverage existing *Username* and *UserAuthenticationSource* properties in **LogEntry** and **Event**
  - These were added in 2024.3
- Propose to add *OriginIPAddress* property to **LogEntry** and **Event**
  - **Session** contains a *ClientOriginIPAddress* property for similar usage
- Question 1: Is the protocol/interface (SSH vs HTTPS) useful information for these events?
- Question 2: Is the client port necessary?

Non-Repudiation

```
GET /redfish/v1/Managers/BMC/LogServices/Log/Entries/1

{
    "@odata.id": "/redfish/v1/Managers/BMC/LogServices/Log/Entries/1",
    "@odata.type": "#LogEntry.v1_19_0.LogEntry",
    "Id": "1",
    "Name": "Log Entry 1",
    "EntryType": "Event",
    "Severity": "OK",
    "Created": "2012-03-07T14:44:00Z",
    "Message": "Log Cleared",
    "MessageId": "Event.1.0.LogClear",
    "MessageArgs": [],
    "Username": "admin",
    "UserAuthenticationSource": "/redfish/v1/AccountService",
    "OriginIPAddress": "192.168.1.113"
}
```

Thank you!

For more information,
visit us online at
dmtf.org

Visit the
Redfish Developers Hub at
redfish.dmtf.org