



VANTAGEO Server

Redfish Interface Description (BMC V4)

Version: R1.3

VANTAGEO PRIVATE LIMITED

Corporate Address: 617, Lodha Supremus II,

Road No. 22, Wagle Estate,

Thane - 400604

URL: <https://vantageo.com>

E-mail: support@vantageo.com

Helpdesk - +91 18002669898

LEGAL INFORMATION

Copyright 2024 VANTAGEO PRIVATE LIMITED.

The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of VANTAGEO PRIVATE LIMITED is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of VANTAGEO PRIVATE LIMITED or of their respective owners.

This document is provided as is, and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. VANTAGEO PRIVATE LIMITED and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

VANTAGEO PRIVATE LIMITED or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between VANTAGEO PRIVATE LIMITED and its licensee, the user of this document shall not acquire any license to the subject matter herein.

VANTAGEO PRIVATE LIMITED reserves the right to upgrade or make technical change to this product without further notice.

Users may visit the VANTAGEO technical support website <https://www.vantageo.com/support> to inquire for related information.

The ultimate right to interpret this product resides in VANTAGEO PRIVATE LIMITED.

Statement on the Use of Third-Party Embedded Software:

If third-party embedded software such as Oracle, Sybase/SAP, Veritas, Microsoft, VMware, and Redhat is delivered together with this product of VANTAGEO, the embedded software must be used as only a component of this product. If this product is discarded, the licenses for the embedded software must be void either and must not be transferred. VANTAGEO will provide technical support for the embedded software of this product.

Revision History

Revision No.	Revision Date	Revision Reason
R1.3	2025-02-08	Add "Chapter 11, Operations on Fabric Resources" and "Chapter 12, Operations on Registries Resources"; Updated "Chapter 4, Operations on Manager Resources".
R1.2	2024-07-01	Updated "Chapter 4, Operations on Manager Resources".
R1.1	2024-05-30	Added "Chapter 10, Operations on AccountService Resources". Updated "Chapter 4, Operations on Manager Resources".
R1.0	2023-07-31	First edition.

Serial Number: VT20240304

Publishing Date: 2025-02-08 (R1.3)

Contents

1.Redfish Overview.....	12
1.1 Basic Concepts	12
1.2 General Descriptions	12
2.Redfish Resource Tree	17
3.Operations on Public Fixed Resources	21
2.1 Querying the Redfish Version Information.....	23
2.2 Querying the Current Root Service Resources	24
4.Operations on Manager Resources	29
4.1 Querying Information About the Manager Resource Collection.....	49
4.2 Querying Information About a Specified Manager Resource.....	51
4.3 Modifying Information About a Specified Manager Resource	57
4.4 Querying Information About the Syslog Configuration	59
4.5 Configuring Information About the Syslog Server	62
4.6 Submitting a Syslog Test Log	69
4.7 Querying Information About the NtpService Configuration Resource	70
4.8 Modifying Properties of the NTP Resource	72
4.9 Querying Information About the BMC Service	75
4.10 Modifying Information About a Specified BMC Service.....	80
4.11 Querying the BMC Management Interface Resource Collection.....	88
4.12 Querying Information About a Specified BMC Management Interface Resource....	90
4.13 Modifying a Specified BMC Management Interface Resource.....	97
4.14 Restarting the BMC	104
4.15 Querying Information About the LLDP Service Configuration Resource.....	107
4.16 Modifying Properties of the LLDP Service Resource	109
4.17 Querying Information About the SNMP Resource.....	111
4.18 Modifying Properties of the SNMP Resource.....	115
4.19 Submitting an SNMP Trap Test Event	122
4.20 Querying the Virtual Media Resource Collection	124
4.21 Querying a Virtual Media Resource.....	126
4.22 Connecting to the Virtual Media	129
4.23 Disconnecting the Virtual Media	131
4.24 Sending a One-Click Collection Request	133
4.25 Querying the One-Click Collection Progress.....	136
4.26 Exporting Logs	138
4.27 Querying the KVM Service Resource	140

4.28	Modifying Information About the KVM Resource	142
4.29	Querying Information About a Specified SEL Log Service Resource	145
4.30	Capturing the Screen Manually	147
4.31	Downloading the Manually Captured Screen Image.....	149
4.32	Querying Information About the ISDT Resource.....	150
4.33	Modifying Properties of the ISDT Service Resource	152
4.34	Mounting and Dismounting Navigation Disks.....	154
4.35	Querying Information About the ISDT FWUpdate Collection.....	156
4.36	Querying Information About an ISDT FWUpdate Task.....	157
4.37	Burning an ISDT Image	160
4.38	Adding Routes	162
4.39	Deleting Routes	164
4.40	Querying Information About the SecurityService Resource	166
4.41	Querying Information About SecurityService Rules	168
4.42	Adding a Firewall Rule.....	171
4.43	Deleting a Firewall Rule.....	174
4.44	Attaching Remote Media to the Virtual Media Device	175
4.45	Detaching Remote Media from the Virtual Media Device	177
4.46	Setting the BMC Time.....	179
4.47	Importing the Syslog Root Certificate	181
4.48	Importing a Local Syslog Certificate	185
4.49	Importing a Private Key Certificate	188
4.50	Querying SSL Certificate Information	191
4.51	Importing an SSL Certificate.....	196
4.52	Exporting BIOS or BMC Configurations.....	200
4.53	Importing BIOS and BMC Configurations	202
4.54	Downloading a Redfish File.....	204
4.55	Enabling the GPU Module to Start Collecting Logs.....	205
4.56	Enabling the GPU Module to Obtain Log Files	207
4.57	Querying Information About the DNS Service.....	208
4.58	Modifying Information About the DNS Service	210
5	Operations on System Resources	215
5.1	Querying Information About the System Resource Collection	228
5.2	Querying Information About a Specified System Resource	230
5.3	Remotely Powering On, Powering Off, and Resetting a System Resource	239
5.4	Modifying Properties of a Specified System Resource	241
5.5	Querying Information About the CPU Resource Collection.....	245

5.6	Querying Information About a Specified CPU Resource.....	247
5.7	Querying Information About All CPU Resources.....	251
5.8	Querying Information About the Memory Resource Collection	254
5.9	Querying Information About a Specified Memory Resource	256
5.10	Querying Information About All Memory Resources	260
5.11	Querying Information About the Storage Resource Collection.....	263
5.12	Querying Information About a Specified Storage Controller Resource	265
5.13	Querying Information About All Storage Controller Resources	271
5.14	Querying Information About the Logical Volume Resource Collection.....	276
5.15	Querying Information About a Specified Logical Volume Resource.....	278
5.16	Creating a Logical Volume.....	282
5.17	Deleting a Logical Volume	287
5.18	Querying Properties of the BIOS Resource	290
5.19	Querying Information About the BIOS Settings.....	292
5.20	Modifying the BIOS Settings.....	294
5.21	Setting the BIOS Password	296
5.22	Restoring the Default BIOS Settings	298
5.23	Querying Information About the Ethernet Interface Resource Collection.....	299
5.24	Querying Information About a Specified Ethernet Interface Resource.....	301
5.25	Querying Information About the SimpleStorage Resource Collection.....	305
5.26	Querying Information About a Specified SimpleStorage Resource.....	307
6.	Operations on Chassis Resources	310
6.1	Querying Information About the Chassis Resource Collection.....	331
6.2	Querying Information About a Specified Chassis Resource	333
6.3	Modifying the Position Indicator Status of a Chassis	338
6.4	Querying Information About the Network Adapter Resource Collection.....	340
6.5	Querying Information About a Specified Network Adapter Resource	342
6.6	Querying Information About All Network Adapter Resources	348
6.7	Querying Information About a Specified Network Port Resource.....	355
6.8	Querying Information About the Optical Module Resource Connected to a Network Port	359
6.9	Modifying the LLDP Switch of a Specified Network Port.....	363
6.10	Querying Information About the PCIe Device Resource Collection	367
6.11	Querying Information About a Specified PCIe Device Resource	369
6.12	Querying Information About All PCIe Device Resources	376
6.13	Querying Information About the Drive Resource Collection	382
6.14	Querying Information About a Specified Drive Resource.....	384

6.15	Querying Information About All Drive Resources	389
6.16	Querying the Power Supply Information About a Specified Chassis.....	392
6.17	Collecting Information About Power Statistics.....	401
6.18	Modifying Properties of a Specified Power Supply	403
6.19	Querying Cooling Resource Information About a Specified Chassis	415
6.20	Querying Information About the Expansion Board Resource Collection	423
6.21	Querying Information About the Hard Disk Backplane Resource Collection	425
6.22	Querying Information About a Specified Hard Disk Backplane Resource.....	427
6.23	Querying Information About the Riser Card Resource Collection	430
6.24	Querying Information About a Specified Riser Card Resource	432
6.25	Modifying the Cooling Resource Information About a Specified Chassis	433
6.26	Querying Information About a Specified PCIe Device Function Resource	443
6.27	Querying Information About the Collection of Leak Detection Device Resources .	446
6.28	Querying Information About the Leak Detector Resource Collection	448
6.29	Querying Information About a Specified Leak Detector	450
6.30	Modifying Information About a Specified Drive Resource	452
6.31	Querying Information About the Network Port Resource Collection of a Specified Network Adapter.....	454
6.32	Querying Historical Environmental Humidity Information About a Chassis.....	456
7.	Operations on Ses- sionService Resources	459
7.1	Querying Information About the Session Service	460
7.2	Modifying Information About the Session Service.....	462
7.3	Creating Information About a Session.....	464
7.4	Querying Information About the Session Resource Collection	466
7.5	Querying Information About a Specified Session Resource	467
7.6	Deleting Information About a Specified Session Resource.....	469
8.	Operations on EventSer- vice Resources	471
8.1	Querying Information About the EventService Resource	477
8.2	Querying Information About the Event Subscription Resource Collection	480
8.3	Creating an Event Subscription Resource	482
8.4	Querying Information About an Event Subscription Resource.....	486
8.5	Modifying Information About an Event Subscription Resource	489
8.6	Deleting an Event Subscription Resource	492
8.7	Resuming Event Subscription.....	494
8.8	Reporting an Event	495
8.9	Querying Information About the Event Resource Collection	498
8.10	Deleting All Event Resources	500

8.11	Querying Information About the Current Alarm Resource Collection	501
8.12	Querying Information About the Current Alarm Resource.....	504
8.13	Deleting the Current Alarm Resource.....	506
8.14	Deleting All Current Alarm Resource.....	507
8.15	Querying Information About the Current Alarm Event Resource Collection	508
8.16	Modifying Event Service Resource Information.....	512
9.Operations on Up- dateService Resources		514
9.1	Querying Information About an UpdateService Resource.....	518
9.2	Querying Information About an Updateable Firmware Resource Collection.....	520
9.3	Querying Information About a Specified Updateable Firmware Resource	523
9.4	Updating Firmware.....	525
9.5	Querying Information About PCIe Switch Firmware Update	529
9.6	Updating Third-Party Module Firmware.....	531
9.7	Uploading a Firmware File to a Server	534
9.8	Updating the Firmware of a Server.....	535
9.9	Querying Information About a Specified Task.....	539
10.Operations on AccountService Resources		543
10.1	Querying User Service Information.....	546
10.2	Modifying User Service Information	549
10.3	Querying Information About the User Resource Collection	552
10.4	Querying Information About a Specified Account Resource	554
10.5	Creating an Account	556
10.6	Deleting an Account.....	559
10.7	Modifying Information About a Specified Account.....	560
10.8	Querying Information About the Role Resource Collection	563
10.9	Querying Information About a Specified Role Resource.....	565
10.10	Querying Information About the LDAP Service Resource.....	567
10.11	Querying Information About the Collection of LDAP Domain Controller Resources	569
10.12	Querying the Active Directory Information	571
10.13	Modifying the Active Directory Information	574
10.14	Querying LDAP Information	580
10.15	Modifying the LDAP Information	583
11.Operations on Fabric Re- sources.....		589
11.1	Querying Information About the Fabrics Resource Collection	591
11.2	Querying Information About a Specified Fabrics Resource	593
11.3	Querying Information About the Switch Resource Collection	594

11.4	Querying Information About a Specified Switch Resource	596
11.5	Querying Information About the Port Resource Collection of a Specified Switch..	598
11.6	Querying Information About a Specified Port of a Specified Switch	600
12.	Operations on Registry Resources	603
12.1	Querying Information About the Registry Resource Collection.....	605
12.2	Querying Information About a Specified Registry Resource	606
12.3	Querying Information About a Specified Registry Resource File	609
13.	Redfish Installation and Use	612
13.1	Environment Installation.....	612
13.2	Use Case	612
	Glossary	616

About This Manual

Purpose

This manual describes the [iBMC](#) Redfish interfaces of the VANTAGEO server and the related management operations on various resources.

Intended Audience

This manual is intended for:

- Data configuration engineers
- Maintenance engineers

What Is in This Manual

This manual contains the following chapters.

Chapter 1, Redfish Overview	Describes the basic concept of the Redfish interfaces.
Chapter 2, Redfish Resource Tree	Describes the Redfish interface resource paths and the operations allowed for various resources.
Chapter 3, Operations on Public Fixed Resources	Describes the operations on public fixed resources through Redfish interfaces.
Chapter 4, Operations on Manager Resources	Describes the operations on Manager resources through Redfish interfaces.
Chapter 5, Operations on System Resources	Describes the operations on System resources through Redfish interfaces.
Chapter 6, Operations on Chassis Resources	Describes the operations on Chassis resources through Redfish interfaces.
Chapter 7, Operations on SessionService Resources	Describes the operations on SessionService resources through Redfish interfaces.
Chapter 8, Operations on EventService Resources	Describes the operations on EventService resources through Redfish interfaces.
Chapter 9, Operations on UpdateService Resources	Describes the operations on UpdateService resources through Redfish interfaces.
Chapter 10, Operations on AccountService Resources	Describes the operations on AccountService resources through Redfish interfaces.
Chapter 11, Operations on Fabric Resources	Describes the operations on Fabric resources through Redfish interfaces.

Chapter 12, Operations on Registry Resources	Describes the operations on Registry resources through Redfish interfaces.
Chapter 13, Redfish Installation and Use	Describes how to install the environment and use a Redfish interface.

Conventions

This manual uses the following conventions.

	Note: provides additional information about a topic.
---	--

Chapter 1

Redfish Overview

Table of Contents

Basic Concepts.....	12
General Descriptions.....	12

1.1 Basic Concepts

Redfish is an [HTTPS](#)-based management standard. Each HTTPS operation submits or returns a resource in [JSON](#) format encoded in UTF-8 through a RESTful interface to implement device management.

The Redfish's goal of addressing all the components in the data center with a consistent [API](#) adapts to the development trend towards universal software interfaces in the Internet industry. Redfish provides advantages, such as reduced development complexity, easy to implement and use, and high scalability, and is called the next-generation data center management standard.

1.2 General Descriptions

This section describes the Redfish interfaces from the following five aspects: resource operations, resource functions, request headers, response headers, and returned status codes.

Resource Operations

A resource operation supported by a Redfish interface includes two parts: method and [URI](#). For a description of the resource operations supported by a Redfish interface, refer to [Table 1-1](#).

Table 1-1 Resource Operation Descriptions

Operation	Description
GET resource URI	Returns the requested resource.
POST resource URI	Creates a resource or performs a specified action for a resource.
PATCH resource URI	Modifies the properties of a resource.
DELETE resource URI	Deletes a specified resource.

The URI described in this manual is in the following format: `https://device_ip/redfish/v1/path`, which is divided into three parts:

- The first part indicates the URI address, that is, `https://device_ip`, where `device_ip` indicates the [HDM IP](#) address of the server to be accessed.
- The second part indicates the service and version, that is, `/redfish/v1/`. The Redfish interface of the current device is developed based on Redfish v1.
- The third part indicates the unique resource path, that is, `/path/`.



Note

Some resource operations also need request parameters, including request headers and request bodies, which are described in the command format of each resource operation.

Resource Functions

For a description of the resources and their main operations supported by a Redfish interface, refer to [Table 1-2](#).

Table 1-2 Resource Function Descriptions

Resource	Function
Managers	Used for managing BMC resources, including network resources (such as NTP , SNMP , SMTP , LLDP , and SYSLOG), security resources (such as certificates and services), operation logs, and virtual media.
Systems	Used for device management such as host CPU , memory, RAID card, volume, and GPU management, and resource management such as BIOS option, KVM , and event log management.
Chassis	Used for managing physical disks, power supplies, fans, UID , PCIe , NICs , and other devices in the chassis.
SessionService	Used for managing BMC sessions.
EventService	Used for reporting and managing BMC SEL events.
UpdateService	Used for managing updateable BMC firmware resources.

Request Headers

For a description of the request headers of the Redfish interface, refer to [Table 1-3](#).

Table 1-3 Request Header Descriptions

Request Header	Description
Content-Type	Request message format, which is used for operations with a request body. Services shall accept the Content-Type header set to application/json or application/json; charset=utf-8 . It is recommended that clients use either of the above values in requests because other values may cause errors.

Request Header	Description
Odata-Version	OData version. ● If a request contains an unsupported OData version, a service shall reject the request. ● If a service receives a request that contains an unsupported OData version, the service shall reject the request by using the HTTP 412 status code.
Origin	Enables a Web application to use a Redfish service while preventing CSRF attacks.
If-None-Match	● If the ETag of a resource does not match the ETag sent in the request header, the service returns the latest resource and its ETag and the client replaces the cached version with the latest version. ● If the ETag in the request header matches the ETag of the resource, the GET operation returns the HTTP 304 status code.
If-Match	To ensure that clients update the resource from a known status, PATCH requests for resources for which a service returns ETags must support If-Match.
X-Auth-Token	Authenticates the identity of a user in a session. The token value is indistinguishable from the random value. If a service supports this request header, a client can access unsecured resources without establishing a session.
Accept	Communicates to the server the media type or types that the client is prepared to accept. Services shall support the following media types: ● Resource requests whose Accept message header is set to application/json or application/json; charset=utf-8 (that is, requests in JSON format). ● Metadata requests whose Accept message header is set to application/xml or application/ xml; charset=utf-8(that is, requests in XML format).
Authorization	Used for basic authentication. In a system that supports basic authentication, a client can access unsecured resources without this request header.

Response Headers

For a description of the response headers of the Redfish interface, refer to [Table 1-4](#).

Table 1-4 Response Header Descriptions

Response Header	Description
OData-Version	Describes the version number of the OData protocol that the payload complies with in the response message.
Content-Type	Describes the media type used in the message body. ● Services shall set Content-Type to application/json when returning resources as JSON.

Response Header	Description
	- Services shall set Content-Type to application/xml when returning metadata as XML. ;charset=utf-8 shall be appended to the Content-Type if Content-Type is specified in the selected media type in the Accept header for the request.
Content-Length	Describes the size of the message body. To indicate the size of the body, a client preferentially uses the Transfer-Encoding: chunked header instead of the Content Length header, because the Transfer-Encoding: chunked header allows the length of the currently transmitted message to be repeatedly sent. If a service does not support Transfer-Encoding and needs to use Content-Length, the service shall return status code 411.
ETag	Identifier for a specified version of a resource, which is usually a message digest. The ETag header shall be included in responses to GET requests for Manager-Account resources.
Link	Link headers shall be returned as described in the Link headers clause.
Cache-Control	Shall be supported and indicates whether a response can or cannot be cached.
Allow	Description requests supported by services. If a service receives an unsupported request, the service returns a 405 status code together with all supported requests.

Status Codes

For a description of the returned status codes of the Redfish interface, refer to [Table 1-5](#).

Table 1-5 Status Code Descriptions

Status Code	Description
200	The request is successful.
201	The resource is created successfully.
202	The task is created successfully.
204	The request is successful, but no content is returned in the response message body.
301	The requested resource resides under a different URI.
302	The requested resource resides temporarily under a different URI.
304	The service has performed a conditional GET request where access is allowed, but the resource content is not changed.
400	The request is illegal. An error occurs on the client and an error message is returned.

Status Code	Description
401	Invalid user request.
403	The server rejects the request.
404	The requested resource does not exist.
405	The operation is not supported.
406	The Accept header is specified in the request. The resource identified in the request cannot generate a resource representation corresponding to a media type contained in the Accept header.
409	The request causes a conflict in the current state of the resources.
410	The requested resource is unavailable to the service, and no forwarding address is known. This condition is considered permanent. Clients with hyperlink editing capabilities shall delete references to the URI in the client request after user approval. If the service does not know, or has no facility to determine, whether or not the condition is permanent, the status code 404 (Not Found) is used instead. Unless otherwise specified, this response can be cached.
411	The request does not specify the length of its content using the Content-Length header (perhaps Transfer-Encoding: chunked was used instead). The addressed resource requires the Content-Length header.
412	The precondition (such as OData-Version or If-Match) check fails.
415	The request specifies a Content-Type for an unsupported message body.
500	An internal error occurs on the server.
501	The requested function is not available.
503	The service is temporarily overloaded or in maintenance, so it cannot process requests. ● A service may use this response to indicate that the request URI is valid but the service is performing initialization or other maintenance on the resource. ● The service can also use this response to indicate that the service itself is in maintenance. For example, the service is being initialized after reboot.

Others

N/A: indicates that the field value cannot be obtained or the result cannot be confirmed.

NULL: Indicates that the field value is not supported and the obtained value is null.

Chapter 2

Redfish Resource Tree

For a description of the operations allowed for various resources through the Redfish interface, refer to [Table 2-1](#).

Table 2-1 Redfish Resource Tree

URL	Operation
Public fixed resources	
/redfish	GET
/redfish/v1	GET
Managers resources	
/redfish/v1/Managers	GET
/redfish/v1/Managers/manager_id	GET/PATCH
/redfish/v1/Managers/manager_id/SyslogService	GET/PATCH
/redfish/v1/Managers/manager_id/SyslogService/Actions/SyslogService.SubmitTestEvent	POST
/redfish/v1/Managers/manager_id/NtpService	GET/PATCH
/redfish/v1/Managers/manager_id/NetworkProtocol	GET/PATCH
/redfish/v1/Managers/manager_id/EthernetInterfaces	GET
/redfish/v1/Managers/manager_id/EthernetInterfaces/id	GET/PATCH
/redfish/v1/Managers/manager_id/Actions/Manager.Reset	POST
/redfish/v1/Managers/manager_id/LldpService	GET/PATCH
/redfish/v1/Managers/manager_id/SnmpService	GET/PATCH
/redfish/v1/Managers/manager_id/SnmpService/Actions/SnmpService.SubmitTestEvent	POST
/redfish/v1/Managers/manager_id/VirtualMediae	GET
/redfish/v1/Managers/manager_id/VirtualMedia/Media_type	GET

URL	Operation
/redfish/v1/Managers/manager_id/VirtualMedia/media_type/Actions/VirtualMedia.Vmm-Control	POST
/redfish/v1/Managers/manager_id/LogServices/Actions/LogServices.Dump	POST
/redfish/v1/Managers/manager_id/LogServices/Actions/LogServices.Dump/Progress	GET
/redfish/v1/Managers/manager_id/LogServices/Actions/LogServices.ExportLogs	POST
/redfish/v1/Managers/manager_id/KvmService	GET/PATCH
/redfish/v1/Managers/manager_id/LogServices/SEL/Entries/entries_id	GET
/redfish/v1/Managers/manager_id/ISDTService	GET/PATCH
/redfish/v1/Managers/manager_id/ISDTService/Actions/ISDTService.VmmControl	POST
Systems resources	
/redfish/v1/Systems	GET
/redfish/v1/Systems/system_id	GET/PATCH
/redfish/v1/Systems/system_id/Actions/ComputerSystem.Reset	POST
/redfish/v1/Systems/system_id/Processors	GET
/redfish/v1/Systems/system_id/Processors/cpu_id	GET
/redfish/v1/Systems/system_id/Processors?\$expand=.	GET
/redfish/v1/Systems/system_id/Memory	GET
/redfish/v1/Systems/system_id/Memory/memory_id	GET
/redfish/v1/Systems/system_id/Memory?\$expand=.	GET
/redfish/v1/Systems/system_id/Storages	GET
/redfish/v1/Systems/system_id/Storages/storage_id	GET
/redfish/v1/Systems/system_id/Storages?\$expand=.	GET
/redfish/v1/Systems/system_id/Storages/storage_id/Volumes	GET/POST
/redfish/v1/Systems/system_id/Storages/storage_id/Volumes/volume_id	GET/DELETE
/redfish/v1/Systems/system_id/Bios	GET
/redfish/v1/Systems/system_id/Bios/SD	GET/PATCH
/redfish/v1/Systems/system_id/Bios/Actions/Bios.ChangePassword	POST
/redfish/v1/Systems/system_id/Bios/Actions/Bios.ResetBios	POST
Chassis resources	

URL	Operation
/redfish/v1/redfish/v1/Chassis	GET
/redfish/v1/redfish/v1/Chassis/chassis_id	GET/PATCH
/redfish/v1/Chassis/chassis_id/NetworkAdapters	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters?\$expand=.	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/NetworkPorts	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/NetworkPorts/networkports_id	GET/PATCH
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/NetworkPorts/networkports_id/OpticalModule	GET
/redfish/v1/Chassis/chassis_id/PCleDevices	GET
/redfish/v1/Chassis/chassis_id/PCleDevices/pciedevices_id	GET
/redfish/v1/Chassis/chassis_id/PCleDevices/pciedevices_id/Functions/functions_id	GET
/redfish/v1/Chassis/chassis_id/PCleDevices?\$expand=.	GET
/redfish/v1/Chassis/chassis_id/Drives	GET
/redfish/v1/Chassis/chassis_id/Drives/drives_id	GET
/redfish/v1/Chassis/chassis_id/Drives?\$expand=.	GET
/redfish/v1/Chassis/chassis_id/Power	GET/PATCH
/redfish/v1/Chassis/Chassis_id/Power/Actions/Power.CollectHistoryData	POST
/redfish/v1/Chassis/chassis_id/Thermal	GET/PATCH
/redfish/v1/Chassis/chassis_id/Boards	GET
/redfish/v1/Chassis/Chassis_id/Boards/DiskBackplanes	GET
/redfish/v1/Chassis/Chassis_id/Boards/DiskBackplanes/DiskBackplaneId	GET
/redfish/v1/Chassis/Chassis_id/Boards/Risercard	GET
/redfish/v1/Chassis/Chassis_id/Boards/Risercard/RisercardId	GET
/redfish/v1/Chassis/chassis_id/PCleDevices/pciedevices_id/Functions/functions_	GET
SessionService resources	
/redfish/v1/SessionService	GET/PATCH
/redfish/v1/SessionService/Sessions	GET/POST
/redfish/v1/SessionService/Sessions/Session_id	GET/DELETE

URL	Operation
EventService resources	
/redfish/v1/EventService	GET/PATCH
/redfish/v1/EventService/Subscriptions	GET/POST
/redfish/v1/EventService/Subscriptions/id	GET/PATCH/ DELETE
/redfish/v1/EventService/Alarms?\$skip=skip_value&\$top=top_value	GET
/redfish/v1/EventService/DeleteAlarmsAll	DELETE
redfish/v1/EventService/CurrentAlarms	GET
/redfish/v1/EventService/CurrentAlarms/alarm_id	GET/DELETE
/redfish/v1/EventService/DeleteCurrentAlarmsAll	DELETE
/redfish/v1/EventService/CurrentAlertEvents	GET
UpdateService resources	
/redfish/v1/UpdateService	GET
/redfish/v1/UpdateService/FirmwareInventory	GET
/redfish/v1/UpdateService/FirmwareInventory/softid	GET
/redfish/v1/UpdateService/upload	POST
/redfish/v1/UpdateService/InsideFirmwareInventory	GET
/redfish/v1/UpdateService/InsideFirmwareInventory/softid	GET
/redfish/v1/UpdateService/Actions/UpdateService.SimpleUpdat	POST
AccountService resources	
/redfish/v1/AccountService	GET/PATCH
/redfish/v1/AccountService/Accounts	GET/POST
/redfish/v1/AccountService/Accounts/account_id	GET/DELETE/ PATCH
/redfish/v1/AccountService/Roles	GET
/redfish/v1/AccountService/Roles/role_id	GET
/redfish/v1/AccountService/LdapService	GET
/redfish/v1/AccountService/LdapService/LdapControllers	GET
/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory	GET/PATCH

Chapter 3

Operations on Public Fixed Resources

Table of Contents

Querying the Redfish Version Information.....	23
Querying the Current Root Service Resources.....	24

Figure 3-1 shows the path requirements for the public fixed resources supported by VANTAGEO servers.

Figure 3-1 Public Fixed Resources Path Requirements



For a description of the properties of public fixed resources and the operations supported by the properties, refer to [Table 3-1](#).

Table 3-1 Descriptions for Properties of Public Fixed Resources

URL	Property	Description	Operation
/redfish	v1	Redfish version information.	GET
/redfish/v1	Description	Root service description.	GET
	Id	ID of the root server.	GET
	Name	Name of the root service resource.	GET
	Product	Products.	GET
	Redfish Version	Detailed Redfish version information.	GET
	UUID	UUID of the device.	GET
	AccountService	AccountService resources.	GET
	CertificateService	Certificate service resources.	GET
	Systems	System resources.	GET
	Chassis	Chassis resources.	GET

URL	Property	Description	Operation
	EventService	EventService resources.	GET
	JsonSchemas	JSON schema file resources in array format.	GET
	Links	Links.	GET
	Sessions	Session service resources.	GET
	Managers	Manager resources.	GET
	RtpVersion	RTP version information.	GET
	ProtocolFeaturesSupported	Information about protocol features supported by related services.	GET
	ProtocolFeaturesSupported/DeepOperations	Deep operations.	GET
	DeepOperations/DeepPATCH	(AMI native)	GET
	DeepOperations/DeepPOST	(AMI native)	GET
	DeepOperations/MaxLevels	(AMI native)	GET
	ProtocolFeaturesSupported/ExpandQuery	Support for the "expand" query parameter.	GET
	ExpandQuery/ExpandAll	Whether to expand all entries.	GET
	ExpandQuery/Levels	Whether to support the "Levels" qualifier.	GET
	ExpandQuery/Links	Whether to expand hyperlinks inside the Links property.	GET
	ExpandQuery/MaxLevels	Maximum depth to which resources are expanded.	GET
	ExpandQuery/NoLinks	Whether to expand hyperlinks outside the Links property.	GET
	ProtocolFeaturesSupported/SelectQuery	Whether to support the use of the "select" query parameter for the query operation.	GET

URL	Property	Description	Operation
	ProtocolFeaturesSupported/ExcerptQuery	Whether to support the use of the "excerpt" query parameter.	GET
	ProtocolFeaturesSupported/FilterQuery	Whether to support the use of the "filter" query parameter.	GET
	ProtocolFeaturesSupported/OnlyMemberQuery	(AMI native)	GET
	Registries	Message registry resources.	GET
	SessionService	SessionService resources.	GET
	Systems	System resources.	GET
	Tasks	TaskService resources.	GET
	TelemetryService	Network telemetry service resources.	GET
	SessionService	SessionService resources.	GET

2.1 Querying the Redfish Version Information

Function

Query the current version of the Redfish protocol.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish`
- Request Header: None
- Request Message Body: None

Parameters

For a description of the parameters for querying the Redfish version information, refer to [Table 3-2](#).

Table 3-2 Parameter Description for Querying Redfish Version Information

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish
```

- Request Header: None
- Request Message Body: None
- Response Example:

```
{
  "v1": "/redfish/v1/"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the Redfish version information, refer to [Table 3-3](#).

Table 3-3 Output Descriptions for Querying the Redfish Version Information

Field	Type	Description
v1	String	Redfish version information.

2.2 Querying the Current Root Service Resources

Function

Query the current root service resources of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1`

- Request Header: None
- Request Message Body: None

Parameters

For a description of the parameters for querying the current root service resources, refer to [Table 3-4](#).

Table 3-4 Parameter Descriptions for Querying the Current Root Service Resources

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1

- Request Header: None
- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#ServiceRoot.ServiceRoot",
  "@odata.etag": "\"1717400038\"",
  "@odata.id": "/redfish/v1",
  "@odata.type": "#ServiceRoot.v1_7_0.ServiceRoot",
  "AccountService": {
    "@odata.id": "/redfish/v1/AccountService"
  },
  "CertificateService": {
    "@odata.id": "/redfish/v1/CertificateService"
  },
  "Chassis": {
    "@odata.id": "/redfish/v1/Chassis"
  },
  "Description": "The service root for all Redfish requests on this host",
  "EventService": {
    "@odata.id": "/redfish/v1/EventService"
  },
  "Fabrics": {
```

```
    "@odata.id": "/redfish/v1/Fabrics"
  },
  "Id": "RootService",
  "JsonSchemas": {
    "@odata.id": "/redfish/v1/JsonSchemas"
  },
  "Links": {
    "Sessions": {
      "@odata.id": "/redfish/v1/SessionService/Sessions"
    }
  },
  "Managers": {
    "@odata.id": "/redfish/v1/Managers"
  },
  "Name": "Root Service", "Product":
  "Vantageo Redfish Server",
  "ProtocolFeaturesSupported": {
    "DeepOperations": {
      "DeepPATCH": true,
      "DeepPOST": false,
      "MaxLevels": 6
    },
    "ExcerptQuery": true,
    "ExpandQuery": {
      "ExpandAll": true,
      "Levels": true,
      "Links": true,
      "MaxLevels": 5,
      "NoLinks": true
    },
    "FilterQuery": true,
    "OnlyMemberQuery": true,
    "SelectQuery": true
  },
  "RedfishVersion": "1.15.1",
  "Registries": {
    "@odata.id": "/redfish/v1/Registries"
  },
  "SessionService": {
    "@odata.id": "/redfish/v1/SessionService"
  },
  "Systems": {
    "@odata.id": "/redfish/v1/Systems"
  },
}
```

```

    "Tasks": {
      "@odata.id": "/redfish/v1/TaskService"
    },
    "TelemetryService": {
      "@odata.id": "/redfish/v1/TelemetryService"
    },
    "UUID": "30e72400-0000-1000-0000-000000000000",
    "UpdateService": {
      "@odata.id": "/redfish/v1/UpdateService"
    }
  }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the current root service resources, refer to [Table 3-5](#).

Table 3-5 Output Descriptions for Querying the Current Root Service Resources

Field	Type	Description
@odata.context	String	OData description of the root service resource model.
@odata.id	String	Access path of the root service resource node.
@odata.type	String	Type of root service resource.
Description	String	Root service description.
Id	String	ID of the root service.
Name	String	Name of the root service resource.
Product	String	Products.
RedfishVersion	String	Detailed Redfish version information.
UUID	String	UUID of the device.
AccountService	Object	AccountService resources.
CertificateService	Object	Certificate service resources.
Chassis	Object	Chassis resources.
EventService	Object	EventService resources.
JsonSchemas	Object	JSON schema file resources in array format.
Links	Object	Links.
Sessions	Object	SessionService resources.
Managers	Object	Manager resources.

Field	Type	Description
RtpVersion	String	RTP version information.
ProtocolFeaturesSupported	Object	Information about protocol features supported by related services.
ProtocolFeaturesSupported/DeepOperations	Object	Deep operations.
DeepOperations/DeepPATCH	Boolean	(AMI native)
DeepOperations/DeepPOST	Boolean	(AMI native)
DeepOperations/MaxLevels	Number	(AMI native)
ProtocolFeaturesSupported/ExpandQuery	Object	Support for the "expand" query parameter.
ExpandQuery/ExpandAll	Boolean	Whether to expand all entries.
ExpandQuery/Levels	Boolean	Whether to support the "Levels" qualifier.
ExpandQuery/Links	Boolean	Whether to expand hyperlinks inside the Links property.
ExpandQuery/MaxLevels	Number	Maximum depth to which resources are expanded.
ExpandQuery/NoLinks	Boolean	Whether to expand hyperlinks outside the Links property.
ProtocolFeaturesSupported/SelectQuery	Boolean	Whether to support the use of the "select" query parameter for the query operation.
ProtocolFeaturesSupported/ExcerptQuery	Boolean	Whether to support the use of the "excerpt" query parameter.
ProtocolFeaturesSupported/FilterQuery	Boolean	Whether to support the use of the "filter" query parameter.
ProtocolFeaturesSupported/OnlyMemberQuery	Boolean	(AMI native)
Registries	Object	Message registry resources.
SessionService	Object	SessionService resources.
Systems	Object	System resources.
Tasks	Object	TaskService resources.
TelemetryService	Object	Network telemetry service resources.
UpdateService	Object	UpdateService resources.

Chapter 4

Operations on Manager Resources

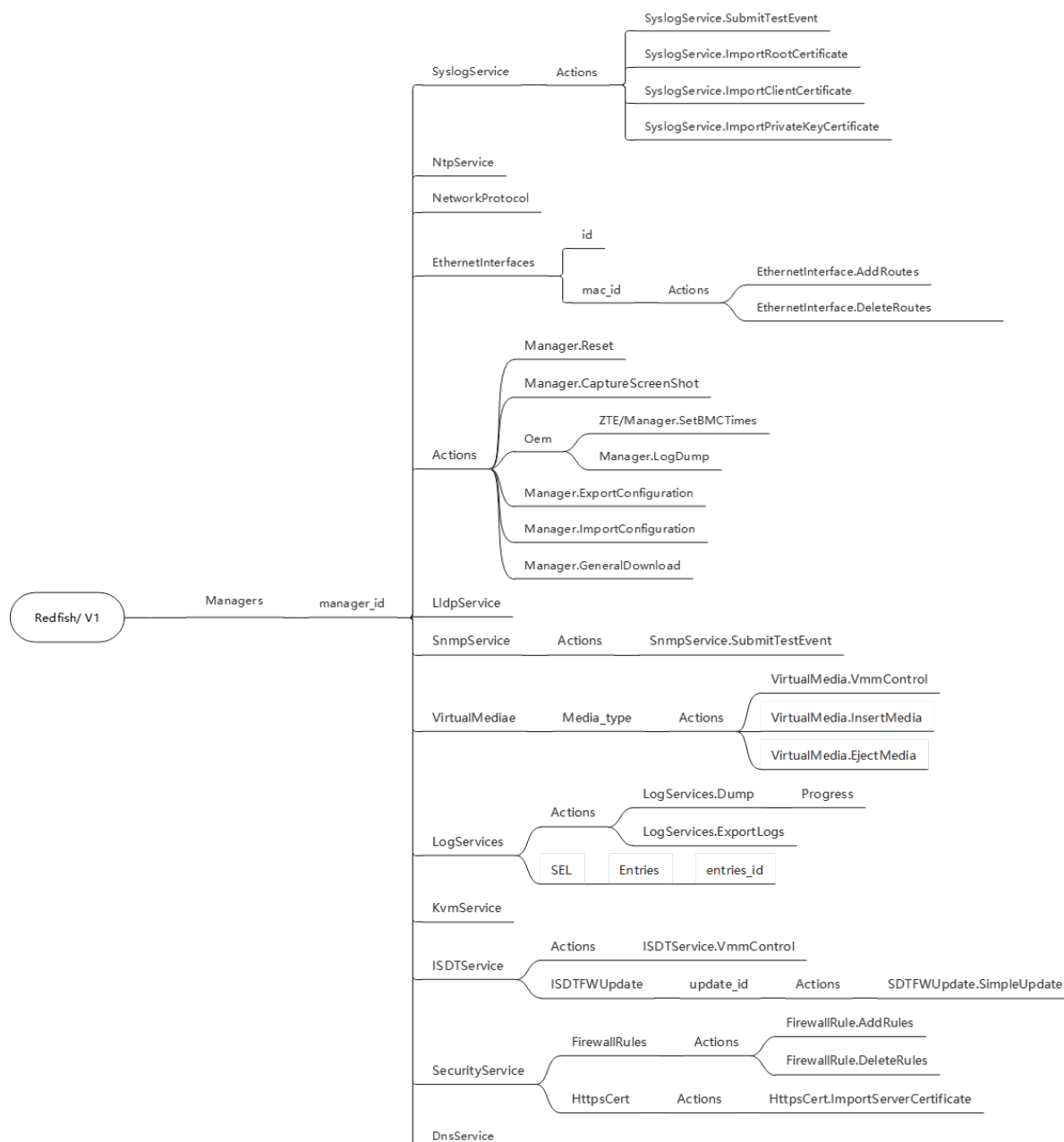
Table of Contents

Querying Information About the Manager Resource Collection	49
Querying Information About a Specified Manager Resource.....	51
Modifying Information About a Specified Manager Resource.....	57
Querying Information About the Syslog Configuration	59
Configuring Information About the Syslog Server	62
Submitting a Syslog Test Log.....	69
Querying Information About the NtpService Configuration Resource.....	70
Modifying Properties of the NTP Resource	72
Querying Information About the BMC Service.....	75
Modifying Information About a Specified BMC Service	80
Querying the BMC Management Interface Resource Collection.....	88
Querying Information About a Specified BMC Management Interface Resource	90
Modifying a Specified BMC Management Interface Resource	97
Restarting the BMC	104
Querying Information About the LLDP Service Configuration Resource.....	107
Modifying Properties of the LLDP Service Resource.....	109
Querying Information About the SNMP Resource.....	111
Modifying Properties of the SNMP Resource.....	115
Submitting an SNMP Trap Test Event.....	122
Querying the Virtual Media Resource Collection	124
Querying a Virtual Media Resource.....	126
Connecting to the Virtual Media.....	129
Disconnecting the Virtual Media.....	131
Sending a One-Click Collection Request.....	133
Querying the One-Click Collection Progress.....	136
Exporting Logs.....	138
Querying the KVM Service Resource.....	140

Modifying Information About the KVM Resource.....	142
Querying Information About a Specified SEL Log Service Resource.....	145
Capturing the Screen Manually.....	147
Downloading the Manually Captured Screen Image.....	149
Querying Information About the ISDT Resource.....	150
Modifying Properties of the ISDT Service Resource.....	152
Mounting and Dismounting Navigation Disks.....	154
Querying Information About the ISDT FWUpdate Collection.....	156
Querying Information About an ISDT FWUpdate Task.....	157
Burning an ISDT Image.....	160
Adding Routes.....	162
Deleting Routes.....	164
Querying Information About the SecurityService Resource.....	166
Querying Information About SecurityService Rules.....	168
Adding a Firewall Rule.....	171
Deleting a Firewall Rule.....	174
Attaching Remote Media to the Virtual Media Device.....	175
Detaching Remote Media from the Virtual Media Device.....	177
Setting the BMC Time.....	179
Importing the Syslog Root Certificate.....	181
Importing a Local Syslog Certificate.....	185
Importing a Private Key Certificate.....	188
Querying SSL Certificate Information.....	191
Importing an SSL Certificate.....	196
Exporting BIOS or BMC Configurations.....	200
Importing BIOS and BMC Configurations.....	202
Downloading a Redfish File.....	204
Enabling the GPU Module to Start Collecting Logs.....	205
Enabling the GPU Module to Obtain Log Files.....	207
Querying Information About the DNS Service.....	208
Modifying Information About the DNS Service.....	210

Figure 4-1 shows the path requirements for the Managers resources supported by VANTAGEO servers.

Figure 4-1 Managers Resource Path Requirements



For a description of the properties of Manager resources and the operations supported by the properties, refer to [Table 4-1](#).

Table 4-1 Description for Properties of Manager Resources

URL	Property	Description	Operation
/redfish/v1/Managers	Name	Name of the Manager resource collection.	GET

URL	Property	Description	Operation
	Members@odata.count	Number of Manager resource members.	GET
	Members	Manager resource list.	GET
/redfish/v1/Managers/manager_id	Id	ID of the Manager resource.	GET
	Name	Name of the Manager resource.	GET
	ManagerType	Type of Manager resource.	GET
	FirmwareVersion	Firmware version of the Manager resource.	GET
	FirmwareVersionDate	BMC version date.	GET
	Model	Model of the Manager resource.	GET
	UUID	UUID of the Manager resource.	GET
	DateTime	System time of the Manager resource.	GET
	DateTimeLocalOffset	Time zone of the Manager resource.	GET/PATCH
	NetworkProtocol	Access path of the network protocol supported by the specified Manager resource.	GET
	EthernetInterfaces	Access path of the Ethernet interface information about the specified Manager resource.	GET
	NtpService	Access path of the NTP service of the specified Manager resource.	GET
	SyslogService	Access path of the Syslog service of the specified Manager resource.	GET
	KvmService	Access path of the KVM service the specified Manager resource.	GET
	SnmpService	Access path of the KVM service the specified Manager resource.	GET
	SntpService	Access path of the KVM service the specified Manager resource.	GET
	LldpService	Access path of the KVM service the specified Manager resource.	GET

URL	Property	Description	Operation
	VirtualMedia	Access path of the virtual media service of the specified Manager resource.	GET
	Links	Links to the related resources.	GET
	Actions	Available actions for the specified Manager resource.	GET
	Oem	Customized properties.	GET
	#Manager.Rollback	OS operation.	GET
	RollBackType@Redfish.AllowableValues	OS operations allowed through the Redfish interface, including: RollBack	GET
	target	Operation path.	GET
	Manager.Rollback	Switches BMC versions.	GET
	Manager.ImportConfiguration	Imports the configuration.	GET
	Manager.ExportConfiguration	Exports the configuration.	GET
	Manager.FactoryReset	Resets factory settings.	GET
	Oem.Public	Customized field.	GET
	USB0InterfaceEnabled	Whether the virtual network interface named usb0 is enabled: ● true: yes. ● false: no.	GET
	IfMatchEnabled	Whether the match operation is enabled: ● true: yes. ● false: no.	GET
	ISDTService	Access path of the ISDT service the specified Manager resource.	GET
	FirewallService	Access path of the firewall service the specified Manager resource.	GET
	NAT	Access path of the NAT resource.	GET
	Manufacturer	BMC chip manufacturer.	GET
/redfish/v1/Managers/manager_id/SyslogService	Id	ID of the Syslog resource.	GET
	Name	Name of the Syslog resource.	GET
	ServiceEnabled	Syslog service enabled.	GET/PATCH

URL	Property	Description	Operation
	ServerIdentitySource	- Board serial number: BoardSN - Asset tag: ProductAssetTag - Host name: HostName	GET/PATCH
	TransmissionProtocol	Transmission protocol: - UDP - TCP	GET/PATCH
	AuthenticateMode	Authentication mode: - OneWay: unidirectional authentication. - TwoWay: bidirectional authentication.	GET
	SyslogServers	Syslog servers.	GET/PATCH
	MemberId	0 1 2 3	GET
	Enabled	Channel enabled.	GET/PATCH
	Address	Server address.	GET/PATCH
	Port	Server port number.	GET/PATCH
	LogType	Log type.	GET/PATCH
/redfish/v1/Managers/manager_id/NtpService	AlternateNtpServer	Address of the alternate NTP server.	GET
	CurrentPollingInterval	Current polling interval.	GET
	Description	Description of the NTP resource.	GET
	ExtraNtpServer	Address of the extra NTP server.	GET
	MaxPollingInterval	Maximum polling interval.	GET
	MinPollingInterval	Minimum polling interval.	GET
	PreferredNtpServer	Address of the preferred NTP server.	GET
	ServerAuthenticationEnabled	Whether server security authentication is enabled.	GET
	ServiceEnabled	Whether the NTP service is enabled: - true - false	GET
/redfish/v1/Managers/manager-	Description	BMC resource description.	GET/PATCH
	Id	BMC network protocol resource ID.	GET/PATCH

URL	Property	Description	Operation
er_id/NetworkProtocol	Name	BMC network protocol resource name.	GET/PATCH
	HostName	BMC management host name.	GET/PATCH
	HTTPS/KVMIP/SNMP/SSH/VirtualMedia/IPMI	Service information supported by BMC.	GET/PATCH
	ProtocolEnabled	Whether the protocol is enabled: ● true ● false	GET/PATCH
	Port	Service port number.	GET/PATCH
	Oem.Public	-	GET/PATCH
	VirtualMedia-CD/VirtualMedia-HD	-	GET/PATCH
	Timeout	Service timeout period, unit: minutes.	GET/PATCH
	ProtocolEnabled	Whether the protocol is enabled: ● true ● false	GET/PATCH
	Port	Service port number.	GET/PATCH
	Instance	Number of instances.	GET/PATCH
	NotifyMulticastIntervalSeconds	Time interval between transmissions of the multicast SSDP NOTIFY message.	GET/PATCH
	NotifyIPv6Scope	IPv6 scope for multicast SSDP NOTIFY messages. ● Link: SSDP Notify messages are sent to addresses in the IPv6 local link scope. ● Site: SSDP Notify messages are sent to addresses in the IPv6 local site scope. ● Organization: SSDP Notify messages are sent to addresses in the IPv6 local organization scope.	GET/PATCH
	NotifyEnabled	Whether SSDP NOTIFY messages are multicast.	GET/PATCH
	VNC	VNC service.	GET/PATCH
	SecurePort	Secure port.	GET/PATCH

URL	Property	Description	Operation
/redfish/v1/Managers/manager_id/EthernetInterfaces	Description	Description of the BMC management interface resource collection.	GET
	Name	Name of the BMC management interface resource collection.	GET
	Members@odata.count	Number of resources in the management interface resource collection.	GET
	Members	List of resources in the management interface resource collection.	GET
/redfish/v1/Managers/manager_id/EthernetInterfaces/id	Id	ID of the specified BMC management interface resource.	GET
	Name	Name of the specified BMC management interface resource.	GET
	PermanentMACAddress	Permanent MAC address of the specified BMC management interface resource.	GET
	InterfaceEnabled	Whether the interface is enabled.	GET
	MTUSize	MTU configured on the current interface (in bytes).	GET
	AutoNeg	Whether the rate and multiplexing are automatically negotiated: ● true ● false	GET
	FullDuplex	Whether full duplex mode is used: ● true ● false	GET
	SpeedMbps	Current rate (in Mbps).	GET
	Description	Description of the specified BMC management interface resource.	GET
	HostName	DNS hostname, which does not contain any domain information.	GET
	IPv4Addresses	IPv4 information object.	GET
	Address	IPv4 address.	GET
	AddressOrigin	Source of the IPv4 address: ● Static ● DHCP	GET

URL	Property	Description	Operation
	Gateway	Gateway of the IPv4 address.	GET
	SubnetMask	IPv4 subnet mask.	GET
	IPv6DefaultGateway	Default IPv6 gateway.	GET
	IPv6Addresses	IPv6 information object.	GET
	Address	IPv6 address.	GET
	AddressOrigin	Source of the IPv6 address: • Static • DHCPv6 • LinkLocal	GET
	PrefixLength	Prefix length of the IPv6 address.	GET
	IPv6StaticAddresses	Static IPv6 information object.	GET
	Address	Static IPv6 address.	GET
	PrefixLength	Prefix length of the static IPv6 address.	GET
	Oem.Public	OEM object.	GET
	IPStacks	Whether IPv4 and IPv6 are enabled: • null: interface not enabled • IPv4: IPv4 enabled only • IPv6: IPv6 enabled only • IPv4AndIPv6: IPv4 and IPv6 both enabled	GET
	DNSServiceEnabled	Whether the DNS service is enabled.	GET
	DNSDhcpEnabled	Whether DNS DHCP is enabled: • true: automatic • false: manual	GET
	PatchInProgress	Configuration validity flag: • true: being configured • false: applied successfully	GET
	DoMain	Domain name.	GET
	VLANPriority	VLAN priority, range: 0–7.	GET
	NetworkPortMode	Network port mode: • Automatic • Fixed: fixed mode • Standalone: standalone mode	GET

URL	Property	Description	Operation
	NCSIModeSelect	NCSI mode: - Automatic - Manual - null: default for non-standalone mode and automatic mode	GET
	ManagementNetworkPort	In fixed mode of the specified management network interface, there is only one group of BMC management network interface data. In automatic mode and standalone mode, there are dedicated interface data and shared interface data.	GET
	Type	- Dedicated: dedicated network interface. - ShareLink: shared network interface.	GET
	CardNumber	The default value for a dedicated network interface is null, and the default value for a shared network interface is: 1: NIC 1 2: NIC 2	GET
	PortNumber	For a dedicated network port, the default serial number is set to 0. For a shared network port, this parameter indicates the silkscreen number of the network interface, ranging from 1 through 4.	GET
	ActualPortNumber	Actual silk screen number of the network interface, range: 1–4. This field is displayed only when the network interface mode is set to standalone or automatic (the selected network interface is not a dedicated interface), and the NCSI mode is set to automatic.	GET
	ManagementNetworkPort@Redfish.AllowableValues	All available network interfaces of the BMC.	GET
	NameServers	Domain name server list.	GET

URL	Property	Description	Operation
	Status	Status information about the specified BMC management interface resource. ● State: enabling status of the BMC management interface. ● Health: health status of the BMC management interface.	GET
	VLAN	VLAN information object.	GET
	VLANEnable	Whether VLAN is enabled: ● true: enabled ● false: disabled	GET
	VLANId	Configured VLAN ID, range: 2–4094.	GET
	IPv4Routes	IPv4 route information about the NIC.	GET
	IPv6Routes	IPv6 route information about the NIC.	GET
	Actions	Operations that can be performed on the resource.	GET
	EthernetInterface.AddRoutes	Adds a route.	GET
	EthernetInterface.DeleteRoutes	Deletes a route.	GET
	target	Access path of the route operation.	GET
/redfish/v1/Managers/manager_id/Actions/Manager.Reset	code	String indicating the specified message ID in the message registry.	POST
	message	Readable message for the code in the message registry.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity level. Options: ● OK ● Warning ● Critical	POST
	Resolution	Recommended solution.	POST

URL	Property	Description	Operation
/redfish/v1/Managers/manager_id/LldpService	Description	Description of the LLDP resource.	GET
	Id	ID of the LLDP resource.	GET
	Name	Name of the LLDP resource.	GET
	LldpEnabled	LLDP enabled.	GET/PATCH
	WorkMode	LLDP operation mode.	GET/PATCH
/redfish/v1/Managers/manager_id/SnmpService	Actions	Operations that can be performed on the SNMP resource.	GET
	SnmpService.SubmitTestEvent	Submits an SNMP trap test event.	GET
	target	Access path for sending the SNMP trap test event.	GET
	Description	Description of the LLDP resource.	GET
	Id	ID of the LLDP resource.	GET
	Name	Name of the LLDP resource.	GET
	ComplexPwdEnable	Complex password switch: ● true: turns on the switch. ● false: turns off the switch.	GET
	ReadOnlyCommunity	SNMP read-only community. Note: This property contains sensitive information and is displayed as null. The PATCH operation is available.	GET
	ReadWriteCommunity	SNMP readwrite community. Note: This property contains sensitive information and is displayed as null. The PATCH operation is available.	GET
	SnmpServiceEnable	Whether SNMP is enabled: ● true: yes. ● false: no.	GET
	SnmpServicePort	SNMP port number.	GET
	SnmpTrapNotification	SNMP Trap properties.	GET
	TrapServer	SNMP Trap server information.	GET
	MemberId	SNMP Trap group member number.	GET
	TrapServerAddress	SNMP Trap server address.	GET
	TrapServerEnable	Current Trap Server status:	GET

URL	Property	Description	Operation
		● true: enabled ● false: disabled	
	TrapServerPort	Trap server port number.	GET
	AlarmSeverity	Event severity: ● Critical ● Major ● Minor ● Normal	GET
	TrapHostIdentify	Trap host ID: ● BoardSN: board SN. ● ProductAssetTag: product asset tag. ● HostName: host name.	GET
	TrapV3User	SNMPv3 username.	GET
	TrapVersion	SNMP trap version number: ● V1 ● V2C ● V3	GET
	TrapServer@odata.count	Number of SNMP trap servers.	GET
	snmpTrapCommunity	SNMP trap community name.	GET
	snmpTrapEnable	Whether to enable the SNMP trap function. ● true: yes. ● False: no.	GET
	SnmpV3AuthUser	This array lists all users with the SNMP permission.	GET
	snmpV3AuthProtocol	SNMPv3 user authentication algorithm: ● SHA ● MD5 ● SHA256 ● SHA384 ● SHA512	GET
	snmpV3PrivProtocol	NMPv3 user encryption algorithm: ● DES ● AES ● AES256	GET

URL	Property	Description	Operation
	UserName	Username with the SNMP permission.	GET
	SnmpV3AuthUser@odata.count	Number of users with the SNMP permission.	GET
	SnmpV3EngineID	SNMPv3 Engine ID.	GET
/redfish/v1/Managers/manager_id/VirtualMediae	Description	Description.	GET
	Members	virtual media resource list, where the CD1 and USBStick1 resources can be queried and used only after the number of entities is set to two.	GET
	Members@odata.count	Number of virtual media resource members that can be connected currently.	GET
	Name	Name of the virtual media resource collection.	GET
/redfish/v1/Managers/manager_id/VirtualMedia/Media_type	Description	Description.	GET
	ConnectedVia	Connection method.	GET
	Id	ID of the virtual media resource.	GET
	Name	Name of the virtual media resource.	GET
	MediaTypes	Media plane type: - CD - USBStick	GET
	TransferProtocolType	Transfer protocol: - NFS - CIFS - HTTPS	GET
	TransferMethod	Transfer method: stream.	GET
	Image	Image path.	GET
	ImageName	Image name.	GET
	ConnectedVia	Connection method.	GET
	Inserted	Connection status: - true: mounting (inserted) - false: removed	GET

URL	Property	Description	Operation
	Oem	Customized properties of a specified session.	GET
/redfish/v1/Managers/manager_id/VirtualMedia/media_type/Actions/VirtualMedia.VmmControl	Information	-	POST
	target	Access path of the current virtual media resource.	POST
/redfish/v1/Managers/manager_id/LogServices/Actions/LogServices.Dump	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity level. Options: • OK • Warning • Critical	POST
	Resolution	Recommended solution.	POST
/redfish/v1/Managers/manager_id/LogServices/Actions/LogServices.Dump/Progress	Percentage	Task progress percentage.	GET
	State	State.	GET
	Type	Type.	GET
	Message	Task progress status.	GET
	TarName	File name of the compressed package, in which UnknownProductSN is replaced with the actual SN number. If it is not obtained, it is UnknownProductSN .	GET
	TarPath	Storage path of the local compressed package.	GET
/redfish/v1/Managers/manager_id/LogServices/Actions/LogServices.ExportLogs	code	ID of the specified message in the message registry.	POST
	message	Readable message for the code in the message registry.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST

URL	Property	Description	Operation
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity. Options: ● OK ● Warning ● Critical	POST
	Resolution	Recommended solution.	POST
/redfish/v1/Managers/manager_id/KvmService	MaximumNumberOfSessions	Maximum number of KVM sessions.	POST/PATCH
	KvmUrl	URL for logging in to the KVM. When you log in through this URL, the Web session is automatically logged out.	POST
	NumberOfActivatedSessions	Number of current KVM sessions.	POST/PATCH
	ActivatedSessionsType	Type of KVM session: ● Shared: shared ● Private: exclusive	POST/PATCH
	EncryptionEnabled	Whether KVM encryption is enabled: ● true: yes. ● false: no.	POST/PATCH
	SessionTimeoutMinutes	Session timeout period. Range: 1–60, unit: minutes.	POST/PATCH
/redfish/v1/Managers/manager_id/LogServices/SEL/Entries/entries_id	Created	Time when the SEL log instance is created.	GET
	Description	Log resource description information.	GET
	EntryCode	Type of SEL log instance.	GET
	EntryType	Type of SEL log instance.	GET
	EventTimestamp	Timestamp of the SEL log instance information.	GET
	Id	ID of the SEL log instance.	GET
	Message	Message content of the SEL log instance information.	GET
	Name	Name of the SEL log instance.	GET
	SensorNumber	ID of the sensor that creates the SEL log instance.	GET

URL	Property	Description	Operation
	SensorType	Type of the sensor that creates the SEL log instance.	GET
	Message	Details.	GET
	Severity	Log severity level of the SEL log instance information.	GET
	Oem.Public	Customized properties.	GET
	OwnerLUN	SensorNumber extension.	GET
/redfish/v1/Managers/manager_id/ISDTService	ImageInstalled	Whether there is a navigation disk image.	GET
	Actions	Available actions for the ISDT resource.	GET
	#ISDTService.VmmControl	Control operation on the navigation disk.	GET
	target	Path of the control operation on the navigation disk.	GET
	ServiceEnabled	Whether service is enabled.	PATCH
/redfish/v1/Managers/manager_id/ISDTService/Actions/ISDTService.VmmControl	Information	-	POST
	target	Access path of the current ISDT resource.	POST
/redfish/v1/Managers/manager_id/ISDTService/ISDTFWUpdate	Name	Name of the ISDT FWUpdate collection.	GET
	Members@odata.count	Number of ISDT FWUpdate tasks, which is fixed to one.	GET
	Members.@odata.id	ISDT FWUpdate task.	GET
/redfish/v1/Managers/manager_id/ISDTService/ISDTFWUpdate/updateid	Id	Updateable resource, which is fixed to 1.	GET
	Name	Interface description.	GET
	TransferState	File transfer status. Value: Initiating.	GET
	TransferFileName	Name of the file being transferred. Value: ImageUrl carried in the request during upgrade.	GET

URL	Property	Description	Operation
	UpgradeProgress	Task completion progress, range: 0–100.	GET
	Messages	Task progress description, which is not fixed. A completion time string is available when the task is completed.	GET
	Actions	Operations that can be performed on the resource.	GET
/redfish/v1/Managers/manager_id/ISDTSERVICE/ISDTFWUpdate/update_id/Actions/SDTFWUpdate.SimpleUpdate	code	Response code description.	POST
	message	Prompt message that is returned.	POST
/redfish/v1/Managers/manager_id/SecurityService	Id	Unique identifier.	GET
	Name	Resource name.	GET
	FirewallRules	Lower-level firewall rule URI.	GET
/redfish/v1/Managers/manager_id/SecurityService/FirewallRules	Id	Unique identifier.	GET
	Name	Resource name.	GET
	ActiveStrategy	Currently valid policy: ● Accept: enables rules that accept data, that is, the allowlist takes effect. ● Drop: enables rules that drop data, that is, the blocklist takes effect.	GET
	Rules	Rule list.	GET
	Actions	Operations that can be performed on the resource.	GET
	RuleType	Mode type of this rule.	GET
	StartDateTime	Time when the rule takes effect.	GET
	EndDateTime	Time when the rule becomes invalid.	GET
	StartIPAddress	Start IP address corresponding to the rule.	GET

URL	Property	Description	Operation
	EndIPAddress	End IP address corresponding to the rule.	GET
	StartMacAddress	Start MAC address corresponding to the rule.	GET
	EndMacAddress	End MAC address corresponding to the rule.	GET
	WorkdayOnly	Whether the rule is effective on work-days only.	GET
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.SetBMCTimes	Message	Details.	POST
	MessageId	Message ID.	POST
	Resolution	Recommended solution.	POST
	Severity	Severity level. Options: • OK • Warning • Critical	POST
/redfish/v1/Managers/manager_id/SecurityService/HttpsCert	Id	Resource ID.	GET
	Name	Resource name.	GET
	Version	Version.	GET
	IssuerAddress	Issuer's email address.	GET
	KeyUsage	Certificate usage.	GET
	PublicKey	Public key.	GET
	PublicKeyLengthBits	Public key length.	GET
	SerialNumber	Serial number.	GET
	SignatureAlgorithm	Signature algorithm.	GET
	Issuer	Certificate issuer.	GET
	Subject	Certificate receiver.	GET
	City	City or area.	GET
	CommonName	Common name.	GET
	Country	Country.	GET
	Organization	Organization.	GET
	OrganizationalUnit	Organizational unit.	GET

URL	Property	Description	Operation
	State	Province (state).	GET
	SubjectAddress	Recipient's email address.	GET
	ValidNotAfter	End time of the validity period of the certificate.	GET
	ValidNotBefore	Start time of the validity period of the certificate.	GET
/redfish/v1/Managers/manager_id/SecurityService/HttpsCert/Actions/HttpsCert.ImportServerCertificate	Message	Details.	POST
	MessageId	Message ID.	POST
	MessageArgs	Message arguments.	POST
	Resolution	Recommended solution.	POST
	Severity	Severity level. Options: ● OK ● Warning ● Critical	POST
/redfish/v1/Managers/manager_id/Actions/Manager.ExportConfiguration	Messages	Message list.	POST
	Message	Details.	POST
	MessageId	Message ID.	POST
	Resolution	Recommended solution.	POST
	Severity	Severity level. Options: ● OK ● Warning ● Critical	POST
/redfish/v1/Managers/manager_id/DnsService	DnsIpConfig	DnsIpConfig resource list.	GET
	DnsDhcpEnable	Whether the DNS service is enabled.	GET
	DnsEnable	Whether DNS is enabled.	GET
	NameServers	The first value indicates the primary server, the second value indicates standby server 1, and the third value indicates standby server 2.	GET
	DomainConfig	Domain name configuration.	GET
	DomainName	Domain name.	GET
	HostNameConfig	Hostname object.	GET
	HostSetting	Hostname configuration mode.	GET

URL	Property	Description	Operation
	PatchInProgress	Configuration validity flag.	GET
	RegisterBMC	Registration mode.	GET

4.1 Querying Information About the Manager Resource Collection

Function

Query information about the Manager resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** *https://device_ip/redfish/v1/Managers*
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the Manager resource collection, refer to [Table 4-2](#).

Table 4-2 Parameter Descriptions for Querying Information About the Manager Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Managers

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#ManagerCollection.ManagerCollection",
  "@odata.id": "/redfish/v1/Managers",
  "@odata.type": "#ManagerCollection.ManagerCollection",
  "Description": "The collection for Managers",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Managers/1"
    }
  ],
  "Members@odata.count": 1,
  "Name": "Manager Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the Manager resource collection, refer to [Table 4-3](#).

Table 4-3 Output Descriptions for Querying Information About the Manager Resource Collection

Field	Type	Description
@odata.context	String	OData description of the Manager resource collection model.
@odata.id	String	Access path of the Manager resource collection node.
@odata.type	String	Type of Manager resource collection.
Description	String	Description of the Manager resource collection.
Name	String	Name of the Manager resource collection.
Members@odata.count	Number	Number of Manager resource members.
Members	Object	Manager resource list.
@odata.id	String	Access path of a single Manager resource node.

4.2 Querying Information About a Specified Manager Resource

Function

Query information about a specified Manager resource of a server.



Note

Only the **BMC** resource information about the server itself can be queried.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified Manager resource, refer to [Table 4-4](#).

Table 4-4 Parameter Descriptions for Querying Information About the Specified Manager Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Managers/1

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Manager.Manager",
  "@odata.id": "/redfish/v1/Managers/1",
  "@odata.type": "#Manager.v1_13_0.Manager",
  "Manufacturer": "ASPEED",
  "Actions": {
    "Oem": {
      "#Manager.FactoryReset": {
        "target": "/redfish/v1/Managers/1/Actions/Manager.FactoryReset",
        "FactoryResetType@Redfish.AllowableValues": [
          "ResetAll"
        ]
      },
      "#Manager.Rollback": {
        "target": "/redfish/v1/Managers/1/Actions/Manager.Rollback",
        "RollbackType@Redfish.AllowableValues": [
          "RollBack"
        ]
      }
    },
    "#Manager.Reset": {
      "target": "/redfish/v1/Managers/1/Actions/Manager.Reset",
      "ResetType@Redfish.AllowableValues": [
        "ForceRestart"
      ]
    },
    "#Manager.CaptureScreenShot": {
      "target": "/redfish/v1/Managers/1/Actions/Manager.CaptureScreenShot"
    },
    "#Manager.DownloadScreenShot": {
      "target": "/redfish/v1/Managers/1/Actions/Manager.DownloadScreenShot"
    },
    "#Manager.ImportConfiguration": {
      "target": "/redfish/v1/Managers/1/Actions/Manager.ImportConfiguration"
    },
    "#Manager.ExportConfiguration": {
      "target": "/redfish/v1/Managers/1/Actions/Manager.ExportConfiguration"
    }
  }
}
```



```
    "#Manager.GeneralDownload": {
      "target": "/redfish/v1/Managers/1/Actions/Manager.GeneralDownload"
    },
    "CommandShell": {
      "MaxConcurrentSessions": 36,
      "ServiceEnabled": true
    },
    "DateTime": "2010-03-24T12:34:27+08:00",
    "DateTimeLocalOffset": "+08:00",
    "Description": "BMC",
    "EthernetInterfaces": {
      "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces"
    },
    "GraphicalConsole": {
      "MaxConcurrentSessions": 4,
      "ServiceEnabled": true
    },
    "Id": "1",
    "ManagerType": "BMC",
    "Model": "43707000",
    "Name": "Manager",
    "NetworkProtocol": {
      "@odata.id": "/redfish/v1/Managers/1/NetworkProtocol"
    },
    "SerialConsole": {
      "MaxConcurrentSessions": 3,
      "ServiceEnabled": true
    },
    "Status": {
      "Health": "OK",
      "State": "Enabled"
    },
    "VirtualMedia": {
      "@odata.id": "/redfish/v1/Managers/1/VirtualMedia"
    },
    "Links": {
      "ManagerForChassis": [
        {
          "@odata.id": "/redfish/v1/Chassis/1"
        }
      ],
      "ManagerForServers": [
        {
```

```

        "@odata.id": "/redfish/v1/Systems/1"
    },
    ],
    "ManagerInChassis": [
        {
            "@odata.id": "/redfish/v1/Chassis/1"
        }
    ],
    },
    "NtpService": {
        "@odata.id": "/redfish/v1/Managers/1/NtpService"
    },
    "LogServices": {
        "@odata.id": "/redfish/v1/Managers/1/LogServices"
    },
    "LldpService": {
        "@odata.id": "/redfish/v1/Managers/1/LldpService"
    },
    "SyslogService": {
        "@odata.id": "/redfish/v1/Managers/1/SyslogService"
    },
    "KvmService": {
        "@odata.id": "/redfish/v1/Managers/1/KvmService"
    },
    "SnmpService": {
        "@odata.id": "/redfish/v1/Managers/1/SnmpService"
    },
    "FirmwareVersion": "04.22.01.01",
    "UUID": "30e72400-0000-1000-0000-000000000000",
    "ServiceEntryPointUUID": "30e72400-0000-1000-0000-000000000000",
    "Oem": {
        "NAT": {
            "@odata.id": "/redfish/v1/Managers/1/NAT"
        },
        "Public": {
            "FirmwareVersionDate": "May 09 2024",
            "IfMatchEnabled": false,
            "USB0InterfaceEnabled": false,
            "ISDTSservice": {
                "@odata.id": "/redfish/v1/Managers/1/ISDTSservice"
            },
            "DnsService": {
                "@odata.id": "/redfish/v1/Managers/1/DnsService"
            }
        }
    },

```

```

        "FirewallService":{
            "@odata.id": "/redfish/v1/Managers/1/SecurityService"
        }
    }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified Manager resource, refer to [Table 4-5](#).

Table 4-5 Output Descriptions for Querying Information About the Specified Manager Resource

Field	Type	Description
@odata.context	String	OData description of the specified Manager resource collection model.
@odata.id	String	Access path of the specified Manager resource node.
@odata.type	String	Type of the specified Manager resource.
Id	String	ID of the Manager resource.
Name	String	Name of the Manager resource.
ManagerType	String	Type of Manager resource.
FirmwareVersion	String	Firmware version of the Manager resource.
UUID	String	UUID of the Manager resource.
ServiceEntryPointUUID	String	UUID of the service entry point of the Manager resource.
Model	String	Model of the Manager resource.
DateTime	String	System time of the Manager resource.
DateTimeLocalOffset	String	Time zone of the Manager resource, in time zone format, for example, +08:00, or time zone/region format, for example, Asia/Shanghai or America/New_York.
Description	String	Description of the Manager resource.
NetworkProtocol	Object	Access path of the network protocol supported by the specified Manager resource.
EthernetInterfaces	Object	Access path of the Ethernet interface information about the specified Manager resource.

Field	Type	Description
NtpService	Object	Access path of the NTP service of the specified Manager resource.
SyslogService	Object	Access path of the Syslog service of the specified Manager resource.
KvmService	Object	Access path of the KVM service of the specified Manager resource.
SnmpService	Object	Access path of the SNMP service of the specified Manager resource.
LldpService	Object	Access path of the LIDP service of the specified Manager resource.
LogServices	Object	Log service access path of the specified Manager resource.
VirtualMedia	Object	Access path of the virtual media service of the specified Manager resource.
Links	Object	Links to the related resources.
Actions	Object	Available actions for the specified Manager resource.
RollBackType@Redfish.AllowableValues	Array	OS operations allowed through the Redfish interface, including: RollBack
#Manager.FactoryReset.target	String	Resets factory settings.
#Manager.RollBack.target	Object	Switches BMC versions.
#Manager.Reset.target	String	Access path of BMC restart.
ResetType@Redfish.AllowableValues	Array	BMC restart operations allowed by the Redfish, including: ForceRestart.
#Manager.CaptureScreenShot.target	String	Access path for manual screenshot resources.
#Manager.DownloadScreenShot.target	String	Access path for downloading screenshots.
#Manager.ImportConfiguration.target	String	Imports configurations.
#Manager.ExportConfiguration.target	String	Exports configurations.
#Manager.GeneralDownload.target	String	Access path for the general download interface.
CommandShell	Object	Command shell properties.

Field	Type	Description
GraphicalConsole	Object	GUI console properties.
Manufacturer	String	BMC chip manufacturer.
MaxConcurrentSessions	Number	Maximum number of concurrent sessions.
ServiceEnabled	Boolean	Whether the service is enabled.
SerialConsole	Object	Serial console properties.
Links.ManagerForChassis	Array	Array of references to the chassis that this manager has control over.
Links.ManagerForServers	Array	Links to servers.
Links.ManagerInChassis	Array	Reference to the chassis that this manager is located in.
Oem.Public.FirmwareVersion-Date	String	BMC firmware version date.
Oem.Public.IfMatchEnabled	Boolean	Whether the match operation is enabled: ● true: yes. ● false: no.
Oem.Public.USB0InterfaceEnabled	Boolean	Whether the virtual network interface named usb0 is enabled: ● true: yes. ● false: no.
Oem.Public.ISDTSERVICE	Object	Access path of the ISDT service of the specified Manager resource.
Oem.Public.DnsService	Object	Access path of the specified DNS service.
Oem.Public.FirewallService	Object	Access path of the firewall service of the specified Manager resource.
Oem.NAT	Object	Access path of the NAT resource.

4.3 Modifying Information About a Specified Manager Resource

Function

Modify information about a specified Manager resource of a server.

Permission Required

Basic management.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/Managers/manager_id*
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "DateTimeLocalOffset": datetimelocaloffset_value
}
```

Parameters

For a description of the parameters for querying information about the Syslog configuration, refer to [Table 4-6](#).

Table 4-6 Parameter Descriptions for Querying Information About the Syslog Configuration

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
datetimelocaloffset_value	Time zone of the Manager resource.	Format: • GMT+ time zone, for example, GMT +09 :00. • Time zone string, for example, Asia/Shanghai.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Managers/1
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
  "DateTimeLocalOffset": "Asia/Shanghai"
}
```

- Response Example: None
- Response Code: 204

Output Description

None

4.4 Querying Information About the Syslog Configuration

Function

Query information about the Syslog configuration.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/SyslogService`
- Request Header:

```
x-auth-token:auth_value
```

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the Syslog configuration, refer to [Table 4-7](#).

Table 4-7 Parameter Descriptions for Querying Information About the Syslog Configuration

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/SyslogService
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#SyslogService.SyslogService",
  "@odata.id": "/redfish/v1/Managers/Self/SyslogService",
  "@odata.type": "#SyslogService.v1_2_0.SyslogService",
  "Actions": {
    "#SyslogService.SubmitTestEvent": {
      "target":
        "/redfish/v1/Managers/Self/SyslogService/Actions/
        SyslogService.SubmitTestEvent"
    }
  },
  "Id": "SyslogService",
  "Name": "SyslogService",
  "ServerIdentitySource": "BoardSN",
  "ServiceEnabled": true,
  "TransmissionProtocol": "TLS",
  "AuthenticateMode": "TwoWay",
  "SyslogServers": [
    {
      "Address": "192.168.1.6",
      "Enabled": false,
      "LogType": [
        "SecurityLog",
        "OperationLog",
        "EventLog"
      ],
      "MemberId": "0",
      "Port": 111
    }
  ],
  {
```



```

        "Address": "192.168.1.5",
        "Enabled": false,
        "LogType": [
            "EventLog"
        ],
        "MemberId": "1",
        "Port": 222
    },
    {
        "Address": "",
        "Enabled": false,
        "LogType": [],
        "MemberId": "2",
        "Port": 514
    },
    {
        "Address": "",
        "Enabled": false,
        "LogType": [],
        "MemberId": "3",
        "Port": 514
    }
]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the Syslog configuration, refer to [Table 4-8](#).

Table 4-8 Output Descriptions for Querying Information About the Syslog Configuration

Field	Type	Description
@odata.context	String	OData description of the Syslog resource model.
@odata.id	String	Access path of the Syslog resource.
@odata.type	String	Type of Syslog resource.
Id	String	ID of the Syslog resource.
Name	String	Name of the Syslog resource.
ServiceEnabled	Boolean	Syslog service enabled.
ServerIdentitySource	String	Host ID: • Board serial number: BoardSN

Field	Type	Description
		- Asset tag: ProductAssetTag - Host name: HostName
TransmissionProtocol	String	Transmission protocol. - UDP - TCP - TLS
AuthenticateMode	Character string	Authentication mode: - OneWay: unidirectional authentication. - TwoWay: bidirectional authentication.
SyslogServers	Object	Syslog servers.
MemberId	String	Member ID: "0" "1" "2" "3"
Enabled	Boolean	Channel enabled: - true - false
Address	String	Server address.
Port	Number	Server port number.
LogType	Array.	Log type: - OperationLog - SecurityLog - EventLog
#SyslogService.SubmitTestEvent.target	Character string	Access path for submitting test event resources.

4.5 Configuring Information About the Syslog Server

Function

Configure information about the Syslog server.

Permission Required

Query.

Syntax

- Operation Type: PATCH

- **URL:** `https://device_ip/redfish/v1/Managers/manager_id/SyslogService`
- **Request Header:**

```
x-auth-token:auth_value
Content-Type:header_type
```

- **Request Message Body:**

```
{
  "ServerIdentitySource": ServerIdentitySource,
  "TransmissionProtocol": TransmissionProtocol,
  "AuthenticateMode": AuthenticateMode_value,
  "ServiceEnabled": ServiceEnabled_value,
  "SyslogServers": [
    {
      "Address": add_value,
      "Enabled": enabled_value,
      "LogType": logtype_value,
      "Port": port_value,
      "MemberId": memberid_value
    },
    {
      "Address": add_value,
      "Enabled": enabled_value,
      "LogType": logtype_value,
      "Port": port_value,
      "MemberId": memberid_value
    }
  ]
}
```

Parameters

For parameter description of configuring the Syslog server information, refer to [Table 4-9](#).

Table 4-9 Parameter Description of Configuring the Syslog Server Information

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json

Parameter	Description	Value
ServerIdentitySource	Host ID.	Host ID: - Board serial number: BoardSN - Asset tag: ProductAssetTag - Host name: HostName Value descriptions: - When ServiceEnabled is set to true, there must be a value. - When ServiceEnabled is set to false, no verification is performed. - ServerIdentitySource must be set together with ServiceEnabled and TransmissionProtocol.
TransmissionProtocol	Transmission protocol.	Transmission protocol: - UDP - TCP - TLS Value descriptions: - When ServiceEnabled is set to true, there must be a value. - When ServiceEnabled is set to false, no verification is performed. - ServerIdentitySource must be set together with ServiceEnabled and TransmissionProtocol.
AuthenticateMode	Authentication mode	Authentication mode: - OneWay: unidirectional authentication. - TwoWay: bidirectional authentication. This parameter is required only when TransmissionProtocol is set to TLS.
ServiceEnabled	Whether the Syslog service is enabled.	Whether the Syslog service is enabled: - true: enabled - false: disabled Value descriptions: - If ServiceEnabled is set to true, ServerIdentitySource and TransmissionProtocol must also be set. - If ServiceEnabled is set to false, this parameter can be set independently. The original settings of ServerIdentitySource and TransmissionProtocol are retained.

Parameter	Description	Value
enabled_value	Whether the channel is enabled.	Whether the channel is enabled: • true • false
add_value	Server address format.	Server address format: • IP address. • FQDN format. When enabled_value of a channel is set to true in SyslogServers, add_value of the corresponding channel must be unique.
port_value	Server port number.	Server port number, range: 1–65535.
logtype_value	Log type.	Log type: • OperationLog • SecurityLog • EventLog
memberid_value	Serial number of the server.	Serial number of the server, optional, string type. This parameter is required for all servers. Range: 0–3.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Managers/1/SyslogService
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

Configuration without MemberId:

```
{
  "ServerIdentitySource": "ProductAssetTag",
  "TransmissionProtocol": "UDP",
  "ServiceEnabled": true,
  "SyslogServers": [
    {
      "Address": "ABCD:9A8C:39A0:FE80:02D0:BCFF:FEA6:6C01",
```

```

        "Enabled": false,
        "LogType": ["EventLog", "OperationLog", "SecurityLog"],
        "Port": 1
    },
    {
        "Address": "2020::12a",
        "Enabled": false,
        "LogType": ["EventLog", "SecurityLog", "OperationLog"],
        "Port": 65535
    },
    {
        "Address": "ABCD:9A8C:39A0::FE80:02D0",
        "Enabled": false,
        "LogType": ["EventLog", "OperationLog", "SecurityLog"],
        "Port": 1
    },
    {
        "Address": "192.168.1.5",
        "Enabled": true,
        "LogType": ["SecurityLog"],
        "Port": 444
    }
]
}

```

Configuration with MemberId:

```

{
    "ServerIdentitySource": "HostName",
    "TransmissionProtocol": "TCP",
    "ServiceEnabled": true,
    "SyslogServers": [
        {
            "Address": "ABCD:9A8C:39A0:FE80:02D0:BCFF:FEA6:6C01",
            "Enabled": true,
            "LogType": ["EventLog", "OperationLog", "SecurityLog"],
            "Port": 1,
            "MemberId": "2"
        }, {
            "Address": "2020::12a",
            "Enabled": false,
            "LogType": ["EventLog", "SecurityLog", "OperationLog"],
            "Port": 65535,
            "MemberId": "3"
        }, {

```

```

        "Address": "test.test.test.test",
        "Enabled": false,
        "LogType": ["EventLog", "OperationLog", "SecurityLog"],
        "Port": 698,
        "MemberId": "1"
    }, {
        "Address": "192.168.1.5",
        "Enabled": true,
        "LogType": ["SecurityLog"],
        "Port": 444,
        "MemberId": "0"
    }
]
}

```

Configure the Syslog function separately:

```

{
  "ServerIdentitySource": "ProductAssetTag",
  "TransmissionProtocol": "UDP",
  "ServiceEnabled": true
}

```

Configure the Syslog Server separately:

```

{
  "SyslogServers": [
    {
      "Address": "ABCD:9A8C:39A0:FE80:02D0:BCFF:FEA6:6C01",
      "Enabled": false,
      "LogType": ["EventLog", "OperationLog", "SecurityLog"],
      "Port": 1
    }, {
      "Address": "2020::12a",
      "Enabled": false,
      "LogType": ["EventLog", "SecurityLog", "OperationLog"],
      "Port": 65535
    }, {
      "Address": "ABCD:9A8C:39A0:FE80:02D0",
      "Enabled": false,
      "LogType": ["EventLog", "OperationLog", "SecurityLog"],
      "Port": 1
    }, {
      "Address": "10.228.34.156",
      "Enabled": true,

```

```

        "LogType": ["SecurityLog"],
        "Port": 444
    }
]
}

```

Configure the Syslog server separately, with MemberId:

```

{
  "SyslogServers": [
    {
      "Address": "ABCD:9A8C:39A0:FE80:02D0:BCFF:FEA6:6C01",
      "Enabled": true,
      "LogType": ["EventLog", "OperationLog", "SecurityLog"],
      "Port": 1,
      "MemberId": "2"
    }, {
      "Address": "2020::12a",
      "Enabled": false,
      "LogType": ["EventLog", "SecurityLog", "OperationLog"],
      "Port": 65535,
      "MemberId": "3"
    }, {
      "Address": "test.test.test.test",
      "Enabled": false,
      "LogType": ["EventLog", "OperationLog", "SecurityLog"],
      "Port": 698,
      "MemberId": "1"
    }, {
      "Address": "192.168.1.5",
      "Enabled": true,
      "LogType": ["SecurityLog"],
      "Port": 444,
      "MemberId": "0"
    }
  ]
}

```

Use MemberId to configure a separate server (for example, the second server).

```

{
  "SyslogServers": [
    {
      "Address": "test.test.test.test",
      "Enabled": false,

```



```
        "LogType":["EventLog","OperationLog","SecurityLog"],
        "Port":698,
        "MemberId":"1"
      }
    ]
  }
```

- Response Example: None
- Status Code: 200

Output Description

None

4.6 Submitting a Syslog Test Log

Function

Submit a Syslog test log.

Permission Required

Diagnosis.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/Managers/manager_id/SyslogService/Actions/SyslogService.SubmitTestEvent*
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
}
```

Parameters

None

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/SyslogService/Actions/SyslogService.SubmitTestEvent
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
}
```

- Response Example: None
- Status Code: 204

Output Description

None

4.7 Querying Information About the NtpService Configuration Resource

Function

Query information about the NtpService configuration resource.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Managers/manager_id/NtpService*
- Request Header:

```
x-auth-token:auth_value
```

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the NtpService configuration resource, refer to [Table 4-10](#).

Table 4-10 Parameter Descriptions for Querying Information About the NtpService Configuration Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/NtpService
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#NtpService.NtpService",
  "@odata.id": "/redfish/v1/Managers/Self/NtpService",
  "@odata.type": "#NtpService.v1_2_0.NtpService",
  "AlternateNtpServer": "",
  "CurrentPollingInterval": 65,
  "Description": "NtpService",
  "ExtraNtpServer": "time.nist.gov",
  "MaxPollingInterval": 65535,
  "MinPollingInterval": 60,
  "PreferredNtpServer": "pool.ntp.org",
  "ServerAuthenticationEnabled": false,
  "ServiceEnabled": false,
  "NtpSynResult": "successful"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the NtpService resource, refer to [Table 4-11](#).

Table 4-11 Output Descriptions for Querying Information About the NtpService Configuration Resource

Field	Type	Description
@odata.context	String	OData description of the NTP resource model.
@odata.id	String	Access path of the NTP resource.
@odata.type	String	Type of NTP resource.
ServiceEnabled	Boolean	NTP enabled.
AlternateNtpServer	String	Alternate NTP server address.
CurrentPollingInterval	Number	Current synchronization interval. Range: MinPollingInterval through MaxPollingInterval .
Description	String	Description of the NTP resource.
ExtraNtpServer	String	Address of the extra NTP server.
MaxPollingInterval	Number	Maximum synchronization interval.
MinPollingInterval	Number	Minimum synchronization interval.
PreferredNtpServer	String	Address of the preferred NTP server.
ServerAuthenticationEnabled	Boolean	Whether server authentication is enabled.
ServiceEnabled	Boolean	Whether the NTP service is enabled: • true • false
NtpSynResult	Character string	NTP synchronization result: • successful • fail • NULL: The configuration file is null. • mode is not NTP: non-NTP mode. • get NTP result fail: configuration file reading failure.

4.8 Modifying Properties of the NTP Resource

Function

Modify properties of the **NTP** resource.

Permission Required

Basic management.

Syntax

- Operation Type: PATCH
- URL: `https://device_ip/redfish/v1/Managers/manager_id/NtpService`
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "ServiceEnabled": ServiceEnabled,
  "AlternateNtpServer": AlternateNtpServer,
  "PreferredNtpServer": PreferredNtpServer,
  "ExtraNtpServer": ExtraNtpServer,
  "CurrentPollingInterval": CurrentValue,
  "NtpAddressOrigin": "static"
}
```

Parameters

For a description of the parameters for modifying properties of the NTP resource, refer to [Table 4-12](#).

Table 4-12 Parameter Descriptions for Modifying Properties of the NTP Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
ServiceEnabled	Boolean	Whether the NTP service is enabled: • true • false: If this parameter is set to false, the request body cannot carry other parameters. If another parameter is carried, an error is reported, indicating

Parameter	Description	Value
		that the ServiceEnabled value is incorrect.
AlternateNtpServer	String	Alternate NTP server address.
PreferredNtpServer	String	Preferred NTP server address.
ExtraNtpServer	String	Address of the extra NTP server.
CurrentPollingInterval	Number	Current polling interval. Range: Min-PollingInterval through MaxPollingInterval.
NtpAddressOrigin	Address mode.	Address mode: - static - IPv4: not supported in this version. IPv6 : not supported in this version.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Managers/1/NtpService
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
  "ServiceEnabled":true,
  "NtpAddressOrigin":"static",
  "PreferredNtpServer": "pool.ntp.org",
  "ExtraNtpServer":"time.nist.gov",
  "CurrentPollingInterval": 65
}
```

- Response Example: None
- Status Code: 204

Output Description

None

4.9 Querying Information About the BMC Service

Function

Query the status and port information supported by the current BMC of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/NetworkProtocol`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the BMC service, refer to [Table 4-13](#).

Table 4-13 Parameter Descriptions for Querying Information About the BMC Service

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Managers/1/NetworkProtocol

- Request Header:

x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None

- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#ManagerNetworkProtocol.ManagerNetworkProtocol",
  "@odata.id": "/redfish/v1/Managers/1/NetworkProtocol",
  "@odata.type": "#ManagerNetworkProtocol.v1_6_0.ManagerNetworkProtocol",
  "Description": "Network Protocol Details",
  "HTTPS": {
    "ProtocolEnabled": true,
    "Port": 443
  },
  "HostName": "iSAC26C4F96B1676",
  "IPMI": {
    "Port": 623,
    "ProtocolEnabled": true
  },
  "Id": "NetworkProtocol",
  "KVMIP": {
    "ProtocolEnabled": true,
    "Port": 7578
  },
  "Name": "Manager Network Protocol",
  "Oem": {
    "Public": {
      "HTTPS": {
        "Timeout": 30
      },
      "KVMIP": {
        "Timeout": 30
      },
      "VirtualMedia-CD": {
        "ProtocolEnabled": true,
        "Port": 5124,
        "Instance": 1
      },
      "VirtualMedia-HD": {
        "ProtocolEnabled": false,
        "Port": 5127,
        "Instance": 0
      }
    },
    "VNC": {
      "Port": 5900,
      "ProtocolEnabled": true,
    }
  }
}
```



```

        "SecurePort": 5901
    },
    "SSDP": {
        "NotifyEnabled": true
    }
},
"SNMP": {
    "ProtocolEnabled": true,
    "Port": 161
},
"SSH": {
    "ProtocolEnabled": true,
    "Port": 22
},
"VirtualMedia": {
    "ProtocolEnabled": true
},
"SSDP": {
    "ProtocolEnabled": true,
    "Port": 1900,
    "NotifyMulticastIntervalSeconds": 600,
    "NotifyIPv6Scope": "Site"
}
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the BMC service, refer to [Table 4-14](#).

Table 4-14 Output Descriptions for Querying Information About the BMC Service

Field	Type	Description
@odata.context	String	OData description of the BMC service resource collection model.
@odata.id	String	Access path of the BMC service resource collection.
@odata.type	String	Type of BMC service resource collection.
Description	String	Description of the BMC resource.

Field	Type	Description
HTTPS.Port	Number	HTTPS service port number (secure port number of the Web service).
HTTPS.ProtocolEnabled	Boolean	Whether the HTTPS service is enabled.
HostName	String	BMC host name.
IPMI.Port	Number	IPMI service port number.
IPMI.ProtocolEnabled	Boolean	Whether the IPMI service is enabled.
Id	String	ID of the network protocol resource.
KVMIP.Port	Number	KVMIP service port number.
KVMIP.ProtocolEnabled	Boolean	KVMIP service enabling status: true/false
Name	String	Name of the service resource collection.
Oem.Public.HTTPS.Timeout	Number	HTTPS service timeout period. Unit: seconds.
Oem.Public.KVMIP.Timeout	Number	KVMIP service timeout period. Unit: seconds.
Oem.Public.VirtualMedia-CD.ProtocolEnabled	Boolean	Whether the virtual media CD service is enabled.
Oem.Public.VirtualMedia-CD.Port	Number	Port number of the virtual media CD service.
Oem.Public.VirtualMedia-CD.Instance	Number	Number of virtual media CD instances.
Oem.Public.VirtualMedia-HD.ProtocolEnabled	Boolean	Whether the virtual media HD service is enabled.
Oem.Public.VirtualMedia-HD.Port	Number	Port number of the virtual media HD service.
Oem.Public.VirtualMedia-HD.Instance	Number	Number of virtual media HD instances.
Oem.Public.SSDP.NotifyEnabled	Boolean	Whether SSDP NOTIFY messages are multicast.

Field	Type	Description
Oem.Public.VNC.ProtocolEnabled	Boolean	Whether the VNC service is enabled.
Oem.Public.VNC.Port	Number	Port number of the VNC service.
Oem.Public.VNC.SecurePort	Number	Secure port of the VNC service.
SNMP.Port	Number	Port number of the SNMP service.
SNMP.ProtocolEnabled	Boolean	Whether the SNMP service is enabled.
SSH.Port	Number	Port number of the SSH service.
SSH.ProtocolEnabled	Boolean	Whether the DNS service is enabled.
VirtualMedia.ProtocolEnabled	Boolean	Whether the virtual media service is enabled.
SSDP.Port	Number	Port number of the SSDP service.
SSDP.ProtocolEnabled	Boolean	Whether the SSDP service is enabled.
SSDP.NotifyMulticastIntervalSeconds	Number	Time interval between transmissions of the multicast SSDP NOTIFY message.
SSDP.NotifyIPv6Scope	String	IPv6 scope for multicast SSDP NOTIFY messages. ● Link: SSDP Notify messages are sent to addresses in the IPv6 local link scope. ● Site: SSDP Notify messages are sent to addresses in the IPv6 local site scope. ● Organization: SSDP Notify messages are sent to addresses in the IPv6 local organization scope.

4.10 Modifying Information About a Specified BMC Service

Function

Modify the information about a specified [BMC](#) service of a server.

Permission Required

Security management

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/Managers/manager_id/NetworkProtocol*
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "Service_type": {
    "ProtocolEnabled": protocolenabled_value,
    "Port": port_value,
    "NotifyMulticastIntervalSeconds": time_value,
    "NotifyIPv6Scope": scope_value
  },
  "Oem": {
    "Public": {
      "OEMServerType": {
        "Port": oem_port_value,
        "ProtocolEnabled": oem_protocolEnabled_value,
        "Timeout": oem_timeout_value,
        "NotifyEnabled": oem_notify_enabled_value,
        "SecurePort": oem_secure_port_value,
        "Password": oem_password_value
      }
    }
  }
}
```

Parameters

For a description of the parameters for modifying information about the specified BMC service, refer to [Table 4-15](#).

Table 4-15 Parameter Descriptions for Modifying Information About the Specified BMC Service

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
Service_type	Specified BMC services of the server.	• HTTPS • KVMIP • VirtualMedia • SSH • SNMP • SSDP
Service_type.protocolenabled_value	Whether the service is enabled.	Boolean: • true • false The service cannot be enabled when Service_type is set to HTTPS . When Service_type is set to VirtualMedia , the enabling status can be modified, and the modification affects the VirtualMedia-CD and VirtualMedia-HD parameters.
Service_type.port_value	Modifies the server port number.	Integer type: 1–65535. This parameter is not supported when Service_type is set to VirtualMedia .
Service_type.time_value	Time interval between transmissions of the multicast SSDP NOTIFY message (for SSDP only).	Integer type, unit: seconds, range: 0–1800.
Service_type.scope_value	IPv6 scope for multicast SSDP NOTIFY messages (for SSDP only).	• Link: SSDP Notify messages are sent to addresses in the IPv6 local link scope.

Parameter	Description	Value
		● Site: SSDP Notify messages are sent to addresses in the IPv6 local site scope. ● Organization: SSDP Notify messages are sent to addresses in the IPv6 local organization scope.
Oem.Public.OEMServerType	OEM service type to be set.	Modifiable service type: ● VirtualMedia-CD ● VirtualMedia-HD ● HTTPS ● KVMIP ● VNC
Oem.Public.OEMServerType.oem_port_value	OEM service port.	Number, range: 1–65535.
Oem.Public.OEMServerType.oem_protocolEnabled_value	Whether to enable the OEM service.	Boolean type: ● true ● false
Oem.Public.OEMServerType.oem_timeout_value	Service timeout period. Only the HTTPS and KVMIP services support this parameter.	Number type, unit: minutes, range: 1–60.
Oem.Public.OEMServerType.oem_notify_enabled_value	Whether SSDP NOTIFY messages are multicast. (Only the SSDP function supports this parameter.)	Boolean type: ● true ● false
Oem.Public.OEMServerType.oem_secure_port_value	Secure port, which is supported by the VNC service only.	Number, range: 1–65535.
Oem.Public.OEMServerType.oem_password_value	VNC password, which is supported by the VNC service only.	Type: string.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Managers/1/NetworkProtocol
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=  
Content-Type:application/json
```

- Request Message Body:

```
{  
  "HTTPS": {  
    "Port": 443  
  },  
  "KVMIP": {  
    "ProtocolEnabled": true,  
    "Port": 7578  
  },  
  "SSDP": {  
    "ProtocolEnabled": true,  
    "Port": 1900,  
    "NotifyMulticastIntervalSeconds": 600,  
    "NotifyIPv6Scope": "Site"  
  },  
  "Oem": {  
    "Public": {  
      "HTTPS": {  
        "Timeout": 30  
      },  
      "KVMIP": {  
        "Timeout": 30  
      },  
      "VirtualMedia-CD": {  
        "Port": 5123,  
        "ProtocolEnabled": true  
      },  
      "VNC": {  
        "Port": 5900,  
        "ProtocolEnabled": true,  
        "SecurePort": 5901,  
        "Password": "123456"  
      },  
      "SSDP": {
```

```

        "NotifyEnabled": true
    }
}
}
}

```

- Response Example:

```

{
  "@odata.context":
    "/redfish/v1/$metadata#ManagerNetworkProtocol.ManagerNetworkProtocol",
  "@odata.id": "/redfish/v1/Managers/1/NetworkProtocol",
  "@odata.type": "#ManagerNetworkProtocol.v1_6_0.ManagerNetworkProtocol",
  "Description": "Network Protocol Details",
  "Id": "NetworkProtocol",
  "Name": "Manager Network Protocol",
  "HostName": "iSAC26C4F96B1676",
  "HTTPS": {
    "ProtocolEnabled": true,
    "Port": 443
  },
  "KVMIP": {
    "ProtocolEnabled": true,
    "Port": 7578
  },
  "Oem": {
    "Public": {
      "HTTPS": {
        "Timeout": 30
      },
      "KVMIP": {
        "Timeout": 30
      },
      "VirtualMedia-CD": {
        "ProtocolEnabled": true,
        "Port": 5120,
        "Instance": 1
      },
      "VirtualMedia-HD": {
        "ProtocolEnabled": false,
        "Port": 5123,
        "Instance": 0
      },
      "VNC": {
        "Port": 5900,

```



```

        "ProtocolEnabled": true,
        "SecurePort": 5901
    },
    "SSDP": {
        "NotifyEnabled": true
    }
},
"SSH": {
    "ProtocolEnabled": true,
    "Port": 22
},
"SNMP": {
    "ProtocolEnabled": true,
    "Port": 161
},
"IPMI": {
    "Port": 623,
    "ProtocolEnabled": true
},
"VirtualMedia": {
    "ProtocolEnabled": true
},
"SSDP": {
    "ProtocolEnabled": true,
    "Port": 1900,
    "NotifyMulticastIntervalSeconds": 600,
    "NotifyIPv6Scope": "Site"
}
}

```

- Status Code: 200

Output Description

For a description of the output returned when you modify information about the specified BMC service, refer to [Table 4-16](#).

Table 4-16 Output Descriptions for Modifying Information About the Specified BMC Service

Field	Type	Description
@odata.context	String	OData description of the BMC service resource collection model.
@odata.id	String	Access path of the BMC service resource collection.

Field	Type	Description
@odata.type	String	Type of BMC service resource collection.
Description	String	Description of the BMC resource.
HTTPS.Port	Number	HTTPS service port (secure port of the Web service).
HTTPS.ProtocolEnabled	Boolean	Whether the HTTPS service is enabled.
HostName	String	BMC hostname.
IPMI.Port	Number	Port number of the IPMI service.
IPMI.ProtocolEnabled	Boolean	Whether the IPMI service is enabled.
Id	String	BMC network protocol resource ID.
KVMIP.Port	Number	Port number of the KVMIP service.
KVMIP.ProtocolEnabled	Boolean	Whether the KVMIP service is enabled.
Name	String	BMC network protocol resource name.
Oem.Public.HTTPS.Timeout	Number	Timeout period of the HTTPS service, unit: minutes.
Oem.Public.KVMIP.Timeout	Number	Timeout period of the KVMIP service, unit: minutes.
Oem.Public.VirtualMedia-CD.ProtocolEnabled	Boolean	Whether the virtual media CD service is enabled.
Oem.Public.VirtualMedia-CD.Port	Number	Port number of the virtual media CD service.
Oem.Public.VirtualMedia-CD.Instance	Number	Number of virtual media CD instances.
Oem.Public.VirtualMedia-HD.ProtocolEnabled	Boolean	Whether the virtual media HD service is enabled.
Oem.Public.VirtualMedia-HD.Port	Number	Port number of the virtual media HD service.

Field	Type	Description
Oem.Public.VirtualMedia-HD.Instance	Number	Number of virtual media HD instances.
Oem.Public.SSDP.NotifyEnabled	Boolean	Whether SSDP NOTIFY messages are multicast.
Oem.Public.VNC.ProtocolEnabled	Boolean	Whether the VNC service is enabled.
Oem.Public.VNC.Port	Number	Port number of the VNC service.
Oem.Public.VNC.SecurePort	Number	Secure port of the VNC service.
SNMP.Port	Number	Port number of the SNMP service.
SNMP.ProtocolEnabled	Boolean	Whether the SNMP service is enabled.
SSH.Port	Number	Port number of the SSH service.
SSH.ProtocolEnabled	Boolean	Whether the SSH service is enabled.
VirtualMedia.ProtocolEnabled	Boolean	Whether the virtual media service is enabled.
SSDP.Port	Number	Port number of the SSDP service.
SSDP.ProtocolEnabled	Boolean	Whether the SSDP service is enabled.
SSDP.NotifyMulticastIntervalSeconds	Number	Time interval between transmissions of the multicast SSDP NOTIFY message.
SSDP.NotifyIPv6Scope	String	IPv6 scope for multicast SSDP NOTIFY messages. ● Link: SSDP Notify messages are sent to addresses in the IPv6 local link scope. ● Site: SSDP Notify messages are sent to addresses in the IPv6 local site scope.

Field	Type	Description
		Organization: SSDP Notify messages are sent to addresses in the IPv6 local organization scope.

4.11 Querying the BMC Management Interface Resource Collection

Function

Query the management port resource collection supported by the current [BMC](#) of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/EthernetInterfaces`
- Request Header:

x-auth-token:auth_value
- Request Message Body: None

Parameters

For a description of the parameters for querying the BMC management interface resource collection, refer to [Table 4-17](#).

Table 4-17 Parameter Descriptions for Querying the BMC Management Interface Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/EthernetInterfaces
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None

- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#EthernetInterfaceCollection.EthernetInterfaceCollection",
  "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces",
  "@odata.type": "#EthernetInterfaceCollection.EthernetInterfaceCollection",
  "Description": "Collection of Ethernet Interfaces for this Manager",
  "Name": "Ethernet Network Interface Collection",
  "Members@odata.count": 1,
  "Members": [
    {
      "@odata.id":
        "/redfish/v1/Managers/1/EthernetInterfaces/D64FE89CE17C"
    }
  ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the BMC management interface resource collection, refer to [Table 4-18](#).

Table 4-18 Output Descriptions for Querying the BMC Management Interface Resource Collection

Field	Type	Description
@odata.context	String	OData description of the BMC management interface resource collection model.
@odata.id	String	Type of BMC management interface resource collection.
@odata.type	String	Access path of the BMC management interface resource collection.

Field	Type	Description
Description	String	Description of the BMC management interface resource collection.
Name	String	Name of the BMC management interface resource collection.
Members@odata.count	Number	Number of members in the BMC management interface resource collection.
Members	Object	List of members in the BMC management interface resource collection.
@odata.id	String	Access path of a single BMC management interface resource node.

4.12 Querying Information About a Specified BMC Management Interface Resource

Function

Query information about a specified [BMC](#) management interface resource.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Managers/manager_id/EthernetInterfaces/id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified BMC management interface resource, refer to [Table 4-19](#).

Table 4-19 Parameter Descriptions for Querying Information About the Specified BMC Management Interface Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.

Parameter	Description	Value
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
id	ID of the BMC management interface resource.	-
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/EthernetInterfaces/D64FE89CE17C
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#EthernetInterface.EthernetInterface",
  "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces/D64FE89CE17C",
  "@odata.type": "#EthernetInterface.v1_6_2.EthernetInterface",
  "Id": "D64FE89CE17C",
  "Name": "D64FE89CE17C",
  "MACAddress": "D6:4F:E8:9C:E1:7C",
  "PermanentMACAddress": "BE:0B:64:49:40:C0",
  "InterfaceEnabled": true,
  "MTUSize": 1500,
  "AutoNeg": true,
  "FullDuplex": true,
  "SpeedMbps": 1000,
  "Description": "Ethernet Interface D64FE89CE17C",
  "HostName": "iSACD64FE89CE17C",
  "IPv4Addresses": [
    {
      "Address": "192.168.5.7",
      "Gateway": "0.0.0.0",
      "SubnetMask": "255.255.255.0",
```

```
        "AddressOrigin": "Static"
      }
    ],
    "IPv6DefaultGateway": ":::",
    "IPv6Addresses": [
      {
        "Address": "fe80::4e09:b4ff:fe07:622",
        "AddressOrigin": "LinkLocal",
        "PrefixLength": 64
      },
      {
        "Address": ":::",
        "PrefixLength": 80,
        "AddressOrigin": "DHCPv6"
      }
    ],
    "IPv6StaticAddresses": [
      {
        "Address": ":::",
        "PrefixLength": 0
      }
    ],
    "Oem": {
      "Public": {
        "IPStacks": "IPv4AndIPv6",
        "DNSServiceEnabled": true,
        "DNSDhcpEnabled": true,
        "PatchInProgress": false,
        "DoMain": "",
        "VLANPriority": 0,
        "NetworkPortMode": "Automatic",
        "NCSIModeSelect": null,
        "ManagementNetworkPort": [
          {
            "Type": "Dedicated",
            "CardNumber": null,
            "PortNumber": 0
          }
        ],
        "ManagementNetworkPort@Redfish.AllowableValues": [
          {
            "Type": "Dedicated",
            "CardNumber": null,
            "PortNumber": 0
          }
        ]
      }
    }
  }
}
```



```
    },
    {
      "Type": "ShareLink",
      "CardNumber": 1,
      "PortNumber": 1
    },
    {
      "Type": "ShareLink",
      "CardNumber": 1,
      "PortNumber": 2
    },
    {
      "Type": "ShareLink",
      "CardNumber": 2,
      "PortNumber": 1
    },
    {
      "Type": "ShareLink",
      "CardNumber": 2,
      "PortNumber": 2
    }
  ]
}
},
"NameServers": [
  ":",
  "0.0.0.0",
  ":"
],
"Status": {
  "Health": "OK",
  "State": "Enabled"
},
"VLAN": {
  "VLANEnable": false,
  "VLANId": 0
}
"IPv4Routes": [
  {
    "Address": "192.168.1.5",
    "Netmask": "255.255.255.192"
  }
],
"IPv6Routes": [
```

```

    {
      "Address": "ff00::",
      "PrefixLength": 8
    }
  ],
  "Actions": {
    "#EthernetInterfaces.AddRoute": {
      "target": "/redfish/v1/Managers/1/EthernetInterfaces/D64FE89CE17C/
        Actions/EthernetInterface.AddRoutes"
    },
    "#EthernetInterfaces.DeleteRoute": {
      "target": "/redfish/v1/Managers/1/EthernetInterfaces/D64FE89CE17C/
        Actions/EthernetInterface.DeleteRoutes"
    }
  }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified BMC management interface resource, refer to [Table 4-20](#).

Table 4-20 Output Descriptions for Querying Information About the Specified BMC Management Interface Resource

Field	Type	Description
@odata.context	String	OData description of the specified BMC management interface resource model.
@odata.id	String	Access path of the specified BMC management interface resource node.
@odata.type	String	Type of the specified BMC management interface resource.
Id	String	ID of the specified BMC management interface resource.
Name	String	Name of the specified BMC management interface resource.
MACAddress	Character string	MAC address of the specified BMC network interface.
PermanentMACAddress	String	Permanent MAC address allocated to the interface.
InterfaceEnabled	Boolean	Whether the interface is enabled.
MTUSize	Number	MTU configured on the current interface (in bytes).

Field	Type	Description
AutoNeg	Boolean	Whether auto-negotiation is enabled. including: ● true ● false
FullDuplex	Boolean	Whether full-duplex mode is used. including: ● true ● false
SpeedMbps	Number	Current rate (in Mbps).
Description	String	Description of the specified BMC management interface resource.
HostName	String	DNS hostname, which does not contain any domain information.
IPv4Addresses	Array	IPv4 information object.
IPv4Addresses.Address	String	IPv4 address.
IPv4Addresses.AddressOrigin	String	Origin of the IPv4 address. including: ● Static ● DHCP
IPv4Addresses.Gateway	String	IPv4 gateway address.
IPv4Addresses.SubnetMask	String	IPv4 subnet mask.
IPv6DefaultGateway	String	Default IPv6 gateway.
IPv6Addresses	Array	IPv6 information object.
IPv6Addresses.Addresses	String	IPv6 address.
IPv6Addresses.AddressOrigin	String	Origin of the IPv6 address. including: ● Static ● DHCP
IPv6Addresses.PrefixLength	Number	Prefix length of the IPv6 address.
IPv6StaticAddresses	Array	Static IPv6 information object.
IPv6StaticAddresses.Address	String	Static IPv6 address.
IPv6StaticAddresses.Pre-fixLength	Number	Prefix length of the static IPv6 address.
Oem.Public	Object	OEM object.
IPStacks	String	IPv4/IPv6 enabling switch: ● null: interface not enabled ● IPv4: IPv4 enabled only ● IPv6: IPv6 enabled only

Field	Type	Description
		IPv4AndIPv6: IPv4 and IPv6 both enabled
DNSServiceEnabled	Boolean	Whether the DNS service is enabled.
DNSDhcpEnabled	Boolean	Manual or automatic DNS switch: - true: automatic - false: manual
PatchInProgress	Boolean	Configuration validity flag: - true: being configured - false: applied successfully
DoMain	String	Domain name.
VLANPriority	Number	VLAN priority, range: 0–7.
NetworkPortMode	String	Network port mode: - Automatic - Fixed - Standalone
NCSIModeSelect	String	NCSI mode: - Automatic - Manual - null: default setting when NetworkPortMode is set to Fixed.
ManagementNetworkPort	Array	In fixed mode of the specified management network port, there is only one group of BMC management network port data. In automatic mode and standalone mode, the data is dedicated port data and shared port data respectively.
Type	String	- Dedicated: dedicated network port - ShareLink: shared network port
CardNumber	Number	The default value of the dedicated network port is null, and the default value of the shared network port is: 1: NIC 1 2: NIC 2
PortNumber	Number	For a dedicated network port, the default serial number is set to 0. For a shared network port, the silkscreen number of the network port is set to 1 through 4.
ActualPortNumber	Number	Actual silk screen number of the network interface, range: 1–4. This field is displayed only when the net-

Field	Type	Description
		work port mode is set to standalone or automatic (the selected network port is not a dedicated port) and the NCSI mode is set to automatic.
ManagementNetworkPort @Redfish.AllowableValues	Array	All available network ports of the BMC.
NameServers	Array	Domain name server list.
Status	Object	Status information about the specified BMC management interface resource. ● State: whether the BMC management interface is enabled. ● Health: health status of the BMC management interface.
VLAN	Object	VLAN information object.
VLANEnable	Boolean	Whether VLAN is enabled: ● true: enabled ● false: disabled
VLANId	Number	Configured VLAN ID, range: 2–4094.
IPv4Routes	Object	IPv4 route information about the NIC.
IPv4Routes.Address	Character string	Address information about the IPv4 route of the NIC.
IPv4Routes.Netmask	Character string	Mask information about the IPv4 route of the NIC.
IPv6Routes.Address	Character string	Address information about the IPv6 route of the NIC.
IPv6Routes.PrefixLength	Digit	Prefix length information about the IPv6 route of the NIC.
Actions	Object	Operations that can be performed on the resource.
#EthernetInterface.AddRoutes.target	Character string	Access path for adding route information.
#EthernetInterface.DeleteRoutes.target	Character string	Access path for deleting route information.

4.13 Modifying a Specified BMC Management Interface Resource

Function

Modify information about a specified **BMC** management interface resource.

Permission Required

Basic management.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/Managers/manager_id/EthernetInterfaces/id*

- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

→ IPv4 configuration:

```
{
  "IPv4Addresses": [
    {
      "Address": ipv4_address,
      "AddressOrigin": ipv4_address_origin,
      "Gateway": ipv4_gateway,
      "SubnetMask": ipv4_subnet_mask
    }
  ],
  "Oem": {
    "Public": {
      "IPStacks": ip_stack
    }
  }
}
```

→ IPv6 configuration:

```
{
  "IPv6Addresses": [
    {
      "Address": ipv6_address,
      "AddressOrigin": ipv6_address_origin,
      "PrefixLength": ipv6_prefix
    }
  ],
  "IPv6DefaultGateway": Gw_value,
  "Oem": {
    "Public": {
```

```
        "IPStacks": ip_stack
    }
}
```

→ **VLAN** configuration:

```
{
  "VLAN":{
    "VLANEnable": vlan_enable,
    "VLANId": vlan_id
  },
  "Oem": {
    "Public": {
      "VLANPriority": priority
    }
  }
}
```

→ **HostName** configuration:

```
{
  "HostName": hostname
}
```

→ **NameServers** configuration:

```
{
  "NameServers": [nameserver, nameserver, nameserver],
  "Oem": {
    "Public": {
      "DoMain": "domain"
    }
  }
}
```

→ **Network port mode** configuration:

```
{
  "Oem": {
    "Public": {
      "NetworkPortMode": network_port_mode,
      "NCSIModeSelect" : ncsi_mode,
      "ManagementNetworkPort":{
        "Type": type,
        "CardNumber":card_number,
        "PortNumber":port_number
      }
    }
  }
}
```

```

    }
  }
}

```

Parameters

For a description of the parameters for modifying the specified BMC management interface resource, refer to [Table 4-21](#).

Table 4-21 Parameter Descriptions for Modifying the Specified BMC Management Interface Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
id	ID of the BMC management interface resource.	-
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
hostname	Hostname.	Customized hostname: • Cannot exceed 64 characters. • Consists of digits, letters, and hyphens (-). • Cannot begin or end with a hyphen.
ipv4_address	IPv4 IP address	String, valid IPv4 address.
ipv4_address_origin	Origin of the IPv4 address.	• "Static": configures a static IPv4 address. • "DHCP": assigns the address through DHCP.
ipv4_subnet_mask	IPv4 subnet mask.	String, valid IPv4 address.
ipv4_gateway	IPv4 gateway.	String, valid IPv4 gateway.
ipv6_address	IPv6 address.	String, valid IPv6 address.
ipv6_address_origin	Origin of the IPv4 address.	• "Static": configures a static IPv6 address. • "DHCPv6": assigns the address through DHCP.
ipv6_prefix	Prefix length of the IPv6 address.	Integer type, range: 1–128.
Gw_value	Default IPv6 gateway.	In IPv6 format.

Parameter	Description	Value
nameserver	Domain name server.	One primary server and two secondary servers are included. Valid IPv4 or IPv6 addresses are used.
ip_stack	Whether to enable IPv4/IPv6.	• "IPv4": Only IPv4 is enabled. The parameters related to IPv4 cannot be null. • "IPv6": Only IPv6 is enabled. The parameters related to IPv6 cannot be null. • "IPv4AndIPv6": IPv4 and IPv6 are both enabled. The parameters related to IPv4 and IPv6 cannot be null.
domain	String	Domain name.
priority	VLAN priority.	Range: 0–7.
vlan_enable	Whether to enable the VLAN.	• true: enables the VLAN. Values of vlan_id and priority must be set together. • false: disables the VLAN. Values of vlan_id and priority are not verified.
vlan_id	VLAN ID.	Range: 2–4094.
network_port_mode	String	Network port mode: • Automatic • Fixed • Standalone Description of ManagementNetworkPort data reporting: In automatic mode, standalone mode, and fixed mode, only one group of data needs to be reported. In automatic mode and standalone mode, dedicated port data does not need to be reported, and only shared port data is reported.
ncsi_mode	String	NCSI mode: • Automatic • Manual In fixed mode, you do not need to set this parameter. In automatic mode or standalone mode, you can set this parameter.
type	String	• Dedicated: dedicated network port • ShareLink: shared network port

Parameter	Description	Value
		This parameter cannot be set to Dedicated and shared link information must be provided if network_port_mode is set to Automatic or Standalone .
card_number	Number	The value of the dedicated network port does not need to be reported. The value of the shared network port is as follows: • 1: NIC 1 • 2: NIC 2
port_number	Number	For a dedicated network port, the default value is 0. For a shared network port, the silkscreen number of the network port is used. Range: 1–4.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Managers/1/EthernetInterfaces/D64FE89CE17C
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

→ [IPv4](#) configuration:

```
{
  "IPv4Addresses": [
    {
      "Address": "192.168.5.7",
      "Addressorigin": "Static",
      "Gateway": "192.168.5.1",
      "SubnetMask": "255.255.255.0"
    }
  ],
  "oem": {
    "Public": {
      "IPStacks": "IPv4"
    }
  }
}
```

```
}  
}
```

→ **IPv6** configuration:

```
{  
  "IPv6Addresses": [  
    {  
      "Address": "2020::211",  
      "AddressOrigin": "Static",  
      "PrefixLength": 64  
    }  
  ],  
  "IPv6DefaultGateway": "2020::1",  
  "Oem": {  
    "Public": {  
      "IPStacks": "IPv6"  
    }  
  }  
}
```

→ **VLAN** configuration:

```
{  
  "VLAN": {  
    "VLANEnable": true,  
    "VLANId": 3  
  },  
  "Oem": {  
    "Public": {  
      "VLANPriority": 1  
    }  
  }  
}
```

→ **HostName** configuration:

```
{  
  "HostName": "BMC-012"  
}
```

→ **NameServers** configuration:

```
{  
  "NameServers": ["1.2.3.4", "2.3.4.5", ""],  
  "Oem": {  
    "Public": {  
      "DoMain": "test.vantageo.com.cn"  
    }  
  }  
}
```

```

    }
  }
}

```

→ Network port mode configuration:

```

{
  "oem": {
    "Public": {
      "NetworkPortMode": "Fixed",
      "NCSIModeSelect": null,
      "ManagementNetworkPort": {
        "Type": "ShareLink",
        "CardNumber": 2,
        "PortNumber": 1
      }
    }
  }
}

```

- Response Example: None
- Status Code: 204

Output Description

None

4.14 Restarting the BMC

Function

Restart the [BMC](#) of the server.

Permission Required

Power control.

Syntax

- Operation Type: POST
- **URL:** `https://device_ip/redfish/v1/Managers/manager_id/Actions/Manager.Reset`
- Request Header:

```

Content-Type:header_type
X-Auth-Token: auth_value

```

- Request Message Body:

```
{
  "ResetType": value
}
```

Parameters

For a description of the parameters for restarting the BMC, refer to [Table 4-22](#).

Table 4-22 Parameter Descriptions for Restarting the BMC

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
value	Operation type.	ForceRestart : forcibly reboots the BMC.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/Actions/Manager.Reset
```

- Request Header:

```
Content-Type:application/json
```

- Request Message Body:

```
{
  "ResetType":"ForceRestart"
}
```

- Response Example:

```
{
  "error": {
    "@Message.ExtendedInfo": [
      {
```

```

        "@odata.type": "#Message.v1_0_5.Message",
        "Message": "Successfully Completed Request",
        "MessageArgs": [],
        "MessageId": "Base.1.0.Success",
        "RelatedProperties": [],
        "Resolution": "None",
        "Severity": "OK"
    }
],
"code": "Base.1.0.Success",
"message": "Successfully Completed Request"
}
}

```

- Response Code: 200

Output Description

For a description of the output returned when you restart the BMC, refer to [Table 4-23](#).

Table 4-23 Output Descriptions for Restarting the BMC

Field	Type	Description
code	String	String indicating the specified message ID in the message registry.
message	String	Readable message for the code in the message registry.
@odata.type	String	OData description of the message resource.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Message details.
MessageArgs	Array	Message arguments.
Severity	String	Severity level. Options: • OK • Warning • Critical
Resolution	String	Solution.

4.15 Querying Information About the LLDP Service Configuration Resource

Function

Query information about the [LLDP](#) service configuration resource.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Managers/manager_id/LldpService*
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the LLDP service configuration resource, refer to [Table 4-24](#).

Table 4-24 Parameter Descriptions for Querying Information About the LLDP Service Configuration Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Managers/1/LldpService

- Request Header:

x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#LldpService.LldpService",
  "@odata.etag": "\"1596405264\"",
  "@odata.id": "/redfish/v1/Managers/1/LldpService",
  "@odata.type": "#LldpService.v1_0_0.LldpService",
  "Description": "LLDP Service",
  "Id": "LldpService",
  "LldpEnabled": true,
  "Name": "LldpService",
  "WorkMode": "TxRx"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the LLDP service configuration resource, refer to [Table 4-25](#).

Table 4-25 Output Descriptions for Querying Information About the LLDP Service Configuration Resource

Field	Type	Description
@odata.context	String	OData description of the LLDP resource model.
@odata.id	String	Access path of the LLDP resource.
@odata.type	String	Type of LLDP resource.
Description	String	Description of the LLDP resource.
Id	String	ID of the LLDP resource.
Name	String	Name of the LLDP resource.
LldpEnabled	Boolean	Whether LLDP is enabled: • true: enabled • false: disabled
WorkMode	String	LLDP operation mode: • TxRx: enables LLDP packet transmission and reception. • Rx: enables LLDP packet reception only. • Disabled: disables LLDP packet transmission and reception. If this parameter is set to Disabled , LldpEnabled cannot be set to true .

4.16 Modifying Properties of the LLDP Service Resource

Function

Modify properties of the [LLDP](#) service resource.

Permission Required

Security Configuration

Syntax

- Operation Type: PATCH
- URL: `https://device_ip/redfish/v1/Managers/manager_id/LldpService`
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "LldpEnabled":enable_value,
  "workMode" : workmode_value
}
```

Parameters

For a description of the parameters for modifying properties of the LLDP service resource, refer to [Table 4-26](#).

Table 4-26 Parameter Descriptions for Modifying Properties of the LLDP Service Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
enable_value	Whether LLDP is enabled.	• true: enabled • false: disabled Required.
workmode_value	String	LLDP operation mode: • TxRx: enables LLDP packet transmission and reception. • Rx: enables LLDP packet reception only. • Disabled: disables LLDP packet transmission and reception on a port.

Parameter	Description	Value
		When LLDP is enabled, the default setting is TxRx. If LLDP is disabled, workmode_value is unavailable.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Managers/manager_id/LldpService
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=  
Content-Type:application/json
```

- Request Message Body:

```
{  
  "LldpEnabled":true,  
  "WorkMode" : "Rx"  
}
```

- Response Example:

```
{  
  "@odata.context":"/redfish/v1/$metadata#LldpService.LldpService",  
  "@odata.id": "/redfish/v1/Managers/1/LldpService",  
  "@odata.type": "#LldpService.v1_0_0.LldpService",  
  "Description": "LLDP Service",  
  "Id": "LldpService",  
  "LldpEnabled": true,  
  "Name": "LldpService",  
  "WorkMode": "TxRx"  
}
```

- Status Code: 200

Output Description

For a description of the output returned when you modify properties of the LLDP service resource, refer to [Table 4-27](#).

Table 4-27 Output Descriptions for Modifying Properties of the LLDP Service Resource

Field	Type	Description
@odata.context	String	OData description of the LLDP resource model.
@odata.id	String	Access path of the LLDP resource.
@odata.type	String	Type of LLDP resource.
Description	String	Description of the LLDP resource.
Id	String	ID of the LLDP resource.
Name	String	Name of the LLDP resource.
LldpEnabled	Boolean	Whether LLDP is enabled: ● true: enabled ● false: disabled
WorkMode	String	LLDP operation mode: ● TxRx: enables LLDP packet transmission and reception. ● Rx: enables LLDP packet reception only. ● Disabled: disables LLDP packet transmission and reception.

4.17 Querying Information About the SNMP Resource

Function

Query information about the [SNMP](#) resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/SnmpService`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the SNMP resource, refer to [Table 4-28](#).

Table 4-28 Parameter Descriptions for Querying Information About the SNMP Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/SnmpService
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#SnmpService.SnmpService",
  "@odata.id": "/redfish/v1/Managers/1/SnmpService",
  "@odata.type": "#SnmpService.v1_2_0.SnmpService",
  "Actions": {
    "#SnmpService.SubmitTestEvent": {
      "target":
        "/redfish/v1/Managers/1/SnmpService/Actions/SnmpService.SubmitTestEvent"
    }
  },
  "Id": "SnmpService",
  "Name": "SnmpService",
  "ComplexPwdEnable": true,
  "ReadOnlyCommunity": null,
  "ReadWriteCommunity": null,
  "SnmpServiceEnable": true,
  "SnmpServicePort": 161,
  "SnmpTrapNotification": {
    "TrapServer": [
      {
        "MemberId": "0",
```

```

        "TrapServerAddress": "1.2.3.4",
        "TrapServerEnable": true,
        "TrapServerPort": 110
    }, {
        "MemberId": "1",
        "TrapServerAddress": "1.2.3.4",
        "TrapServerEnable": false,
        "TrapServerPort": 111
    }, {
        "MemberId": "2",
        "TrapServerAddress": "2.3.4.5",
        "TrapServerEnable": false,
        "TrapServerPort": 111
    }
],
"AlarmSeverity": "Normal",
"TrapHostIdentify": "BoardSN",
"TrapV3User": "",
"TrapVersion": "V2C",
"TrapServer@odata.count": 3,
"snmpTrapCommunity": "public",
"snmpTrapEnable": true
},
"SnmpV3AuthUser": [
    {
        "snmpV3AuthProtocol": "SHA",
        "snmpV3PrivProtocol": "AES",
        "UserName": "Administrator"
    }
],
"SnmpV3AuthUser@odata.count": 1,
"SnmpV3EngineID": "0x80000f3e035ed7580e2ddd"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the SNMP resource, refer to [Table 4-29](#).

Table 4-29 Output Descriptions for Querying Information About the SNMP Resource

Field	Type	Description
@odata.context	String	OData description of the resource model.
@odata.id	String	Access path of the SNMP resource.

Field	Type	Description
@odata.type	String	Type of SNMP resource.
Actions	Object	Operations that can be performed on the SNMP resource.
#SnmpService.SubmitTestEvent.target	Object	Access path for sending the SNMP trap test event.
Id	String	ID of the SNMP resource.
Name	String	Name of the SNMP resource.
ComplexPwdEnable	Boolean	Complex password switch: ● true: on. ● false: off.
ReadOnlyCommunity	String	Name of the SNMP read-only community. This attribute contains sensitive information and is displayed as null. The PATCH operation is supported.
ReadWriteCommunity	String	Name of the SNMP read/write community. This attribute contains sensitive information and is displayed as null. The PATCH operation is supported.
SnmpServiceEnable	Boolean	SNMP switch: ● true: on. ● false: off.
SnmpServicePort	Number	SNMP service port.
SnmpTrapNotification	Object	SNMP Trap properties.
TrapServer	Array	SNMP Trap server information.
MemberId	String	SNMP Trap group member ID.
TrapServerAddress	String	SNMP Trap server address.
TrapServerEnable	Boolean	Current Trap Server status: ● true: enabled ● false: disabled
TrapServerPort	Number	SNMP Trap server port number.
AlarmSeverity	String	Event severity: ● Critical ● Major ● Minor ● Normal
TrapHostIdIdentify	String	Trap host ID: ● BoardSN: board serial number.

Field	Type	Description
		- ProductAssetTag: product asset tag. - HostName: hostname.
TrapV3User	String	SNMPv3 username.
TrapVersion	String	SNMP Trap version number.: - V1 - V2C - V3
TrapServer@odata.count	Number	Number of SNMP Trap servers.
snmpTrapCommunity	String	SNMP Trap community name.
snmpTrapEnable	Boolean	SNMP Trap switch: - true: on. - false: off.
SnmpV3AuthUser	Array	This array lists the information about all users with the SNMP permission.
snmpV3AuthProtocol	String	SNMPv3 user authentication algorithm: - SHA - MD5 - SHA256 - SHA384 - SHA512
snmpV3PrivProtocol	String	SNMPv3 user encryption algorithm: - DES - AES - AES256
UserName	String	Username of the account with the SNMP permission.
SnmpV3AuthUser@odata.count	Number	Number of users with the SNMP permission.
SnmpV3EngineID	String	SNMPv3 engine ID.

4.18 Modifying Properties of the SNMP Resource

Function

Modify the [SNMP](#) resource information about a server.

Permission Required

Basic management.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/Managers/manager_id/SnmpService*
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "ComplexPwdEnable": ComplexPwdEnable,
  "ReadWriteCommunity": ReadwriteCommunity,
  "ReadOnlyCommunity": ReadOnlyCommunity,
  "SnmpServiceEnable": SnmpServiceEnable,
  "SnmpServicePort": SnmpServicePort,
  "SnmpTrapNotification": {
    "snmpTrapCommunity": snmpTrapCommunity,
    "snmpTrapEnable": snmpTrapEnable,
    "AlarmSeverity": AlarmSeverity,
    "TrapHostIdentify": TrapHostIdentify,
    "TrapVersion": TrapVersion,
    "TrapV3User": TrapV3User,
    "TrapServer": [
      {
        "MemberId": MemberId,
        "TrapServerAddress": TrapServerAddress,
        "TrapServerEnable": TrapServerEnable,
        "TrapServerPort": TrapServerPort
      },
      {
        "MemberId": MemberId,
        "TrapServerAddress": TrapServerAddress,
        "TrapServerEnable": TrapServerEnable,
        "TrapServerPort": TrapServerPort
      }
    ]
  }
}
```

Parameters

For a description of the parameters for modifying the SNMP resource information, refer to [Table 4-30](#).

Table 4-30 Parameter Descriptions for Modifying the SNMP Resource

Field	Type	Description
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
ComplexPwdEnable	String	Complex password switch: ● true: on. ● false: off. If SnmpServiceEnable is set to true, this parameter must be set. If SnmpServiceEnable is set to false, no verification is performed.
ReadWriteCommunity	String	This parameter can be configured when SnmpServiceEnable is set to true. SNMP read-write community name. The naming rule for this parameter is as follows: ● Community name rule when the complex password switch is on: The name supports 8–32 characters, including at least letters, Numbers, and one special character, which can be any visible characters except for a space (" "), single quotation mark ("'"), or backslash("\"). The name cannot begin with a pound sign ("#"). ● Community name rule when the complex password switch is off: The name supports 1–32 characters including Numbers, letters, and special characters. Allowed special characters: visible characters except for a space (" "), single quotation mark ("'"), or backslash("\"). The name cannot begin with a pound sign ("#").

Field	Type	Description
		ReadWriteCommunity is not required. If it is set, verification is performed. If it is not set, no verification is performed.
ReadOnlyCommunity	String	This parameter can be configured when SnmpServiceEnable is set to true. SNMP read-only community name. The naming rule for this parameter is as follows: - Community name rule when the complex password switch is on: The name supports 8–32 characters, including at least letters, Numbers, and one special character, which can be any visible characters except for a space (" "), single quotation mark ("'"), or backslash("\"). The name cannot begin with a pound sign ("#"). - Community name rule when the complex password switch is off: The name supports 1–32 characters including Numbers, letters, and special characters. Allowed special characters: visible characters except for a space (" "), single quotation mark ("'"), or backslash("\"). The name cannot begin with a pound sign ("#"). ReadOnlyCommunity is not required, and will be checked only if there is a value.
SnmpServiceEnable	Boolean	SNMP switch: - true: on. - false: off.
SnmpServicePort	Number	SNMP port number, range: 1–65535, which cannot be null. If SnmpServiceEnable is set to true, this parameter must be set. If SnmpServiceEnable is set to false, no verification is performed.
snmpTrapCommunity	String	SNMP Trap community name, which is a string of 1–18 characters including Numbers, letters, and special characters. Allowed special characters: visible characters except for a space (" "), single quotation mark ("'"), or backslash("\"). The name cannot begin with a pound sign ("#").

Field	Type	Description
		If TrapVersion is set to V1 or V2C, this parameter must be set. If TrapVersion is set to V3, no verification is performed.
snmpTrapEnable	Boolean	SNMP Trap switch: ● true: on. ● false: off.
AlarmSeverity	String	Event severity: ● Critical ● Major ● Minor ● Normal If snmpTrapEnable is set to true, this parameter must be set. If snmpTrapEnable is set to false, no verification is performed.
TrapHostIdentify	String	Trap host ID: ● BoardSN: board serial number. ● ProductAssetTag: product asset tag. ● HostName: hostname. If snmpTrapEnable is set to true, this parameter must be set. If snmpTrapEnable is set to false, no verification is performed.
TrapVersion	String	SNMP Trap version number: ● V1 ● V2C ● V3 If snmpTrapEnable is set to true, this parameter must be set. If snmpTrapEnable is set to false, no verification is performed.
TrapV3User	String	SNMPv3 username. Select a user from those with SNMP permissions as the SNMPv3 Trap user (it is valid when TrapVersion V3 is adopted). If TrapVersion is set to V1 and v2c, no verification is performed. If TrapVersion is set to V2, this parameter must be set.
MemberId	String	SNMP Trap member ID, range: 1–4.

Field	Type	Description
		If Trap Server is set, MemberId must be set.
TrapServerAddress	String	SNMP Trap server address, which can be an IPv4 or IPv6 address. If Trap Server is set, TrapServerAddress must be set.
TrapServerEnable	Boolean	Current Trap server status: ● true: enabled ● false: disabled If Trap Server is set, TrapServerEnable must be set.
TrapServerPort	Number	Port number of the SNMP Trap server. Range: 1 – 65535, which cannot be null. If Trap Server is set, TrapServerPort must be set.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Managers/1/SnmpService
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
  "ComplexPwdEnable": true,
  "SnmpServiceEnable": true,
  "SnmpServicePort": 161,
  "ReadWriteCommunity": "7654321b&",
  "ReadOnlyCommunity": "1234567a$",
  "SnmpTrapNotification": {
    "snmpTrapEnable": true,
    "snmpTrapCommunity": "public",
    "AlarmSeverity": "Normal",
    "TrapHostIdentify": "BoardSN",
    "TrapVersion": "v2C", "TrapServer": [
      {
```

```
        "MemberId": "0",
        "TrapServerAddress": "1.2.3.4",
        "TrapServerEnable": false,
        "TrapServerPort": 110
    },
    {
        "MemberId": "1",
        "TrapServerAddress": "1.2.3.4",
        "TrapServerEnable": false,
        "TrapServerPort": 111
    },
    {
        "MemberId": "2",
        "TrapServerAddress": "2.3.4.5",
        "TrapServerEnable": false,
        "TrapServerPort": 111
    }
]
}
```

Separate SNMP instance configuration:

```
{
  "ComplexPwdEnable": true,
  "SnmpServiceEnable": true,
  "SnmpServicePort": 161,
  "ReadwriteCommunity": "7654321b&",
  "ReadOnlyCommunity": "1234567a$"
}
```

Separate SNMP Trap instance configuration:

```
{
  "SnmpTrapNotification": {
    "snmpTrapEnable": true,
    "snmpTrapCommunity": "public",
    "AlarmSeverity": "Normal",
    "TrapHostIdentify": "BoardSN",
    "TrapVersion": "V2C"
  }
}
```

Separate SNMP Trap Server instance configuration:

```
{
```

```
"SnmpTrapNotification": {
  "TrapServer": [
    {
      "MemberId": "0",
      "TrapServerAddress": "1.2.3.4",
      "TrapServerEnable": false,
      "TrapServerPort": 110
    },
    {
      "MemberId": "1",
      "TrapServerAddress": "1.2.3.4",
      "TrapServerEnable": false,
      "TrapServerPort": 111
    },
    {
      "MemberId": "2",
      "TrapServerAddress": "2.3.4.5",
      "TrapServerEnable": false,
      "TrapServerPort": 111
    }
  ]
}
```

- Response Example: None
- Response Code: 204

Output Description

None

4.19 Submitting an SNMP Trap Test Event

Function

Submit an [SNMP](#) Trap test event.

Permission Required

Diagnosis.

Syntax

- Operation Type: POST
- **URL:** `https://device_ip/redfish/v1/Managers/manager_id/SnmpService/Actions/SnmpService.SubmitTestEvent`

- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "MemberId": MemberId
}
```

Parameters

For a description of the parameters for submitting an SNMP Trap test event, refer to [Table 4-31](#)

Table 4-31 Parameter Descriptions for Submitting an SNMP Trap Test Event

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
MemberId	Trap group member ID.	Range: 1–4.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/SnmpService/Actions/SnmpService.SubmitTestEvent
```

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
  "MemberId": 1
}
```

- Response Example: None

- Response Code: 204

Output Description

None

4.20 Querying the Virtual Media Resource Collection

Function

Query the virtual media resource collection.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** *https://device_ip/redfish/v1/Managers/manager_id/VirtualMedia*
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the virtual media resource collection, refer to [Table 4-32](#).

Table 4-32 Parameter Descriptions for Querying the Virtual Media Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Managers/1/VirtualMedia

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#VirtualMediaCollection.VirtualMediaCollection",
  "@odata.id": "/redfish/v1/Managers/1/VirtualMedia",
  "@odata.type": "#VirtualMediaCollection.VirtualMediaCollection",
  "Description": "Virtual Media Services Settings",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Managers/1/VirtualMedia/CD"
    },
    {
      "@odata.id": "/redfish/v1/Managers/1/VirtualMedia/CD1"
    },
    {
      "@odata.id": "/redfish/v1/Managers/1/VirtualMedia/USBstick"
    },
    {
      "@odata.id": "/redfish/v1/Managers/1/VirtualMedia/USBstick1"
    }
  ],
  "Members@odata.count": 4,
  "Name": "Virtual Media Services"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the virtual media resource collection, refer to [Table 4-33](#).

Table 4-33 Output Descriptions for Querying the Virtual Media Resource Collection

Field	Type	Description
@odata.context	String	OData description of the virtual media resource collection model.
@odata.id	String	Access path of the virtual media resource collection.
@odata.type	String	Type of virtual media resource collection.
Description	String	Description

Field	Type	Description
Members	Array	Virtual media resource list. The CD1 and USBStick1 resources can be queried and used only when the number of entities is set to two.
@odata.id	String	Access path of the virtual media resource collection.
Members@odata.count	Number	Number of virtual media resource members that can be connected currently.
Name	String	Name of the virtual media resource collection.

4.21 Querying a Virtual Media Resource

Function

Query a virtual media resource.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/VirtualMedia/Media_type`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the virtual media resource, refer to [Table 4-34](#).

Table 4-34 Parameter Descriptions for Querying the Virtual Media Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
Media_type	Virtual Media Type	Supports CD/CD1/USBStick/USBStick1.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/VirtualMedia/CD
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#VirtualMedia.VirtualMedia",
  "@odata.id": "/redfish/v1/Managers/1/VirtualMedia/CD",
  "@odata.type": "#VirtualMedia.v1_2_0.VirtualMedia",
  "Description": "CD VirtualMedia",
  "ConnectedVia": "NotConnected",
  "Id": "CD",
  "Name": "VirtualMedia",
  "Image": null,
  "ImageName": null,
  "Inserted": false,
  "MediaTypes": [
    "CD"
  ],
  "TransferMethod": null,
  "TransferProtocolType": null,
  "Actions": {
    "#VirtualMedia.InsertMedia": {
      "target": "/redfish/v1/Managers/1/VirtualMedia/CD/Actions/
virtualMedia.InsertMedia"
    },
    "#VirtualMedia.EjectMedia": {
      "target": "/redfish/v1/Managers/1/VirtualMedia/CD/Actions/
virtualMedia.EjectMedia"
    },
    "Oem": {
      "Public": {
        "#VirtualMedia.VmmControl": {
          "@Redfish.ActionInfo":
            "/redfish/v1/Managers/1/VirtualMedia/CD/VmmControlActionInfo",
```

```

        "target":
        "/redfish/v1/Managers/1/VirtualMedia/CD/Actions/
        VirtualMedia.VmmControl"
    }
}
}
}
}
}
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the virtual media resource, refer to [Table 4-35](#).

Table 4-35 Output Descriptions for Querying the Virtual Media Resource

Field	Type	Description
@odata.context	String	OData description of the virtual media resource model.
@odata.id	String	Access path of the virtual media resource.
@odata.type	String	Type of virtual media resource.
Description	String	Description.
ConnectedVia	String	Connection method.
Id	String	ID of the virtual media resource.
Name	String	Name of the virtual media resource.
MediaTypes	Array	Media plane type: • CD • USBStick
TransferProtocolType	String	Transmission protocol type: • NFS • CIFS • HTTPS • HTTP
TransferMethod	String	Transfer method: stream
Image	String	Image path.
ImageName	String	Image name.
ConnectedVia	String	Connection method.
Inserted	Boolean	Connection status:

Field	Type	Description
		● true: mounting (inserted) ● false: Uninstalled (removed)
Oem	Object	Customized properties of a specified session.
Actions	Object	Available actions for the virtual media resource.
#VirtualMedia.InsertMedia	String	Access path for attaching the remote media to the virtual media device.
#VirtualMedia.EjectMedia	String	Access path for detaching the remote media from the virtual media device.
#VirtualMedia.VmmControl	String	Access path for connecting to the virtual media.

4.22 Connecting to the Virtual Media

Function

Connect to the virtual media.

Permission Required

Remote media

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/VirtualMedia/media_type/Actions/VirtualMedia.VmmControl`
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "Image": Image_value,
  "Username": username_value,
  "Password": password_value,
  "VmmControlType": value
}
```

Parameters

For a description of the parameters for connecting to the virtual media, refer to [Table 4-36](#).

Table 4-36 Parameter Descriptions for Connecting to the Virtual Media

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
Media_type	Virtual Media Type	CD, CD1, USBStick, and USBStick1 are supported.
auth_value	When executing this POST request, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
Image_value	Type: string, shared path, determined by the shared server.	The maximum length is 256 characters. The format is as follows: "Image": "protocol://server_ip/file_path/file_name"
username_value	Type: string. This field needs to be provided when the CIFS protocol and the HTTPS protocol are used. The maximum length is 32 characters.	This field is not required when the NFS protocol is used.
password_value	Type: string. This field needs to be provided when the CIFS protocol is used. This field needs to be provided when the HTTPS protocol is used. The maximum length is 32 characters.	This field is not required when the NFS protocol is used.
value	Virtual media operation type	Connect : connects to virtual media.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/VirtualMedia/CD/Actions/VirtualMedia.VmmControl
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
  "Image": "cifs://device_ip/home/mount_test/isocfg-tool-v1.iso",
  "Username": "test",
  "Password": "123",
  "VmmControlType": "Connect"
}
```

- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#VirtualMedia.VirtualMedia",
  "@odata.id": "/redfish/v1/Managers/1/VirtualMedia/CD/Actions/
VirtualMedia.VmmControl",
  "@odata.type": "#VirtualMedia.v1_2_0.VirtualMedia",
  "Information": {
    "target": "/redfish/v1/Managers/1/VirtualMedia/CD"
  }
}
```

- Status Code: 200

Output Description

For a description of the output returned when the virtual media is accessed, refer to [Table 4-37](#).

Table 4-37 Output Descriptions for Connecting to the Virtual Media

Field	Type	Description
@odata.context	String	OData description of the virtual media resource.
@odata.id	String	Path to connect the virtual media resource.
@odata.type	String	Type of virtual media resource.
Information	Object	-
target	String	Access path of the current virtual media resource.

4.23 Disconnecting the Virtual Media

Function

Disconnect the virtual media.

Permission Required

Remote media

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/VirtualMedia/media_type/Actions/VirtualMedia.VmmControl`
- Request Header:

x-auth-token:auth_value

Content-Type:header_type

- Request Message Body:

{

"vmmControlType":value

}

Parameters

For the parameter descriptions for disconnecting the virtual media, refer to [Table 4-38](#).

Table 4-38 Parameter Descriptions for Disconnecting the Virtual Media

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
Media_type	Virtual Media Type	CD, CD1, USBStick, and USBStick1 are supported.
auth_value	When executing this POST request, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
value	Virtual media operation type	Disconnect : disconnects the virtual media.

Usage Guidelines

None

Example

- Request Example:

POST https://device_ip/redfish/v1/Managers/1/VirtualMedia/CD/Actions/VirtualMedia.VmmControl

- Request Header:


```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
  "vmmControlType": "Disconnect"
}
```

- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#VirtualMedia.VirtualMedia",
  "@odata.id": "/redfish/v1/Managers/1/VirtualMedia/CD/Oem/VANTAGEO/Actions/
VirtualMedia.vmmControl",
  "@odata.type": "#VirtualMedia.v1_2_0.VirtualMedia",
  "Information": {
    "target": "/redfish/v1/Managers/1/VirtualMedia/CD"
  }
}
```

- Status Code: 200

Output Description

For a description of the output returned when the virtual media is disconnected, refer to [Table 4-39](#).

Table 4-39 Output Descriptions for Disconnecting the Virtual Media

Field	Type	Description
@odata.context	String	OData description of the virtual media resource.
@odata.id	String	Access path of the disconnected virtual media resource.
@odata.type	String	Type of virtual media resource.
Information	Object	-
target	String	Access path of the current virtual media resource.

4.24 Sending a One-Click Collection Request

Function

Send a one-click collection request.

Permission Required

Diagnosis.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/LogServices/Actions/LogServices.Dump`
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "Type":type_value
}
```

Parameters

For a description of the parameters for sending a one-click collection request, refer to [Table 4-40](#).

Table 4-40 One-Click Collection Request Parameter Descriptions

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	When executing this POST request, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
type_value	Operation Type	Type: Logs

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/LogServices/Actions/LogServices.Dump
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
  "Type": "Logs"
}
```

- Response Example:

```
{
  "error": {
    "code": "Base.1.8.1.Success",
    "message": "Successfully Completed Request",
    "@Message.ExtendedInfo": [
      {
        "@odata.type": "#Message.v1_1_1.Message",
        "MessageId": "Base.1.8.1.Success",
        "Message": "Successfully Completed Request",
        "Severity": "OK",
        "Resolution": "None."
      }
    ]
  }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you send a one-click collection request, refer to [Table 4-41](#)

Table 4-41 Output Descriptions for One-Click Collection Requests

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Readable message for the code in the message registry.
@odata.type	String	OData description of the message resource.
MessageId	String	Message ID.
Message	String	Details.
Severity	String	Severity level. Options: ● OK ● Warning ● Critical

Field	Type	Description
Resolution	String	Solution.

4.25 Querying the One-Click Collection Progress

Function

Query the one-click collection progress.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Managers/managers_id/LogServices/Actions/LogServices.Dump/Progress`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the one-click collection progress, refer to [Table 4-42](#).

Table 4-42 Parameter Descriptions for Querying the One-Click Collection Progress

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Managers/1/LogServices/Actions/LogServices.Dump/Progress

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata",
  "@odata.id": "/redfish/v1/Managers/Self/LogServices/Actions/LogServices.Dump/Progress",
  "@odata.type": "#Message.v1_1_1.Message",
  "Message": "SUCCEEDED",
  "Percentage": "100",
  "State": "STATE_SUCCEEDED",
  "TarName": "bmcinfo_UnknownProductSN.tar.gz",
  "TarPath": "/var/bmcdata/bmcinfo_UnknownProductSN.tar.gz",
  "Type": "Logs"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the one-click collection progress, refer to [Table 4-43](#).

Table 4-43 Output Descriptions for Querying the One-Click Collection Progress

Field	Type	Description
@odata.context	String	OData description for the query of the one-click log collection progress.
@odata.id	String	Access path for the query of the one-click log collection progress.
@odata.type	String	Type of query of the one-click log collection progress.
Percentage	String	Task progress percentage.
State	String	Status, options: • STATE_FAILED • STATE_SUCCEEDED • STATE_RUNNING • STATE_SILENT
Type	String	Type. Only the Logs type is available in this version.
Message	String	Task progress status, including: • SILENT: indicates that collection is triggered.

Field	Type	Description
		● RUNNING: indicates that collection is in progress. ● SUCCEEDED: indicates that collection is completed and successful. ● FAILED: indicates that an error occurs during collection.
TarName	String	File name of the compressed package, in which UnknownProductSN varies with the actual SN . If the actual SN is not obtained, UnknownProductSN is used.
TarPath	String	Storage path of the local compressed package.

4.26 Exporting Logs

Function

Export the log information about a server.

Permission Required

Diagnosis.

Syntax

- Operation Type: POST
- **URL**: `https://device_ip/redfish/v1/Managers/manager_id/LogServices/Actions/LogServices.ExportLogs`
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "Type":type_value,
  "Content":content_value
}
```

Parameters

For a description of the parameters for exporting logs, refer to [Table 4-44](#).

Table 4-44 Log Export Parameter Descriptions

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	Supported message formats: application and json
type_value	Operation type.	Type: Logs
content_value	File path.	Path for exporting log files: - Remote download. TFTP is supported. Value: remote service address. - Local download. Value: TarPath in the response returned through the progress query interface.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/LogServices/Actions/LogServices.ExportLogs
```

- Request Header:

```
Content-Type: application/json
```

- Request Message Body:

```
{
  "Type": "Logs",

  "Content": "tftp://10.10.10.191/ID_config.tar.gz"
}
```

- Response Example:

```
{
  "error": {
    "code": "Base.1.8.1.Success",
    "message": "Successfully Completed Request",
  }
}
```

```

    "@Message.ExtendedInfo": [
      {
        "@odata.type": "#Message.v1_1_1.Message",
        "MessageId": "Base.1.8.1.Success",
        "Message": "Successfully Completed Request",
        "Severity": "OK",
        "Resolution": "None."
      }
    ]
  }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you export the logs, refer to [Table 4-45](#).

Table 4-45 Log Export Descriptions

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Readable message for the code in the message registry.
@odata.type	String	OData description of the message resource.
MessageId	String	Message ID.
Message	String	Details.
Severity	String	Severity. The Redfish supports the following severity levels: • OK • Warning • Critical
Resolution	String	Solution.

4.27 Querying the KVM Service Resource

Function

Query [KVM](#) resource information.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/KvmService`
- Request Header:

```
x-auth-token:auth_value
```

- Request Message Body: None

Parameters

For a description of the parameters for querying the KVM service resource, refer to [Table 4-46](#).

Table 4-46 Parameter Descriptions for Querying the KVM Service Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the Get request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/KvmService
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#KvmService.KvmService",
  "@odata.id": "/redfish/v1/Managers/Self/KvmService",
  "@odata.type": "#KvmService.v1_0_0.KvmService",
  "ActivatedSessionsType": "Private",
  "EncryptionEnabled": true,
  "Description": "KvmService",
  "KvmUrl": "https://192.168.5.7/viewer.html?&token=IyWH3U7qkcKzW8akb",
}
```

```

    "MaximumNumberOfSessions": 4,
    "NumberOfActivatedSessions": 0,
    "SessionTimeoutMinutes": 30
  }

```

- Status Code: 200

Output Description

For a description of the output returned when you query the KVM service resource, refer to [Table 4-47](#).

Table 4-47 Output Descriptions for Querying the KVM service Resource

Field	Type	Description
@odata.context	String	OData description of the KVM service resource model.
@odata.id	String	Access path of the KVM resource.
@odata.type	String	Type of KVM service resource.
Description	String	Description of the KVM resource.
MaximumNumberOfSessions	Number	Maximum number of KVM sessions.
KvmUrl	String	URL for accessing the KVM resource. When the URL is used for access, the Web session is automatically logged out.
NumberOfActivatedSessions	Number	Number of current KVM sessions.
ActivatedSessionsType	String	KVM session type. Options: • Shared: Shared • Private: Exclusive
EncryptionEnabled	Boolean	Enables or disables KVM encryption. Options: • true: enabled. • false: disabled.
SessionTimeoutMinutes	Number	Session timeout time, range: 1–60, unit: minutes.

4.28 Modifying Information About the KVM Resource

Function

Modify information about the [KVM](#) resource.

Permission Required

Remote control

Syntax

- Operation Type: PATCH
- URL: `https://device_ip/redfish/v1/Managers/manager_id/KvmService`
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "EncryptionEnabled": EncryptionEnabled_value,
  "SessionTimeoutMinutes": SessionTimeoutMinutes_value
}
```

Parameters

For a description of the parameters for modifying the KVM resource, refer to [Table 4-48](#).

Table 4-48 Parameter Descriptions for Modifying Information About the KVM Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	Supported formats: application and json.
EncryptionEnabled_value	Whether KVM encryption is enabled.	• true: enabled • false: disabled
SessionTimeoutMinutes_value	Session timeout period.	Range: 1–60, unit: minutes.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Managers/1/KvmService
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

Content-Type:application/json

- Request Message Body:

```
{
  "EncryptionEnabled": true,
  "SessionTimeoutMinutes": 10
}
```

- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#KvmService.KvmService",
  "@odata.id": "/redfish/v1/Managers/Self/KvmService",
  "@odata.type": "#KvmService.v1_0_0.KvmService",
  "ActivatedSessionsType": "Private",
  "EncryptionEnabled": true,
  "Description": "KvmService",
  "MaximumNumberOfSessions": 4,
  "NumberOfActivatedSessions": 0,
  "SessionTimeoutMinutes": 10
}
```

- Status Code: 200

Output Description

For a description of the output returned when you modify information about the KVM resource, refer to [Table 4-49](#).

Table 4-49 Output Descriptions for Modifying Information About the KVM Resource

Field	Type	Description
@odata.context	String	OData description of the KVM service resource model.
@odata.id	String	Access path of the KVM resource.
@odata.type	String	Type of KVM service resource.
Description	String	Description of the KVM resource.
MaximumNumberOfSessions	Number	Maximum number of KVM sessions.
NumberOfActivatedSessions	Number	Number of current KVM sessions.
ActivatedSessionsType	String	KVM session type. Options: - Shared: shared. - Private: exclusive.
EncryptionEnabled	Boolean	Enables or disables KVM encryption. Options: true: enabled.

Field	Type	Description
		False: disabled.
SessionTimeoutMinutes	Number	Session timeout time, range: 1–60.

4.29 Querying Information About a Specified SEL Log Service Resource

Function

Query information about the specified [SEL](#) log service resource of a server.

Permission Required

Security management.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/LogServices/SEL/Entries/entries_id`
- Request Header:

X-Auth-Token:auth_value

- Request Message Body: None

Description

For a description of the parameters for querying information about the specified SEL log service resource, refer to [Table 4-50](#).

Table 4-50 Parameter Descriptions for Querying Information About the Specified SEL Log Service Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
entries_id	Log resource ID.	It can be obtained from the log resource collection.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/LogServices/SEL/Entries/1
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#LogEntry.LogEntry",
  "@odata.id": "/redfish/v1/Managers/Self/LogServices/SEL/Entries/631",
  "@odata.type": "#LogEntry.v1_4_3.LogEntry",
  "Created": "2010-03-04T14:56:23+08:00",
  "Description": "SEL LOG info",
  "EntryCode": "Assert",
  "EntryType": "SEL",
  "EventTimestamp": "2010-03-04T14:56:23+08:00",
  "Id": "631",
  "Message": "Initiated By Warm Reset",
  "MessageId": "0x02FFFF",
  "Name": "SEL 1221",
  "SensorNumber": 128,
  "Oem": {
    "Public": {
      "OwnerLUN": 0
    }
  },
  "SensorType": "SystemBoot/Restart",
  "Severity": "OK"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified SEL log service resource, refer to [Table 4-51](#).

Table 4-51 Output Descriptions for Querying Information About the Specified SEL Log Service Resource

Field	Type	Description
@odata.context	String	OData description of the specified SEL log service resource model.
@odata.id	String	Access path of the specified SEL log service resource node.
@odata.type	String	Type of the specified SEL log service resource.
Created	String	Time when the SEL log instance is created.
Description	String	Log resource description information.
EntryCode	String	Type of SEL log instance.
EntryType	String	Type of SEL log instance. • SEL • Oem
EventTimestamp	String	Timestamp of the SEL log instance information.
Id	String	ID of the SEL log instance.
Message	String	Message content of the SEL log instance information.
MessageId	String	Message ID of the SEL log instance information.
Name	String	Name of the SEL log instance.
SensorNumber	Number	ID of the sensor that creates the SEL log instance.
SensorType	String	Type of the sensor that creates the SEL log instance.
Message	String	Details.
Severity	String	Log severity level of the SEL log instance information. • OK • Warning • Critical • Non-recoverable
Oem.Public	Object	Customized properties.
OwnerLUN	Number	SensorNumber extension.

4.30 Capturing the Screen Manually

Function

Capture the screen manually.

Permission Required

Diagnosis.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/Actions/Manager.CaptureScreenShot`
- Request Header:

X-Auth-Token:auth_value

- Request Message Body: None

Description

For a description of the parameters for capturing the screen manually as the query condition, refer to [Table 4-52](#).

Table 4-52 Parameter Descriptions for Capturing the Screen Manually

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

POST https://device_ip/redfish/v1/Managers/1/Actions/Manager.CaptureScreenShot

- Request Header:

X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None
- Response Example: None
- Status Code: 204

Output Description

None

4.31 Downloading the Manually Captured Screen Image

Function

Download the manually captured screen image.

Permission Required

Diagnosis.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/Actions/Manager.DownloadScreenShot`
- Request Header:

x-auth-token:auth_value
- Request Message Body: None

Description

For a description of the parameters for downloading the manually captured screen image, refer to [Table 4-53](#).

Table 4-53 Parameter Descriptions for Downloading the Manually Captured Screen Image

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

POST https://device_ip/redfish/v1/Managers/1/Actions/Manager.DownloadScreenShot

- Request Header:

x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None
- Response Example: None
- Status Code: 200

Output Description

Return the image data of the manually captured screen image.

4.32 Querying Information About the ISDT Resource

Function

Query the information about the ISDT resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: https://device_ip/redfish/v1/Managers/manager_id/ISDTService
- Request Header: None

X-Auth-Token:auth_value

- Request Message Body: None

Description

For a description of the parameters for querying information about the ISDT resource, refer to [Table 4-54](#).

Table 4-54 Parameter Descriptions for Querying Information About the ISDT Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Managers/1/ISDTSERVICE

- Request Header:

x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None
- Response Example:
- Status Code: 200

```
{
  "@odata.context": "/redfish/v1/$metadata#ISDTSERVICE.ISDTSERVICE",
  "@odata.id": "/redfish/v1/Managers/1/ISDTSERVICE",
  "@odata.type": "#ISDTSERVICE.v1_0_0.ISDTSERVICE",
  "ImageInstalled": true,
  "ImageMounted": true,
  "ISDTStartEnabled":
true, "Version": {
  "ISDTVersion": "V01.24.04.00",
  "ISDTBuildDate": "2024-08-12
23:47:19",
  "ISDTPlatform": "X86_64"
},
  "Actions": {
    "#ISDTSERVICE.VmmControl": {
      "target": "/redfish/v1/Managers/1/ISDTSERVICE/Actions/ISDTSERVICE.VmmControl"
    }
  }
}
```

Output Description

For a description of the output returned when you query information about the ISDT resource, refer to [Table 4-55](#).

Table 4-55 Output Descriptions for Querying Information About the ISDT Resource

Field	Type	Description
@odata.context	String	OData description of the ISDT resource model.

Field	Type	Description
@odata.id	String	Access path of the ISDT resource node.
@odata.type	String	Type of the ISDT resource.
ImageInstalled	Boolean	Whether there is a navigation disk image.
ImageMounted	Boolean	Whether the ISDT image is mounted.
ISDTStartEnabled	Boolean	Whether one-click ISDT startup is enabled.
Version	Object	Version number object
Version.ISDTVersion	String	ISDT version number.
Version.ISDTBuildDate	String	ISDT generation date.
Version.ISDTPlatform	String	Platform that supports ISDT.
Actions	Object	Available actions for the ISDT resource.
#ISDTService.VmmControl.target	String	Path of the control operation on the navigation disk.

4.33 Modifying Properties of the ISDT Service Resource

Function

Modify properties of the ISDT Service resource.

Permission Required

VMM.

Syntax

- Operation Type: PATCH
- URL: `https://device_ip/redfish/v1/Managers/manager_id/ISDTService`
- Request Header:

```
x-auth-token:auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "ServiceEnabled": ServiceEnabled_value,
  "ISDTStartEnabled": ISDTStartEnabled_value
}
```

Description

For a description of the parameters for modifying properties of the ISDT Service resource, refer to [Table 4-56](#).

Table 4-56 Parameter Descriptions for Modifying Properties of the ISDT Service Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	During the execution of the PATCH request, the "Headers" field must carry the "X-Auth-Token" value for authentication.	It can be obtained when a session is created through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
ServiceEnabled	Whether service is enabled.	● true: enabled ● false: disabled
ISDTStartEnabled_value	Whether one-click ISDT startup is enabled.	● true: yes. ● false: no.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Managers/1/ISDTService
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type: application/json
```

- Request Message Body:

```
{
  "ServiceEnabled": true,
  "ISDTStartEnabled": true
}
```

- Response Example: None
- Status Code: 204

Output Description

None

4.34 Mounting and Dismounting Navigation Disks

Function

Mount and dismount navigation disks.

Permission Required

VMM.

Syntax

- Operation Type: POST
- **URL:** `https://device_ip/redfish/v1/Managers/manager_id/ISDTSer-vice/Actions/ISDTService.VmmControl`
- Request Header:

```
x-auth-token:auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "VmmControlType": vmm_control_type_value
}
```

Description

For a description of the parameters for mounting and dismounting navigation disks, refer to [Table 4-57](#).

Table 4-57 Parameter Descriptions for Mounting and Dismounting Navigation Disks

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	During the execution of the PATCH request, the "Headers" field must carry the "X-Auth-Token" value for authentication.	It can be obtained when a session is created through <code>/redfish/v1/SessionService/Sessions</code> .
vmm_control_type_value	Type of Vmm control.	• Connect: connected • Disconnect: disconnected

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/ISDTService/Actions/ISDTService.VmmControl
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type: application/json
```

- Request Message Body:

```
{
  "VmmControlType": "Connect"
}
```

- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#ISDTService.ISDTService",
  "@odata.id": "/redfish/v1/Managers/1/ISDTService/Actions/ISDTService.VmmControl",
  "@odata.type": "#ISDTService.v1_0_0.ISDTService",
  "Information": {
    "target": "/redfish/v1/Managers/1/ISDTService"
  }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you mount and dismount navigation disks, refer to [Table 4-58](#).

Table 4-58 Output Descriptions for Mounting and Dismounting Navigation Disks

Field	Type	Description
@odata.context	String	OData description of the ISDT resource model.
@odata.id	String	Access path of the ISDT resource node.
@odata.type	String	Type of ISDT resource.
Information	Object	-
target	String	Access path of the current ISDT resource.

4.35 Querying Information About the ISDT FWUpdate Collection

Function

Query information about the ISDT FWUpdate collection.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/ISDTService/ISDTFWUpdate`
- Request Header:

X-Auth-Token:auth_value

- Request Message Body: None

Description

For a description of the parameters for querying information about the ISDT FWUpdate collection, refer to [Table 4-59](#).

Table 4-59 Parameter Descriptions for Querying Information About the ISDT FWUpdate Collection

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Managers/1/ISDTService/ISDTFWUpdate
--

- Request Header:

X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#ISDTFWUpdateCollection.ISDTFWUpdateCollection",
  "@odata.id": "/redfish/v1/Managers/manager_id/ISDTSservice/ISDTFWUpdate",
  "@odata.type": "#ISDTFWUpdateCollection.ISDTFWUpdateCollection",
  "Name": "ISDT Framework Update Collection",
  "Members@odata.count": 1,
  "Members": [
    {
      "@odata.id": "/redfish/v1/Managers/manager_id/ISDTSservice/ISDTFWUpdate/1"
    }
  ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the ISDT FWUpdate collection, refer to [Table 4-60](#).

Table 4-60 Output Descriptions for Querying Information About the ISDT FWUpdate Collection

Field	Type	Description
@odata.context	String	OData description of the ISDT resource collection model.
@odata.id	String	Access path of the ISDT resource collection node.
@odata.type	String	Type of ISDT resource collection.
Name	String	Name of the ISDT resource collection.
Members@odata.count	Number	Number of ISDT FWUpdate tasks, which is fixed to one.
Members.@odata.id	String	ISDT FWUpdate task.

4.36 Querying Information About an ISDT FWUpdate Task

Function

Query information about an ISDT FWUpdate task.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/ISDTSer-vice/ISDTFWUpdate/updateid`
- Request Header:

X-Auth-Token:auth_value

- Request Message Body: None

Description

For a description of the parameters for querying information about an ISDT FWUpdate task, refer to [Table 4-61](#).

Table 4-61 Parameter Descriptions for Querying Information About an ISDT FWUpdate Task

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
updateid	ID of the available ISDT FWUpdate task.	Fixed to 1.

Usage Guidelines

None

Example

- Request Example:

GET `https://device_ip/redfish/v1/Managers/1/ISDTService/ISDTFWUpdate/12`

- Request Header:

X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None
- Response Example:

{

```

"@odata.context": "/redfish/v1/$metadata#ISDTFWUpdate.ISDTFWUpdate",
"@odata.id": "/redfish/v1/Managers/manager_id/ISDTSservice/ISDTFWUpdate/1",
"@odata.type": "#ISDTFWUpdate.v1_0_0.ISDTFWUpdate",
"Id": "1",
"Name": "ISDT Framework Update",
"TransferState": null,
"TransferFileName": null,
"UpgradeProgress": 0,
"Messages": [],
"Actions": {
    "#ISDTFWUpdate.SimpleUpdate": {
        "target":
            "/redfish/v1/Managers/manager_id/ISDTSservice/ISDTFWUpdate/1/Actions/
            ISDTFWUpdate.SimpleUpdate"
    }
}
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about an ISDT FWUpdate task, refer to [Table 4-62](#).

Table 4-62 Output Descriptions for Querying Information About an ISDT FWUpdate Task

Field	Type	Description
@odata.context	String	OData description of the ISDT FWUpdate resource model.
@odata.id	String	Access path of the ISDT FWUpdate resource.
@odata.type	String	Type of ISDT FWUpdate resource.
Id	Integer	ID of the available ISDT FWUpdate resource, which is fixed to 1.
Name	String	Description of the interface.
TransferState	String	File transfer status. Options: ● Initiating ● Ongoing ● Completed
TransferFileName	String	Name of the file that is transferred. Options: ● ImageUrl carried in the request during update. ● SignalUrl carried in the request during update.
UpgradeProgress	Integer	Task progress, range: 0–100.

Field	Type	Description
Messages	Array	Task progress description, which is not fixed. A completion time string is available when the task is completed.
Actions	String	Operations that can be performed on the resource.
#SDTFWUpdate.SimpleUpdate.target	String	Operation Path for the SimpleUpdate resource.

4.37 Burning an ISDT Image

Function

Burn an ISDT image.

Permission Required

VMM.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/ISDTService/ISDTFWUpdate/update_id/Actions/SDTFWUpdate.SimpleUpdate`
- Request Header:

```
X-Auth-Token:auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "ImageURI":"image_URI_value",
  "SignalURI":"signal_URI_value"
}
```

Description

For a description of the parameters for burning an ISDT image, refer to [Table 4-63](#).

Table 4-63 Parameter Descriptions for Burning an ISDT Image

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
update_id	Update task ID.	-

Parameter	Setting	Value
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
image_URI_value	Remote path of the ISO image.	URL for the remote file path, for example, <code>https://192.168.1.5/abc/xxx.iso</code>
signal_URI_value	Remote path for the authentication file corresponding to the update file.	URL for the authentication file path, for example, <code>https://192.168.1.5/abc/yyy.checksum</code>

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/ISDTSservice/ISDTFWUpdate/12/Actions/SDTFWUpdate.SimpleUpdate
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type: application/json
```

- Request Message Body:

```
{
  "ImageURI": "https://serverip:port/ISDT.iso",
  "SignalURI": "https://serverip:port/checksum.txt"
}
```

- Response Example:

```
{
  "error": {
    "code": "Base.1.0.GeneralError",
    "message":
      "A general error has occurred. See ExtendedInfo for more information.",
    "@Message.ExtendedInfo": [
      {
        "@odata.type": "#Message.v1_0_0.Message",
        "MessageId": "Base.1.0.Success",
        "RelatedProperties": [],
        "Message": "Successfully Completed Request",

```

```

        "MessageArgs": [],
        "Severity": "OK",
        "Resolution": "None"
    }
]
}
}

```

- Response code: 202

Output Description

For a description of the output returned when you burn an ISDT image, refer to [Table 4-64](#).

Table 4-64 Output Descriptions for Burning an ISDT Image

Field	Type	Description
code	String	Response code description.
message	String	Prompt message that is returned.
@Message.ExtendedInfo	Array	Extended information about the message.
@odata.type	String	OData description of the message resource.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Details.
MessageArgs	Array	Message arguments.
Severity	String	Severity level. Options: • OK • Warning • Critical
Resolution	String	Recommended solution.

4.38 Adding Routes

Function

Add routes.

Permission Required

Basic management.

Syntax

- Operation Type: POST

- **URL:** `https://device_ip/redfish/v1/Managers/manager_id/EthernetInterfaces/id/Actions/EthernetInterface.AddRoutes`

- **Request Header:**

```
X-Auth-Token:auth_value
Content-Type: header_type
```

- **Request Message Body:**

```
{
  "IPv4Route": {
    "Address": ipv4_address_value,
    "Netmask": ipv4_netmask_value
  },
  "IPv6Route": {
    "Address": ipv6_address_value,
    "PrefixLength": ipv6_prefixLen_value
  }
}
```

Description

For a description of the parameters for adding routes, refer to [Table 4-65](#).

Table 4-65 Parameter Descriptions for Adding Routes

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
id	ID of the BMC management interface resource.	It can be obtained by querying the collection of BMC management interface resources.
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
ipv4_address_value	String	IP address(IPv4 and IPv6 addresses are set separately)
ipv4_netmask_value	String	Mask.
ipv6_address_value	String	IP address.

Parameter	Setting	Value
ipv6_prefixLen_value	Number	Prefix length.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/EthernetInterfaces/D64FE89CE17C/Actions/EthernetInterface.AddRoutes
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type: application/json
```

- Request Message Body:

```
{
  "IPv4Route": {
    "Address": "192.168.1.5",
    "Netmask": "255.255.255.192"
  },
  "IPv6Route": {
    "Address": "ff00::",
    "PrefixLength": 8
  }
}
```

- Response Example: None
- Response code: 204

Output Description

None

4.39 Deleting Routes

Function

Delete routes.

Permission Required

Basic management.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/EthernetInterfaces/id/Actions/EthernetInterface.DeleteRoutes`

- Request Header:

```
X-Auth-Token:auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "IPv4Route": {
    "Address": "ipv4_address_value",
    "Netmask": "ipv4_netmast_value"
  },
  "IPv6Route": {
    "Address": "ipv6_address_value",
    "PrefixLength": ipv6_prefixLen_value
  }
}
```

Description

For a description of the parameters for deleting routes, refer to [Table 4-66](#).

Table 4-66 Parameter Descriptions for Deleting Routes

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
id	ID of a BMC management interface resource.	It can be obtained by querying the collection of BMC management interface resources.
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
ipv4_address_value	String	IPv4 address.
ipv4_netmast_value	String	IPv4 mask.
ipv6_address_value	String	IPv6 address.

Parameter	Setting	Value
ipv6_prefixLen_value	Number	IPv6 prefix length.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/EthernetInterfaces/D64FE89CE17C/Actions/EthernetInterface.DeleteRoutes
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type: application/json
```

- Request Message Body:

```
{
  "IPv4Route": {
    "Address": "192.168.1.5",
    "Netmask": "255.255.255.192"
  },
  "IPv6Route": {
    "Address": "ff00::",
    "PrefixLength": 8
  }
}
```

- Response Example: None
- Response code: 204

Output Description

None

4.40 Querying Information About the SecurityService Resource

Function

Query information about the SecurityService resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/SecurityService`
- Request Header:

X-Auth-Token:auth_value
- Request Message Body: None

Description

For a description of the parameters for querying information about the SecurityService resource, refer to [Table 4-67](#).

Table 4-67 Parameter Descriptions for Querying Information About the SecurityService Resource

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Managers/1/SecurityService

- Request Header:

X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#SecurityService.SecurityService",
  "@odata.id": "/redfish/v1/Managers/1/SecurityService",
  "@odata.type": "#FirewallService.v1_0_0.SecurityService",
  "Id": "SecurityService",
```

```

    "Name": "Security Service",
    "FirewallRules": {
        "@odata.id": "/redfish/v1/Managers/1/SecurityService/FirewallRules"
    },
    "HttpsCert": {
        "@odata.id": "/redfish/v1/Managers/1/SecurityService/HttpsCert"
    }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the SecurityService resource, refer to [Table 4-68](#).

Table 4-68 Output Descriptions for Querying Information About the SecurityService Resource

Field	Type	Description
@odata.context	String	OData description of the SecurityService resource model.
@odata.id	String	Access path of the SecurityService resource.
@odata.type	String	Type of SecurityService resource.
Id	String	Unique identifier.
Name	String	Resource name.
FirewallRules	String	Lower-level firewall rule URI.
HttpsCert	String	URI for SSL certificate information query.

4.41 Querying Information About SecurityService Rules

Function

Query information about SecurityService rules of a server.

Permission Required

Query.

Syntax

- Operation type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/SecurityService/FirewallRules`
- Request Header:

X-Auth-Token:auth_value

- Request Message Body: None

Description

For a description of the parameters for querying information about SecurityService rules, refer to [Table 4-69](#).

Table 4-69 Parameter Descriptions for Querying Information About SecurityService Rules

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Managers/1/SecurityService/FirewallRules

- Request Header:

X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#FirewallRule.FirewallRule",
  "@odata.id": "/redfish/v1/Managers/1/SecurityService/FirewallRules",
  "@odata.type": "#FirewallRule.v1_0_0.FirewallRule",
  "Id": "FirewallRules",
  "Name": "Firewall Rules",
  "Actions": {
    "#FirewallRule.AddRules": {
      "target":
        "/redfish/v1/Managers/1/SecurityService/FirewallRules/Actions/
        FirewallRule.AddRules"
    },
    "#FirewallRule.DeleteRules": {
```

```

        "target": "
          /redfish/v1/Managers/1/SecurityService/FirewallRules/Actions/
          FirewallRule.DeleteRules"
      }
    },
    "ActiveStrategy": "Drop",
    "Rules": [
      {
        "RuleType": "Drop",
        "@odata.id":
          "/redfish/v1/Managers/1/SecurityService/FirewallRules#/Rules/BlackList_1",
        "StartDateTime": null,
        "EndDateTime": null,
        "StartIPAddress": "192.168.1.1",
        "EndIPAddress": null,
        "StartMacAddress": null,
        "EndMacAddress": null,
        "WorkdayOnly": false
      }
    ]
  }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about SecurityService rules, refer to [Table 4-70](#).

Table 4-70 Output Descriptions for Querying Information About SecurityService Rules

Field	Type	Description
@odata.context	String	OData description of the firewall rule resource model.
@odata.id	String	Access path of the firewall rule resource.
@odata.type	String	Type of firewall rule resource.
Id	String	Unique identifier.
Name	String	Resource name.
ActiveStrategy	String	Currently valid rule policy: ● Accept: enables rules for accepting data, that is, the allowlist takes effect. ● Drop: enables rules for dropping data, that is, the blocklist takes effect.
Rules	Array	Rule list.

Field	Type	Description
Actions	Object	Operations that can be performed on the resource.
#FirewallRule.AddRules.target	String	Operation path for adding a firewall rule.
#FirewallRule.DeleteRules.target	String	Operation path for deleting a firewall rule.
@odata.id	String	Uniquely identifies the rule in IPRules.
RuleType	String	Type of rule.
StartDateTime	String	Time when the rule takes effect.
EndDateTime	String	Time when the rule becomes invalid.
StartIPAddress	String	Start IP address corresponding to the rule.
EndIPAddress	String	End IP address corresponding to the rule.
StartMacAddress	String	Start MAC address corresponding to the rule.
EndMacAddress	String	End MAC address corresponding to the rule.
WorkdayOnly	Boolean	Whether the rule is effective on workdays only. ● true: takes effect on workdays only. ● false: takes effect every day within the specified time range.

4.42 Adding a Firewall Rule

Function

Add a firewall rule.

Permission Required

Security management.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/SecurityService/FirewallRules/Actions/FirewallRule.AddRules`
- Request Header:

```
X-Auth-Token:auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
```

```

"Rules": [
  {
    "RuleType": rule_type_value,
    "StartDateTime": start_data_time_value,
    "EndDateTime": end_data_time_value,
    "StartIPAddress": start_ip_address_value,
    "EndIPAddress": end_ip_address_value,
    "StartMacAddress": start_mac_address_value,
    "EndMacAddress": end_mac_address_value,
    "WorkdayOnly": workday_only_value
  }
]
}

```

Description

For a description of the parameters for adding a firewall rule, refer to [Table 4-71](#).

Table 4-71 Parameter Descriptions for Adding a Firewall Rule

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
rule_type_value	Type of rule.	- Accept - Drop
start_data_time_value	Time when the rule takes effect.	Optional. Format example: 2029-01-11 00:00 If this parameter is configured, EndDateTime also needs to be configured.
end_data_time_value	Time when the rule becomes invalid.	Optional. Format example: 2029-01-11 00:00 If this parameter is configured, StartDateTime also needs to be configured.
start_ip_address_value	Start IP address corresponding to the rule.	One of StartMacAddress and StartIPAddress must be configured.
end_ip_address_value	End IP address corresponding to the rule.	Optional.

Parameter	Setting	Value
start_mac_address_value	Start MAC address corresponding to the rule.	One of StartMacAddress and StartIPAddress must be configured.
end_mac_address_value	End MAC address corresponding to the rule.	Optional. A MAC address segment can contain a maximum of 64 MAC addresses.
workday_only_value	Whether the rule is effective on workdays only.	Optional. ● true: takes effective on workdays only. If this option is selected, the date and time must be configured. ● false: takes effective every day.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/SecurityService/FirewallRules/Actions/FirewallRule.AddRules
```

- Request Header:

```
X-Auth-Token: LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type: application/json
```

- Request Message Body:

```
{
  "Rules": [
    {
      "RuleType": "Drop",
      "StartDateTime": "2024-02-20 00:00",
      "EndDateTime": "2024-02-22 00:00",
      "StartIPAddress": "128.6.0.100",
      "EndIPAddress": "128.6.1.100",
      "StartMacAddress": "11:22:33:44:55:66",
      "EndMacAddress": "11:22:33:44:55:76",
      "WorkdayOnly": false
    }
  ]
}
```

- Response Example: None
- Response code: 204

Output Description

None

4.43 Deleting a Firewall Rule

Function

Delete a firewall rule.

Permission Required

Security management.

Syntax

- Operation Type: POST
- **URL:** *https://device_ip/redfish/v1/Managers/manager_id/SecurityService/FirewallRules/Actions/FirewallRule.DeleteRules*
- Request Header:

```
X-Auth-Token:auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "IPRules": [
    {
      "@odata.id":
        "/redfish/v1/Managers/1/SecurityService/FirewallRules#/Rules/BlackList_1"
    }
  ]
}
```

DescriptionFor a description of the parameters for deleting a firewall rule, refer to [Table 4-72](#).**Table 4-72 Parameter Descriptions for Deleting a Firewall Rule**

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Parameter	Setting	Value
header_type	Format of the request message.	application/json
IPRules	Rule array.	There is at least one element in the array.
@odata.id	Odata.id of the rule to be deleted.	Obtained through "GET https://device_ip/redfish/v1/Managers/1/SecurityService/FirewallRules."

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/SecurityService/FirewallRules/Actions/Firewall-
Rule.DeleteRules
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type: application/json
```

- Request Message Body:

```
{
  "IPRules": [
    {
      "@odata.id":
        "/redfish/v1/Managers/1/SecurityService/FirewallRules#/Rules/BlackList_1"
    }
  ]
}
```

- Response Example: None
- Response code: 204

Output Description

None

4.44 Attaching Remote Media to the Virtual Media Device

Function

Attach remote media to the virtual media device.

Permission Required

VMM.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/Managers/manager_id/VirtualMedia/media_type/Actions/VirtualMedia.InsertMedia*
- Request Header:

```
X-Auth-Token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "Image": ImageURI,
  "Username": username_value,
  "Password": password_value,
  "TransferProtocolType": TransferProtocolType
}
```

Description

For a description of the parameters for attaching remote media to the virtual media device, refer to [Table 4-73](#).

Table 4-73 Parameter Descriptions for Attaching Remote Media to the Virtual Media Device

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
ImageURI	Image address.	Remote image address. The remote server needs to support the corresponding service.
TransferProtocolType	Transfer protocol type.	• CIFS • HTTPS • NFS • HTTP

Parameter	Setting	Value
username_value	Username. Whether this parameter is set or not depends on the service configuration.	String type. A maximum of 32 characters are supported.
password_value	Password Whether this parameter is set or not depends on the service configuration.	String type. A maximum of 32 characters are supported.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/VirtualMedia/CD/Actions/VirtualMedia.InsertMedia
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=  
Content-Type:application/json
```

- Request Message Body:

```
{  
  "Image": "cifs://device_ip/home/mount_test/isocfg-tool-v1.iso",  
  "Username": "test",  
  "Password": "123",  
  "TransferProtocolType": "CIFS"  
}
```

- Response Example:

```
{  
}
```

- Status Code: 200

Output Description

None

4.45 Detaching Remote Media from the Virtual Media Device

Function

Detach remote media from the virtual media device.

Permission Required

VMM.

Syntax

- Operation Type: POST
- **URL:** `https://device_ip/redfish/v1/Managers/manager_id/VirtualMedia/media_type/Actions/VirtualMedia.EjectMedia`
- Request Header:

```
X-Auth-Token:auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
}
```

Description

For a description of the parameters for detaching remote media from the virtual media device, refer to [Table 4-74](#).

Table 4-74 Parameter Descriptions for Detaching Remote Media from the Virtual Media Device

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
media_type	Virtual media type.	The following types are supported: • CD • CD1 • USBStick • USBStick1

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/VirtualMedia/CD/Actions/VirtualMedia.EjectMedia
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=  
Content-Type: application/json
```

- Request Message Body:

```
{  
}
```

- Response Example:

```
{  
}
```

- Status Code: 200

Output Description

None

4.46 Setting the BMC Time

Function

Set the **BMC** time.

Permission Required

Basic management.

Syntax

- Operation Type: POST
- **URL**: *https://device_ip/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.SetBMCTimes*
- Request Header:

```
X-Auth-Token:auth_value  
Content-Type:header_type
```

- Request Message Body:

```
{  
  "Times":times_value  
}
```

Description

For a description of the parameters for setting the BMC time, refer to [Table 4-75](#).

Table 4-75 Parameter Descriptions for Setting the BMC Time

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
times_value	Date and time.	Format: yyyy-mm-dd HH:mm:ss. For example, 2024-05-09 19:56:10.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.SetBMCTimes
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
  "Times": "2024-05-09 19:56:10"
}
```

- Response Example:

```
{
  "error": {
    "code": "Base.1.8.1.Success",
    "message": "Successfully Completed Request",
    "@Message.ExtendedInfo": [
      {
        "@odata.type": "#Message.v1_1_1.Message",
        "MessageId": "Base.1.8.1.Success",
        "Message": "Successfully Completed Request",

```



```

        "Severity": "OK",
        "Resolution": "None."
    }
]
}
}

```

- Status Code: 200

Output Description

For a description of the output returned when you set the BMC time, refer to [Table 4-76](#).

Table 4-76 Output Descriptions for Setting the BMC Time

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Readable message for the code in the message registry.
@Message.ExtendedInfo	Array	Extended information about the message.
@odata.type	String	OData description of the message resource.
MessageId	String	Message ID.
Message	String	Details.
Severity	String	Severity level. Options: • OK • Warning • Critical
Resolution	String	Recommended solution.

4.47 Importing the Syslog Root Certificate

Function

Import the Syslog root certificate into the system.

Permission Required

Basic management.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/SyslogService/Actions/SyslogService.ImportRootCertificate`

- Request Header:

```
X-Auth-Token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "Type":type,
  "Content":value
}
```

Description

For a description of the parameters for importing the Syslog root certificate, refer to [Table 4-77](#).

Table 4-77 Parameter Descriptions for Importing the Syslog Root Certificate

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
type	Method of importing a Syslog certificate.	text: indicates that the value is the content of the certificate. URI: indicates that the value is the local or remote URI.
value	Content or path of the certificate	For remote protocols, only HTTPS is supported. The value varies with the type.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/SyslogService/Actions/SyslogService.ImportRootCertificate
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

Local address:

```
{
  "Type": "URI",
  "Content": "/data/rootCA.pem"
}
```

Remote address:

```
{
  "Type": "URI",
  "Content": "https://10.226.197.41:28000/rootCA.pem"
}
```

Text:

```
{
  "Type": "text",
  "Content": "-----BEGIN CERTIFICATE-----
MIIDNzCCA8CFBibt0Cg4JvSVTy1432ZNxDu9qSGMA0GCSqGSib3DQEBcwUAMFgx
CzAJBgNVBAYTAkNOMRIWEAYDVQQIDA1HdwFuZ2RvbmcxCzAJBgNVBACMA1NamQww
CgYDVQQKDANAVEUXDDAKBgNVBASMA0JNQZEMMAoGA1UEAwDDVVNBMB4XDTI0MDUy
MTA4NDcyN1oxDTI0MDYyMDA4NDcyN1owWDELMAkGA1UEBhMCQ04xejAQBgnVBAGM
Cud1YW5nZG9uZzELMAkGA1UEBwwCU1oxDDAKBgNVBAoMA1pURTEMMAoGA1UECwwD
Qk1DMQwwCgYDVQQDDANVU0EwggeiMA0GCSqGSib3DQEBAQUAA4IBDwAwggEKAoIB
AQc0mcoiDI1bTmmnhhRDJoQAZNS3au022SKwcv0CUQIN03b4YdyJS+x/fFskS6r+
2o1kmob8knt9+/CuneE7jvgaoM1Rp51hTY/mec3x2caPpZVDura1kmVLSBkpCCxf
R6LtJQz/ggnoc3On3Mg6RxyqQh9u1/52G0z50/RSx11cyVoNvffgP9aszawX8Qp
nF4SNojQFIJwwxi5Gv/b71luy8K/ZM4rfoE10LS6dR5V9u3/7x1evm//6Z30XgF
Jb7ZnVAcv5zfVLppiZAJaSbhRvKstu3NuOcEmWCX1ABoXCjzH73WZnGmRhi0b8mQ
5ZYvcECLQz/dx01x501a8CXzAgMBAAEwDQYJKoZIhvcNAQELBQADggEBABoYceg9
FpG0LnZTa9T6mAKmpIbk4FvyojoFie+Rji8rxqfqPjFdg5QQygs4VsJEEDLno8e
bL7FWLkQ5CH01PKc1Mkafbvnj5Xgc78WZmsIOjv4UY9rMkLyhokwqhQ1ZwxMJv
2RTOMA13DT51qbTCGsQtK5QubVpnyN3Bj5y0kg5d7jTtK6iQeDwy0xLWypgsv6wJ
kxixsU6YgGJeRCR70kiAT3eA6LoosoGHeTgP70PAzrjPYLRwEXDnJ6ypd0+SATuX
Z1x7Ruf3DoV9irLLEnkveS8Lqe/QWEedWEZIOBjhvkcyjUOGDy6ppse3ty+dJK2Yp
A/tLBdvTgmrXgl4=
-----END CERTIFICATE-----"
}
```

- Response Example:

```
{
  "error": {
    "code": "Base.1.0.GeneralError",
```

```

    "message":
      "A general error has occurred. See ExtendedInfo for more information.",
      "@Message.ExtendedInfo": [
        {
          "@odata.type":
            "/redfish/v1/$metadata#MessageRegistry.1.0.0.MessageRegistry",
          "MessageId": "Base.1.8.1.Success",
          "RelatedProperties": [],
          "Message": "The certificate has been imported successfully.",
          "MessageArgs": [],
          "Severity": "OK",
          "Resolution": "None"
        }
      ]
    }
  }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you import a Syslog root certificate, refer to [Table 4-78](#).

Table 4-78 Output Descriptions for Importing the Syslog Root Certificate

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Readable message for the code in the message registry.
@Message.ExtendedInfo	Array	Extended information about the message.
@odata.type	String	OData description of the message resource.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Details.
MessageArgs	Array	Message arguments.
Severity	String	Severity level. Options: • OK • Warning • Critical
Resolution	String	Recommended solution.

4.48 Importing a Local Syslog Certificate

Function

Import a local Syslog certificate into the system.

Permission Required

Basic management.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/SyslogService/Actions/SyslogService.ImportClientCertificate`
- Request Header:

```
X-Auth-Token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "Type":type,
  "Content":value
}
```

Description

For a description of the parameters for importing a local Syslog certificate, refer to [Table 4-79](#).

Table 4-79 Parameter Descriptions for Importing a Local Syslog Certificate

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
type	Method of importing a Syslog certificate.	• text: indicates that the value is the content of the certificate. • URI: indicates that the value is the local or remote URI.
value	Content or path of the certificate	For remote protocols, only HTTPS is supported.

Parameter	Setting	Value
		The value varies with the type.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/SyslogService/Actions/SyslogService.ImportClientCertificate
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

Local address:

```
{
  "Type": "URI",
  "Content": "/data/client.pem"
}
```

Remote address:

```
{
  "Type": "URI",
  "Content": "https://10.226.197.41:28000/client.pem"
}
```

Text:

```
{
  "Type": "text",
  "Content": "-----BEGIN CERTIFICATE-----
MIIDODCCAIACFHB4CicZ84cto99USIMDZJ5GPMJYMA0GCSqGSIb3DQEBCwUAMFgx
CzAJBgNVBAYTAkNOMRIWEAYDVQQIDA1HdWZ2RvbmCxCzAJBgNVBACMA1NaMQww
CgYDVQQKDANaVEUXDDAKBgNVBASMA0JNQZEMMAoGA1UEAwDDVNBMB4XDTI0MDUy
MTA4NDcyN1oxDTI1MDUyMTA4NDcyN1owWTElMAkGA1UEBhMCQ04xEjAQBgNVBAGM
CUD1YW5nZG9uZzELMAkGA1UEBwwCU1oxDDAKBgNVBAoMA1pURTEMMAoGA1UECwwD
Qk1DMQ0wCwYDVQQDDARKYXAuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEApibFuUSt85810Fu0Qj5KcJt+972Dr1zbn30X4IPGLy7asdjx5z41N2Qdfy7f
tw29XxPVRq1I1mC4dTRYHB1Tc/C01WTZEtQyE5lynygDr4tGfsDypwsjgUn2t+0T
5cFsd7RxEkLkxjPXvh0q8gr+7NoAJ52PRrSS/Q1S55BpnPxS4VbtoEYRUQXfCP07
-----"
```

```

WktTx66u/Lf3pihw5UpXl8i9mqwXNj7oMwywp1TdnL41TMK8FaJ97LJF9in+EMzh
HZUj8C1iQCrh9xUjgj9RN22YKRIfiCzb0J2VyHkCiWGbHUI0i11PxRJq92r71hn
O5glTIg6GHALPf0/wkZ4lvp72wIDAQABMA0GCSqGSib3DQEBCwUAA4IBAQCQi0jX
vJzpteI8Tp14zSkZ2+ajOfhustQuZaLF8BSOAJ2+bjaNswgqy63X6BqYS1vIbone
Ays6SCjvjbPvNtPKddgM4asj+uLW+GCWYDOL7Cti8muI7fSjyTJo/SR9pgbmUpNn
Rbd0XkbayErbclTtVpsIhhBa/JFz96nPUJ8bBBPBET/hFdv2iI1KhVPgwyj4NjKJ
hb9iIAA5SMTsiJ2VE/PUSHyoiL0V78/uwL8NLPpItoAcY0HwTJbo16hQQELn56V
Z4rt6z1l8nCqtkYsV9FzArICcpZ7UxsDZd229H6ZYeoVsBKj14V5TrP3S4xfZc/
Oe7oFwMuYx+jVgq+
-----END CERTIFICATE----- "
}

```

- Response Example:

```

{
  "error": {
    "code": "Base.1.0.GeneralError",
    "message":
      "A general error has occurred. See ExtendedInfo for more information.",
    "@Message.ExtendedInfo": [
      {
        "@odata.type":
          "/redfish/v1/$metadata#MessageRegistry.1.0.0.MessageRegistry",
        "MessageId": "Base.1.8.1.Success",
        "RelatedProperties": [],
        "Message": "The certificate has been imported successfully.",
        "MessageArgs": [],
        "Severity": "OK",
        "Resolution": "None"
      }
    ]
  }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you import a local Syslog certificate, refer to [Table 4-80](#).

Table 4-80 Output Descriptions for Importing a Local Syslog Certificate

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Readable message for the code in the message registry.

Field	Type	Description
@Message.ExtendedInfo	Array	Extended information about the message.
@odata.type	String	OData description of the message resource.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Details.
MessageArgs	Array	Message arguments.
Severity	String	Severity level. Options: ● Warning ● Critical
Resolution	String	Recommended solution.

4.49 Importing a Private Key Certificate

Function

Import the private key certificate into the system.

Permission Required

Basic management.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/SyslogService/Actions/SyslogService.ImportPrivateKeyCertificate`
- Request Header:

```
X-Auth-Token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "Type":type,
  "Content":value
}
```

Description

For a description of the parameters for importing a private key certificate, refer to [Table 4-81](#).

Table 4-81 Parameter Descriptions for Importing a Private Key Certificate

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
type	Method of importing a Syslog certificate.	- text: indicates that the value is the content of the certificate. - URI: indicates that the value is the local or remote URI.
value	Content or path of the certificate	For remote protocols, only HTTPS is supported. The value varies with the type.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/SyslogService/Actions/SyslogService.ImportPrivateKeyCertificate
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

Local address:

```
{
  "Type": "URI",
  "Content": "/data/cient.key"
}
```

Remote address:

```
{
  "Type": "URI",
  "Content": "https://10.226.197.41:28000/cient.key"
}
```

```
}

```

Text:

```
{
  "Type": "text",
  "Content": "-----BEGIN RSA PRIVATE KEY-----
MIEowIBAACKAQEApbFuUst85810Fu0Qj5KcJt+972Dr1zbN30X4IPGLy7asdJx
5z41N2Qdfy7ftw29XxPVRq1I1mC4dTRYHB1Tc/C01WTZEtQyE51ynygDr4tGfSDy
pwsJgUn2t+0T5cFSd7RxEkLKxjPXVhOq8gr+7NoAJ52PRrSS/Q1S55BpnPxS4Vbt
oEYRUQXfCP07WktTx66u/Lf3pihw5UpXl8i9mqwXNj7oMwywp1TdnL41TMK8FaJ9
7LJF9in+EMzhHZUj8C1iQCrh9xUjgg9RN22YKRIfiCzb0J2VyHkCiWHgbhUI0i11
PxRJq92r71hn05glTIG6GHALPf0/wkZ41vp72wIDAQABAOIBAHqZ0xnCL/jd2Nsm
PgyFj9e1HZi63doQPnu3h8CHZ/3cLiKuu2A4MnibeKUJ6rB2dxkvvnUZVvemqdH0
O/VURqriYckNvr1u9yQ+N8WNeVtUEVVeDFSMB0ZdzTPhQsZzhaFewfnoVXMvqbq
f56LvEMRoveehcaDZ+F0y3qyzSvegem3CkFIIN9EL6CVH8gddfx4xnBMTCLSVGNR
hg4/akhuMd1FSzpu//ZM11f6Pwr8I6mmN/mqI8jTyETi2LdbMFPPFZMCzQVfTDY2
4Xkcs3DhgDm5gzC+UMmXwIndFVT7zoYTUh1uEkSwu41nqIy21hpD193z1LFJgk2C
zceJ4UECgYEA24Eo+6Nwiqg2z24m9aCC/psDgtLF3oBVjwcwwfapT1SbY1GCib7D
d2egPWQ1zNsbdFU0Pkb1514Iwi9eI+5jUw8GNS1ga0yPrF+n6BNyC1BXzrpV0L9v
8+csxQ1KGPPeAQgXZ4YQZXD8+GZ92MUBnVgDKsqyQE7q5gUGmHsSC3ECgYEAwca6
DZNprvJ/Bsc183i+txM47aL3CT0whjo4PZUACJWrWSU1Hnp6SGF1iMOqAoqBd7p0
RSDPS853MVG7mOBW8Guv/zfb0swY5VP6kaBreTC1011RyAr134jgSAtoa0Un3xkp
rKAJjYgodDgGLy/vjyeiICftgXJS2dnsqfI3gsCgYAVubi0BpfMTFcEgIqFiQpP
GLu5CBb/0EqherW9Op9k83hLyaaka0VYCE7S7Tdr4hAZFAufJ8mHz92zfuKcFfeN
IEAGVdujTG3sivJ3ZTnAX3GObzzws1Q/ECbmK+bVW55DxjBgUNZYB/OA2RdoE5A1
iz0jle63Tkv1KkAxvTY1AQKBgQCYS38YhatJt0UM1VD93ZAE+zvoYHzmJfcgP67k
MI/XNALUfCYVL5U/hqkZrn9CA13100S5ORLCfVCGaA86eMdqLKKDr8QmCLOxtg0G
R10M8KpQvshcq057GgUMG/n/1n6GFtHo/DCq/KXPRfrxoofYuvXS9iSyVqId1NMz
zj7HYwKBGf67Rmm/FOBdn5M1Umos6IPvrgZkOTokoTIq8hoiAuDBHZYW/s1vdV2/
ezkFAUzrfodPNJxjgI/UuYhka1ZoiPcR3GwkjbcRzq5zSFDbQucznGobm2I1HkIQ
gsBXo2A/NXDDozaItMQTms1pKtx3T2084M/vf8ad43+oJcxCWVzM
-----END RSA PRIVATE KEY-----"
}
```

- Response Example:

```
{
  "error": {
    "code": "Base.1.0.GeneralError",
    "message":
      "A general error has occurred. See ExtendedInfo for more information.",
    "@Message.ExtendedInfo": [
      {
        "@odata.type":
          "/redfish/v1/$metadata#MessageRegistry.1.0.0.MessageRegistry",

```

```

        "MessageId": "Base.1.8.1.Success",
        "RelatedProperties": [],
        "Message": "The certificate has been imported successfully.",
        "MessageArgs": [],
        "Severity": "OK",
        "Resolution": "None"
    }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you import the private key certificate, refer to [Table 4-82](#).

Table 4-82 Output Descriptions for Importing a Private Key Certificate

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Readable message for the code in the message registry.
@Message.ExtendedInfo	Array	Extended information about the message.
@odata.type	String	OData description of the message resource.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Details.
MessageArgs	Array	Message arguments.
Severity	String	Severity level. Options: • OK • Warning • Critical
Resolution	String	Recommended solution.

4.50 Querying SSL Certificate Information

Function

Query [SSL](#) certificate information.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Managers/manager_id/SecurityService/HttpsCert`
- Request Header:

```
X-Auth-Token:auth_value
```

- Request Message Body: None

Description

For a description of the parameters for querying SSL certificate information, refer to [Table 4-83](#).

Table 4-83 Parameter Descriptions for Querying SSL Certificate Information

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/SyslogService/Actions/SecurityService/HttpsCert
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#SecurityService.HttpsCert",
  "@odata.id": "/redfish/v1/Managers/1/SecurityService/HttpsCert",
  "@odata.type": "#HttpsCert.v1_0_0.HttpsCert",
}
```

```

"Actions": {
  "#HttpsCert.ImportServerCertificate": { "target":
    "/redfish/v1/Managers/1/SecurityService/HttpsCert/Actions/
    HttpsCert.ImportServerCertificate"
  }
},
"Id": "HttpsCert",
"Name": "Https cert
info", "Oem": {
  "Public": {
    "CompletionCode"
    : 0,
    "Description":
    "Success"
  }
},
"Version": "3",
"X509CertificateInformation": {
  "ServerCert": {
    "CertificateString":
    null,
    "CertificateType":
    null, "Issuer": {
      "City": "Hangzhou",
      "CommonName": "H3C",
      "Country": "CN",
      "Organization": "New H3C Technologies Co.,Ltd",
      "OrganizationalUnit": "Compute and Storage Product
      Line", "State": "Zhejiang"
    },
    "IssuerAddress": "service@h3c.com",
    "KeyUsage": "Digital Signature, Non Repudiation, Key Encipherment",
    "PublicKey": "",
    "PublicKeyLengthBits": "2048",
    "SerialNumber": "4FF5D2D1B5A683DE8616801FAE92BA0D888DA5F9",
    "SignatureAlgorithm":
    "sha256WithRSAEncryption", "Subject": {
      "City": "Hangzhou",
      "CommonName": "H3C",
      "Country": "CN",
      "Organization": "New H3C Technologies Co.,Ltd",
      "OrganizationalUnit": "Compute and Storage Product
      Line", "State": "Zhejiang"
    },
    "SubjectAddress": "service@h3c.com",
    "ValidNotAfter": "2036-04-26T09:49:41+08:00",

```

```

        "validNotBefore": "2021-04-30T09:49:41+08:00"
    }
}
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query SSL certificate information, refer to [Table 4-84](#).

Table 4-84 Output Descriptions for Querying SSL Certificate Information

Field	Type	Description
@odata.context	String	OData description of the SecurityService.HttpsCert resource model.
@odata.id	String	Access path of the SecurityService.HttpsCert resource.
@odata.type	String	Type of SecurityService.HttpsCert resource.
Actions.#HttpsCert.ImportServerCertificate.target	String	Operation path for SSL certificate import.
Id	String	Resource ID.
Name	String	Resource name.
Oem.Public.CompletionCode	Number	Success percentage.
Oem.Public.Description	String	Description.
Version	String	Version.
X509CertificateInformation.ServerCert.CertificateString	String	Certificate string.
X509CertificateInformation.ServerCert.CertificateType	String	Certificate format.
X509CertificateInformation.ServerCert.IssuerAddress	String	Issuer's email address.
X509CertificateInformation.ServerCert.KeyUsage	String	Key usage.
X509CertificateInformation.ServerCert.PublicKey	String	Public key.

Field	Type	Description
X509CertificateInformation.ServerCert.PublicKeyLengthBits	String	Public key length.
X509CertificateInformation.ServerCert.SerialNumber	String	Serial number.
X509CertificateInformation.ServerCert.SignatureAlgorithm	String	Signature algorithm.
X509CertificateInformation.ServerCert.SubjectAddress	String	Recipient's email address.
X509CertificateInformation.ServerCert.ValidNotAfter	String	End time of the validity period of the certificate.
X509CertificateInformation.ServerCert.ValidNotBefore	String	Start time of the validity period of the certificate.
X509CertificateInformation.ServerCert.Issuer	String	Same as Subject .
X509CertificateInformation.ServerCert.Subject	String	Same as Issuer .
X509CertificateInformation.ServerCert.Issuer.City	String	City or area.
X509CertificateInformation.ServerCert.Issuer.CommonName	String	Common name.
X509CertificateInformation.ServerCert.Issuer.Country	String	Country.
X509CertificateInformation.ServerCert.Issuer.Organization	String	Organization.
X509CertificateInformation.ServerCert.Issuer.OrganizationalUnit	String	Organizational unit.
X509CertificateInformation.ServerCert.Issuer.State	String	Province (state).

4.51 Importing an SSL Certificate

Function

Import an [SSL](#) certificate into the system.

Permission Required

Security management.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/SecurityService/HttpsCert/Actions/HttpsCert.ImportServerCertificate`
- Request Header:

```
X-Auth-Token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "Certificate": Certificate,
  "Privatekey": Privatekey
}
```

Description

For a description of the parameters for importing an SSL certificate, refer to [Table 4-85](#).

Table 4-85 Parameter Descriptions for Importing an SSL Certificate

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
Certificate	SSL certificate.	Can be a temporary BMC directory of the certificate file, a remote HTTPS file, or the content of the certificate file.
Privatekey	SSL private key.	Can be a temporary BMC directory of the private key file, a remote HTTPS file, or the content of the private key file.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/SecurityService/HttpsCert/Actions/HttpsCert.ImportServerCertificate
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

Local import: Upload the files to the `/tmp/sslcert/` directory, and then invoke the Redfish interface.

```
{
  "certificate": "/tmp/sslcert/server.pem",
  "privatekey": "/tmp/sslcert/privkey.pem"
}
```

Remote import: In this version, only the HTTPS protocol is supported.

```
{
  "certificate": "https://192.168.170.57/server.pem",
  "privatekey": "https://192.168.170.57/privkey.pem"
}
```

Upload the text directly:

```
{
  "certificate": "-----BEGIN CERTIFICATE-----
MIIDODCCAIAcFHB4CICZ84cto99USIMDZJ5GPMJama0GCSqGSib3DQEBcwUAMFgx
CzAJBgNVBAYTAkNOMRIWEAYDVQQIDA1HdwFuZ2RvbmcxCzAJBgNVBACMA1NaMQww
CgYDVQQKDANaVEUXDDAKBgNVBASMA0JNQZEMMAoGA1UEAwDVVNBMb4XDTI0MDUy
NzAyNTQzN1oxDTI1MDUyNzAyNTQzN1owWTElMAkGA1UEBhMCQ04xEjAQBGNVBAGM
Cud1YW5nZG9uZzZELMAkGA1UEBwwCU1oxDDAKBgNVBAoMA1pURTElMAkGA1UECwwD
Qk1DMQ0wCwYDVQQDDARKYXAuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA20Ik2Y4nY1fNgvTqi1HYfDwcr3+71Mi1pfQUOKRQgy1s+T1tmikd2cIhnFQT
1ozOP53oECznbn8XzTszxuWupEXOu60j6FTN1T7QCiUq/b3w2BZ9wM1K6wq70k72
ZX+0VXDMT4FPoQZrb9dI1MrzHOCWgE0LZgqHuxOur51L+xKrpvQmH8fx+1BGFrhG
pB9Z2jcnzkUTLC126Fu/L3jLOfQ7vv7kruZi8omOLqLzk0xYneOSHj+3+AWY02u4
LWI4k/XWwVAnFssHKBu3EvqTHT2Q0x5PxBCEkFg/o8DSMgrEehADbSP00xupHUo
45gHG+j291ELtNMGzTTVP6WswIDAQABMA0GCSqGSib3DQEBcwUAA4IBAQTZ7IR
```

```

maUAYLS3f69+tFREYtr4yyoCmu46QMAN5eFO079jLXwvQnQU7fNZmxwo0yo65m2x
Hs6EgegfhREff5ecjPoTV5Gfgfkyw76aYsvxfoYx2dp4Tr1BQm7LTdC+pkqi kmqz
u5ri3kxz+7k5fsFsSo+FeeMwnMPHioBYDb4F8MsPpwTNfPAev1ZVAVjNZXLLoB+3
gzSRGT2/98BY1Rd8PhMKVaHofXeM/Xkkd/6iNfjsPbZQgaU4IrQAvXfp1vQ697Q+
AVwj/prIVOI7p8XGyoJI1v5mTq8w3JkdK3zs+T4uxdSr1acu/g0ECBPL/bmQ4KuW
P6pshnQq2/OTmbuN
-----END CERTIFICATE-----",
"Privatekey": "-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA20Ik2Y4nY1fNgvTqi1hYfDwcr3+71MilpfQUOKRQgy1s+T1t
MiKd2cIhnFQT1ozOP53oECznbn8XzTsZxuWUPExOu60j6FTN1T7QCiuq/b3w2BZ9
wM1K6wq7Ok72ZX+0VXDMT4FPoQZrb9dI1MrzHOCWgE0LZgqHuxOur51L+xKrpVqM
h8fx+1BGFrhGpB9Z2jcnZKUTLC126Fu/L3jLofQ7vv7kruzi8om0LqLzk0xYneOS
Hj+3+AWY02u4LWI4k/XwWVANfSSHkBU3EVqTHT2Q0x5PxRBCEkFg/o8DSMgrEehA
DbSP00xUPHuo45gHG+j291ELtNMgzTTvVP6wswIDAQABAoIBAQDSfw/tpWH/J95v
at56iNTZgKoNon3rbK5LQqbFmjDxnvzN08EvrrgoxQ2LjdQ4Zvnjbw/Lh7CuFwfu
yo+M1f/8LeCpmBLWDASIQ4NrGf/KFyVZ003reav/p64T7pbzHSU8ecxMT/Lovsck
wn7be/Qmtx8GEFFth5KDCgP1Kwg2oxEov2a9pv0QSo04pbb6P4I9zOGfQwA31vp+
hC/fC78PnbgRtcUY/JOmRjM6xv8xZLC9p1HE34r5U808PIqo2MxUQX1uoEsSCHNM
ZruBhaqsY8HTnSH08fJ5e6Er6hnqT49cvaQkj/mYABz7beTPdcSrY1CqHwmhv4Af
JyFvy2XxAoGBAO5oiGwgjAqjvZow3CorNuuXZLS4Txy0ydcUu9fSma0DRPzUXrL/
y4KP8PpH8SnXNvHL1L1/e3NPMxdLMOUNZ9gZFX5Wxg6verZZpatdUCMRmoLaLatI
KoJi8XuYyAgFHY34pbIiyHZ8EbitafYjEhyu03Z01ucghGCUws80hjGfAoGBA0tv
36nAzBk9n+8dBFPiFH5h/jpLrTsxotA89ng/UM4D9ZzXvTwabcFP+/6YcGcAqp4V
vHskfI99M62jw1zABZ5DqeeZP3G4Xw53xt1f1ZCk9IsbREmaKP3uc3y3t6zn6tx0
5KS1JF6j84Ha4Bo6X3DVA0es1MLuSbXXjXPOzMptAoGBANvVYDLtMHKwBLhentxh
s91XHUK/NprMhia3uTOOpfGxsptmxSEbP+azVtm6bn10JjI3DI5aAvtIfETuw+e0
CLO+QS/JwosDLqjxt5s0/v1mWR2s1KHCUJJkykZ0kSAC9EiVwkGoQI9RA8yB1q/0
1dI3aaSzE/2JbvnIMus/6q0hAoGAQpmCEJ4cXkuDcZwoxJSYLYQ08XK051jLuYST
qEJo7k5KbXrN6Frud1A7/bJLoaebnCqT7c5ym/iT5Nuf1Trwm+uSJZTBUL8R1w1E
ek1its8i6jL1Z1i3ndwVT8N8runQE1rxzu10U11xpFuvjdVTYcywJ9dpPFdB/LGk
Lw1h+yUCgYEA0RNVBTLtu8dZwtaeUFuan93r5o/VHvw90JkTIVvTIMTvDsF6cedJ
kUJPzLVfCva8Mhm4nyU5GzrDyVh333Juo3JaBhfZadFFs8w+xqDzvHRY0IBmLAD
ebvNBeuxgkf6vj1Y1m519dvza3/FV///8DhEf0VLXqg6/hej1XWL2jI=
-----END RSA PRIVATE KEY-----"
}

```

- Response Example:

```

{
  "error": {
    "code": "Base.1.0.GeneralError",
    "message":
      "A general error has occurred. See ExtendedInfo for more information.",
    "@Message.ExtendedInfo": [
      {

```

```

    "@odata.type":
    "/redfish/v1/$metadata#MessageRegistry.1.0.0.MessageRegistry",
    "MessageId": "Base.1.8.1.Success",
    "RelatedProperties": [],
    "Message":
    "The certificate has been imported successfully, wait for service
    reboot.",
    "MessageArgs": [],
    "Severity": "OK",
    "Resolution": "None"
  }
]
}
}

```

- Status Code: 200

Output Description

For a description of the output returned when you import an SSL certificate, refer to [Table 4-86](#).

Table 4-86 Output Descriptions for Importing an SSL Certificate

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Readable message for to the code in the message registry.
@Message.ExtendedInfo	Array	Extended information about the message.
@odata.type	String	OData description of the message resource.
Message	String	Details.
MessageId	String	Message ID.
RelatedProperties	String	Message-related properties.
MessageArgs	Array	Message arguments.
Resolution	String	Recommended solution.
Severity	String	Severity level. Options: • OK • Warning • Critical

4.52 Exporting BIOS or BMC Configurations

Function

Export BIOS or BMC configurations.

Permission Required

User management.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/Actions/Manager.ExportConfiguration`

- Request Header:

```
X-Auth-Token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "Type":type_value
}
```

Description

For a description of the parameters for exporting BIOS and BMC configurations, refer to [Table 4-87](#).

Table 4-87 Parameter Descriptions for Exporting BIOS and BMC Configurations

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
type_value	String	Type of configuration that is exported. Options: • BIOS • BMC

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/Actions/Manager.ExportConfiguration
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=  
Content-Type:application/json
```

- Request Message Body:

```
{  
  "Type": "BMC"  
}
```

- Response Example:

```
{  
  "@odata.type": "#Manager.v1_13_0.Manager",  
  "Messages": [  
    {  
      "@odata.type": "#Message.v1_0_8.Message",  
      "Message": "A new task /redfish/v1/TaskService/Tasks/1 was created.",  
      "MessageArgs": [  
        "/redfish/v1/TaskService/Tasks/1"  
      ],  
      "MessageId": "Task.1.0.New",  
      "Resolution": "None",  
      "Severity": "OK"  
    },  
    {  
      "@odata.type": "#Message.v1_0_8.Message",  
      "Message":  
        "Device is preparing BMC/BIOS config export for action  
        Manager.ExportConfiguration.",  
      "MessageArgs": [  
        "Manager.ExportConfiguration"  
      ],  
      "MessageId": "Manager.1.0.ExportConfiguration",  
      "Resolution": "None",  
      "Severity": "OK"  
    }  
  ]  
}
```

```
    ]
  }
```

- Response code: 202

Output Description

For a description of the output returned when you export BIOS and BMC configurations, refer to [Table 4-88](#).

Table 4-88 Output Descriptions for Exporting BIOS and BMC Configurations

Field	Type	Description
@odata.type	String	OData description of the message resource.
Messages	Array	Message list.
Message	String	Details.
MessageId	String	Message ID.
MessageArgs	Array	Message arguments.
Resolution	String	Recommended solution.
Severity	String	Severity level. Options: • OK • Warning • Critical

4.53 Importing BIOS and BMC Configurations

Function

Import BIOS and BMC configurations.

Permission Required

User management.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/Actions/Manager.ImportConfiguration`
- Request Header:

X-Auth-Token:auth_value
Content-Type:header_type
- Request Message Body:

```
File: flie_value,
Type: type_value
```

Description

For a description of the parameters for importing BIOS and BMC configurations, refer to [Table 4-89](#).

Table 4-89 Parameter Descriptions for Importing BIOS and BMC Configurations

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
file_value	Configuration file that is uploaded.	- The BIOS configuration file is a JSON file. - The BMC configuration file is a TAR.GZ file.
type_value	Configuration type.	Configuration type. Options: - BIOS - BMC

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/Actions/Manager.ImportConfiguration
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

In the **VALUE** column for the **File** parameter, select the configuration file to be uploaded. In the **VALUE** column, enter the configuration type.

```
File: biosconfig.json,
Type: BIOS
```

- Response Example:

```
{
}
```

- Status Code: 200

Output Description

None

4.54 Downloading a Redfish File

Function

Download a Redfish file to the local PC.

Permission Required

User management.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/Managers/manager_id/Actions/Manager.GeneralDownload*

- Request Header:

```
X-Auth-Token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "TransferProtocol":transfer_protocol_value,
  "Path": path_value
}
```

Description

For a description of the parameters for downloading the Redfish file, refer to [Table 4-90](#).

Table 4-90 Parameter Descriptions for Downloading the Redfish File

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .

Parameter	Setting	Value
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
transfer_protocol_value	Protocol type.	Supported protocols: HTTPS .
path_value	Path from which files are to be downloaded.	Path from which a file is downloaded.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/Actions/Manager.GeneralDownload
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
  "TransferProtocol": "HTTPS",
  "Path": "/bmconfig_20240328111244.tar.gz"
}
```

- Response Example: File streams are returned.
- Status Code: 200

Output Description

None

4.55 Enabling the GPU Module to Start Collecting Logs

Function

Enable the GPU module to start collecting logs.

Permission Required

Diagnosis.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Managers/manager_id/Actions/Oem/Manager.LogDump`
- Request Header:

X-Auth-Token:auth_value
 Content-Type:header_type
- Request message body: defined based on the module.

Description

For a description of the parameters for the module to start collecting logs, refer to [Table 4-91](#).

Table 4-91 Parameter Descriptions for the Module to Start Collecting Logs

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json

Usage Guidelines

Only servers with GPUs support this function.

Example

- Request Example:

POST https://device_ip/redfish/v1/Managers/Ubb/Actions/Oem/Manager.LogDump

- Request Header:

X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
 Content-Type:application/json

- Request Message Body:

```
{
}
```

- Response Example: None
- Response code: 202

Output Description

None

4.56 Enabling the GPU Module to Obtain Log Files

Function

Obtain the TXT log files collected with one click.

Permission Required

Diagnosis.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/Actions/Oem/Manager.LogDump`
- Request Header:

X-Auth-Token:auth_value

- Request Message Body: None

Description

For a description of the parameters for the module to obtain log files, refer to [Table 4-92](#).

Table 4-92 Module Parameter Descriptions for the Module to Obtain Log Files

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

Only servers with GPUs support this function.

Example

- Request Example:

GET https://device_ip/redfish/v1/Managers/Ubb/Actions/Oem/Manager.LogDump

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example: Log files are returned.
- Response code:
 - 200 OK: The log is obtained successfully, and the contents of the log file are returned.
 - 204 No Content: Log collection is not completed.
 - 500 Internal Server Error: An error occurs during log collection.

Output Description

None

4.57 Querying Information About the DNS Service

Function

Query information about the DNS service.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Managers/manager_id/DnsService`
- Request Header:

```
X-Auth-Token:auth_value
```

- Request Message Body: None

Description

For a description of the parameters for querying information about the DNS service, refer to [Table 4-93](#).

Table 4-93 Parameter Descriptions for Querying Information About the DNS Service

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/DnsService
```

- Request Header:

```
X-Auth-Token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#DnsService.DnsService",
  "@odata.type": "#DnsService.v1_0_0.DnsService",
  "@odata.id": "/redfish/v1/Managers/1/DnsService",
  "HostNameConfig": {
    "HostName": "BMC123",
    "HostSetting": "manu"
  },
  "PatchInProgress": false,
  "DnsIpConfig": {
    "DnsEnable": true,
    "DnsDhcpEnable": "manu",
    "NameServers": [
      "192.168.1.1",
      "192.168.1.2",
      "2001:db8::1"
    ]
  },
  "DomainConfig": {
    "DomainName": "DomainName.com.cn"
  },
  "RegisterBMC": "hostname"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the DNS service, refer to [Table 4-94](#).

Table 4-94 Output Descriptions for Querying Information About the DNS Service

Field	Type	Description
@odata.context	String	OData description of the DNS resource collection.
@odata.id	String	Access path of the DNS service resource collection.
@odata.type	String	Type of DNS resource collection.
DnsIpConfig	Object	List of DNS IP Configurations.
DnsDhcpEnable	String	Whether the DNS service is enabled: ● manu: manual ● ipv4: automatically obtains an IPv4 DNS address. ● ipv6: Automatically obtains an IPv6 DNS address.
DnsEnable	Boolean	Whether the DNS client on the BMC is enabled: ● true: yes. ● false: no. If this parameter is disabled, the DnsDhcpEnable and NameServers parameters do not need to be set.
NameServers	Array	The first value indicates the primary server, the second value indicates standby server 1, and the third value indicates standby server 2.
DomainConfig	Object	Domain name configuration.
DomainName	String	Domain name.
HostNameConfig	Object	Hostname object.
HostName	String	Hostname.
HostSetting	String	Hostname setting mode. ● Auto: ● Manual
PatchInProgress	Boolean	Configuration validity flag: ● true: being configured ● false: configured completely
RegisterBMC	String	Registration mode: ● hostname: hostname ● fqdn: DHCP Client FQDN

4.58 Modifying Information About the DNS Service

Function

Modify information about the DNS service.

Permission Required

Basic management.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/Managers/manager_id/DnsService*
- Request Header:

```
X-Auth-Token: auth_value
Content-Type: header_type
```

- Request Message Body:
 - Configure the hostname information:

```
{
  "HostNameConfig": {
    "HostName": host_name_value,
    "HostSetting": host_setting_value
  }
}
```

- Configure the DNS IP information:

```
{
  "DnsIpConfig": {
    "DnsDhcpEnable": dns_dhcp_enable_value,
    "DnsEnable": dns_enable_value,
    "NameServers": name_servers_value
  }
}
```

- Configure the domain name information:

```
{
  "DomainConfig": {
    "DomainName": domain_name_value
  }
}
```

- Register the BMC:

```
{
  "RegisterBMC": register_bmc_value
}
```

Description

For a description of the parameters for modifying information about the DNS service, refer to [Table 4-95](#).

Table 4-95 Parameter Descriptions for Modifying Information About the DNS Service

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
dns_dhcp_enable_value	String	Whether the DNS service is enabled: - manu: manual - ipv4: automatically obtains an IPv4 DNS address. - ipv6: Automatically obtains an IPv6 DNS address.
dns_enable_value	Boolean	Whether the DNS client on the BMC is enabled: - true: enabled - false: no. If this parameter is disabled, the DnsDhcpEnable and NameServers parameters do not need to be set.
name_servers_value	Array	The first value indicates the primary server, the second value indicates standby server 1, and the third value indicates standby server 2.
domain_name_value	String	Domain name.
host_name_value	String	Hostname, range: 1–64 characters.
host_setting_value	String	Hostname setting mode. - auto - manual
register_bmc_value	String	Registration mode: - hostname: hostname - fqdn: DHCP Client FQDN

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Managers/1/DnsService
```

- Request Header:

```
X-Auth-Token: LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=  
Content-Type: application/json
```

- Request Message Body:

→ Configure the hostname information:

```
{  
  "HostNameConfig": {  
    "HostName": "iSACAA621D33E326",  
    "HostSetting": "manu"  
  }  
}
```

→ Configure the DNS IP information:

```
{  
  "DnsIpConfig": {  
    "DnsDhcpEnable": "manu",  
    "DnsEnable": true,  
    "NameServers": ["192.168.1.1", "192.168.1.2", "2001:db8::1"]  
  }  
}
```

→ Configure the domain name information:

```
{  
  "DomainConfig": {  
    "DomainName": "DomainName.com.cn"  
  }  
}
```

→ Register the BMC:

```
{  
  "RegisterBMC": "hostname"  
}
```

- Response Example: None

- Response code: 204

Output Description

None

Chapter 5

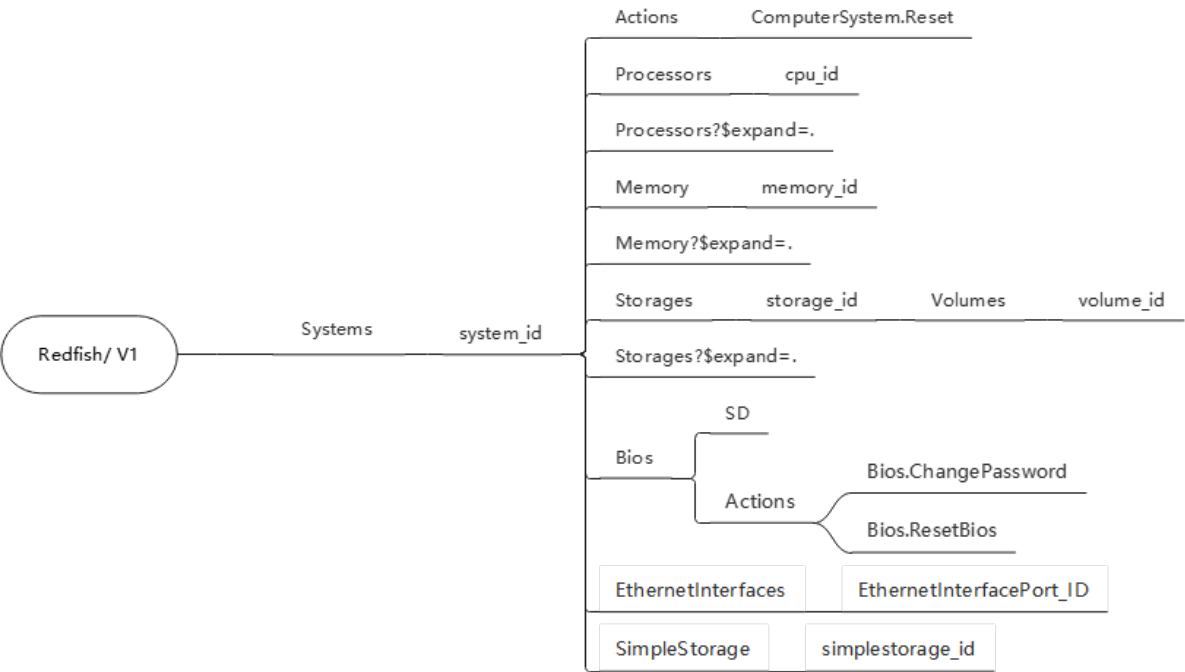
Operations on System Resources

Table of Contents

Querying Information About the System Resource Collection.....	228
Querying Information About a Specified System Resource.....	230
Remotely Powering On, Powering Off, and Resetting a System Resource.....	239
Modifying Properties of a Specified System Resource.....	241
Querying Information About the CPU Resource Collection.....	245
Querying Information About a Specified CPU Resource.....	247
Querying Information About All CPU Resources.....	251
Querying Information About the Memory Resource Collection.....	254
Querying Information About a Specified Memory Resource.....	256
Querying Information About All Memory Resources.....	260
Querying Information About the Storage Resource Collection.....	263
Querying Information About a Specified Storage Controller Resource.....	265
Querying Information About All Storage Controller Resources.....	271
Querying Information About the Logical Volume Resource Collection.....	276
Querying Information About a Specified Logical Volume Resource.....	278
Creating a Logical Volume.....	282
Deleting a Logical Volume.....	287
Querying Properties of the BIOS Resource.....	290
Querying Information About the BIOS Settings.....	292
Modifying the BIOS Settings.....	294
Setting the BIOS Password.....	296
Restoring the Default BIOS Settings.....	298
Querying Information About the Ethernet Interface Resource Collection.....	299
Querying Information About a Specified Ethernet Interface Resource.....	301
Querying Information About the SimpleStorage Resource Collection.....	305
Querying Information About a Specified SimpleStorage Resource.....	307

Figure 5-1 shows the path requirements for the Systems resources supported by VANTAGEO servers.

Figure 5-1 Systems Resource Path Requirements



For a description of the properties of System resources and the operations supported by the properties, refer to Table 5-1.

Table 5-1 Descriptions of System Resource Properties

URL	Property	Description	Operation
/redfish/v1/Systems	Name	Name of the System resource collection.	GET
	Members@odata.count	Number of System resource members.	GET
	Members	System resource list, which provides references for all System resource URLs.	GET
/redfish/v1/Systems/system_id	Actions	Operations that can be performed for the specified system resource through the Redfish interface.	GET
	#ComputerSystem.Reset	OS operation.	GET
	target	Access path of the restart operation attribute.	GET
	ResetType@Redfish.AllowableValues	OS operations allowed through the Redfish interface.	GET

URL	Property	Description	Operation
	AssetTag	Asset tag of the specified System resource.	GET
	BiosVersion	BIOS versions of the specified System resource.	GET
	Boot	Boot parameters of the specified System resource.	GET
	BootSourceOverrideEnabled	State of the boot source override feature of the system.	GET
	BootSourceOverrideMode	Boot mode to use when the system boots from the BootSourceOverride-Target` boot source.	GET
	BootSourceOverrideTarget	Current boot source used by the system at the next boot instead of the normal boot device, if `BootSourceOverrideEnabled` does not contain `Disabled`.	GET
	BootSourceOverrideEnabled@Redfish.AllowableValues	Allowable states of the boot source override feature of the system.	GET
	BootSourceOverrideMode@Redfish.AllowableValues	Allowable boot modes of the system.	GET
	BootSourceOverrideTarget@Redfish.AllowableValues	Allowable boot sources defined by Redfish.	GET
	Description	Description of the specified system resource.	GET
	EthernetInterfaces	Access path of the Ethernet interfaces of the host.	GET
	HostName	Name of the specified System resource.	GET
	Id	ID of a specified System resource.	GET
	IndicatorLED	Position indicator status of the specified drive.	GET
	Links	Resources link.	GET
	Chassis	Access path of the chassis resource node.	GET

URL	Property	Description	Operation
	CooledBy	Access path of the fan resource node.	GET
	ManagedBy	Access path of the Manager resource node.	GET
	PoweredBy	Access path of the power resource.	GET
	LogServices	Access path of the log service resource node.	GET
	Manufacturer	Manufacturer of the specified System resource.	GET
	Memory	Memory properties of the specified System resource.	GET
	MemoryDomains	V3 field.	GET
	Model	Model of the specified System resource.	GET
	Name	Name of the specified System resource.	GET
	NetworkInterfaces	Access path of the network interfaces.	GET
	Oem.Public	Customized properties of the System resource.	GET
	CPUUsagePercent	Dynamic CPU usage detected by CUPS.	GET
	IOUsagePercent	Dynamic I/O usage detected by CUPS.	GET
	MemoryUsagePercent	Dynamic memory usage detected by CUPS.	GET
	PowerOnDelayEnabled	Whether power-on delay is enabled.	GET
	PowerOnDelayMode	Power-on delay mode.	GET
	PowerOnDelaySeconds	Power-on delay.	GET
	PowerOnStrategy	Power-on policy.	GET
	ConfigurationModel	Year + typical configuration model. The configuration value must be in dictionary format.	GET
	ProductSpecificIdentity	Internally defined product name.	GET

URL	Property	Description	Operation
	BiosVersionDate	BIOS version date.	GET
	ProductVersion	Product version.	GET
	ProductName	Product name.	GET
	ProductExtra	Additional product information.	GET
	PartNumber	Part number of the specified system resource.	GET
	PowerState	Power-on status of the specified System resource.	GET
	Processors	CPU properties of the specified System resource.	GET
	SerialNumber	Serial number of the specified System resource.	GET
	Status	Status of the specified System resource.	GET
	Storage	Access path of the storage resource node.	GET
	Storages	Access path of the storage resource node.	GET
	UUID	UID of the specified System resource.	GET
	Bios	Access path of the BIOS function resource node.	GET
	DiskIndex	Disk partition number.	GET
	PartitionName	Disk partition name.	GET
	TotalCapacityGB	Total capacity of a disk partition.	GET
	UsagePercent	Usage of a disk partition in percentage.	GET
	CmccVersion	China Mobile version number.	GET
	code	ID of the specified message in the message registry.	PATCH
	message	Readable message for the code in the message registry.	PATCH
	MessageId	Message ID.	PATCH

URL	Property	Description	Operation
	Message	Details.	PATCH
	Severity	Severity level.	PATCH
	Resolution	Recommended solution.	PATCH
/redfish/v1/Sys-tems/system_id/Actions/ComputerSystem.Reset	code	ID of the specified message in the message registry.	POST
	message	Readable message for the code in the message registry.	POST
	MessageId	Message ID.	POST
	Message	Details.	POST
	Severity	Severity level.	POST
	Resolution	Recommended solution.	POST
/redfish/v1/Systems/system_id/Processors	Name	Name of the CPU resource collection.	GET
	Members@odata.count	Number of CPU resource members.	GET
	Members	CPU resource list, which provides references for all CPU resource URL s.	GET
/redfish/v1/Systems/system_id/Processors/cpu_id	Name	CPU name.	GET
	Id	UID of CPU in the iBMC system.	GET
	InstructionSet	Instruction set of the specified CPU resource.	GET
	ProcessorArchitecture	CPU architecture.	GET
	Manufacturer	CPU manufacturer.	GET
	Model	CPU type.	GET
	MaxSpeedMHz	Maximum CPU speed.	GET
	TotalCores	Total number of CPU cores.	GET
	TotalThreads	Total number of CPU threads.	GET
	Socket	CPU socket ID.	GET
	Status	CPU status.	GET
	Oem.Public	Customized properties of the CPU resource.	GET

URL	Property	Description	Operation
	L1CacheKiB	Level I cache of the specified CPU resource.	GET
	L2CacheKiB	Level II cache of the specified CPU resource.	GET
	L3CacheKiB	Level III cache of the specified CPU resource.	GET
	FrequencyMHz	Frequency of the specified CPU resource.	GET
	SerialNumber	Serial number of the specified CPU resource.	GET
	OperatingSpeedMHz	Current rate of the specified CPU resource.	GET
	TDPWatts	TDP (W) of the specified CPU resource.	GET
	Voltage	Voltage of the specified CPU resource.	GET
/redfish/v1/Systems/system_id/Processors?\$expand=.	Name	Name of the CPU resource collection.	GET
	Members@odata.count	Number of CPU resource members.	GET
	Members	Information about all CPU resources.	GET
/redfish/v1/Systems/system_id/Memory	Name	Name of the memory resource collection.	GET
	Members@odata.count	Number of memory resource members.	GET
	Members	Memory resource list, which provides references for all memory resource URLs.	GET
/redfish/v1/Systems/system_id/Memory/memory_id	Id	ID of the specified memory resource.	GET
	Name	Name of the specified memory resource.	GET
	AllowedSpeedsMHz	Maximum frequency of the specified memory resource, unit: MHz.	GET
	CapacityMiB	Capacity of the specified memory resource.	GET

URL	Property	Description	Operation
	Manufacturer	Manufacturer of the specified memory resource.	GET
	OperatingSpeedMhz	Speed of the specified memory resource.	GET
	SerialNumber	Serial number of the specified memory resource.	GET
	MemoryDeviceType	Type of the specified memory resource.	GET
	DataWidthBits	Data bandwidth of the specified memory resource.	GET
	RankCount	Number of ranks of the specified memory resource.	GET
	PartNumber	Part number of the specified memory resource.	GET
	DeviceLocator	Screen printing of the specified memory resource.	GET
	BaseModuleType	Basic module type of the specified memory resource.	GET
	MemoryLocation	Location of the specified memory resource.	GET
	Socket	Slot ID of the CPU of the specified memory resource.	GET
	Controller	Controller ID of the specified memory resource.	GET
	Channel	Channel ID of the specified memory resource.	GET
	Slot	Slot ID of the specified memory resource.	GET
	Status	Status of the specified memory resource.	GET
	Oem.Public	-	GET
	VoltageVolt	Voltage of the specified memory resource, unit: Volt.	GET
/redfish/v1/Systems/sys-	Name	Name of the memory resource collection.	GET

URL	Property	Description	Operation
tem_id/Memory?\$expand=.	Members@odata.count	Number of current memory resources.	GET
	Members	Information about all memory resources.	GET
/redfish/v1/Systems/system_id/Storages	Name	Name of the storage resource collection.	GET
	Members@odata.count	Number of storage resource members.	GET
	Members	Storage resource list, which provides references for all storage resource URLs.	GET
/redfish/v1/Systems/system_id/Storages/storage_id	Drives	Drive list managed by the specified storage controller.	GET
	Drives@odata.count	Number of drives managed by the storage controller.	GET
	Name	Name of the specified storage resource.	GET
	StorageControllers	Information about the storage controllers.	GET
	Name	Name of a storage controller.	GET
	MemberId	ID of the specified storage controller.	
	SpeedGbps	Interface speed of the storage controller.	GET
	FirmwareVersion	Firmware version of the storage controller.	GET
	Model	Model of the storage controller.	GET
	SupportedDeviceProtocols	Protocol type supported by the storage controller.	GET
	Manufacturer	Manufacturer of the storage controller.	GET
	CardManufacturer	Manufacturer of the specified storage controller.	GET
	CardModel	Model of the specified storage controller.	GET

URL	Property	Description	Operation
	Oem.Public	Manufacturer-customized properties.	GET
	MemorySizeMiB	Memory size of the specified storage controller.	GET
	CapacitanceStatus	BBU status of the specified storage controller. - Health: BBU health status - State: BBU presence status	GET
	Drives@odata.count	Number of drives managed by the storage controller.	GET
	Drives	Drive list.	GET
	Status	Status of the storage controller.	GET
	Description	Information about the specified storage controller.	GET
/redfish/v1/Systems/system_id/Storages?\$expand=.	Name	Name of the storage resource collection.	GET
	Members@odata.count	Number of current storage resources.	GET
	Members	Storage resource list. The information about all storage controller resources is displayed.	GET
/redfish/v1/Systems/system_id/Storages/storage_id/Volumes	Name	Name of the logical volume resource collection.	GET
	Members@odata.count	Number of logical volume resource members.	GET
	Members	Logical volume resource list.	GET
	code	ID of the specified message in the message registry.	POST
	message	Readable message for the code in the message registry.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity level.	POST

URL	Property	Description	Operation
	Resolution	Recommended solution.	POST
/redfish/v1/ Systems/sys- tem_id/Stor- ages/stor- age_id/Volumes/vol- ume_id	Name	Name of a logical volume.	GET
	Id	ID of the specified logical volume ID.	GET
	VolumeType	Redundancy type of the logical volume.	GET
	CapacityBytes	Capacity of the logical volume.	GET
	OptimumIOSizeBytes	Stripe size of the logical volume.	GET
	Links	Member logical volume list.	GET
	Drives	Drive list managed by the specified storage controller.	GET
	Drives@odata.count	Number of member physical disks included in the RAID .	GET
	Status	Status of the specified logical volume resource.	GET
	Oem.Public	Customized logical volume information.	GET
	RaidControllerID	Controller ID of the logical volume.	GET
	VolumeRaidLevel	RAID level of the logical volume.	GET
	DriveCachePolicy	Hard disk cache policy.	GET
	NumDrive	Number of physical disk members.	GET
	ReadPolicy	Read policy of the logical volume.	GET
	WritePolicy	Write policy of the logical volume.	GET
	AccessPolicy	Access policy of the logical volume.	GET
	IoPolicy	IO policy of the logical volume.	GET
	VolumeName	Name of the logical volume.	GET
	State	Status of the logical volume.	GET
	NumDriveperspan	Number of drive members in a span.	GET
	SpanNumber	Number of spans of a volume.	GET
	@Redfish.OperationApply-TimeSupport	Application time of the resource creation, deletion, or operation requested by the logical disk through the OperationApplyTime item.	GET

URL	Property	Description	Operation
	RAIDType	RAID level of the logical volume.	GET
	code	ID of the specified message in the message registry.	DELETE
	message	Readable message for the code in the message registry.	DELETE
	MessageId	Message ID.	DELETE
	RelatedProperties	Message-related properties.	DELETE
	MessageArgs	Message arguments.	DELETE
	Message	Details.	GET
	Severity	Severity level.	DELETE
	Resolution	Recommended solution.	DELETE
/redfish/v1/Systems/system_id/Bios	Id	ID of the BIOS resource.	GET
	Name	Name of the BIOS resource.	GET
	AttributeRegistry	Registry resource ID for BIOS properties.	GET
	Attributes	BIOS property list.	GET
	@Redfish.Settings	Information about the BIOS setting resource.	GET
/redfish/v1/Systems/system_id/Bios/SD	Id	ID of the BIOS setting resource.	GET
	Name	Name of the BIOS setting resource.	GET
	AttributeRegistry	Registry resource ID for BIOS properties.	GET
	Attributes	Property list of the current BIOS setting resource.	GET/PATCH
	@Redfish.Settings	Information about BIOS settings.	GET
/redfish/v1/Systems/system_id/EthernetInterfaces	Description	Description of the Ethernet interface resource collection.	GET
	Name	Name of the Ethernet interface resource collection.	GET
	Members@odata.count	Number of Ethernet interface resources.	GET
	Members	Ethernet interface resource list.	GET

URL	Property	Description	Operation
/redfish/v1/Systems/system_id/EthernetInterfaces/EthernetInterface-Port_ID	AutoNeg	Whether auto-negotiation is used.	GET
	Description	Position information about an Ethernet interface.	GET
	FullDuplex	Whether full duplex mode is used.	GET
	Id	Name of the Ethernet interface resource.	GET
	LinkStatus	Link status.	GET
	MACAddress	MAC address of the Ethernet interface.	GET
	PermanentMACAddress	Fixed MAC address of the Ethernet interface.	GET
	SpeedMbps	Current speed.	GET
	Health	Link quality.	GET
	State	Whether the Ethernet interface is enabled.	GET
/redfish/v1/Systems/system_id/MemorySummary	Description	System memory information description.	GET
	Name	System memory resource name.	GET
	TotalSystemMemoryGiB	Total accessible memory (RAM) of the operating system, unit: GiB.	GET
/redfish/v1/Systems/system_id/ProcessorSummary	Name	Name of the CPU resource collection.	GET
	Description	Name of the CPU resource collection.	GET
	Count	Number of CPUs.	GET
	CoreCount	Total number of CPU cores.	GET
	Model	CPU model of the system.	GET
/redfish/v1/Systems/system_id/IndicatorLED	Name	System indicator name.	GET
	Description	System indicator description.	GET
	IndicatorLED	System indicator status.	GET
/redfish/v1/Systems/sys-	Name	Name of the SimpleStorage resource collection.	GET

URL	Property	Description	Operation
tem_id/SimpleStorage	Members@odata.count	Number of SimpleStorage resources.	GET
	Members	SimpleStorage resource list.	GET
/redfish/v1/Systems/sys-tem_id/SimpleStorage/simplestorage_id	Name	Name of the specified SimpleStorage resource.	GET
	Devices	Hard disk resource list.	GET
	CapacityBytes	Capacity of a hard disk.	GET
	Manufacturer	Manufacturer of a hard disk.	GET
	Model	Model of a hard disk.	GET
	Name	Name of a hard disk.	GET
	Status	Status of a hard disk.	GET

5.1 Querying Information About the System Resource Collection

Function

Query information about the current System resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the System resource collection, refer to [Table 5-2](#).

Table 5-2 Parameter Descriptions for Querying Information About the System Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.

Parameter	Description	Value
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems
```

- Request Header:

```
x-auth-token:QnaWfqvKOY0ZGc2LK5Ay6+CaSYWjEYcxE6GcWKNFyjU=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#ComputerSystemCollection.ComputerSystemCollection",
  "@odata.id": "/redfish/v1/Systems",
  "@odata.type": "#ComputerSystemCollection.ComputerSystemCollection",
  "Description": "Collection of Computer Systems",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Systems/1"
    }
  ],
  "Members@odata.count": 1,
  "Name": "Systems Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the System resource collection, refer to [Table 5-3](#).

Table 5-3 Output Descriptions for Querying Information About the System resource Collection

Field	Type	Description
@odata.context	String	OData description of the System resource collection model.
@odata.id	String	Access path of the System resource collection.
@odata.type	String	Type of System resource collection.
Description	Character string	Description of the system resource collection.
Name	String	Name of the System resource collection.
Members@odata.count	Number	Number of System resource members.
Members	Object	System resource list.
@odata.id	String	Access path of a single System resource node.

5.2 Querying Information About a Specified System Resource

Function

Query information about a specified System resource of a server.



Note

Only the System resource information about the server itself can be queried.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems/system_id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified System resource, refer to [Table 5-4](#).

Table 5-4 Parameter Descriptions for Querying Information About the Specified System Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/1
```

- Request Header:

x-auth-token:QnaWfqvKOY0ZGc2LK5Ay6+CaSYWjEYcxE6GcWKNFyjU=

- Request Message Body: None
- Response Example:

[illegible]

```
"Boot": {
  "BootSourceOverrideEnabled": "Continuous",
  "BootSourceOverrideMode": "UEFI",
  "BootSourceOverrideTarget": "Hdd",
  "BootSourceOverrideEnabled@Redfish.AllowableValues": [
    "Once",
    "Continuous"
  ],
  "BootSourceOverrideMode@Redfish.AllowableValues": [
    "No Override",
    "Legacy",
    "UEFI"
  ],
  "BootSourceOverrideTarget@Redfish.AllowableValues": [
    "None",
    "Pxe",
    "Cd",
    "Floppy",
    "Hdd",
    "BiosSetup"
  ]
},
"Description": "System 1",
"EthernetInterfaces": {
  "@odata.id": "/redfish/v1/Systems/1/EthernetInterfaces"
},
"HostName": "iSACE2814D77795F",
"Id": "1",
"IndicatorLED": "Blinking",
"Links": {
  "Chassis": [
    {
      "@odata.id": "/redfish/v1/Chassis/1"
    }
  ],
  "CooledBy": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Thermal"
    }
  ],
  "ManagedBy": [
    {
      "@odata.id": "/redfish/v1/Managers/1"
    }
  ]
}
```

```

    ],
    "PoweredBy": [
        {
            "@odata.id": "/redfish/v1/Chassis/1/Power"
        }
    ]
},
"Manufacturer": "VANTAGEO",
"Memory": {
    "@odata.id": "/redfish/v1/Systems/1/Memory"
},
"MemorySummary": {
    "TotalSystemMemoryGiB": 120
},
"Model": "",
"Name": "System",
"NetworkInterfaces": {
    "@odata.id": "/redfish/v1/Systems/1/NetworkInterfaces"
},
"Oem": {
    "Public": {
        "CPUUsagePercent": 0,
        "CmccVersion": "2023V1",
        "IOUsagePercent": 0,
        "MemoryUsagePercent": 0,
        "PowerOnDelayEnabled": true,
        "PowerOnDelayMode": "RandomDelay",
        "PowerOnDelaySeconds": 120,
        "PowerOnStrategy": "RestorePreviousState",
        "ConfigurationModel": "20220905",
        "ProductSpecificIdentity": "2240-RE,Intel", "BiosVersionDate": "Dec 12
        2012",
        "ProductVersion": "?/",
        "ProductName": "a6",
        "ProductExtra": "q6n dtHiGUC12TK6npW6HSjKEiJiuQE
        5H791PVofffbKxe2f6f8j5qjxmy2Pe6J4fzaFbmwMojynG
        5nocSqPD bnYEV76KGxa2bmqFJOBW8XY7joaOMJOK
        PeDtEokxqq7R3lAw1S68nToF1hGey9fCX03hH9532Rjv
        uuu8tYn7p 5QwE9s48wL3gVCP3yw6mCV7lHXoM2VQ
        N201GWAx9f2c2MHCwk7DxBdH2qbCfYhqpWfH7
        8MNVOW15hu5g029vKrpLk",
        "PartitionLists": [
            {
                "DiskIndex": 1,

```

```
        "PartitionName": "/",
        "UsagePercent": 13,
        "TotalCapacityGB": 50
    },
    {
        "DiskIndex": 2,
        "PartitionName": "/boot",
        "UsagePercent": 17,
        "TotalCapacityGB": 1
    },
    {
        "DiskIndex": 3,
        "PartitionName": "/boot/efi",
        "UsagePercent": 5,
        "TotalCapacityGB": 0.2
    },
    {
        "DiskIndex": 4,
        "PartitionName": "/home",
        "UsagePercent": 0,
        "TotalCapacityGB": 2896.9
    }
]
}
},
"PartNumber": "",
"PowerState": "On",
"Processors": {
    "@odata.id": "/redfish/v1/Systems/1/Processors"
},
"SerialNumber": "",
"SimpleStorage": {
    "@odata.id": "/redfish/v1/Systems/1/SimpleStorage"
},
"Status": {
    "Health": "OK",
    "State": "Enabled"
},
"Storage": {
    "@odata.id": "/redfish/v1/Systems/1/Storage"
},
"Storages": {
    "@odata.id": "/redfish/v1/Systems/1/Storages"
},
}
```

```

    "SystemType": "Physical",
    "UUID": "30e72400-0000-1000-0000-000000000000",
    "ProcessorSummary": {
        "Count": 0,
        "CoreCount": 0,
        "Model": null
    },
    "Bios": {
        "@odata.id": "/redfish/v1/Systems/1/Bios"
    }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified Manager resource, refer to [Table 5-5](#).

Table 5-5 Output Descriptions for Querying Information About the Specified Manager Resource

Field	Type	Description
@odata.context	String	OData description of the specified System resource model.
@odata.id	String	Access path of the specified System resource.
@odata.type	String	Type of System resource.
Actions	Object	Operations that can be performed for the specified System resource through the Redfish interface.
#ComputerSystem.Reset.target	String	Access path of the restart operation properties.
ResetType@Redfish. AllowableValues	Array	OS operations allowed through the Redfish interface, including: • On • ForceOff • GracefulShutdown • ForceRestart • ForcePowerCycle • Nmi
AssetTag	String	Asset tag of the specified System resource.

Field	Type	Description
BiosVersion	String	BIOS version of the specified System resource.
Boot	Object	Boot parameters of the specified System resource.
BootSourceOverrideEnabled	String	Mode for applying the current boot settings of the System.
BootSourceOverrideMode	String	System boot mode.
BootSourceOverrideTarget	String	Current boot source of the system.
BootSourceOverrideEnabled@Redfish.AllowableValues	Array	Options of the mode for applying the current boot settings of the System, including: - Once: effective only once - Continuous: effective permanently
BootSourceOverrideMode@Redfish.AllowableValues	Array	Allowable boot modes of the system. Options: - Legacy - UEFI
BootSourceOverrideTarget@Redfish.AllowableValues	Array	Range of the boot devices defined by Redfish, including: - None - PXE - Floppy - CD - HDD - BiosSetup
Description	String	Description of the specified System resource.
EthernetInterfaces	Object	Access path of the Ethernet interfaces of the host.
HostName	String	Hostname of the specified System resource.
Id	String	ID of the specified System resource.
IndicatorLED	String	Position indicator status of the specified Chassis resource, including:
Links	Object	System resource links.
Chassis	Array	Access path of the Chassis resource node.

Field	Type	Description
CooledBy	Array	Access path of the fan resource node.
ManagedBy	Array	Access path of the Manager resource node.
PoweredBy	Array	Access path of the power resource.
Manufacturer	String	Manufacturer of the specified System resource.
Memory	Object	Access path of the memory resource node.
MemoryDomains	Object	V3 field.
Model	String	Model of the specified System resource.
Name	String	Name of the specified System resource.
NetworkInterfaces	Object	Access path of the network interfaces.
Oem.Public	Object	Customized properties.
CPUUsagePercent	Number	Dynamic CPU usage detected by CUPS.
IOUsagePercent	Number	Dynamic I/O usage detected by CUPS.
MemoryUsagePercent	Number	Dynamic memory usage detected by CUPS.
PowerOnDelayEnabled	Boolean	Whether to enable power-on delay: ● true ● false
PowerOnDelayMode	String	Power-on delay mode: ● CustomDelay: custom delay mode. ● RandomDelay: random delay mode.
PowerOnDelaySeconds	Number	Power-on delay.
PowerOnStrategy	String	Power-on policy upon power loss. ● TurnOn: stays on. ● StayOff: stays off. ● RestorePreviousState: same as before.
ConfigurationModel	String	Year + typical configuration model. The configuration value must be in dictionary format.
ProductSpecificIdentity	String	Internally defined product name.
BiosVersionDate	String	BIOS version date.

Field	Type	Description
ProductVersion	String	Product version.
ProductName	String	Product name.
ProductExtra	String	Additional product information.
PartNumber	String	Part number of the specified System resource.
PowerState	String	Power-on status of the specified System resource: ● On ● Off
Processors	Object	Access path of the processor resource node.
SerialNumber	String	Serial number of the specified System resource.
SimpleStorage	String	Access path of the SimpleStorage resource node.
Status	Object	Status of the specified System resource: ● Health: The System resource is healthy. ● Status: The System resource is enabled.
Storage	Object	Access path of the storage resource node.
Storages	Object	Access path of the storage resource node.
SystemType	String	System type of the specified system resource.
UUID	String	Globally unique ID of the specified System resource.
Bios	Object	Access path of the BIOS resource node.
PartitionLists.DiskIndex	Number	Disk partition number.
PartitionLists.PartitionName	String	Disk partition name.
PartitionLists.UsagePercent	Number	Disk partition usage.
PartitionLists.TotalCapacityGB	Number	Total disk partition capacity.
ProcessorSummary	Object	Processor summary.
Count	Number	Number of CPUs.

Field	Type	Description
CoreCount	Number	Total number of CPU cores.
Model	String	CPU model.

5.3 Remotely Powering On, Powering Off, and Resetting a System Resource

Function

Remotely power on, power off, and reset a System resource.

Permission Required

Power control

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Systems/system_id/Actions/ComputerSystem.Reset`
- Request Header:

```
Content-Type: header_type
X-Auth-Token: auth_value
```

- Request Message Body:

```
{
  "ResetType": value
}
```

Parameters

For a description of the parameters for remote operations, refer to [Table 5-6](#).

Table 5-6 Parameter Descriptions for Remote Operations

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
value	Operation type.	• On: power-on

Parameter	Description	Value
		● ForceOff: forcible power-off ● GracefulShutdown: normal power-off ● ForceRestart: forcible reboot ● ForcePowerCycle: forcible power-off and power-on

Usage Guidelines

When the setting is completed, you can query the "PowerState" field in the specified System resource to view the [OS](#) power-on or power-off status.

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Systems/1/Actions/ComputerSystem.Reset
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234e
Content-Type: application/json
```

- Request Message Body:

```
{
  "ResetType": "On"
}
```

- Response Example:

```
{
  "error": {
    "code": "Base.1.8.1.Success",
    "message": "Successfully Completed Request",
    "@Message.ExtendedInfo": [
      {
        "@odata.type": "#Message.v1_1_1.Message",
        "MessageId": "Base.1.8.1.Success",
        "Message": "Successfully Completed Request",
        "Severity": "OK",
        "Resolution": "None."
      }
    ]
  }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you perform a remote operation, refer to [Table 5-7](#).

Table 5-7 Output Descriptions for Remote Operations

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Readable message for the code in the message registry.
@odata.type	String	OData description of the message resource.
MessageId	String	Message ID.
Message	String	Message details.
Severity	String	Severity level supported by the Redfish interface. Options: • OK • Warning • Critical
Resolution	String	Solution.

5.4 Modifying Properties of a Specified System Resource

Function

Modify properties of a specified System resource, including the asset number, host name, and typical configuration model.

Permission Required

Basic management.

Syntax

- Operation Type: PATCH
- URL: `https://device_ip/redfish/v1/Systems/system_id`
- Request Header:

```
Content-Type: header_type
X-Auth-Token: auth_value
```

- Request Message Body:

```
{
```

```

    "AssetTag": tag,
    "HostName": name,
    "Oem": {
        "Public": {
            "ConfigurationModel": model,
            "PowerOnDelayEnabled": powerondealy_enable,
            "PowerOnDelayMode": powerondealy_mode,
            "PowerOnDelaySeconds": powerondealy_seconds,
            "CmccVersion": cmcc_version,
            "PowerOnStrategy": poweron_strategy
        }
    },
    "Boot": {
        "BootSourceOverrideMode": bootsourceoverride_mode,
        "BootSourceOverrideEnabled": bootsourceoverride_state,
        "BootSourceOverrideTarget": bootsourceoverride_target
    }
}

```

Parameters

For a description of the parameters for properties of the specified System resource, refer to [Table 5-8](#).

Table 5-8 Parameter Descriptions for Properties of the Specified System Resource

Parameter	Description	Value
tag	Customized asset tags.	- Length: 2–63 characters. - Consists of digits or letters, case-sensitive. - Allowed special characters: hyphen, underscore, space, and at (@). The tag cannot start or end with a hyphen, an underscore, or a space.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
tag	Customized asset tag.	- Length: 2–63 characters. - Consists of digits or letters, case-sensitive. - Allowed special characters: hyphen, underscore, space, and at (@). The tag

Parameter	Description	Value
		cannot start or end with a hyphen, an underscore, or a space.
name	Customized host name.	• The length cannot exceed 63 characters. • The name can only contain letters, digits, and the minus signs. No blank or space is allowed. The name is not case-sensitive. • The first character must be a letter, and the last character cannot be a minus sign.
model	Customized typical configuration model.	Year + typical configuration model. The configuration value must be in dictionary format, for example 2019C1, and the string length is 1–63.
powerondealy_enable	Whether to enable power-on delay:	• true • false
poweronde-lay_mode	Power-on delay mode:	• RandomDelay: random delay mode. • CustomDelay: custom delay mode.
powerondealy_seconds	Delay duration.	Delay duration, range: 1–120 s.
bootsourceoverride_mode	Boot mode.	• No Override • Legacy • UEFI The server configured with the ARM processor does not support legacy mode.
bootsourceoverride_state	Mode for applying the boot settings.	• Once: effective only once • Continuous: effective permanently
bootsourceoverride_target	Type of boot mode.	Boot devices defined by Redfish: • None: no override • Pxe: network • Cd: CD-ROM • Floppy: Usb • Hdd: hard disk • BiosSetup: BIOS • RemotelyHdd: volume.
poweron_strategy	Power-on policy.	• TurnOn: stays on. • StayOff: stays off. • RestorePreviousState: same as before.

Usage Guidelines

In the setting results, the "AssetTag", "HostName", and "ConfigurationModel" fields in the specified system resource information can be queried to verify the setting results.

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Systems/1
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234e
Content-Type: application/json
```

- Request Message Body:

```
{
  "AssetTag": "zichanbiaoqian-001",
  "HostName": "iSAC-20221022",
  "Oem": {
    "Public": {
      "ConfigurationModel": "2022C2",
      "PowerOnDelayEnabled": true,
      "PowerOnDelayMode": "CustomDelay",
      "PowerOnDelaySeconds": 100,
      "CmccVersion": "2023V1",
      "PowerOnStrategy": "RestorePreviousState"
    }
  },
  "Boot": {
    "BootSourceOverrideMode": "Legacy",
    "BootSourceOverrideEnabled": "Continuous",
    "BootSourceOverrideTarget": "Pxe"
  }
}
```

- Separate asset tag configuration:

```
{
  "AssetTag": "zichanbiaoqian-001"
}
```

- Separate hostname configuration:

```
{
  "HostName": "iSAC-20221022"
}
```



```
}

```

→ Separate typical configuration model configuration:

```
{
  "oem": {
    "Public": {
      "ConfigurationModel": "2022c2"
    }
  }
}
```

→ Separate typical configuration model configuration:

```
{
  "oem": {
    "Public": {
      "PowerOnDelayEnabled": true,
      "PowerOnDelayMode": "CustomDelay",
      "PowerOnDelaySeconds": 100
    }
  }
}
```

→ Separate power-on delay configuration:

```
{
  "Boot": {
    "BootSourceOverrideMode": "Legacy",
    "BootSourceOverrideEnabled": "Continuous",
    "BootSourceOverrideTarget": "Pxe"
  }
}
```

- Response Example: response of the **GET redfish/v1/Systems/system_id** interface. For details, refer to [5.2 Querying Information About a Specified System Resource](#).
- Status Code: 200

Output Description

None

5.5 Querying Information About the CPU Resource Collection

Function

Query information about the [CPU](#) resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems/system_id/Processors`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the CPU resource collection, refer to [Table 5-9](#).

Table 5-9 Parameter Descriptions for Querying Information About the CPU Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET `https://device_ip/redfish/v1/Systems/1/Processors`

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#ProcessorCollection.ProcessorCollection",
```

```

"@odata.id": "/redfish/v1/Systems/1/Processors",
"@odata.type": "#ProcessorCollection.ProcessorCollection",
"Description": "Collection of processors for this system",
"Name": "Processors Collection",
"Members@odata.count": 2,
"Members": [
    {
        "@odata.id": "/redfish/v1/Systems/1/Processors/0"
    },
    {
        "@odata.id": "/redfish/v1/Systems/1/Processors/1"
    }
]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the CPU resource collection, refer to [Table 5-10](#).

Table 5-10 Output Descriptions for Querying Information About the CPU Resource Collection

Field	Type	Description
@odata.context	String	OData description of the CPU resource collection model.
@odata.id	String	Access path of the CPU resource collection.
@odata.type	String	Type of CPU resource collection.
Description	Character string	Description of the CPU resource collection.
Name	String	Name of the CPU resource collection.
Members@odata.count	Number	Number of CPU resource members.
Members	Array	CPU resource list.
@odata.id	String	Access path of a single CPU resource node.

5.6 Querying Information About a Specified CPU Resource

Function

Query information about a specified [CPU](#) resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems/system_id/Processors/cpu_id`
- Request Header:

X-Auth-Token: auth_value
- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified CPU resources, refer to [Table 5-11](#).

Table 5-11 Parameter Descriptions for Querying Information About the Specified CPU Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resources.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
cpu_id	ID of the CPU resource.	It can be obtained from the CPU resource collection.

Usage Guidelines

None

Example

- Request Example:

GET : `https://device_ip/redfish/v1/Systems/1/Processors/0`

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

{
 "@odata.context": "/redfish/v1/\$metadata#Processor.Processor",

```

"@odata.id": "/redfish/v1/Systems/1/Processors/0",
"@odata.type": "#Processor.v1_10_0.Processor",
"Name": "Intel Processor 1",
"Id": "1",
"InstructionSet": "x86,x86-64",
"Manufacturer": "Intel(R) Corporation",
"MaxSpeedMHz": 3600,
"Model": "Genuine Intel(R) CPU 0000%@",
"Oem": {
  "Public": {
    "FrequencyMHz": 1700,
    "L1CacheKiB": 4480,
    "L2CacheKiB": 114688,
    "L3CacheKiB": 107520,
    "SerialNumber": "2F8A6BEB959A73D6",
    "Voltage": "1.6"
  }
},
"OperatingSpeedMHz": 2000,
"ProcessorArchitecture": "x86",
"ProcessorId": {
  "IdentificationRegisters": "f2-06-08-00-ff-fb-eb-bf"
},
"ProcessorType": "CentralProcessor",
"Socket": 1,
"Status": {
  "State": "Enabled",
  "Health": "OK"
},
"TDPWatts": 350,
"TotalCores": 56,
"TotalThreads": 112
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified CPU resource, refer to [Table 5-12](#).

Table 5-12 Output Descriptions for Querying Information About the Specified CPU Resource

Field	Type	Description
@odata.context	String	OData description of the specified CPU resource model.

Field	Type	Description
@odata.id	String	Access path of the specified CPU resource.
@odata.type	String	Type of the specified CPU resource.
Name	String	Name of the specified CPU resource.
Id	String	UID of the specified CPU resource in the iBMC system.
InstructionSet	String	Instruction set of the specified CPU resource: • x86 • x86-64 • IA-64 • ARM-A32 • ARM-A64 • MIPS32 • MIPS64 • OEM
ProcessorArchitecture	String	Architecture of the specified CPU resource: • x86 • IA-64 • ARM • MIPS • OEM
ProcessorId.IdentificationRegisters	String	Processor ID register.
ProcessorType	String	Type of the specified CPU resource.
Manufacturer	String	Manufacturer of the specified CPU resource.
Model	String	Model of the specified CPU resource.
MaxSpeedMHz	Number	Maximum frequency of the specified CPU resource.
TotalCores	Number	Total number of cores of the specified CPU resource.
TotalThreads	Number	Total number of threads of the specified CPU resource.
Socket	Number	Slot ID of the specified CPU resource.
Status	Object	Status of the specified CPU resource, including: • State: whether the CPU is isolated • Health: CPU resource health status
Oem.Public	Object	Customized vendor properties.
L1CacheKiB	Number	Level I cache of the specified CPU resource.

Field	Type	Description
L2CacheKiB	Number	Level II cache of the specified CPU resource.
L3CacheKiB	Number	Level III cache of the specified CPU resource.
FrequencyMHz	Number	Frequency of the specified CPU resource.
SerialNumber	String	Serial number of the specified CPU resource.
Voltage	String	Voltage of the specified CPU resource.
OperatingSpeedMHz	Number	Current speed of the specified CPU resource.
TDPWatts	Number	TDP(W) of the specified CPU resource.

5.7 Querying Information About All CPU Resources

Function

Query information about all [CPU](#) resources of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Systems/system_id/Processors?$expand=.`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about all CPU resources, refer to [Table 5-13](#).

Table 5-13 Parameter Descriptions for Querying Information About All CPU Resources

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET : https://10.43.211.250/redfish/v1/Systems/1/Processors?$expand=.
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#ProcessorCollection.ProcessorCollection",
  "@odata.id": "/redfish/v1/Systems/1/Processors",
  "@odata.type": "#ProcessorCollection.ProcessorCollection",
  "Description": "Collection of processors for this system",
  "Name": "Processors Collection",
  "Members@odata.count": 2,
  "Members": [
    {
      "@odata.id": "/redfish/v1/Systems/1/Processors/0",
      "@odata.type": "#Processor.v1_10_0.Processor",
      "Name": "Intel Processor 1",
      "Id": "1",
      "InstructionSet": "X86,X86-64",
      "Manufacturer": "Intel(R) Corporation",
      "MaxSpeedMHz": 3300,
      "Model": "Genuine Intel(R) CPU 0000%@",
      "Oem": {
        "Public": {
          "FrequencyMHz": 1500,
          "L1CacheKiB": 3840,
          "L2CacheKiB": 98304,
          "L3CacheKiB": 92160,
          "SerialNumber": "B65FD4F4B77D6755",
          "Voltage": "1.6"
        }
      },
      "OperatingSpeedMHz": 2000,
      "ProcessorArchitecture": "x86",
      "ProcessorId": {
```



```

        "IdentificationRegisters": "f3-06-08-00-ff-fb-eb-bf"
    },
    "ProcessorType": "CentralProcessor",
    "Socket": 1,
    "Status": {
        "State": "Enabled",
        "Health": "OK"
    },
    "TDPWatts": 350,
    "TotalCores": 48,
    "TotalThreads": 96
},
{
    "@odata.id": "/redfish/v1/Systems/1/Processors/1",
    "@odata.type": "#Processor.v1_10_0.Processor",
    "Name": "Intel Processor 2",
    "Id": "2",
    "InstructionSet": "x86,x86-64",
    "Manufacturer": "Intel(R) Corporation",
    "MaxSpeedMHz": 3300,
    "Model": "Genuine Intel(R) CPU 0000%@",
    "Oem": {
        "Public": {
            "FrequencyMHz": 1500,
            "L1CacheKiB": 3840,
            "L2CacheKiB": 98304,
            "L3CacheKiB": 92160,
            "SerialNumber": "B65FA8F41D9829E7",
            "Voltage": "1.6"
        }
    },
    "OperatingSpeedMHz": 2000,
    "ProcessorArchitecture": "x86",
    "ProcessorId": {
        "IdentificationRegisters": "f3-06-08-00-ff-fb-eb-bf"
    },
    "ProcessorType": "CentralProcessor",
    "Socket": 2,
    "Status": {
        "State": "Enabled",
        "Health": "OK"
    },
    "TDPWatts": 350,
    "TotalCores": 48,

```

```
        "TotalThreads": 96
      }
    ]
  }
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all CPU resources, refer to [Table 5-14](#).

Table 5-14 Output Descriptions for Querying Information About All CPU Resources

Field	Type	Description
@odata.context	String	OData description of the CPU resource collection model.
@odata.id	String	Access path of the CPU resource collection.
@odata.type	String	Type of CPU resource collection.
Description	String	Description of the CPU resource collection.
Name	String	Name of the CPU resource collection.
Members@odata.count	Number	Number of CPU resource members.
Members	Array	Information about all CPU resources.

For a description of the parameters of the CPU resource information, refer to [Table 5-12](#).

5.8 Querying Information About the Memory Resource Collection

Function

Query information about the current memory resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems/system_id/Memory`
- Request Header:

```
X-Auth-Token: auth_value
```

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the memory resource collection, refer to [Table 5-15](#).

Table 5-15 Parameter Descriptions for Querying Information About the Memory Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/1/Memory
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#MemoryCollection.MemoryCollection",
  "@odata.id": "/redfish/v1/Systems/1/Memory",
  "@odata.type": "#MemoryCollection.MemoryCollection",
  "Description": "Collection of Memories for this system",
  "Name": "Memory Collection",
  "Members@odata.count": 2,
  "Members": [
    {
      "@odata.id": "/redfish/v1/Systems/1/Memory/CPU0_E0"
    },
    {
      "@odata.id": "/redfish/v1/Systems/1/Memory/CPU1_E0"
    }
  ]
}
```

```
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the memory resource collection, refer to [Table 5-16](#).

Table 5-16 Output Descriptions for Querying Information About the Memory Resource Collection

Field	Type	Description
@odata.context	String	OData description of the memory resource collection model.
@odata.id	String	Access path of the memory resource collection.
@odata.type	String	Type of memory resource collection.
Description	Character string	Description of the memory resource collection.
Name	String	Name of the memory resource collection.
Members@odata.count	Number	Number of memory resource members.
Members	Array	Memory resource list.
@odata.id	String	Access path of a single memory resource node.

5.9 Querying Information About a Specified Memory Resource

Function

Query information about a specified memory resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems/system_id/Memory/memory_id`
- Request Header:

```
X-Auth-Token: auth_value
```

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified memory resource, refer to [Table 5-17](#).

Table 5-17 Parameter Descriptions for Querying Information About the Specified Memory Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
memory_id	Memory resource ID.	It can be obtained from the memory resource collection.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/1/Memory/DIMM1
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Memory.Memory",
  "@odata.id": "/redfish/v1/Systems/1/Memory/CPU1_A0",
  "@odata.type": "#Memory.v1_11_0.Memory",
  "AllowedSpeedsMHz": 4800,
  "BaseModuleType": "RDIMM",
  "CapacityMiB": 65536,
  "DataWidthBits": 64,
  "DeviceLocator": "CPU1_A0",
  "ECCType": "Multi-bit ECC",
  "Id": "CPU1_A0",
  "Manufacturer": "Samsung",
  "MemoryDeviceType": "DDR5",
```

```

    "MemoryLocation": {
      "Channel": 0,
      "Controller": 0,
      "Slot": 0,
      "Socket": 1
    },
    "Name": "CPU1_A0",
    "OperatingSpeedMhz": 4800,
    "PartNumber": "M321R8GA0BB0-CQKEG",
    "RankCount": 2,
    "SerialNumber": "01E2FC6C",
    "Status": {
      "State": "Enabled",
      "Health": "OK"
    }
  }
  "Oem": {
    "Public": {
      "VoltageVolt": 1.1,
      "Temperature": null
    }
  }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified memory resource, refer to [Table 5-18](#).

Table 5-18 Output Descriptions for Querying Information About the Specified Memory Resource

Field	Type	Description
@odata.context	String	OData description of the specified memory resource model.
@odata.id	String	Access path of the specified memory resource.
@odata.type	String	Type of the specified memory resource.
Name	String	Name of the specified memory resource.
Id	String	ID of the specified memory resource.
AllowedSpeedsMHz	Number	Maximum frequency of the specified memory resource, unit: MHz.
CapacityMiB	Number	Capacity of the specified memory resource, in MB.

Field	Type	Description
ECCType	String	ECC type of the specified memory.
Manufacturer	String	Manufacturer of the specified memory device.
OperatingSpeedMhz	Number	Operating speed of the specified memory resource.
SerialNumber	String	Serial number of the specified memory resource.
MemoryDeviceType	String	Type of the specified memory resource. The value should be in dictionary type, such as DDR4 and DDR3 .
DataWidthBits	Number	Data bandwidth of the specified memory resource.
RankCount	Number	Number of ranks of the specified memory resource.
PartNumber	String	Part number of the specified memory resource.
DeviceLocator	String	Screen printing of the specified memory resource.
BaseModuleType	String	Basic module type of the specified memory resource, including: ● RDIMM ● UDIMM ● SO_DIMM ● LRDIMM ● Mini_RDIMM ● Mini_UDIMM ● SO_RDIMM_72b ● SO_UDIMM_72b ● SO_DIMM_16b ● SO_DIMM_32b
MemoryLocation	Object	Location of the specified memory device.
Socket	Number	Slot ID of the CPU of the specified memory resource.
Controller	Number	Controller ID of the specified memory resource.
Channel	Number	Channel ID of the specified memory resource.
Slot	Number	Slot ID of the specified memory resource.
Status	Object	Status of the specified memory resource, including: ● Health: health status of the specified memory resource ● State: whether the specified memory resource is enabled
Oem.Public	Object	Customized field.
VoltageVolt	Number	Voltage of the specified memory resource, unit: Volt.

Field	Type	Description
Temperature	Number	Temperature of the specified memory resource, unit: °C.

5.10 Querying Information About All Memory Resources

Function

Query information about the current memory resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems/system_id/Memory?$expand=.`
- Request Header:

X-Auth-Token: auth_value
- Request Message Body: None

Parameters

For a description of the parameters for querying information about all memory resources, refer to [Table 5-19](#).

Table 5-19 Parameter Descriptions for Querying Information About All Memory Resources

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Systems/1/Memory?\$expand=.

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.id": "/redfish/v1/Systems/Self/Memory",
  "@odata.type": "#MemoryCollection.MemoryCollection",
  "Description": "Collection of Memories for this system",
  "Name": "Memory Collection",
  "Members@odata.count": 2,
  "Members": [
    {
      "@odata.id": "/redfish/v1/Systems/Self/Memory/DIMM9",
      "@odata.type": "#Memory.v1_11_0.Memory",
      "BaseModuleType": "RDIMM",
      "CapacityMiB": 16384,
      "DataWidthBits": 64,
      "DeviceLocator": "DIMM9",
      "ECCType": "Multi-bit ECC",
      "Id": "9",
      "Manufacturer": "Hynix",
      "MemoryDeviceType": "DDR5",
      "MemoryLocation": {
        "Channel": 0,
        "Controller": 0,
        "Slot": 0,
        "Socket": 1
      },
      "Name": "DIMM9",
      "OperatingSpeedMhz": 4800,
      "PartNumber": "HMCG78MEBRA115N",
      "RankCount": 1,
      "SerialNumber": "137A8358",
      "Status": {
        "State": "Enabled",
        "Health": "OK"
      }
    },
    {
      "@odata.id": "/redfish/v1/Systems/Self/Memory/DIMM25",
      "@odata.type": "#Memory.v1_11_0.Memory",
      "BaseModuleType": "RDIMM",
```

```

        "CapacityMiB": 16384,
        "DataWidthBits": 64,
        "DeviceLocator": "DIMM25",
        "ECCType": "Multi-bit ECC",
        "Id": "25",
        "Manufacturer": "Hynix",
        "MemoryDeviceType": "DDR5",
        "MemoryLocation": {
            "Channel": 0,
            "Controller": 0,
            "Slot": 0,
            "Socket": 2
        },
        "Name": "DIMM25",
        "OperatingSpeedMhz": 4800,
        "PartNumber": "HMC78MEBRA115N",
        "RankCount": 1,
        "SerialNumber": "138B9C40",
        "Status": {
            "State": "Enabled",
            "Health": "OK"
        }
    }
]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all memory resource, refer to [Table 5-20](#).

Table 5-20 Output Descriptions for Querying Information About All Memory Resources

Field	Type	Description
@odata.context	String	OData description of the memory resource collection model.
@odata.id	String	Access path of the memory resource collection.
@odata.type	String	Type of memory resource collection.
Description	String	Description of the memory resource collection.
Name	String	Name of the memory resource collection.
Members@odata.count	Number	Number of memory resource members.

Field	Type	Description
Members	Array	Information about all memory resources.

For a description of the parameters of the memory resource information, refer to [Table 5-18](#).

5.11 Querying Information About the Storage Resource Collection

Function

Query information about the current storage resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL 1: `https://device_ip/redfish/v1/Systems/system_id/Storage`
- URL 2: `https://device_ip/redfish/v1/Systems/system_id/Storages`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the storage resource collection, refer to [Table 5-21](#).

Table 5-21 Parameter Descriptions for Querying Information About the Storage Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example 1:

```
GET https://device_ip/redfish/v1/Systems/1/Storage
```

- Request Example 2:

```
GET https://device_ip/redfish/v1/Systems/1/Storages
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#StorageCollection.StorageCollection",
  "@odata.id": "/redfish/v1/Systems/1/Storages",
  "@odata.type": "#StorageCollection.StorageCollection",
  "Name": "Storage Collection",
  "Members@odata.count": 2,
  "Members": [
    {
      "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage19"
    },
    {
      "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage5"
    }
  ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the storage resource collection, refer to [Table 5-22](#).

Table 5-22 Output Descriptions for Querying Information About the Storage Resource Collection

Field	Type	Description
@odata.context	String	OData description of the storage resource collection model.
@odata.id	String	Access path of the storage resource collection.

Field	Type	Description
@odata.type	String	Type of storage resource collection.
Name	String	Name of the storage resource collection.
Members@odata.count	Number	Number of storage resource members.
Members	Array	Storage resource list.
@odata.id	String	Access path of a single storage resource node.

5.12 Querying Information About a Specified Storage Controller Resource

Function

Query information about the specified storage controller resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Systems/system_id/Storage/stor-age_id*
- URL2: *https://device_ip/redfish/v1/Systems/system_id/Storages/stor-age_id*
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about a specified storage controller resource, refer to [Table 5-23](#).

Table 5-23 Parameter Descriptions for Querying Information About the Specified Storage Controller Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.

Parameter	Description	Value
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
storage_id	ID of the specified storage resource.	It can be obtained by querying the information about the storage resource collection.

Usage Guidelines

None

Example

- Request Example 1:

```
GET https://device_ip/redfish/v1/Systems/1/Storage/RAIDStorage5
```

- Request Example 2:

```
GET https://device_ip/redfish/v1/Systems/1/Storages/RAIDStorage5
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Storage.Storage",
  "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage5",
  "@odata.type": "#Storage.v1_9_0.Storage",
  "Drives": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk16",
      "CapacityBytes": 666
    },
    {
      "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk18",
      "CapacityBytes": 666
    },
    {
      "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk20",
      "CapacityBytes": 777
    },
    {
```

```
        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk22",
        "CapacityBytes": 888
    }
],
"Drives@odata.count": 4,
"Name": "RAIDStorage5",
"StorageControllers": [
    {
        "@odata.id":
        "/redfish/v1/Systems/1/Storages/RAIDStorage5#/StorageControllers/
        RAIDStorage5",
        "CapacitanceStatus": null,
        "CapacitanceModel": null,
        "Description": "RAID Controller",
        "FirmwareVersion": "3.22",
        "Manufacturer": "Microchip",
        "MemberId": "RAIDStorage5",
        "Model": "PM8236",
        "CardManufacturer": "VT",
        "CardModel": "RS241-18i 2G",
        "Name": "RS241-18i 2G(RAIDStorage5)",
        "Oem": {
            "Public": {
                "CapacitanceName": null,
                "CapacitanceStatus": {
                    "Health": null,
                    "State": "Absent"
                },
            },
            "MemorySizeMiB": 2048,
            "OOBSupport": true,
            "SASAddress": null,
            "SupportedRAIDLevels": [
                "RAID0",
                "RAID1",
                "RAID5",
                "RAID6",
                "RAID10",
                "RAID50",
                "RAID60"
            ]
        }
    },
    {
        "SerialNumber": "743551500214",
        "PartNumber": "ASM1026R",
```

```

        "SpeedGbps": 12,
        "status": {
            "Health": "OK",
            "State": "Enabled"
        },
        "SupportedDeviceProtocols": [
            "SAS",
            "SATA"
        ],
        "TotalCacheSizeMiB": null
    },
    ],
    "StorageControllers@odata.count": 1,
    "Volumes": {
        "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes"
    }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about a specified storage controller resource, refer to [Table 5-24](#).

Table 5-24 Output Descriptions for Querying Information About the Specified Storage Controller Resource

Field	Type	Description
@odata.context	String	OData description of the specified storage controller model.
@odata.id	String	Access path of the specified storage controller.
@odata.type	String	Type of the specified storage controller.
Drives	Array	Drive list managed by the specified storage controller.
Drives.CapacityBytes	Number	Capacity of the drives managed by the specified storage controller.
Drives.@odata.id	String	Access path of the drives managed by the specified storage controller.
Drives@odata.count	Number	Number of drives managed by the specified storage controller.
Name	String	Name of the specified storage controller.
StorageControllers	Array	Information about the storage controller.

Field	Type	Description
StorageControllers.@odata.id	String	Access path of the specified storage controller.
StorageControllers.CapacitanceStatus	String	Capacitance (BBU) status of the specified storage controller.
StorageControllers.CapacitanceModel	String	Capacitance (BBU) name of the specified storage controller.
StorageControllers.Description	String	Description of the specified storage controller.
StorageControllers.FirmwareVersion	String	Firmware version of the specified storage controller.
StorageControllers.MemberId	String	ID of the specified storage controller. ● PCIe: RAIDStorage + slot number ● Onboard: RAIDStorage0
StorageControllers.Model	String	Chip model of the specified storage controller.
StorageControllers.Manufacturer	String	Chip manufacturer of the specified storage controller.
StorageControllers.CardManufacturer	String	Manufacturer of the specified storage controller.
StorageControllers.CardModel	String	Model of the specified storage controller.
StorageControllers.Name	String	Name of the specified storage controller. (storage controller name + MemberId)
StorageControllers.Oem.Public	Object	Manufacturer-customized properties.
StorageControllers.Oem.Public.CapacitanceName	String	Capacitance (BBU) name of the specified storage controller.
StorageControllers.Oem.Public.CapacitanceStatus	Object	BBU status of the specified storage controller. ● Health: BBU health status ● State: BBU presence status
StorageControllers.Oem.Public.MemorySizeMiB	Number	Memory size of the specified storage controller.
StorageControllers.Oem.Public.OOBSupport	Boolean	Whether the specified storage controller supports out-of-band management.
StorageControllers.Oem.Public.SASAddress	String	Address of the specified storage controller.
StorageControllers.Oem.Public.SupportedRAIDLevels	Array	RAID level supported by the specified storage controller.

Field	Type	Description
StorageControllers.SerialNumber	String	Serial number of the specified storage controller.
StorageControllers.PartNumber	String	Part number of the specified storage controller.
StorageControllers.SpeedGbps	Number	Interface speed of the specified storage controller.
StorageControllers.Status	Object	Status of the specified storage controller. ● State: whether the specified storage controller is enabled. ● Health: health status of the specified storage controller.
StorageControllers.Supported-DeviceProtocols	Array	Protocol supported by the specified storage controller: ● SPI ● PCIe ● AHCI ● UHCI ● SAS ● SATA ● USB ● NVMe ● FC ● iSCSI ● FCoE ● NVMeOverFabrics ● SMB ● NFSv3 ● NFSv4 ● HTTP ● HTTPS ● FTP ● SFTP
StorageControllers.Total-CacheSizeMiB	Number	Total cache size of the specified storage controller, unit: MiB.
StorageControllers@odata-count	Number	Number of storage controllers.
Volumes	Object	Links to operations on logical volumes.

5.13 Querying Information About All Storage Controller Resources

Function

Query information about all current storage controller resources of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL1: *https://device_ip/redfish/v1/Systems/system_id/Storages?\$expand=.*
- URL2: *https://device_ip/redfish/v1/Systems/system_id/Storage?\$expand=.*
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about all storage controller resources, refer to [Table 5-25](#).

Table 5-25 Parameter Descriptions for Querying Information About All Storage Controller Resources

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example 1:

```
GET https://device_ip/redfish/v1/Systems/s1/Storages?$expand=.
```

- Request Example 2:

```
GET https://device_ip/redfish/v1/Systems/1/Storage?$expand=.
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#StorageCollection.StorageCollection",
  "@odata.id": "/redfish/v1/Systems/1/Storages",
  "@odata.type": "#StorageCollection.StorageCollection",
  "Name": "Storage Collection",
  "Members@odata.count": 2,
  "Members": [
    {
      "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage19",
      "@odata.type": "#Storage.v1_9_0.Storage",
      "Drives": [],
      "Drives@odata.count": 0,
      "Name": "RAIDStorage19",
      "StorageControllers": [
        {
          "@odata.id":
            "/redfish/v1/Systems/1/Storages/RAIDStorage19#/StorageControllers/RAIDStorage19",
          "Description": "RAID Controller",
          "FirmwareVersion": "3.22",
          "Manufacturer": "Microchip",
          "MemberId": "RAIDStorage19",
          "Model": "PM8236",
          "CardManufacturer": "VT",
          "CardModel": "RS241-18i 2G",
          "Name": "RS241-18i 2G(RAIDStorage19)",
          "Oem": {
            "Public": {
              "CapacitanceName": null,
              "CapacitanceStatus": {
                "Health": null,
                "State": "Absent"
              }
            }
          }
        }
      ]
    }
  ]
}
```

```
        "MemorySizeMiB": 2048,
        "OOBSupport": true,
        "SASAddress": null,
        "SupportedRAIDLevels": [
            "RAID0",
            "RAID1",
            "RAID5",
            "RAID6",
            "RAID10",
            "RAID50",
            "RAID60"
        ]
    },
    "SerialNumber": "743551500696",
    "SpeedGbps": 12,
    "status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "SupportedDeviceProtocols": [
        "SAS",
        "SATA"
    ]
},
"StorageControllers@odata.count": 1,
"volumes": {
    "@odata.id":
        "/redfish/v1/Systems/1/Storages/RAIDStorage19/Volumes"
},
{
    "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage5",
    "@odata.type": "#Storage.v1_9_0.Storage",
    "Drives": [
        {
            "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk16"
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk18"
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk20"
```

```

    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk22"
    }
],
"Drives@odata.count": 4,
"Name": "RAIDStorage5",
"StorageControllers": [
    {
        "@odata.id":
        "/redfish/v1/Systems/1/Storages/RAIDStorage5#/
        StorageControllers/RAIDStorage5",
        "Description": "RAID Controller",
        "FirmwareVersion": "3.22",
        "Manufacturer": "Microchip",
        "MemberId": "RAIDStorage5",
        "Model": "PM8236",
        "CardManufacturer": "VT",
        "CardModel": "RS241-18i 2G",
        "Name": "RS241-18i 2G(RAIDStorage5)",
        "Oem": {
            "Public": {
                "CapacitanceName": null,
                "CapacitanceStatus": {
                    "Health": null,
                    "State": "Absent"
                },
            },
            "MemorySizeMiB": 2048,
            "OBSupport": true,
            "SASAddress": null,
            "SupportedRAIDLevels": [
                "RAID0",
                "RAID1",
                "RAID5",
                "RAID6",
                "RAID10",
                "RAID50",
                "RAID60"
            ]
        }
    },
    {
        "SerialNumber": "743551500214",
        "SpeedGbps": 12,
        "Status": {

```

```

        "Health": "OK",
        "State": "Enabled"
    },
    "SupportedDeviceProtocols": [
        "SAS",
        "SATA"
    ]
}
],
"StorageControllers@odata.count": 1,
"Volumes": {
    "@odata.id":
    "/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes"
}
}
]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all storage controller resources, refer to [Table 5-26](#).

Table 5-26 Output Descriptions for Querying Information About All Storage Controller Resources

Field	Type	Description
@odata.context	String	OData description of the storage controller resource collection model.
@odata.id	String	Access path of the storage controller resource collection.
@odata.type	String	Type of storage controller resource collection.
Name	String	Name of the storage controller resource collection.
Members@odata.count	Number	Number of storage controller resource members.
Members	Array	Storage resource list.

For a description of the parameters of the storage controller resource information, refer to [Table 5-24](#).

5.14 Querying Information About the Logical Volume Resource Collection

Function

Query information about the current logical volume resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Systems/system_id/Storage/storage_id/Volumes*
- URL2: *https://device_ip/redfish/v1/Systems/system_id/Storages/storage_id/Volumes*

- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the logical volume resource collection, refer to [Table 5-27](#).

Table 5-27 Parameter Descriptions for Querying Information About the Logical Volume Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
storage_id	ID of the specified storage resource.	It can be obtained by querying the information about the storage resource collection.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example1:

```
GET https://device_ip/redfish/v1/Systems/1/Storage/RAIDStorage5/Volumes
```

- Request Example2:

```
GET https://device_ip/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#VolumeCollection.VolumeCollection",
  "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes",
  "@odata.type": "#VolumeCollection.volumeCollection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes/
LogicalDrive0"
    },
    {
      "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes/
LogicalDrive1"
    },
    {
      "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes/
LogicalDrive2"
    }
  ],
  "Members@odata.count": 3,
  "Name": "Volume Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the logical volume resource collection, refer to [Table 5-28](#).

Table 5-28 Output Descriptions for Querying the Information About the Logical Volume Resource Collection

Field	Type	Description
@odata.context	String	OData description of the logical volume resource collection model.
@odata.id	String	Access path of the logical volume resource collection.
@odata.type	String	Type of logical volume resource collection.
Name	String	Name of the logical volume resource collection.
Members@odata.count	Number	Number of logical volume resource members.
Members	Array	Logical volume resource list.
@odata.id	String	Access path of a single logical volume resource node.

5.15 Querying Information About a Specified Logical Volume Resource

Function

Query information about a specified logical volume resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems/system_id/Storage/storage_id/Volumes/volume_id`
- URL2: `https://device_ip/redfish/v1/Systems/system_id/Storages/storage_id/Volumes/volume_id`
- Request Header: None

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified logical volume resource, refer to [Table 5-29](#).

Table 5-29 Parameter Descriptions for Querying Information About the Specified Logical Volume Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
storage_id	ID of the specified storage resource.	It can be obtained from the storage resource collection.
volume_id	ID of the specified logical volume.	It can be obtained from the logical volume resource collection.

Usage Guidelines

None

Example

- Request Example1:

```
GET https://device_ip/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes/LogicalDrive2
```

- Request Example2:

```
GET https://device_ip/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes/LogicalDrive2
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Volume.Volume",
  "@odata.id":
    "/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes/LogicalDrive0",
  "@odata.type": "#Volume.v1_0_3.Volume",
  "@Redfish.OperationApplyTimeSupport": {
    "SupportedValues": ["Immediate"]
  },
  "RAIDType": "RAID10",
  "Links": {
    "Drives": [
      {
```

```

        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk19"
      }
    ],
    "Drives@odata.count": 1
  },
  "Id": "LogicalDrive0",
  "Name": "2223",
  "Oem": {
    "Public": {
      "AccessPolicy": null,
      "IoPolicy": null,
      "ReadPolicy": null,
      "WritePolicy": null,
      "DriveCachePolicy": null,
      "NumDrive": 1,
      "RaidControllerID": 5,
      "State": "Optimal",
      "VolumeName": "2223",
      "VolumeRaidLevel": "RAID0"
    }
  },
  "OptimumIOSizeBytes": 1048576,
  "CapacityBytes": 1919850381312,
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  },
  "VolumeType": "NonRedundant",
  "NumDriveperspan": null,
  "SpanNumber": null
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified logical volume resource, refer to [Table 5-30](#).

Table 5-30 Output Descriptions for Querying Information About the Specified Logical Volume Resource

Field	Type	Description
@odata.context	String	OData description of the specified logical volume resource model.

Field	Type	Description
@odata.id	String	Access path of the specified logical volume resource.
@odata.type	String	Type of the specified logical volume.
Name	String	Name of the specified logic volume resource.
Id	String	ID of the specified logical volume ID.
VolumeType	String	Redundancy type of the specified logical volume: ● RawDevice ● NonRedundant ● Mirrored ● StripedWithParity ● SpannedMirrors ● SpannedStripesWithParity
CapacityBytes	Number	Capacity of the logical volume.
OptimumIOSizeBytes	Number	Stripe size of the logical volume.
Links	Object	Member logical volume list.
Drives	Array	Drive list managed by the current specified controller.
@odata.id	String	Access path of the specified drive.
Drives@odata.count	Number	Number of member physical disks included in the RAID.
Status	Object	Status of the specified logical volume resource, including: ● State: Status of the logical disk resource. ● Health: health status of the logical volume.
Oem.Public	Object	Customized logical volume information.
RaidControllerID	Number	Controller ID of the logical volume.
VolumeRaidLevel	String	RAID level of the logical volume. The value must be in dictionary format, including: ● RAID0 ● RAID1 ● RAID5 ● RAID6 ● RAID00 ● RAID10 ● RAID50 ● RAID60
DriveCachePolicy	String	Hard disk Cache policy: ● Unchanged

Field	Type	Description
		• Enabled • Disabled
NumDrive	Number	Number of physical disk members.
ReadPolicy	String	Read policy of the logical volume: • NoReadAhead • ReadAhead
WritePolicy	String	Write policy of the logical volume: • WriteThrough • WriteBack • AlwaysWriteBack
AccessPolicy	String	Access policy of the logical volume: • ReadWrite • ReadOnly • Blocked
IoPolicy	String	IO policy of the logical volume: • DirectIO • CachedIO
VolumeName	String	Name of the logical volume.
State	String	Status of the logical volume: • Offline • Partially • Degraded • Optimal • Initializing
NumDriveperspan	Number	Number of drive members in a span.
SpanNumber	Number	Number of spans of a volume.
@Redfish.OperationApply-TimeSupport	Object	Application time of the resource creation, deletion, or operation requested by the logical disk through the OperationApplyTime item.
@Redfish.OperationApply-TimeSupport.SupportedValues	Array	Supported Value
RAIDType	String	RAID level of the logical volume.

5.16 Creating a Logical Volume

Function

Create a logical volume.

Permission Required

Basic management.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/Systems/system_id/Storage/storage_id/Volumes*
- URL2: *https://device_ip/redfish/v1/Systems/system_id/Storages/storage_id/Volumes*
- Request Header:

Content-Type: header_type
X-Auth-Token: auth_value

- Request Message Body:

```
{
  "OptimumIOSizeBytes": optsize,
  "Oem": {
    "Public": {
      "volumeName": name,
      "volumeRaidLevel": raidlevel,
      "ReadPolicy": read_policy,
      "WritePolicy": write_policy,
      "AccessPolicy": access_policy,
      "IoPolicy": io_policy,
      "DriveCachePolicy": disk_cache_policy,
      "InitializationMode": initmode,
      "SpanNumber": spannum,
      "Drives": [drives]
    }
  }
}
```

Parameters

For a description of the parameters for creating the logical volume, refer to [Table 5-31](#).

Table 5-31 Parameter Descriptions for Creating the Logical Volume

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.

Parameter	Description	Value
storage_id	ID of the specified storage resource.	It can be obtained by querying the information about the storage resource collection.
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
optsize	Number	Stripe size of the logical volume, optional, in bytes. Options: • 65536 • 131072 • 262144 • 524288 • 1048576
name	String	Name of the logical volume, required, consisting of 1–31 characters, including letters, digits, minus, and underscores, and cannot be the same as the original logical volume name.
raidlevel	String	RAID level of the logical volume, required, including: • RAID0 • RAID1 • RAID5 • RAID6
read_policy	String	Read policy of the logical volume, optional, including: • NoReadAhead • ReadAhead
write_policy	String	Write policy of the logical volume, optional, including: • WriteThrough • WriteBack • AlwaysWriteBack Note: Assume that there is no BBU on the controller. If "WriteThrough" or "WriteBack" is configured, "WriteThrough" is displayed in the query result. If "AlwaysWriteBack"

Parameter	Description	Value
		is configured, "AlwaysWriteBack" is displayed in the query result.
access_policy	String	Access policy of the logical volume, optional, including: • ReadWrite • ReadOnly • Blocked
io_policy	String	IO policy of the logical volume, optional, including: • DirectIO • CachedIO
disk_cache_policy	String	Caching policy of the logical volume, optional, including: • Unchanged • Enabled • Disabled
initmode	String	Initiation mode of the logical volume, optional, including: • UnInit: no initialization • QuickInit: quick initialization • FullInit: full initialization
spannum	Number	Number of logical volume subgroups, optional, default:1. The value can be set to 1 only. For Broadcom cards RAID00, RAID10, RAID50, and RAID60, this parameter must be a divisor of the number of disks.
drives	Array	Member volume list, required. The format of the drives field is: [HDDPlaneDiskid1,HD-PlaneDiskid2,...,HDDPlaneDiskid3]

Usage Guidelines

The creation completion time of the logical volume is related to parameters. Therefore, after the configuration, you need to periodically refresh the configuration to determine whether the creation process is completed.

Example

- Request Example1:

```
POST https://device_ip/redfish/v1/Systems/1/Storage/RAIDStorage5/Volumes
```

- Request Example2:

```
POST https://device_ip/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes
```

- Request Header:

```
Content-Type: application/json  
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body:

```
{  
  "OptimumIOSizeBytes": 1048576,  
  "Oem": {  
    "Public": {  
      "VolumeName": "2222",  
      "VolumeRaidLevel": "RAID0",  
      "ReadPolicy": "ReadAhead",  
      "WritePolicy": "WriteThrough",  
      "AccessPolicy": "ReadWrite",  
      "IoPolicy": "CachedIO",  
      "DriveCachePolicy": "Enabled",  
      "InitializationMode": "UnInit",  
      "SpanNumber": 2,  
      "Drives": ["HDDPlaneDisk19"]  
    }  
  }  
}
```

- Response Example:

```
{  
  "error": {  
    "@Message.ExtendedInfo": [  
      {  
        "@odata.type": "#Message.v1_1_1.Message",  
        "Message": "Successfully Completed Request",  
        "MessageArgs": [],  
        "MessageId": "Base.1.0.Success",  
        "RelatedProperties": [],  
        "Resolution": "None",  
        "Severity": "OK"  
      }  
    ],  
    },  
  "code": "Base.1.0.Success",  
}
```

```
{
  "message": "Successfully Completed Request"
}
```

- Status Code: 202

Output Description

For a description of the output returned when you create the logical volume, refer to [Table 5-32](#).

Table 5-32 Output Descriptions for Creating the Logical Volume

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Readable message for the code in the message registry.
@odata.type	String	OData description of the message resource.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Message details.
MessageArgs	Array	Message arguments.
Severity	String	Severity level supported by the Redfish interface. Options: • OK • Warning • Critical
Resolution	String	Solution.

5.17 Deleting a Logical Volume

Function

Delete the logical volume.

Permission Required

Basic management.

Syntax

- Operation Type: DELETE
- URL: `https://device_ip/redfish/v1/Systems/system_id/Storage/storage_id/Volumes/volume_id`

- URL2: `https://device_ip/redfish/v1/Systems/system_id/Storages/storage_id/Volumes/volume_id`
- Request Header:

Content-Type: header_type

- Request Message Body: None

Parameters

For a description of the parameters for deleting the logical volume, refer to [Table 5-33](#).

Table 5-33 Parameter Descriptions for Deleting the Logical Volume

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
storage_id	ID of the specified storage resource.	It can be obtained from the storage resource collection.
volume_id	ID of the specified logical volume.	It can be obtained from the logical volume resource collection.
auth_value	X-Auth-Token value contained in Request Header in the DELETE request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example1:

DELETE https://device_ip/redfish/v1/Systems/1/Storage/RAIDStorage5/Volumes/LogicalDrive0

- Request Example2:

DELETE https://device_ip/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes/LogicalDrive0

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

{
 "error": {

```

    "@Message.ExtendedInfo": [
      {
        "@odata.type": "#Message.v1_1_1.Message",
        "Message": "Successfully Completed Request",
        "MessageArgs": [],
        "MessageId": "Base.1.0.Success",
        "RelatedProperties": [],
        "Resolution": "None",
        "Severity": "OK"
      }
    ],
    "code": "Base.1.0.Success",
    "message": "Successfully Completed Request"
  }
}

```

- Status Code: 202

Output Description

For a description of the output returned when you delete the logical volume, refer to [Table 5-34](#).

Table 5-34 Output Descriptions for Deleting the Logical Volume

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Readable message for the code in the message registry.
@odata.type	String	OData description of the message resource.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Message details.
MessageArgs	Array	Message arguments.
Severity	String	Severity level supported by the Redfish interface. Options: • OK • Warning • Critical
Resolution	String	Solution.

5.18 Querying Properties of the BIOS Resource

Function

Query information about the current [BIOS](#) resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Systems/system_id/Bios`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying properties of the BIOS resource, refer to [Table 5-35](#).

Table 5-35 Parameter Descriptions for Querying Properties of the BIOS Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Systems/1/Bios

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```

{
  "@Redfish.Settings": {
    "@odata.type": "#Settings.v1_2_2.Settings",
    "SupportedApplyTimes": ["OnReset"],
    "Oem": {
      "@odata.id": "/redfish/v1/Systems/1/Bios/SD"
    },
    "SettingsObject": {
      "@odata.id": "/redfish/v1/Systems/1/Bios/SD"
    }
  },
  "@odata.context": "/redfish/v1/$metadata#Bios.Bios",
  "@odata.id": "/redfish/v1/Systems/1/Bios",
  "@odata.type": "#Bios.v1_1_0.Bios",
  "Actions": {
    "#Bios.ChangePassword": {
      "@Redfish.ActionInfo":
        "/redfish/v1/Systems/1/Bios/ChangePasswordActionInfo",
      "target": "/redfish/v1/Systems/1/Bios/Actions/Bios.ChangePassword"
    },
    "#Bios.ResetBios": {
      "target": "/redfish/v1/Systems/1/Bios/Actions/Bios.ResetBios"
    }
  },
  "Attributes": {
    "BootMode": "UEFI Only",
    "C1E": "Enabled",
    "EIST": "Disabled",
    "EnergyPerformanceBIAS": "Balanced Performance",
    "HardwarePStates": "Native Mode",
    "HyperThreading": "Enabled",
    "MonitorMWAIT": "Enabled",
    "NUMA": "Enabled",
    "PackageCState": "C0/C1 state",
    "PowerPerformanceTuning": "OS controls EPB",
    "PowerPolicySelect": "Custom",
    "TurboMode": "Enabled"
  },
  "Description": "Current BIOS Settings",
  "Id": "Bios",
  "Name": "Current BIOS Settings"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query properties of the BIOS resource, refer to [Table 5-36](#).

Table 5-36 Output Descriptions for Querying Properties of the BIOS Resource

Field	Type	Description
@odata.context	String	OData description of the BIOS resource model.
@odata.id	String	Access path of the BIOS resource.
@odata.type	String	Type of BIOS resource.
Description	String	Description of the BIOS resource.
Id	String	ID of the BIOS resource.
Name	String	Name of the BIOS resource.
Attributes	Object	BIOS attribute.
Actions	Object	Operations that can be performed on the BIOS resource.
#Bios.ChangePassword.target	String	Operation path for BIOS password modification.
#Bios.ResetBios.target	String	Operation path for BIOS reset.
@Redfish.Settings.@odata.type	String	Type of the BIOS setting resource.
@Redfish.Settings.SupportedApplyTimes	Array	Effective time of settings.
@Redfish.Settings.Oem.@odata.id	String	User-defined operation path for BIOS settings.
@Redfish.Settings.SettingsObject.@odata.id	String	Operation path for BIOS settings.

5.19 Querying Information About the BIOS Settings

Function

Query information about the current [BIOS](#) settings of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems/system_id/Bios/(SD|Settings)`
- Request Header:

X-Auth-Token: auth_value
- Request Message Body: None

Parameters

For a description of the parameters for querying information about the BIOS settings, refer to [Table 5-37](#).

Table 5-37 Parameter Descriptions for Querying Information About the BIOS Settings

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Systems/1/Bios/SD
- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234
- Request Message Body: None
- Response Example:

{
 "@odata.context": "/redfish/v1/\$metadata#Bios.Bios",
 "@odata.id": "/redfish/v1/Systems/1/Bios/SD",
 "@odata.type": "#Bios.v1_1_0.Bios",
 "Attributes": {
 "BootMode": "UEFI Only",
 }
}

```
    "C1E": "Disabled",
    "EIST": "Enabled",
    "EnergyPerformanceBIAS": "Balanced Performance",
    "HardwarePStates": "Native Mode",
    "HyperThreading": "Disabled",
    "MonitorMWAIT": "Enabled",
    "NUMA": "Enabled",
    "PackageCState": "C0/C1 state",
    "PowerPerformanceTuning": "OS controls EPB",
    "PowerPolicySelect": "Custom",
    "TurboMode": "Enabled"
  },
  "Description": "Future BIOS Settings",
  "Id": "SD",
  "Name": "Future BIOS Settings"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the BIOS settings, refer to [Table 5-38](#).

Table 5-38 Output Descriptions for Querying Information About the BIOS Settings

Field	Type	Description
@odata.context	String	OData description of the BIOS setting resource model.
@odata.id	String	Access path of the BIOS setting resource.
@odata.type	String	Type of BIOS setting resource.
Description	String	Description of the BIOS setting resource.
Id	String	ID of the BIOS setting resource.
Name	String	Name of the BIOS setting resource.
Attributes	Object	BIOS attribute.

5.20 Modifying the BIOS Settings

Function

Modify the [BIOS](#) settings.

Permission Required

User management.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/Systems/system_id/Bios/(SD|Settings)*
- Request Header:

```
X-Auth-Token: auth_value  
Content-Type: header_type
```

- Request Message Body:

```
{  
  "Attributes":{  
    "EIST": set_value,  
    "C1E": set_value,  
    ...  
  }  
}
```

Parameters

For details, refer to the BIOS configuration specifications.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Systems/1/Bios/SD
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234  
Content-Type: application/json
```

- Request Message Body:

```
{  
  "Attributes":  
  {  
    "EIST": "Disabled",
```

```
"C1E": "Enabled"
}
}
```

- Response Example: None
- Status Code: 204

Output Description

None

5.21 Setting the BIOS Password

Function

Set the [BIOS](#) password.

Permission Required

User management.

Syntax

- Operation Type: POST
- **URL:** *https://device_ip/redfish/v1/Systems/system_id/Bios/Actions/Bios.ChangePassword*
- Request Header:

```
X-Auth-Token: auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "PasswordName": password_name_value,
  "OldPassword": old_password_value,
  "NewPassword": new_password_value
}
```

Parameters

For a description of the parameters for setting the BIOS password, refer to [Table 5-39](#).

Table 5-39 Parameter Descriptions for Setting the BIOS Password

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.

Parameter	Description	Value
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
password_name_value	BIOS password type.	- AdministratorPassword - UserPassword
old_password_value	Current password.	Character string. If this parameter is set to "", it indicates that there is no password.
new_password_value	New password.	Character string. If this parameter is set to "", it indicates that the password is to be cleared.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Systems/1/Bios/Actions/Bios.ChangePassword
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body:

```
{
  "PasswordName": "AdministratorPassword",
  "OldPassword": "test",
  "NewPassword": ""
}
```

- Response Example: None
- Response Code: 204

Output Description

None

5.22 Restoring the Default BIOS Settings

Function

Restore the default BIOS settings.

Permission Required

User management.

Syntax

- Operation Type: POST
- **URL:** `https://device_ip/redfish/v1/Systems/system_id/Bios/Actions/Bios.ResetBios`
- Request Header:

```
X-Auth-Token: auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "ResetType": value
}
```

Parameters

For a description of the parameters for restoring the default BIOS settings, refer to [Table 5-40](#).

Table 5-40 Descriptions of BIOS Default Settings

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
value	Operation type.	Character string: ResetBios

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Systems/1/Bios/Actions/Bios.ResetBios
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body:

```
{
  "ResetType": "ResetBios"
}
```

- Response Example: None
- Response Code: 204

Output Description

None

5.23 Querying Information About the Ethernet Interface Resource Collection

Function

Query information about the Ethernet interface resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Systems/system_id/EthernetInterfaces`
- Request Header:

```
X-Auth-Token: auth_value
```

- Request Message Body: None

Description

For a description of the parameters for querying information about the Ethernet interface resource collection, refer to [Table 5-41](#).

Table 5-41 Parameter Descriptions for Querying Information About the Ethernet Interface Resource Collection

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/1/EthernetInterfaces
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#EthernetInterfaceCollection.EthernetInterfaceCollection",
  "@odata.id": "/redfish/v1/Systems/1/EthernetInterfaces",
  "@odata.type": "#EthernetInterfaceCollection.EthernetInterfaceCollection",
  "Description": "Collection of Ethernet Interfaces for this system",
  "Name": "System Ethernet Interface Collection",
  "Members@odata.count": 2,
  "Members": [
    {
      "@odata.id":
        "/redfish/v1/Systems/1/EthernetInterfaces/mainboardOCPCard1Port1"
    },
    {
      "@odata.id":
        "/redfish/v1/Systems/1/EthernetInterfaces/mainboardOCPCard1Port2"
    }
  ]
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the Ethernet interface resource collection, refer to [Table 5-42](#).

Table 5-42 Output Descriptions for Querying Information About the Ethernet Interface Resource Collection

Field	Type	Description
@odata.context	String	OData description of the Ethernet interface resource collection model.
@odata.id	String	Access path of the Ethernet interface resource collection.
@odata.type	String	Type of ISDT resource collection.
Description	String	Description of the Ethernet interface resource collection.
Name	String	Name of the Ethernet interface resource collection.
Members@odata.count	Number	Number of Ethernet interface resources.
Members	Array	List of Ethernet interface resources.
@odata.id	String	Access to a single Ethernet interface resource node.

5.24 Querying Information About a Specified Ethernet Interface Resource

Function

Query information about a specified Ethernet interface resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems/system_id/EthernetInterfaces/id`
- Request Header:

X-Auth-Token: auth_value
- Request Message Body: None

Description

For a description of the parameters for querying information about the specified Ethernet interface resource, refer to [Table 5-43](#).

Table 5-43 Parameter Descriptions for Querying Information About the Specified Ethernet Interface Resource

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
id	Network interface ID.	It can be obtained by querying information about the Ethernet interface resource collection.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/1/EthernetInterfaces/mainboardPCleCard1Port1
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#EthernetInterface.EthernetInterface",
  "@odata.id": "/redfish/v1/Systems/1/EthernetInterfaces/mainboardOCPCard1Port2",
  "@odata.type": "#EthernetInterface.v1_5_1.EthernetInterface",
  "AutoNeg": false,
  "Description": "NIC in Slot 1 Port 2",
  "FQDN": null,
  "FullDuplex": true,
  "HostName": null,
  "IPv4Addresses": [],
  "IPv4Addresses@odata.count": 0,
  "IPv6AddressPolicyTable": [],
```

```

    "IPv6AddressPolicyTable@odata.count": 0,
    "IPv6Addresses": [],
    "IPv6Addresses@odata.count": 0,
    "IPv6DefaultGateway": null,
    "IPv6StaticAddresses": [],
    "IPv6StaticAddresses@odata.count": 0,
    "Id": "mainboardOCPCard1Port2",
    "InterfaceEnabled": true,
    "LinkStatus": "LinkUp",
    "Links": {
      "Chassis": {
        "@odata.id": "/redfish/v1/Chassis/1"
      }
    },
    "MACAddress": "40:A6:B7:39:0B:50",
    "MTUSize": null,
    "MaxIPv6StaticAddresses": null,
    "Name": "System Ethernet Interface",
    "NameServers": [],
    "NameServers@odata.count": 0,
    "PermanentMACAddress": "40:A6:B7:39:0B:50",
    "SpeedMbps": 25000,
    "Status": {
      "Health": "OK",
      "State": "Enabled"
    },
    "VLAN": {}
  }

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified Ethernet interface resource, refer to [Table 5-44](#).

Table 5-44 Output Descriptions for Querying Information About the Specified Ethernet Interface Resource

Field	Type	Description
@odata.context	String	OData description of the specified Ethernet interface resource model.
@odata.id	String	Access path of the specified Ethernet interface resource.
@odata.type	String	Type of the specified Ethernet interface resource.

Field	Type	Description
AutoNeg	Boolean	Whether auto-negotiation is used.
Description	String	Position information about the Ethernet interface.
FQDN	String	FQDN of the BMC .
FullDuplex	Boolean	Whether full duplex mode is used.
HostName	String	Hostname.
IPv4Addresses	Array	IPv4 address.
IPv4Addresses@odata.count	Number	Number of IPv4 addresses.
IPv6AddressPolicyTable	Array	Table of policies for IPv6 address selection.
IPv6AddressPolicyTable@odata.count	Number	Number of ipv6 address selection policies in the table.
IPv6Addresses	Array	IPv6 address.
IPv6Addresses@odata.count	Number	Number of IPv6 addresses.
IPv6StaticAddresses	Array	Array of objects that represents the IPv6 static connection characteristics for this interface.
IPv6StaticAddresses@odata.count	Number	Number of arrays of objects that represents the IPv6 static connection characteristics for this interface.
IPv6DefaultGateway	String	Default IPv6 gateway address.
Id	String	Name of the Ethernet interface resource.
InterfaceEnabled	Boolean	Whether the network interface is enabled.
LinkStatus	String	Link status: ● Up ● Down
Links.Chassis.@odata.id	String	Access path referenced by the Chassis resource.
MACAddress	String	MAC address of the Ethernet interface.
MTUSize	String	MTU size of the network interface.
MaxIPv6StaticAddresses	Number	Maximum number of static IPv6 addresses that can be configured on this interface.
Name	String	Resource name.
NameServers	Array	DNS name server of the interface.
NameServers@odata.count	Number	Number of DNS name servers of the interface.
PermanentMACAddress	String	Permanent MAC address assigned to this interface.

Field	Type	Description
SpeedMbps	Number	Current speed.
Status.Health	String	Link quality. • OK • Critical • Warning
Status.State	String	Whether the Ethernet interface is enabled.
VLAN	Object	VLAN of the network interface.

5.25 Querying Information About the SimpleStorage Resource Collection

Function

Query information about the SimpleStorage resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems/system_id/SimpleStorage`
- Request Header:

X-Auth-Token: auth_valuex-auth-token:auth_value

- Request Message Body: None

Description

For a description of the parameters for querying information about the SimpleStorage resource collection, refer to [Table 5-45](#).

Table 5-45 Parameter Descriptions for Querying Information About the SimpleStorage Resource Collection

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Systems/1/SimpleStorage

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#SimpleStorageCollection.SimpleStorageCollection",
  "@odata.id": "/redfish/v1/Systems/1/SimpleStorage",
  "@odata.type": "#SimpleStorageCollection.SimpleStorageCollection",
  "Name": "Simple Storage Collection",
  "Members@odata.count": 2,
  "Members": [
    {
      "@odata.id": "redfish/v1/Systems/1/SimpleStorage/RAIDStorage1"
    },
    {
      "@odata.id": "redfish/v1/Systems/1/SimpleStorage/RAIDStorage2"
    }
  ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the SimpleStorage resource collection, refer to [Table 5-46](#).

Table 5-46 Output Descriptions for Querying Information About the SimpleStorage Resource Collection

Field	Type	Description
@odata.context	String	OData description of the SimpleStorage resource collection model.

Field	Type	Description
@odata.id	String	Access path of the SimpleStorage resource collection node.
@odata.type	String	Type of SimpleStorage resource collection.
Name	String	Name of the SimpleStorage resource collection.
Members@odata.count	Number	Number of SimpleStorage resources.
Members	Array	SimpleStorage resource list.
@odata.id	String	Access path of a single SimpleStorage resource node.

5.26 Querying Information About a Specified SimpleStorage Resource

Function

Query information about a specified SimpleStorage resource.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems/system_id/SimpleStorage/simplestorage_id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Description

For a description of the parameters for querying information about the specified SimpleStorage resource, refer to [Table 5-47](#).

Table 5-47 Parameter Descriptions for Querying Information About the Specified SimpleStorage Resource

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_id	ID of the System resource.	For a rack server, the value is 1 or Self .

Parameter	Setting	Value
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
simplestorage_id	ID of the SimpleStorage resource.	It can be obtained by querying information about the SimpleStorage resource collection.

Usage Guideline

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/1/SimpleStorage/RAIDStorage10
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#SimpleStorage.SimpleStorage",
  "@odata.id": "/redfish/v1/Systems/1/SimpleStorage/RAIDStorage10",
  "@odata.type": "#SimpleStorage.v1_3_1.SimpleStorage",
  "Name": "Simple Storage",
  "Id": "RAIDStorage10",
  "Devices": [
    {
      "CapacityBytes": 1920383410176,
      "Manufacturer": "xxx",
      "Model": "xxx",
      "Name": "Disk52",
      "Status": {
        "State": "Enabled",
        "Health": "OK"
      }
    },
    {
      "CapacityBytes": 1919850381312,
      "Manufacturer": "xxx",
      "Model": "xxx",

```



```

        "Name": "Disk53",
        "Status": {
            "State": "Enabled",
            "Health": "OK"
        }
    }
]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified SimpleStorage resource, refer to [Table 5-48](#).

Table 5-48 Output Descriptions for Querying Information About the Specified SimpleStorage Resource

Field	Type	Description
@odata.context	String	OData description of the SimpleStorage resource model.
@odata.id	String	Access path of the SimpleStorage resource node.
@odata.type	String	Type of the specified SimpleStorage resource.
Id	String	ID of the specified SimpleStorage resource.
Name	String	Name of the specified SimpleStorage resource.
Devices	Array	Hard disk resource list.
CapacityBytes	Number	Capacity of a hard disk.
Manufacturer	String	Manufacturer of a hard disk.
Model	String	Model of a hard disk.
Name	String	Name of a hard disk.
Status	Object	Hard disk status, including: ● State: Hard disk enabling status ● Health: Hard disk health status

Chapter 6

Operations on Chassis Resources

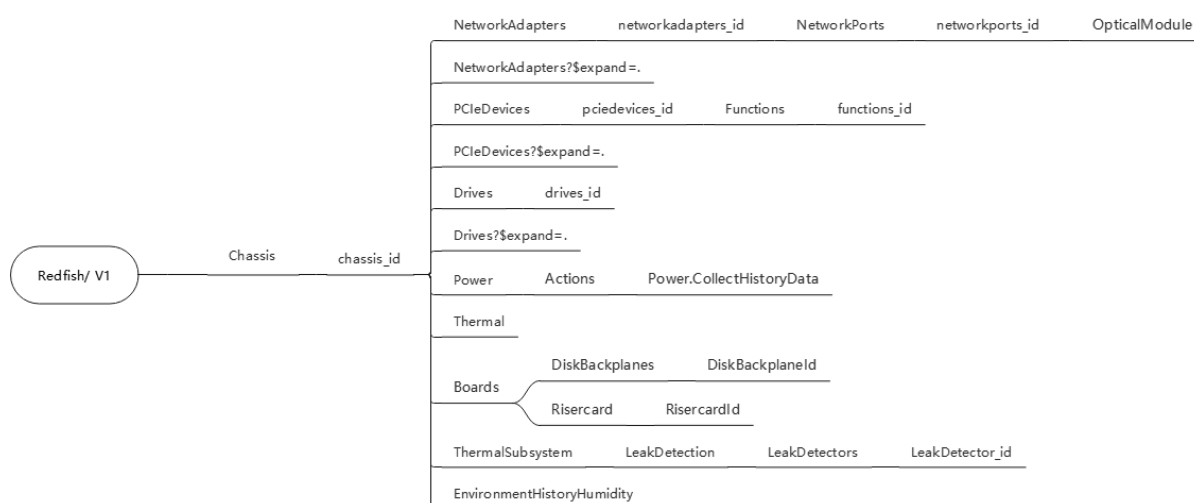
Table of Contents

Querying Information About the Chassis Resource Collection	331
Querying Information About a Specified Chassis Resource	333
Modifying the Position Indicator Status of a Chassis	338
Querying Information About the Network Adapter Resource Collection	340
Querying Information About a Specified Network Adapter Resource	342
Querying Information About All Network Adapter Resources	348
Querying Information About a Specified Network Port Resource	355
Querying Information About the Optical Module Resource Connected to a Network Port	359
Modifying the LLDP Switch of a Specified Network Port	363
Querying Information About the PCIe Device Resource Collection	367
Querying Information About a Specified PCIe Device Resource	369
Querying Information About All PCIe Device Resources	376
Querying Information About the Drive Resource Collection	382
Querying Information About a Specified Drive Resource	384
Querying Information About All Drive Resources	389
Querying the Power Supply Information About a Specified Chassis	392
Collecting Information About Power Statistics	401
Modifying Properties of a Specified Power Supply	403
Querying Cooling Resource Information About a Specified Chassis	415
Querying Information About the Expansion Board Resource Collection	423
Querying Information About the Hard Disk Backplane Resource Collection	425
Querying Information About a Specified Hard Disk Backplane Resource	427
Querying Information About the Riser Card Resource Collection	430
Querying Information About a Specified Riser Card Resource	432
Modifying the Cooling Resource Information About a Specified Chassis	433
Querying Information About a Specified PCIe Device Function Resource	443
Querying Information About the Collection of Leak Detection Device Resources	446

Querying Information About the Leak Detector Resource Collection	448
Querying Information About a Specified Leak Detector.....	450
Modifying Information About a Specified Drive Resource	452
Querying Information About the Network Port Resource Collection of a Specified Network Adapter.....	454
Querying Historical Environmental Humidity Information About a Chassis.....	456

Figure 6-1 shows the path requirements for the Chassis resources supported by VANTAGEO servers.

Figure 6-1 Chassis Resource Path Requirements



For a description of properties of Chassis resources and operations supported by the properties, refer to [Table 6-1](#).

Table 6-1 Descriptions of Chassis Resources Properties

URL	Property	Description	Operation
/redfish/v1/Chassis	Description	Description of the Chassis resource collection.	GET
	Name	Name of the Chassis resource collection.	GET
	Members@odata.count	Number of Chassis resource members.	GET
	Members	Access path of the specified Chassis resource node.	GET
/redfish/v1/Chassis/chassis_id	Id	ID of the specified Chassis resource. The ID is the unique identifier of the chassis in the chassis collection.	GET
	Name	Name of the specified Chassis resource.	GET

URL	Property	Description	Operation
	Manufacturer	Manufacturer information about the Chassis.	GET
	PartNumber	Part number of the Chassis.	GET
	Model	Model of the Chassis.	GET
	AssetTag	Asset tag of the Chassis.	GET
	IndicatorLED	Position indicator status of the Chassis resource.	GET/PATCH
	IndicatorLED@Redfish.AllowableValues	Position indicator state range of the specified chassis resource.	GET
	Status	Status of the specified System resource.	GET
	PowerState	Power-on status of the specified system resource.	GET
	Oem.Public	Vendor-defined attribute.	GET
	DeviceMaxNum	Maximum number of board parts.	GET
	CPU Num	Maximum number of CPUs.	GET
	DiskNum	Maximum number of hard disks.	GET
	FanNum	Maximum number of fans.	GET
	MemoryNum	Maximum number of memory modules.	GET
	PCIeNum	Maximum number of PCIe cards.	GET
	PowerSupplyNum	Maximum number of power supplies.	GET
	Mainboard	Mainboard information.	GET
	BoardName	Mainboard name.	GET
	SerialNumber	Serial number of the mainboard.	GET
	PartNumbe	Part number of the board.	GET
	BoardDate	Manufacturing date of the board.	GET
	ProductSpecificIdentity	Internally defined product name.	GET
	Links	Links related to the chassis resource.	GET
	ComputerSystems	Link to system resources.	GET
	ManagedBy	Link to Manager resources.	GET

URL	Property	Description	Operation
	PCleDevices	Navigation of the PCIe device resources.	GET
	Drives	Navigation of the drive resources.	GET
	NetworkAdapters	Information about the related network adapters.	GET
	Power	Information about the related power supplies.	GET
	Thermal	Chassis cooling resource information.	GET
	Boards	Board-level resource links.	GET
	SerialNumber	Serial number of the chassis.	GET
	ProductName	Product name.	GET
	BoardProductVer	Board product version number.	GET
	PartNumber	Material code.	GET
	ChassisHeight	Chassis size.	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters	Description	Description the network adapter resource collection.	GET
	Name	Name of the network adapter resource.	GET
	Members@odata.count	Number of network adapter resource members.	GET
	Members	List of network adapter resources.	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id	Id	ID of the specified network adapter resource.	GET
	Name	Name of the specified network adapter resource.	GET
	NetworkPorts	List of network port resources.	GET
	Manufacturer	Manufacturer of the specified network adapter.	GET
	Model	Model the specified network adapter.	GET
	Controllers	Controllers of the specified network adapter.	GET

URL	Property	Description	Operation
	FirmwarePackageVersion	Firmware version of the specified network adapter.	GET
	Links	Links to the related resources.	GET
	NetworkPorts	Network port resource description.	GET
	@odata.id	Access path of the network port resource collection.	GET
	NetworkPorts@odata.count	Number of network port resources.	GET
	Oem.Public	Vendor-defined attribute.	GET
	CardManufacturer	Manufacturer of the specified network adapter.	GET
	Name	Name of the specified network adapter.	GET
	CardModel	Interface mode of the specified network adapter.	GET
	CardType	Type of the specified network adapter.	GET
	NicCardType	NIC interface type of the specified network adapter. Common cards and smart cards are distinguished.	GET
	CurrentPower	NIC power of the specified network adapter.	GET
	CardCelsius	NIC temperature of the specified network adapter.	GET
	DriverVersion	Driver version of the specified network adapter.	GET
	NetworkTechnology	Network protocol of the specified network adapter.	GET
	DeviceLocator	Silk screen of the specified network adapter.	GET
	SlotNumber	Slot number of the specified network adapter.	GET
	RootBDF	Root port BDF of the specified network adapter.	GET

URL	Property	Description	Operation
	AlarmTmp	Alarm temperature of the specified network adapter. The setting cannot be queried. By default, null is displayed.	GET
	CurrentTmp	Temperature of the main chip of the specified network adapter. The setting cannot be queried. By default, null is displayed.	GET
	FpgaStatus	FPGA status of the specified network adapter. This field is displayed only for an FPGA card.	GET
	HistoryMaxTmp	Maximum historical temperature of the specified network adapter in the historical process. This field is displayed only for an FPGA card.	GET
	NicMemory	Memory information about the specified network adapter. This field is displayed only for an FPGA card.	GET
	CapacityGb	Memory capacity of the specified network adapter. This field is displayed only for an FPGA card.	GET
	Model	Memory model of the specified network adapter. The default value is DDR4_2400MHz. This field is displayed only for an FPGA card.	GET
	Status	Memory status of the specified network adapter. This field is displayed only for an FPGA card.	GET
	Status	Status of the specified network adapter, including: ● Health: health status ● State: enabling status	GET
	SerialNumber	Serial number of the specified network adapter.	GET
redfish/v1/Chassis/chassis_id/NetworkAdapters?	Name	Name of the network adapter resource collection.	GET

URL	Property	Description	Operation
	Members@odata.count	Number of network adapter resources.	GET
	Members	Network adapter resource information.	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapteras_id/NetworkPorts/networkports_id	Id	UID of the specified network port resource in the iBMC system.	GET/PATCH
	Name	Name of the specified network port resource.	GET/PATCH
	AutoNeg	Negotiation Mode	GET/PATCH
	LinkStatus	Status of the specified network port.	GET/PATCH
	AssociatedNetworkAddresses	Network address of the specified network port.	GET/PATCH
	Oem.Public	Vendor-defined attribute.	GET/PATCH
	PortMaxSpeed	Network port rate of the specified network port, unit: Mb/s.	GET/PATCH
	PortType	Type of the specified network port.	GET/PATCH
	BDF	Root port BDF of the specified network port.	GET/PATCH
	CurrentSpeed	Current speed.	GET/PATCH
	DriverVersion	Driver version of the specified network port.	GET/PATCH
	FirmwarePackageVersion	Firmware version of the specified network port.	GET/PATCH
	LldpService	LLDP -related properties.	GET/PATCH
	LldpEnable	Whether LLDP is enabled for the specified network port.	GET/PATCH
	ServiceEnabled	Whether the specified network port supports LLDP information query.	GET
	WorkMode	Operational mode of LLDP.	GET/PATCH
	SupportSpeed	Supported speed of the specified network port.	GET/PATCH
	OpticalModule	Optical module resource connected to the specified network port.	GET

URL	Property	Description	Operation
	PhysicalPortNumber	Physical silk screen of the specified network port.	GET/PATCH
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapteras_id/NetworkPorts/networkports_id/OpticalModule	Id	ID of the optical module resource.	GET
	Name	Name of the optical module resource.	GET
	Status	Status of the optical module resource. ● State: whether the optical module is enabled.	GET
	Manufacturer	Optical module manufacturer name.	GET
	PartNumber	Part number of the optical module.	GET
	SerialNumber	Serial number of the optical module.	GET
	ProductionDate	Production date of the optical module.	GET
	WaveLengthNanometer	Wavelength of the optical module.	GET
	BR_Nominal	Nominal bit rate of the optical module.	GET
	Voltage	Voltage of the optical module.	GET
	ReadingVolts	Current voltage reading of the optical module.	GET
	LowerThresholdCritical	Critical alarm threshold for undervoltage.	GET
	UpperThresholdCritical	Critical alarm threshold for overvoltage.	GET
	RXPower	Receive power of the optical module.	GET
	ReadingMilliWatts	Current receive power reading of the optical module.	GET
	LowerThresholdCritical	Critical alarm threshold for too low receive power.	GET
	UpperThresholdCritical	Critical alarm threshold for too high receive power.	GET
	TXPower	Transmit power information about the optical module.	GET

URL	Property	Description	Operation
	ReadingMilliWatts	Current transmit power reading of the optical module.	GET
	LowerThresholdCritical	Critical alarm threshold for too low transmit power.	GET
	UpperThresholdCritical	Critical alarm threshold for too high transmit power.	GET
	TXBiasCurrent	Transmit bias current of the optical module.	GET
	ReadingMilliAmperes	Current bias current reading of the optical module.	GET
	LowerThresholdCritical	Critical alarm threshold for too low bias current.	GET
	UpperThresholdCritical	Critical alarm threshold for too high bias current.	GET
	Temperature	Temperature of the optical module.	GET
	ReadingCelsius	Current temperature reading of the optical module.	GET
	LowerThresholdCritical	Critical alarm threshold for too low temperature.	GET
	UpperThresholdCritical	Critical alarm threshold for too high temperature.	GET
/redfish/v1/Chassis/chassis_id/PCleDevices	Description	Description of the PCle device resource collection.	GET
	Name	Name of the PCle device resource collection.	GET
	Members@odata.count	Number of PCIe device resource members.	GET
	Members	Access path of the specified PCIe device resource node.	GET
/redfish/v1/Chassis/chassis_id/PCleDevices/pcidevices_id	CardManufacturer	PCIe device manufacturer, which is the same as the CardManufacturer value of the storage controller and NIC.	GET
	CardModel	PCIe device model, which is the same as the CardModel of the stor-	GET

URL	Property	Description	Operation
		age controller and the Oem.Public.Name of the NIC.	
	Name	Name of the specified PCIe device resource.	GET
	Id	ID of the specified PCIe device resource.	GET
	Description	Description of the specified PCIe device resource.	GET
	Manufacturer	Manufacturer of the specified PCIe device resource.	GET
	Model	Model of the specified PCIe device resource.	GET
	Links	Resources links.	GET
	FirmwareVersion	Version number of the specified PCIe device.	GET
	SerialNumber	Serial number of the specified PCIe device.	GET
	Status	Status of the specified PCIe device resource.	GET
	PCIeInterface	Interface information about the specified PCIe device.	GET
	LanesInUse	Number of currently negotiated PCIe lanes of the specified PCIe device.	GET
	MaxLanes	Maximum number of PCIe lanes supported by the specified PCIe device.	GET
	Oem.Public	-	GET
	LinkSpeed	Current link speed of the specified PCIe device, unit: GT/s.	GET
	MaxLinkSpeed	Maximum link speed supported by the specified PCIe device, unit: GT/s.	GET
	DeviceBDF	Device BDF of the specified PCIe device.	GET
	DeviceLocator	Silk screen of the specified PCIe device.	GET

URL	Property	Description	Operation
	MemorySizeMiB	Total memory capacity of the specified PCIe device.	GET
	MemoryBandWidth	Bandwidth of the display memory data of the specified GPU or NPU when PCIeCardType is GPU or NPU, unit: GB/s.	GET
	PowerCapacityWatts	Maximum Thermal Design Power (TDP) of the specified GPU.	GET
	PowerConsumedWatts	Actual power consumed by the specified GPU.	GET
	ReadingCelsius	Actual temperature of the specified GPU.	GET
	PCleCardType	Type of the specified PCIe device.	GET
	PowerWatts	Power of the specified PCIe device.	GET
	RootPortBDF	Root port BFD of the specified PCIe device.	GET
	SlotNumber	Slot number of the specified PCIe device.	GET
	Oem.Public.GpuCore	-	GET
	BuildTime	Production date of memory of the specified PCIe device.	GET
	CapacityGB	Memory capacity of the specified PCIe device.	GET
	MemberId	Index of memory of the specified PCIe device.	GET
	PartNum	Part number of memory of the specified PCIe device.	GET
	Power	Power of the specified PCIe device.	GET
	Temperature	Temperature of the specified PCIe device.	GET
	Oem.Public.NVMeAIC	-	GET
	CapacityGB	Storage capacity of the specified PCIe device.	GET

URL	Property	Description	Operation
	iskTemperatureCelsius	Temperature of the specified PCIe device.	GET
	MediaType	Media type of the specified PCIe device.	GET
	PredictedMediaLifeLeftPercent	Remaining lifetime of the specified PCIe device.	GET
	Interface	Interface type of the specified PCIe device.	GET
	CapacityBytes	Capacity of the specified PCIe device, unit: bytes.	GET
	HealthStatus	Health status of the specified PCIe device.	GET
	Model	Model of the specified PCIe device.	GET
	Vendor	Manufacturer of specified PCIe device.	GET
	SerialNumber	Serial number of the specified PCIe device.	GET
/redfish/v1/Chassis/chassis_id/PCleDevices?\$expand=.	Description	Description of the PCIe device resource collection.	GET
	Name	Name of the PCIe device resource collection.	GET
	Members@odata.count	Number of PCIe device resources.	GET
	Members	PCIe device resources.	GET
/redfish/v1/Chassis/chassis_id/Drives	Name	Name of the drive resource collection.	GET
	Members@odata.count	Number of drive resource members.	GET
	Members	Access path of the specified drive resource node.	GET
/redfish/v1/Chassis/chassis_id/Drives/drives_id	Id	ID of the specified drive resource.	GET
	Name	Name of the specified drive resource.	GET
	Model	Model of the specified drive.	GET
	Revision	Version information about the specified drive.	GET

URL	Property	Description	Operation
	Status	Status of the specified drive.	GET
	CapableSpeedGbs	Maximum speed of the interface of the specified drive.	GET
	NegotiatedSpeedGbs	Negotiated speed of the interface of the specified drive.	GET
	Oem.Public	-	GET
	TemperatureCelsius	Temperature unit (Celsius) of the specified drive.	GET
	BackpanelId	Backplane ID of the specified drive.	GET
	BackPanelLocation	Backplane position of the specified drive.	GET
	SASAddress	-	GET
	CapacityBytes	Capacity of the specified drive, in bytes.	GET
	FailurePredicted	Whether a failure is predicted by the specified drive.	GET
	HotspareType	Hotspare status of the specified drive.	GET
	Protocol	Compliant protocol of the specified drive.	GET
	MediaType	Media type of the specified drive.	GET
	Manufacturer	Manufacturer of the specified drive.	GET
	PredictedMediaLifeLeftPercent	Percentage of the remaining service life of the specified drive.	GET
	SerialNumber	Serial number of the specified drive.	GET
	PartNumber	Part number of the specified drive.	GET
	SlotNumber	Slot number of the hard disk.	GET
	IndicatorLED	Position indicator status of the specified drive.	GET
	Location	Screen printing of the specified drive.	GET
	Info	Silk screen of the specified drive.	GET
	InfoFormat	Silk screen format of the specified drive.	GET

URL	Property	Description	Operation
	RotationSpeedRPM	Rotation speed of the specified drive, unit: RPM.	GET
	BelongCPU	Controller CPU of the specified drive.	GET
	ControllerBDF	Controller BDF of the specified drive.	GET
	ControllerPortNum	Controller port number of the specified drive.	GET
/redfish/v1/Chassis/chassis_id/Drives?\$expand=.	Name	Name of the drive resource collection.	GET
	Members@odata.count	Number of drive resources.	GET
	Members	All drive resources.	GET
/redfish/v1/Chassis/Chassis_id/Power	Description	Description.	GET
	Id	ID of the power resource.	GET/PATCH
	Name	Name of the power resource.	GET
	PowerControl	Power control list.	GET
	Name	Name of the specified power control.	GET/PATCH
	MemberId	ID of the power control. The ID is the unique identifier of the power control in the power control list.	GET/PATCH
	PowerLimit	Power capping setting.	GET/PATCH
	LimitInWatts	Server power limit.	GET/PATCH
	PowerLimitEnable	Whether power capping is enabled.	GET/PATCH
	LimitException	Action to be taken when the power capping becomes invalid.	GET/PATCH
	PowerConsumedWatts	Current power of the device.	GET/PATCH
	Oem.Public	Customized properties.	GET/PATCH
	ExpectedActivePSU	Expected active PSU list.	GET/PATCH
	CurrentCPUPowerWatts	Current power consumption of the CPUs.	GET/PATCH
	CurrentFanPowerWatts	Current power consumption of the fans.	GET/PATCH
	CurrentMemoryPowerWatts	Current power consumption of the memory.	GET/PATCH

URL	Property	Description	Operation
	CurrentHDDPowerWatts	Current power consumption of the hard disks.	GET/PATCH
	PowerSupplies	Power module list. The power modules in the list are displayed no matter whether they are present or not. Status is used for indicating the current status of a power module.	GET/PATCH
	FirmwareVersion	Firmware version of the specified power supply.	GET/PATCH
	LineInputVoltage	Input voltage of the specified power supply.	GET/PATCH
	Manufacturer	Manufacturer of the specified power supply.	GET/PATCH
	Model	Model of the specified power supply.	GET/PATCH
	Name	Name of the specified power control.	GET/PATCH
	PowerCapacityWatts	Rated power of the specified power supply.	GET/PATCH
	PowerInputWatts	Input power of the specified power supply.	GET/PATCH
	PowerOutputWatts	Output power of the specified power supply.	GET/PATCH
	PowerSupplyType	Type of the specified power supply.	GET/PATCH
	ProductionDate	Production date of the specified power module.	GET
	SerialNumber	Serial number of the specified power supply.	GET/PATCH
	Status	Power supply status.	GET/PATCH
	Oem.Public	Customized properties.	GET/PATCH
	ActiveStandby	Active or standby power supply mode.	GET/PATCH
	SlotNumber	Slot number of the specified power supply.	GET/PATCH

URL	Property	Description	Operation
	MemberId	ID of the specified power supply. The ID is the unique identifier of the power supply in the power supply list.	GET/PATCH
	PowerSupplies@odata.count	Number of power supplies.	GET/PATCH
	Voltages	Voltage sensor list.	GET/PATCH
	LowerThresholdCritical	Critical warning threshold for low voltage of the specified voltage sensor.	GET/PATCH
	LowerThresholdFatal	Fatal warning threshold for low voltage of the specified voltage sensor.	GET/PATCH
	LowerThresholdNonCritical	Noncritical warning threshold for low voltage of the specified voltage sensor.	GET/PATCH
	MaxReadingRange	Maximum voltage reading for the specified voltage sensor.	GET/PATCH
	MinReadingRange	Minimum voltage reading for the specified voltage sensor.	GET/PATCH
	Name	Name of the specified voltage sensor.	GET/PATCH
	SensorNumber	Serial number of the specified voltage sensor.	GET/PATCH
	Status	Status of the specified voltage sensor.	GET/PATCH
	ReadingVolts	Current reading of the specified voltage sensor.	GET/PATCH
	UpperThresholdCritical	Critical warning threshold for high voltage of the specified voltage sensor.	GET/PATCH
	UpperThresholdFatal	Fatal warning threshold for high voltage of the specified voltage sensor.	GET/PATCH
	LowerThresholdNonCritical	Noncritical warning threshold for high voltage of the specified voltage sensor.	GET
	Redundancy	Power redundancy group list.	GET/PATCH

URL	Property	Description	Operation
	Name	Name of the specified power redundancy group.	GET/PATCH
	Mode	Redundancy mode of the specified power redundancy group.	GET/PATCH
	Actions	Available actions for power supplies.	GET
	#Power.CollectHistoryData	Collects historical power statistics.	GET
/redfish/v1/Chassis/Chassis_id/Thermal	Description	Description of the cooling resource.	GET
	Id	ID of the cooling resource.	GET
	Name	Name of the cooling resource.	GET
	Oem.Public	Customized information about the cooling resource.	GET/PATCH
	FanSpeedAdjustmentMode	Fan speed adjustment mode.	GET/PATCH
	FanSmartCoolingMode	Fan speed smart adjustment mode.	GET/PATCH
	SpeedRatio	Fan rotation speed ratio.	GET/PATCH
	Temperatures	Temperature sensor list.	GET/PATCH
	LowerThresholdCritical	Critical warning threshold for low speed rotation of the specified fan sensor.	GET/PATCH
	LowerThresholdFatal	Fatal warning threshold for low speed rotation of the specified fan sensor.	GET/PATCH
	LowerThresholdNonCritical	Noncritical warning threshold for low speed rotation of the specified fan sensor.	GET/PATCH
	MemberId	ID of the specified temperature sensor.	GET/PATCH
	Name	Name of the specified temperature sensor.	GET/PATCH
	PhysicalContext	Area or device used for temperature measurement.	GET/PATCH
	ReadingCelsius	Current reading of the specified temperature sensor.	GET/PATCH
	SensorNumber	Serial number of the specified temperature sensor.	GET/PATCH

URL	Property	Description	Operation
	Status	Status of the specified fan sensor.	GET/PATCH
	UpperThresholdCritical	Critical warning threshold for high temperature of the specified temperature sensor.	GET/PATCH
	UpperThresholdFatal	Fatal warning threshold for high temperature of the specified temperature sensor.	GET/PATCH
	UpperThresholdNonCritical	Noncritical warning threshold for high temperature of the specified temperature sensor.	GET/PATCH
	MinReadingRangeTemp	Minimum temperature reading for the specified temperature sensor.	GET/PATCH
	MaxReadingRangeTemp	Maximum temperature reading for the specified temperature sensor.	GET/PATCH
	FanSummary	Information about the specified fan sensors.	GET/PATCH
	Count	Number of fan sensors.	GET/PATCH
	Fans	Fan sensor list.	GET/PATCH
	Name	Name of the specified fan sensor.	GET
	Status	Status of the specified fan sensor.	GET/PATCH
	MemberId	ID of the specified fan sensor.	GET/PATCH
	ReadingUnits	Unit of the fan rotation speed reading for the fan sensor, including: RPM and Percent.	GET/PATCH
	Oem.Public	Customized information about the cooling resource.	GET
	SlotNumber	Slot number of the specified fan sensor.	GET
	FanName	Name of the fan that the specified fan sensor belongs to.	GET/PATCH
	MinReadingRange	Minimum rotation speed reading for the specified fan sensor.	GET/PATCH
	MaxReadingRange	Maximum rotation speed reading for the specified fan sensor.	GET/PATCH

URL	Property	Description	Operation
	Reading	Current reading of the specified fan sensor.	GET/PATCH
	Model	Model of the specified fan sensor.	GET
/redfish/v1/Chassis/chassis_id/Boards	Description	Description of the expansion board resource collection.	GET
	DiskBackplanes	Information about hard disk backplanes.	GET
	Risercard	Information about riser cards.	GET
	Id	ID of the expansion board resource collection.	GET
	Name	Name of the expansion board resource collection.	GET
/redfish/v1/Chassis/Chassis_id/Boards/DiskBackplanes	Name	Name of the hard disk backplane resource collection.	GET
	Members@odata.count	Number of hard disk backplane resources.	GET
/redfish/v1/Chassis/Chassis_id/Boards/DiskBackplanes/DiskBackplaneId	Name	Name of the hard disk backplane resource collection.	GET
	CPLDVersion	CPLD version of the specified hard disk backplane.	GET
	MaxDiskCountSupported	Maximum number of hard disks supported by the specified hard disk backplane resource.	GET
	PartNumber	Part number of the specified hard disk backplane resource.	GET
	Location	Location of the specified hard disk backplane.	GET
	Manufacturer	Manufacturer of the specified hard disk backplane resource.	GET
	OnlineDiskCount	Number of present hard disks supported by the specified hard disk backplane resource.	GET
	ID	Serial number of the specified hard disk backplane resource.	GET

URL	Property	Description	Operation
	PcbID	PCB ID of the specified hard disk backplane.	GET
/redfish/v1/Chassis/Chassis_id/Boards/Risercard	Description	Description of the riser card resource collection.	GET
	Name	Name of the riser card resource collection.	GET
	Members	List of riser card resources.	GET
/redfish/v1/Chassis/Chassis_id/Boards/Risercard/RisercardId	Manufacturer	Manufacturer of the specified riser card resource.	GET
	Name	Name of the specified riser card resource.	GET
	PartNumber	Part number of the specified riser card resource.	GET
	SerialNumber	Serial number of the specified riser card resource.	GET
/redfish/v1/Chassis/chassis_id/PCleDevices/pcidevices_id/Functions/functions_	DeviceClass	Class of the specified PCIe device function resource.	GET
	DeviceId	DID of the specified PCIe device.	GET
	Id	UID of the specified PCIe device function resource in the iBMC system.	GET
	Links	Links to the related resources.	GET
	PCleDevice	PCIe device resource list.	GET
	Name	Name of the specified PCIe device function resource.	GET
	Oem	Customized properties.	GET
	Public	Customized properties.	GET
	AssociatedResource	Associated resource of the specified PCIe device function resource.	GET
	BusNumber	Bus number of the specified PCIe device root port.	GET
	DeviceNumber	Device number of the specified PCIe device root port.	GET

URL	Property	Description	Operation
	FunctionNumber	Function number of the specified PCIe device root port.	GET
	SubsystemId	SDID of the specified PCIe device root port.	GET
	SubsystemVendorId	SVID of the specified PCIe device root port.	GET
	VendorId	VID of the specified PCIe device root port.	GET
/redfish/v1/Chassis/chassis_id/ThermalSubsystem/LeakDetection	Id	ID of the collection of leak detection device resources.	GET
	Name	Name of the collection of leak detection device resources.	GET
	LeakDetectors	Collection of leak detectors.	GET
redfish/v1/Chassis/chassis_id/ThermalSubsystem/LeakDetection/LeakDetectors	Name	Name of the leak detector resource collection.	GET
	Members@odata.count	Number of leak detector resources.	GET
	Members	List of leak detector resources.	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapter_s_id/NetworkPorts	Name	Name of the network port resource collection of the specified network adapter.	GET
	Description	Description of the network port resource collection of the specified network adapter.	GET
	Members	Members of the network port resource collection.	GET
	Members@odata.count	Number of network port resources.	GET
/redfish/v1/Chassis/chassis_id/EnvironmentHistoryHumidity	Id	ID of the historical environmental humidity information about the specified chassis.	GET
	Name	Name of the historical environmental humidity information about the specified chassis.	GET
	Description	Description of the historical environmental humidity information about the specified chassis.	GET

URL	Property	Description	Operation
	Data	Data array of the historical environmental humidity information about the specified chassis.	GET
	Time	Humidity information collection time.	GET
	HumidityPercent	Humidity value.	GET

6.1 Querying Information About the Chassis Resource Collection

Function

Query information about the current Chassis resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the Chassis resource collection, refer to [Table 6-2](#).

Table 6-2 Parameter Descriptions for Querying Information About the Chassis Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis
```

- Request Header:

```
x-auth-token:QnaWfqvKOY0ZGc2LK5Ay6+CaSYWjEYcxE6GcWKNFyjU=
```

- Request Message Body: None

- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#ChassisCollection.ChassisCollection",
  "@odata.id": "/redfish/v1/Chassis",
  "@odata.type": "#ChassisCollection.ChassisCollection",
  "Description": "The Collection for Chassis",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Chassis/1"
    }
  ],
  "Members@odata.count": 1,
  "Name": "Chassis Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the Chassis resource collection, refer to [Table 6-3](#).

Table 6-3 Output Descriptions for Querying Information About the Chassis Resource Collection

Field	Type	Description
@odata.context	String	OData description of the chassis resource collection model.
@odata.id	String	Access path of the Chassis resource collection.
@odata.type	String	Type of Chassis resource collection.
Description	String	Description of the Chassis resource collection.
Name	String	Name of the Chassis resource collection.
Members@odata.count	Number	Number of Chassis resource members.

Field	Type	Description
Members	Array	Chassis resource list.
@odata.id	String	Access path of a single Chassis resource node.

6.2 Querying Information About a Specified Chassis Resource

Function

Query information about the specified Chassis resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified Chassis resource, refer to [Table 6-4](#).

Table 6-4 Parameter Descriptions for Querying Information About the Specified Chassis Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
chassis_id	ID of the Chassis resource.	• For a rack server, the value is 1 or Self. • For a high-density server, the value is BladeN (where N indicates slot number of the node), for example, "Blade1". • For a blade server, the value is BladeN (where N indicates the slot number of the computing node) or SwiN (where N

Parameter	Description	Value
		indicates the slot number of the switching module), for example, "Swi1".

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1
```

- Request Header:

```
x-auth-token:QnaWfqvKOY0ZGc2LK5Ay6+CaSYWjEYcxE6GcWKNFyjU=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Chassis.Chassis",
  "@odata.id": "/redfish/v1/Chassis/1",
  "@odata.type": "#Chassis.v1_14_0.Chassis",
  "AssetTag": "1234",
  "ChassisType": "RackMount",
  "Description": "Chassis Self",
  "Drives": {
    "@odata.id": "/redfish/v1/Chassis/1/Drives"
  },
  "Id": "1",
  "IndicatorLED": "Blinking",
  "IndicatorLED@Redfish.AllowableValues": [
    "Lit",
    "Blinking",
    "off"
  ],
  "Links": {
    "ComputerSystems": [
      {
        "@odata.id": "/redfish/v1/Systems/1"
      }
    ],
    "ManagedBy": [
      {
        "@odata.id": "/redfish/v1/Managers/1"
      }
    ]
  }
}
```

```

    }
  ]
},
"Manufacturer": "VANTAGEO",
"Model": "2240-RE",
"Name": "Computer System Chassis",
"NetworkAdapters": {
  "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters"
},
"Oem": {
  "Public": {
    "DeviceMaxNum": {
      "CPUNum": 2,
      "DiskNum": 25,
      "FanNum": 12,
      "MemoryNum": 32,
      "PCIeNum": 32,
      "PowerSupplyNum": 4
    },
    "ProductName": "a6",
    "BoardProductVer": null,
    "PartNumber": null,
    "Mainboard": {
      "Manufacturer": "VANTAGEO",
      "BoardName": "VANTAGEO",
      "SerialNumber": "749973700038",
      "PartNumber": "21080102",
      "BoardDate": "Tue Jan 10 09:00:00 2023"
    },
    "ProductSpecificIdentity": "4440-RE,Intel",
    "ChassisHeight": "4U",
    "OverallHealthStatus": "Major",
    "Boards": {
      "@odata.id": "/redfish/v1/Chassis/1/Boards"
    }
  }
},
"PCIeDevices": {
  "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices"
},
"PartNumber": "NULL",
"PhysicalSecurity": {
  "IntrusionSensor": "HardwareIntrusion"
},

```

```

    "Power": {
        "@odata.id": "/redfish/v1/Chassis/1/Power"
    },
    "PowerState": "On",
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "Thermal": {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal"
    },
    "SerialNumber": null
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified Chassis resource, refer to [Table 6-5](#).

Table 6-5 Output Descriptions for Querying Information About the Specified Chassis Resource

Field	Type	Description
@odata.context	String	OData description of the specified Chassis resource model.
@odata.id	String	Access path of the specified Chassis resource.
@odata.type	String	Type of the specified Chassis resource.
Id	String	ID of the specified Chassis resource.
Name	String	Name of the specified Chassis resource.
Manufacturer	String	Manufacturer information about the Chassis.
PartNumber	String	Part number of the Chassis.
Model	String	Model of the Chassis.
AssetTag	String	Asset tag of the Chassis.
ChassisType	String	Chassis type.
Description	String	Description of the specified chassis resource.
IndicatorLED	String	Position indicator status of the specified Chassis resource, including: ● Lit ● Blinking

Field	Type	Description
		Off
IndicatorLED@Redfish.AllowableValues	Array	Position indicator status range of the specified Chassis resource.
Status	Object	Status of the specified Chassis resource, including: - State: whether the Chassis is enabled - Health: health status of the Chassis
PowerState	String	The power-on status of the specified System resource, including - On - Off
Oem.Public	Object	Manufacturer-customized properties.
Oem.Public.DeviceMaxNum	Object	Maximum number of board parts.
Oem.Public.DeviceMaxNum.CPUNum	Number	Maximum number of CPUs.
Oem.Public.DeviceMaxNum.DiskNum	Number	Maximum number of hard disks.
Oem.Public.DeviceMaxNum.FanNum	Number	Maximum number of fans.
Oem.Public.DeviceMaxNum.MemoryNum	Number	Maximum number of memory modules.
Oem.Public.DeviceMaxNum.PCIENum	Number	Maximum number of PCIe cards.
Oem.Public.DeviceMaxNum.PowerSupplyNum	Number	Maximum number of power supplies.
Oem.Public.Mainboard	Object	Mainboard information.
Oem.Public.BoardName	String	Mainboard name.
Oem.Public.SerialNumber	String	Serial number of the mainboard.
Oem.Public.PartNumber	String	Part number of the board.
Oem.Public.BoardDate	String	Manufacturing date of the board.
ProductSpecificIdentity	String	Internally defined product name.
Links	Object	Links related to the Chassis resource.
Links.ComputerSystems	Array	Link to System resources.
Links.ManagedBy	Array	Link to Manager resources.

Field	Type	Description
PCleDevices	Object	Navigation of the PCIe device resources.
Drives	Object	Navigation of the drive resources.
NetworkAdapters	Object	Information about the related network adapters.
Power	Object	Information about the related power supplies.
Thermal	Object	Chassis cooling resource information.
Oem.Public.Boards	Object	Board-level resource links.
Oem.Public.ProductName	String	Product name.
Oem.Public.BoardProductVer	String	Product version of the board.
Oem.Public.PartNumber	String	Material code.
Oem.Public.ProductSpecificIdentity	String	Internally defined product name.
Oem.Public.ChassisHeight	String	Chassis size.
Oem.Public.OverallHealthStatus	String	Overall health status.
SerialNumber	String	Serial number of the chassis.
PhysicalSecurity.IntrusionSensor	String	Chassis intrusion status, including: • Normal • HardwareIntrusion: Null is displayed if it is not supported by the board.

6.3 Modifying the Position Indicator Status of a Chassis

Function

Turn on or off the position indicator of a chassis.

Permission Required

Basic management.

Syntax

- Operation Type: PATCH
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id`
- Request Header:

```
Content-Type: header_type
X-Auth-Token: auth_value
```

- Request Message Body:

```
{
  "IndicatorLED": state
}
```

Parameters

For a description of the parameters for modifying the position indicator status of the Chassis, refer to [Table 6-6](#).

Table 6-6 Parameter Descriptions for Modifying the Position Indicator Status of the Chassis

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
state	Position indicator status of the Chassis resource.	Including: - Lit - Blinking - Off

Usage Guidelines

After configuration, you can view the result through **GET** `https://device_ip/redfish/v1/Chassis/1`.

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Chassis/1
```

- Request Header:

```
Content-Type: application/json
```

- Request Message Body:

```
{
  "IndicatorLED": "Lit"
}
```

- Response Example: None

- Status Code: 204

Output Description

None

6.4 Querying Information About the Network Adapter Resource Collection

Function

Query information about the network adapter resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the network adapter resource collection, refer to [Table 6-7](#).

Table 6-7 Parameter Information of Querying Information About the Network Adapter Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/NetworkAdapters
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#NetworkAdaptersCollection.NetworkAdaptersCollection",
  "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters",
  "@odata.type": "#NetworkAdapterCollection.NetworkAdapterCollection",
  "Description": "Collection of Network Adapters for this Manager",
  "Name": "Network Adapters Collection",
  "Members@odata.count": 4,
  "Members": [
    {
      "@odata.id":
        "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard7"
    },
    {
      "@odata.id":
        "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard8"
    },
    {
      "@odata.id":
        "/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1"
    },
    {
      "@odata.id":
        "/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2"
    }
  ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the network adapter resource collection, refer to [Table 6-8](#).

Table 6-8 Output Descriptions for Querying Information About the Network Adapter Resource Collection

Field	Type	Description
@odata.context	String	OData description of the network adapter resource collection model.
@odata.id	String	Access path of the network adapter resource collection.
@odata.type	String	Type of network adapter resource collection.
Name	String	Name of the network adapter resource collection.
Name	String	Name of the network adapter resource collection.
Members@odata.count	Number	Number of network adapter resource members.
Members	Array	Network adapter resource list.
@odata.id	String	Access path of a single network adapter resource node.

6.5 Querying Information About a Specified Network Adapter Resource

Function

Query information about a specified network adapter resource.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified network adapter resource, refer to [Table 6-9](#).

Table 6-9 Parameter Descriptions for Querying Information About the Specified Network Adapter Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
networkadapters_id	ID of the specified network adapter resource.	It can be obtained by querying information about the network adapter resource collection.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#NetworkAdapter.NetworkAdapter",
  "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard5",
  "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
  "Id": "mainboardPCIeCard5",
  "Name": "mainboardPCIeCard5",
  "NetworkPorts": {
    "@odata.id":
      "/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2/NetworkPorts"
  },
  "Manufacturer": "xilinx",
  "Model": "FPGA-xi7p",
  "Controllers": [
    {
      "ControllerCapabilities": {
        "NetworkPortCount": 4
      }
    }
  ]
}
```

```
    },
    "FirmwarePackageVersion": "0101",
    "Links": {
      "NetworkPorts": [
        {
          "@odata.id":
            "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard5/
            NetworkPorts/1"
        },
        {
          "@odata.id":
            "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard5/
            NetworkPorts/2"
        },
        {
          "@odata.id":
            "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard5/
            NetworkPorts/3"
        },
        {
          "@odata.id":
            "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard5/
            NetworkPorts/4"
        }
      ],
      "NetworkPorts@odata.count": 4
    }
  },
  "Oem": {
    "Public": {
      "CardManufacturer": "VT",
      "Name": "XI410",
      "CardModel": "4*25GE",
      "CardType": "fiber",
      "CurrentPower": null,
      "CardCelsius": null,
      "NicCardType": "NIC",
      "DriverVersion": null,
      "NetworkTechnology": [
        "Ethernet"
      ],
      "DeviceLocator": "mainboardPCIECard5",
      "SlotNumber": 5,
```

```

    "RootBDF": "0000:98:00.0",
    "AlarmTmp": 100,
    "CurrentTmp": 46,
    "FpgaStatus": 0,
    "HistoryMaxTmp": 51,
    "NicMemory": [
      {
        "CapacityGb": 80,
        "Model": "DDR4_2400MHz",
        "Status": 0
      },
      {
        "CapacityGb": 32,
        "Model": "DDR4_2400MHz",
        "Status": 0
      },
      {
        "CapacityGb": 16,
        "Model": "DDR4_2400MHz",
        "Status": 0
      }
    ]
  },
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  },
  "SerialNumber": "202308244444"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified network adapter resource, refer to [Table 6-10](#).

Table 6-10 Output Descriptions for Querying Information About the Specified Network Adapter Resource

Field	Type	Description
@odata.context	String	OData description of the specified network adapter resource model.

Field	Type	Description
@odata.id	String	Access path of the specified network adapter resource.
@odata.type	String	Type of the specified network adapter resource.
Id	String	Unique ID of the network adapter resource in the iBMC system.
Name	String	Name of the specified network adapter resource.
NetworkPorts	Array	Network port resource list.
@odata.id	String	Access path of a single network port resource.
Manufacturer	String	Manufacturer of the specified network adapter.
Model	String	Model of the specified network adapter.
Controllers	Array	Information about adapter controllers.
FirmwarePackageVersion	String	Firmware version of the specified network adapter.
ControllerCapabilities.NetworkPortCount	Number	Number of network ports of the specified network adapter.
Links	Object	Links to the related resources.
NetworkPorts	Array	Network port resource information.
@odata.id	String	Access path of the network port resource collection.
NetworkPorts@odata.count	Number	Number of network port resources.
Oem.Public	Object	Manufacturer-customized properties.
CardManufacturer	String	Manufacturer of the specified network adapter.
Name	String	Name of the specified network adapter.
CardModel	String	Interface mode of the specified network adapter.
CardType	String	Type of the specified network adapter.
NicCardType	Character string	NIC type of the specified network adapter. Common cards and smart cards are distinguished.
CurrentPower	Number	NIC power of the specified network adapter.
CardCelsius	Number	NIC temperature of the specified network adapter.
DriverVersion	String	Driver version of the specified network adapter.
NetworkTechnology	Array	Network protocol of the specified network adapter: • Ethernet • FC • iSCSI

Field	Type	Description
		• FCoE • OPA • IB
DeviceLocator	String	Screen printing of the specified network adapter.
SlotNumber	Number	Slot number of the specified network adapter.
RootBDF	String	Root, port, and BDF of the specified network adapter.
AlarmTmp	Number	Alarm temperature of the network adapter. Query is not supported. By default, null is displayed.
CurrentTmp	Number	Main chip temperature of the network adapter. Query is not supported. By default, null is displayed.
FpgaStatus	Number	FPGA status of the network adapter: • 0: The FPGA status of the network adapter is normal. • 1: The FPGA status of the network adapter is abnormal. This field is displayed only for an FPGA card.
HistoryMaxTmp	Number	Maximum historical temperature of the network adapter. This field is displayed only for an FPGA card.
NicMemory	Array	Memory information of the network adapter. This field is displayed only for an FPGA card.
CapacityGb	Number	Memory capacity of the network adapter. This field is displayed only for an FPGA card.
Model	String	Memory model of the network adapter. Default: DDR4_2400MHz. This field is displayed only for an FPGA card.
Status	Number	Memory status of the specified network adapter, options: • 0: normal memory status of the network adapter • 1: abnormal memory status of the network adapter
Status	Object	Status of the network adapter, including: • Health: health status of the network adapter • State: enabling status of the network adapter
SerialNumber	String	Serial number of the specified network adapter.

6.6 Querying Information About All Network Adapter Resources

Function

Query information about all network adapter resources of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters?$expand=.`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about all network adapter resources, refer to [Table 6-11](#).

Table 6-11 Parameter Descriptions for Querying Information About All Network Adapter Resources

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Chassis/1/NetworkAdapters?\$expand=.

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#NetworkAdaptersCollection.NetworkAdaptersCollection",
  "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters?$expand=.",
  "@odata.type": "#NetworkAdapterCollection.NetworkAdapterCollection",
  "Description": "Collection of Network Adapters for this Manager",
  "Name": "Network Adapters Collection",
  "Members@odata.count": 4,
  "Members": [
    {
      "@odata.id":
        "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard7",
      "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
      "Id": "mainboardPCIECard7",
      "Name": "mainboardPCIECard7",
      "NetworkPorts": {
        "@odata.id":
          "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard7/
          NetworkPorts"
      },
      "Manufacturer": "Mellanox",
      "Model": "CX4",
      "Controllers": [
        {
          "ControllerCapabilities": {
            "NetworkPortCount": 2
          },
          "FirmwarePackageVersion": null,
          "Links": {
            "NetworkPorts": [
              {
                "@odata.id":
                  "/redfish/v1/Chassis/1/NetworkAdapters/
                  mainboardPCIECard7/NetworkPorts/1"
              },
              {
                "@odata.id":
                  "/redfish/v1/Chassis/1/NetworkAdapters/
                  mainboardPCIECard7/NetworkPorts/2"
              }
            ]
          }
        }
      ]
    }
  ]
}
```

```

        "NetworkPorts@odata.count": 2
      }
    }
  ],
  "Oem": {
    "Public": {
      "CardManufacturer": "VT",
      "Name": "NS212",
      "CardModel": "2*10GE",
      "CardType": "fiber",
      "DriverVersion": null,
      "NetworkTechnology": [
        "Ethernet"
      ],
      "DeviceLocator": "mainboardPCIECard7",
      "SlotNumber": 7,
      "RootBDF": "0000:27:00.0"
    }
  },
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  },
  "SerialNumber": "733320500068"
},
{
  "@odata.id":
  "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard8",
  "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
  "Id": "mainboardPCIECard8",
  "Name": "mainboardPCIECard8",
  "NetworkPorts": {
    "@odata.id":
    "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard8/NetworkPorts"
  },
  "Manufacturer": "Intel",
  "Model": "X710",
  "Controllers": [
    {
      "ControllerCapabilities": {
        "NetworkPortCount": 2
      },
      "FirmwarePackageVersion": "8.40",
      "Links": {

```

```

        "NetworkPorts": [
            {
                "@odata.id":
                "/redfish/v1/Chassis/1/NetworkAdapters/
                mainboardPCIECard8/NetworkPorts/1"
            },
            {
                "@odata.id":
                "/redfish/v1/Chassis/1/NetworkAdapters/
                mainboardPCIECard8/NetworkPorts/2"
            }
        ],
        "NetworkPorts@odata.count": 2
    }
}
],
"oem": {
    "Public": {
        "CardManufacturer": "Intel",
        "Name": "X710T2L",
        "CardModel": "2*10GE",
        "CardType": "copper",
        "DriverVersion": null,
        "NetworkTechnology": [
            "Ethernet"
        ],
        "DeviceLocator": "mainboardPCIECard8",
        "SlotNumber": 8,
        "RootBDF": "0000:38:00.0"
    }
},
"Status": {
    "Health": "OK",
    "State": "Enabled"
},
"SerialNumber": "~MAC-----~"
},
{
    "@odata.id":
    "/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1",
    "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
    "Id": "mainboardOCPCard1",
    "Name": "mainboardOCPCard1",
    "NetworkPorts": {

```

```
        "@odata.id":
        "/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1/NetworkPorts"
    },
    "Manufacturer": "Mellanox",
    "Model": "CX5",
    "Controllers": [
        {
            "ControllerCapabilities": {
                "NetworkPortCount": 2
            },
            "FirmwarePackageVersion": "16.31.1014",
            "Links": {
                "NetworkPorts": [
                    {
                        "@odata.id":
                        "/redfish/v1/Chassis/1/NetworkAdapters/
                        mainboardOCPCard1/NetworkPorts/1"
                    },
                    {
                        "@odata.id":
                        "/redfish/v1/Chassis/1/NetworkAdapters/
                        mainboardOCPCard1/NetworkPorts/2"
                    }
                ],
                "NetworkPorts@odata.count": 2
            }
        }
    ],
    "Oem": {
        "Public": {
            "CardManufacturer": "Mellanox",
            "Name": "MCX562A-ACAB",
            "CardModel": "2*25GE",
            "CardType": "fiber",
            "DriverVersion": null,
            "NetworkTechnology": [
                "Ethernet"
            ],
            "DeviceLocator": "mainboardOCPCard1",
            "SlotNumber": 1,
            "RootBDF": "0000:ba:00.0"
        }
    },
    "Status": {
```

```

        "Health": "OK",
        "State": "Enabled"
    },
    "SerialNumber": "MT2144J28308"
},
{
    "@odata.id":
    "/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2",
    "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
    "Id": "mainboardOCPCard2",
    "Name": "mainboardOCPCard2",
    "NetworkPorts": {
        "@odata.id":
        "/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2/NetworkPorts"
    },
    "Manufacturer": "Mellanox",
    "Model": "CX5",
    "Controllers": [
        {
            "ControllerCapabilities": {
                "NetworkPortCount": 2
            },
            "FirmwarePackageVersion": "16.30.1004",
            "Links": {
                "NetworkPorts": [
                    {
                        "@odata.id":
                        "/redfish/v1/Chassis/1/NetworkAdapters/
                        mainboardOCPCard2/NetworkPorts/1"
                    },
                    {
                        "@odata.id":
                        "/redfish/v1/Chassis/1/NetworkAdapters/
                        mainboardOCPCard2/NetworkPorts/2"
                    }
                ],
                "NetworkPorts@odata.count": 2
            }
        }
    ],
    "Oem": {
        "Public": {
            "CardManufacturer": "Mellanox",
            "Name": "MCX562A-ACAB",

```

```

        "CardModel": "2*25GE",
        "CardType": "fiber",
        "DriverVersion": null,
        "NetworkTechnology": [
            "Ethernet"
        ],
        "DeviceLocator": "mainboard0CPCard2",
        "SlotNumber": 2,
        "RootBDF": "0000:18:00.0"
    },
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "SerialNumber": "MT2030X11548"
}
]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all network adapter resources, refer to [Table 6-12](#).

Table 6-12 Output Descriptions for Querying Information About All Network Adapter Resources

Field	Type	Description
@odata.context	String	OData description of the network adapter resource collection model.
@odata.id	String	Access path of the network adapter resource collection.
@odata.type	String	Type of network adapter resource collection.
Name	String	Name of the network adapter resource collection.
Members@odata.count	Number	Number of network adapter resource members.
Members	Array	Network adapter resource information.

For a description of the parameters of the network adapter resource information, refer to [Table 6-10](#).

6.7 Querying Information About a Specified Network Port Resource

Function

Query the information about a single network port resource of a specified Chassis of a server. The information includes the network port name, status, [MAC](#) address, network port type, and network port [BDF](#) information.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/NetworkPorts/networkports_id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified network port resource, refer to [Table 6-13](#).

Table 6-13 Parameter Descriptions for Querying Information About the Specified Network Port Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
networkadapters_id	ID of the specified network adapter resource.	It can be obtained by querying the information about the network adapter resource collection.
networkports_id	ID of the network port resource.	It can be obtained by querying the information about the network port resource collection.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCleCard8/NetworkPorts/2
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#EthernetInterface.EthernetInterface",
  "@odata.id":
    "/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1/NetworkPorts/1",
  "@odata.type": "#NetworkPort.v1_4_0.NetworkPort",
  "AssociatedNetworkAddresses": [
    "08:c0:eb:84:cb:d3"
  ],
  "AutoNeg": true,
  "Id": "1",
  "LinkStatus": "Up",
  "Name": "1",
  "Oem": {
    "Public": {
      "BDF": "0000:ba:00.1",
      "CurrentSpeed": "1000Mb/s",
      "DriverVersion": null,
      "FirmwarePackageVersion": "16.31.1014",
      "PortMaxSpeed": "25000Mb/s",
      "PortType": "OpticalPort",
      "LldpService": {
        "ServiceEnabled": false,
        "LldpEnabled": false,
        "WorkMode": null
      },
      "SupportSpeed": [
        "10Mb/s",
        "100Mb/s",
        "1000Mb/s",
        "10000Mb/s",

```



```

        "40000Mb/s",
        "25000Mb/s"
    ]
    },
    "OpticalModule": {
        "@odata.id":
        "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard8/
        NetworkPorts/0/OpticalModule"
    },
    "PhysicalPortNumber": "1"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified network port resource, refer to [Table 6-14](#).

Table 6-14 Output Descriptions for Querying Information About the Specified Network Port Resource

Field	Type	Description
@odata.context	String	OData description of the specified network port resource model.
@odata.id	String	Access path of the specified network port resource.
@odata.type	String	Type of the specified network port resource.
Id	String	UID of the specified network port resource in the iBMC system.
Name	String	Name of the specified network port resource.
AutoNeg	Boolean	Negotiation mode: • true: automatic • false: forced
LinkStatus	String	Status of the specified network port, including: • Up: connected • Down: disconnected
AssociatedNetworkAddresses	Array	Network address of the specified network port.

Field	Type	Description
Oem.Public	Object	Manufacturer-customized properties.
PortMaxSpeed	String	Port speed of the specified network port, unit: Mb/s.
PortType	String	Type of the specified network port, including: ● Optical port: OpticalPort ● Electrical port: ElectricalPort ● Location: N/A
BDF	String	BDF of the specified network port.
CurrentSpeed	Number	Current speed.
FirmwarePackageVersion	String	Firmware version of the specified network port.
DriverVersion	String	Driver version of the specified network port.
LldpService	Object	LLDP -related properties.
LldpEnable	Boolean	Whether LLDP is enabled for the specified network port: ● true: enabled ● false: disabled
ServiceEnabled	Boolean	Whether the specified network port supports LLDP information query. ● true: LLDP query is supported. ● false: LLDP query is not supported. If this parameter is set to false , only the default values of LldpEnabled and WorkMode are displayed, making no sense.
WorkMode	String	LLDP operation mode.
SupportSpeed	Array	Supported speed of the specified network port.
OpticalModule	Object	Indicates the optical module resources connected to the network port.
PhysicalPortNumber	String	Physical screen printing of the specified network port.

6.8 Querying Information About the Optical Module Resource Connected to a Network Port

Function

Query the information about the optical module resource connected to a network port of a specified server chassis.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/NetworkPorts/networkports_id/OpticalModule`
- Request Header:

x-auth-token:auth_value
- Request Message Body: None

Parameters

For a description of the parameters for querying the information about the optical module resource connected to a network port, refer to [Table 6-15](#).

Table 6-15 Parameter Descriptions for Querying Information About the Optical Module Resource Connected to the Network Port

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self .
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
networkadapters_id	ID of the network adapter resource.	It can be obtained by querying the information about the network adapter resource collection.
networkports_id	ID of the network port resource.	It can be obtained by querying the information about the network port resource collection.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCleCard8/NetworkPorts/2/OpticalModule
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#OpticalModule.OpticalModule",
  "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCleCard4/NetworkPorts/1/OpticalModule",
  "@odata.type": "#OpticalModule.v1_0_0.OpticalModule",
  "Id": "OpticalModule",
  "Manufacturer": "Hisense",
  "Name": "OpticalModule",
  "PartNumber": "LTF8502-BC+",
  "ProductionDate": "2020-11-09",
  "RXPower": [
    {
      "LowerThresholdCritical": -9.9,
      "ReadingMilliwatts": [
        -40
      ],
      "UpperThresholdCritical": 0.49
    }
  ],
  "SerialNumber": "UHYABJ09852",
  "Status": {
    "State": "Enabled"
  },
  "BR_Nominal": 10300,
  "TXBiasCurrent": [
    {
      "LowerThresholdCritical": 0,
      "ReadingMilliwatts": [
        6.24
      ]
    }
  ]
}
```

```

    ],
    "UpperThresholdCritical": 12
  }
],
"TXPower": [
  {
    "LowerThresholdCritical": -5.5,
    "ReadingMilliwatts": [
      -2.53
    ],
    "UpperThresholdCritical": -1
  }
],
"Temperature": {
  "LowerThresholdCritical": -10,
  "ReadingCelsius": 30.32,
  "UpperThresholdCritical": 75
},
"voltage": {
  "LowerThresholdCritical": 3.1,
  "ReadingVolts": 3.29,
  "UpperThresholdCritical": 3.5
},
"WaveLengthNanometer": 850
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the optical module resource connected to the network port, refer to [Table 6-16](#).

Table 6-16 Output Descriptions for Querying Information About the Optical Module Resource Connected to the Network Port

Field	Type	Description
@odata.context	Character string	OData description of the specified network port resource model.
@odata.id	Character string	Access path of the specified network port resource model.
@odata.type	Character string	Resource type of the specified network port resource model.
Id	Character string	ID of the optical module resource.

Field	Type	Description
Name	Character string	Name of the optical module resource.
Status	Object	Status of the optical module, including: ● Enabled: enabled state.
Manufacturer	Character string	Name of the manufacturer of the optical module.
PartNumber	Character string	Part number of the optical module.
ProductionDate	String	Production date of the optical module.
RXPower.LowerThresholdCritical	Number	Critical alarm threshold for too low receive power.
RXPower.ReadingMilliWatts	Array	Current receive power reading of the optical module.
RXPower.UpperThresholdCritical	Number	Critical alarm threshold for too high receive power.
SerialNumber	Character string	Serial number of the optical module.
Status.State	String	Whether the optical module is enabled.
BR_Nominal	Number	Rate supported by the optical module.
TxBiasCurrent.LowerThresholdCritical	Number	Critical alarm threshold for too low transmit bias current of the optical module.
TxBiasCurrent.ReadingMilliAmperes	Array	Current transmit bias current reading of the optical module.
TxBiasCurrent.UpperThresholdCritical	Number	Critical alarm threshold for too high transmit bias current of the optical module.
TXPower.ReadingMilliWatts	Array	Current reading of the transmission power of the optical module.
TXPower.LowerThresholdCritical	Number	Critical alarm threshold for low transmission power.
TXPower.UpperThresholdCritical	Number	Critical alarm threshold for high transmission power.
Temperature.ReadingCelsius	Number	Current temperature reading of the optical module.
Temperature.LowerThresholdCritical	Number	Critical alarm threshold for low temperature.
Temperature.UpperThresholdCritical	Number	Critical alarm threshold for high temperature.
Voltage.ReadingVolts	Number	Current voltage reading of the optical module.
Voltage.LowerThresholdCritical	Number	Critical alarm threshold for low voltage.

Field	Type	Description
Voltage.UpperThresholdCritical	Number	Critical alarm threshold for high voltage.
WaveLengthNanometer	Number	Wavelength of the optical module.

6.9 Modifying the LLDP Switch of a Specified Network Port

Function

Modify the [LLDP](#) switch of a specified network port.

Permission Required

Security management

Syntax

- Operation Type: PATCH
- **URL:** `https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/NetworkPorts/networkports_id`
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "Oem": {
    "Public": {
      "LldpService": {
        "LldpEnabled": enable_value,
        "WorkMode": workmode_value
      }
    }
  }
}
```

Parameters

For a description of the parameters for modifying the LLDP switch of a network port, refer to [Table 6-17](#).

Table 6-17 Parameter Descriptions for Modifying the LLDP Switch of the Network Port

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.

Parameter	Description	Value
chassis_id	ID of the chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
networkadapters_id	ID of the specified network adapter resource.	It can be obtained by querying the information about the network adapter resource collection.
networkports_id	ID of the network port resource.	-
enable_value	Whether LLDP is enabled.	● true: enabled ● false: disabled
workmode_value	LLDP operation mode.	● TxRx (default): enables LLDP packet transmission and reception. If LLDP is disabled, workmode_value is unavailable. ● Rx: enables LLDP packet reception only. ● Tx: transmitting mode

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCleCard7/NetworkPorts/1
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
  "oem": {
    "Public": {
      "LldpService": {
        "LldpEnabled": true,
        "workMode": "TxRx"
      }
    }
  }
}
```



```

    }
  }
}

```

- Response Example:

```

{
  "@odata.context": "/redfish/v1/$metadata#EthernetInterface.EthernetInterface",
  "@odata.id":
    "/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1/NetworkPorts/1",
  "@odata.type": "#NetworkPort.v1_4_0.NetworkPort",
  "AssociatedNetworkAddresses": [
    "08:c0:eb:84:cb:d3"
  ],
  "AutoNeg": true,
  "Id": "1",
  "LinkStatus": "Up",
  "Name": "1",
  "Oem": {
    "Public": {
      "BDF": "0000:ba:00.1",
      "CurrentSpeed": "1000Mb/s",
      "DriverVersion": null,
      "FirmwarePackageVersion": "16.31.1014",
      "PortMaxSpeed": "25000Mb/s",
      "PortType": "OpticalPort",
      "LldpService": {
        "ServiceEnabled": true,
        "LldpEnabled": false,
        "WorkMode": null
      },
      "SupportSpeed": [
        "10Mb/s",
        "100Mb/s",
        "1000Mb/s",
        "10000Mb/s",
        "40000Mb/s",
        "25000Mb/s"
      ]
    }
  },
  "PhysicalPortNumber": "1"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you modify the LLDP switch of the network port, refer to [Table 6-18](#).

Table 6-18 Output Descriptions for Modifying the LLDP Switch of the Network Port

Field	Type	Description
@odata.context	String	OData description of the specified network port resource model.
@odata.id	String	Access path of the specified network port resource.
@odata.type	String	Type of the specified network port resource.
Id	String	UID of the specified network port resource in the iBMC system.
Name	String	Name of the specified network port resource.
AutoNeg	Boolean	Negotiation mode: ● true: automatic ● false: forced
LinkStatus	String	Status of the specified network port, including: ● Up ● Down
AssociatedNetworkAddresses	Array	Network address of the specified network port.
Oem.Public	Object	Manufacturer-customized properties.
PortMaxSpeed	String	Port speed of the specified network port, unit: Mb/s.
PortType	String	Type of the specified network port, including: ● Optical port: OpticalPort ● Electrical port: ElectricalPort ● Location: N/A
BDF	String	BDF of the specified network port.
CurrentSpeed	Number	Current speed.
FirmwarePackageVersion	String	Firmware version of the specified network port.

Field	Type	Description
DriverVersion	String	Driver version of the specified network port.
LldpService	Object	LLDP-related properties.
LldpEnable	Boolean	Whether LLDP is enabled for the specified network port: ● true: enabled ● false: disabled
ServiceEnabled	Boolean	Whether LLDP information query is supported by the specified network port. ● true: yes. ● false: no. If this parameter is set to false , only the default values are displayed for LldpEnabled and WorkMode .
WorkMode	String	LLDP operation mode.
SupportSpeed	Array	Supported speed of the specified network port.
PhysicalPortNumber	String	Physical screen printing of the specified network port.

6.10 Querying Information About the PCIe Device Resource Collection

Function

Query information about the [PCIe](#) device resources of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/PCIeDevices`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the PCIe device resource collection, refer to [Table 6-19](#).

Table 6-19 Parameter Descriptions for Querying Information About the PCIe Device Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/PCleDevices
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/
  $metadata#PCleDevicesCollection.PCLeDevicesCollection",
  "@odata.id": "/redfish/v1/Chassis/Self/PCLeDevices",
  "@odata.type": "#PCLeDeviceCollection.PCLeDeviceCollection",
  "Description": "PCLe Device Collection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Chassis/Self/PCLeDevices/PCLeCard22"
    },
    {
      "@odata.id": "/redfish/v1/Chassis/Self/PCLeDevices/PCLeCard5"
    },
    {
      "@odata.id": "/redfish/v1/Chassis/Self/PCLeDevices/PCLeCard19"
    }
  ]
}
```

```
    },
    {
        "@odata.id": "/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard8"
    }
],
"Members@odata.count": 4,
"Name": "PCIe Device Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the PCIe device resource collection, refer to [Table 6-20](#).

Table 6-20 Output Descriptions for Querying Information About the PCIe Device Resource Collection

Field	Type	Description
@odata.context	String	OData description of the PCIe device resource collection model.
@odata.id	String	Access path of the PCIe device resource collection.
@odata.type	String	Type of PCIe device resource collection.
Description	String	Description of the PCIe device resource collection.
Name	String	Name of the PCIe device resource collection.
Members@odata.count	Number	Number of PCIe device resource members.
Members	Array	PCIe device resource list.

6.11 Querying Information About a Specified PCIe Device Resource

Function

Query information about a specified [PCIe](#) device resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET

- **URL:** `https://device_ip/redfish/v1/Chassis/chassis_id/PCIeDevices/pcidevices_id`
- **Request Header:**

X-Auth-Token: auth_value

- **Request Message Body:** None

Parameters

For a description of the parameters for querying information about the specified PCIe device resource, refer to [Table 6-21](#).

Table 6-21 Parameter Descriptions for Querying Information About the Specified PCIe Device Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
pcidevices_id	ID of specified PCIe device resource.	It can be obtained by querying the information about the specified resource collection.

Usage Guidelines

None

Example

- **Request Example:**

GET https://device_ip/redfish/v1/Chassis/1/PCIeDevices/PCIeCard5

- **Request Header:**

X-Auth-Token: 8574621d21b84756218c7456821c234

- **Request Message Body:** None
- **Response Example1:**

{
 "@odata.context": "/redfish/v1/\$metadata#PCIeDevices.PCIeDevices",
 "@odata.id": "/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard5",
 "@odata.type": "#PCIeDevice.v1_4_0.PCIeDevice",
}

```
"CardManufacturer": "VT",
"CardModel": null,
"Description": "RS241-18i 2G",
"FirmwareVersion": "3.22",
"Id": "mainboardPCIeCard5",
"Links": {
  "PCIeFunctions": [
    {
      "@odata.id": "/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard5/Functions/1"
    }
  ]
},
"Oem": {
  "Public": {
    "DeviceBDF": "0000:27:00.0",
    "DeviceLocator": "PCIeCard5",
    "MemorySizeMiB": 2097152,
    "LinkSpeed": "3GT/s",
    "MaxLinkSpeed": "3GT/s",
    "Linkwidth": 8,
    "MaxLinkwidth": 8,
    "PCIeCardType": "Storage Card",
    "PowerCapacityWatts": null,
    "PowerWatts": null,
    "PowerConsumedWatts": null,
    "RootPortBDF": "0000:26:01.0",
    "SlotNumber": 5
  }
},
"Manufacturer": null,
"Model": "RAID_SAS8236",
"Name": "Storage Card5",
"PCIeInterface": {
  "LanesInUse": 8,
  "MaxLanes": 8
},
"SerialNumber": "743551500214",
"Status": {
  "Health": "OK",
  "State": "Enabled"
}
}
```

- Response Example2:

```
{
  "@odata.id": "/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard5",
  "@odata.type": "#PCIeDevice.v1_4_0.PCIeDevice",
  "CardManufacturer": "Nvidia",
  "CardModel": "NVIDIA A10",
  "Description": "NVIDIA A10",
  "FirmwareVersion": "94.02.5C.00.04",
  "Id": "mainboardPCIeCard5",
  "Links": {
    "PCIeFunctions": [
      {
        "@odata.id": "/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard5/Functions/1"
      }
    ]
  },
  "Oem": {
    "Public": {
      "DeviceLocator": "mainboardPCIeCard5",
      "GpuCore": [
        {
          "BuildTime": "2021/06/26",
          "CapacityGB": 24,
          "MemberId": 1,
          "PartNum": null,
          "Power": null,
          "Temperature": 40
        }
      ],
      "GpuPerformanceParameters": {
        "EncoderUsagePercent": 20,
        "DecoderUsagePercent": 10,
        "GPUUsagePercent": 30,
        "ReservedCapacityMiB": 1560,
        "ReservedCapacityPercent": 50,
        "TemperatureCelsius": 55,
        "PowerWatts": 120
      },
      "SFP": [
        {
          "MemberId": "0",
          "TemperatureCelsius": 20
        }
      ],
      "LinkSpeed": "16.0GT/s".
    }
  }
}
```



```

        "MaxLinkSpeed": "16.0GT/s",
        "MemoryBandwidth": "600GB/s",
        "MemorySizeMiB": 24576,
        "PCIECardType": "GPU",
        "PowerCapacityWatts": 150,
        "PowerWatts": null,
        "PowerConsumedWatts": null,
        "ReadingCelsius": 40,
        "SlotNumber": 5,
        "Linkwidth": 8,
        "MaxLinkwidth": 8
    }
},
"Manufacturer": "Nvidia",
"Model": "NVIDIA A10",
"Name": "GPU5",
"PCIeInterface": {
    "LanesInUse": 16,
    "MaxLanes": 16
},
"SerialNumber": "1322521044226",
"Status": {
    "Health": "OK",
    "State": "Enabled"
}
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified PCIe device resource, refer to [Table 6-22](#).

Table 6-22 Output Descriptions for Querying Information About the Specified PCIe Device Resource

Field	Type	Description
@odata.context	String	OData description of the specified PCIe device resource model.
@odata.id	String	Access path of the specified PCIe device resource.
@odata.type	String	Type of the specified PCIe device resource.

Field	Type	Description
CardManufacturer	String	PCIe device manufacturer, which is the same as the CardManufacturer value of the storage controller and NIC.
CardModel	String	PCIe device model, which is the same as the CardModel of the storage controller and the Oem.Public.Name of the NIC.
Name	String	Name of the specified PCIe device resource.
Id	String	UID of the specified PCIe device resource in the iBMC system.
Description	String	Description of the specified PCIe device resource.
Manufacturer	String	Manufacturer of the specified PCIe device.
Model	String	Model of the specified PCIe device resource.
Links.PCIeFunctions.@odata.id	String	Access path of the PCIeFunctions resource.
FirmwareVersion	String	Version number of the specified PCIe device.
SerialNumber	String	Serial number of the specified PCIe device.
Status	Object	Status of the specified PCIe device, including: ● Health: health status of the specified PCIe device ● State: whether the specified PCIe device is enabled
PCIeInterface	Object	Interface information about the specified PCIe device.
LanesInUse	Number	Number of currently negotiated PCIe lanes of the specified PCIe device.
MaxLanes	Number	Maximum number of PCIe lanes supported by the specified PCIe device.
Oem.Public	Object	-
LinkSpeed	Number	Current link speed of the specified PCIe device, unit: GT/s.
MaxLinkSpeed	Number	Maximum link speed supported by the specified PCIe device, unit: GT/s.
LinkWidth	Number	Link bandwidth of the specified PCIe device.
DeviceBDF	String	Device BDF of the specified PCIe device.
DeviceLocator	String	Screen printing of the specified PCIe device.
MemorySizeMiB	String	Total memory capacity of the specified PCIe device.

Field	Type	Description
MemoryBandWidth	String	Bandwidth of the display memory data of the specified GPU or NPU when PCIeCardType is GPU or NPU, unit: GB/s.
PowerCapacityWatts	Number	Maximum Thermal Design Power (TDP) of the specified GPU, unit: W.
PowerConsumedWatts	Number	Actual power consumed by the specified GPU, unit: W.
ReadingCelsius	Number	Actual temperature of the specified GPU, unit: centigrade.
PCleCardType	String	Type of the specified PCIe device.
PowerWatts	Number	Power of the specified PCIe device, unit: W.
RootPortBDF	String	Root port BDF of the specified PCIe device.
SlotNumber	Number	Slot number of the specified PCIe device.
Oem.Public.GpuCore	Array	Memory resource list of the specified PCIe device.
BuildTime	String	Production date of the memory of the specified PCIe device.
CapacityGB	Number	Memory capacity of the specified PCIe device, unit: GB.
MemberId	Number	Memory index of the specified PCIe device.
PartNum	String	Memory part number of the specified PCIe device.
Power	String	Power of the specified PCIe device, unit: W.
Temperature	Number	Temperature of the specified PCIe device, unit: centigrade.
Oem.Public.GpuPerformanceParameters.EncoderUsagePercent	Number	Encoder usage.
Oem.Public.GpuPerformanceParameters.DecoderUsagePercent	Number	Decoder Usage.
Oem.Public.GpuPerformanceParameters.GPUUsagePercent	Number	GPU usage.

Field	Type	Description
Oem.Public.GpuPerformanceParameters.ReservedCapacityMiB	Number	Display memory capacity in MiB.
Oem.Public.GpuPerformanceParameters.ReservedCapacityPercent	Number	Display memory capacity in percentage.
Oem.Public.GpuPerformanceParameters.TemperatureCelsius	Number	GPU temperature.
Oem.Public.GpuPerformanceParameters.PowerWatts	Number	GPU power.
Oem.Public.SFP.MemberId	String	Optical module ID.
Oem.Public.SFP.TemperatureCelsius	Number	Optical module temperature.
Oem.Public.NVMeAIC	Object	-
CapacityGB	Number	Storage capacity of the specified PCIe device.
DiskTemperatureCelsius	Number	Temperature of the specified PCIe device.
MediaType	String	Media type of the specified PCIe device.
PredictedMediaLifeLeftPercent	Number	Remaining lifetime of the specified PCIe device.
Interface	String	Interface type of the specified PCIe device.
CapacityBytes	Number	Capacity of the specified PCIe device, unit: bytes.
HealthStatus	String	Health status of the specified PCIe device.
Model	String	Model of the specified PCIe device.
Vendor	String	Manufacturer of specified PCIe device.
SerialNumber	String	Serial number of the specified PCIe device.

6.12 Querying Information About All PCIe Device Resources

Function

Query information about all [PCIe](#) device resources of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/PCIeDevices?$expand=.`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For the parameter descriptions for querying information about all PCIe device resources, refer to [Table 6-23](#).

Table 6-23 Parameter Descriptions for Querying Information About All PCIe Device Resources

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET `https://device_ip/redfish/v1/Chassis/1/PCIeDevices?$expand=.`

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

{
 "@odata.context":
 "/redfish/v1/\$metadata#PCIeDevicesCollection.PCIeDevicesCollection",
 "@odata.id": "/redfish/v1/Chassis/Self/PCIeDevices",
 "@odata.type": "#PCIeDeviceCollection.PCIeDeviceCollection",
}

```
"Description": "PCIe Device Collection",
"Members": [
  {
    "@odata.id": "/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard5",
    "@odata.type": "#PCIeDevice.v1_4_0.PCIeDevice",
    "CardManufacturer": "Nvidia",
    "CardModel": "NVIDIA A10",
    "Description": "NVIDIA A10",
    "FirmwareVersion": "94.02.5C.00.04",
    "Id": "mainboardPCIeCard5",
    "Links": {
      "PCIeFunctions": [
        {
          "@odata.id":
            "/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard5/Functions/1"
        }
      ]
    },
    "Oem": {
      "Public": {
        "DeviceLocator": "mainboardPCIeCard5",
        "GpuCore": [
          {
            "BuildTime": "2021/06/26",
            "CapacityGB": 24,
            "MemberId": 1,
            "PartNum": null,
            "Power": null,
            "Temperature": 40
          }
        ],
        "LinkSpeed": "16.0GT/s",
        "MaxLinkSpeed": "16.0GT/s",
        "MemoryBandwidth": "600GB/s",
        "MemorySizeMiB": 24576,
        "PCIeCardType": "GPU",
        "PowerCapacityWatts": 150,
        "PowerWatts": null,
        "PowerConsumedWatts": null,
        "ReadingCelsius": 40,
        "SlotNumber": 5
      }
    },
    "Manufacturer": "Nvidia",
```

```
"Model": "NVIDIA A10",
"Name": "GPU5",
"PCIeInterface": {
  "LanesInUse": 16,
  "MaxLanes": 16
},
"SerialNumber": "1322521044226",
"Status": {
  "Health": "OK",
  "State": "Enabled"
}
},
{
  "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard6",
  "@odata.type": "#PCIeDevice.v1_4_0.PCIeDevice",
  "CardManufacturer": "Memblaze",
  "CardModel": "P5516CH0160T00",
  "Description": "AIC",
  "FirmwareVersion": "22400560",
  "Id": "mainboardPCIeCard6",
  "Links": {
    "PCIeFunctions": [
      {
        "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard6/
        Functions/1"
      }
    ]
  },
  "Oem": {
    "Public": {
      "DeviceBDF": "0000:e1:00.0",
      "DeviceLocator": "mainboardPCIeCard6",
      "NVMeAIC": {
        "CapacityGB": 1600,
        "CapacityBytes": 1600000000000,
        "DiskTemperatureCelsius": 52,
        "MediaType": "SSD",
        "PredictedMediaLifeLeftPercent": 100,
        "Interface": "PCIe",
        "HealthStatus": "OK",
        "Model": "P5516CH0160T00",
        "Vendor": "Memblaze",
        "SerialNumber": "SH203401337"
      }
    },
  },
}
```

```

        "LinkSpeed": "8.0GT/s",
        "MaxLinkSpeed": "8.0GT/s",
        "MemorySizeMiB": null,
        "PCIECardType": "NVMe AIC",
        "PowerCapacitywatts": null,
        "PowerWatts": null,
        "PowerConsumedwatts": null,
        "RootPortBDF": "0000:e0:01.1",
        "SlotNumber": 6
    }
},
"Manufacturer": "Memblaze",
"Model": "P5516CH0160T00",
"Name": "NVMe AIC6",
"PCIeInterface": {
    "LanesInUse": 4,
    "MaxLanes": 4
},
"SerialNumber": "SH203401337",
"Status": {
    "Health": "OK",
    "State": "Enabled"
}
},
{
    "@odata.id": "/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard7",
    "@odata.type": "#PCIeDevice.v1_4_0.PCIeDevice",
    "CardManufacturer": "Memblaze",
    "CardModel": "P5916CH0320M00",
    "Description": "AIC",
    "FirmwareVersion": "21300BA0",
    "Id": "mainboardPCIeCard7",
    "Links": {
        "PCIeFunctions": [
            {
                "@odata.id":
                "/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard19/Functions/1"
            }
        ]
    },
    "Oem": {
        "Public": {
            "DeviceBDF": "0000:a8:00.0",
            "DeviceLocator": "mainboardPCIeCard7",

```



```

        "LinkSpeed": "8.0GT/s",
        "MaxLinkSpeed": "8.0GT/s",
        "MemorySizeMiB": 3200,
        "PCIECardType": "NVMe AIC",
        "PowerCapacitywatts": null,
        "PowerWatts": null,
        "PowerConsumedwatts": null,
        "RootPortBDF": "0000:a7:01.0",
        "SlotNumber": 7
    },
    {
        "Manufacturer": "Memblaze",
        "Model": "P5916CH0320M00",
        "Name": "NVMe AIC7",
        "PCIEInterface": {
            "LanesInUse": 4,
            "MaxLanes": 8
        },
        "SerialNumber": "SH193800164",
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        }
    }
],
"Members@odata.count": 2,
"Name": "PCIe Device Collection"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all PCIe device resources, refer to [Table 6-24](#).

Table 6-24 Output Descriptions for Querying Information About All PCIe Device Resources

Field	Type	Description
@odata.context	String	OData description of the PCIe device resource collection model.
@odata.id	String	Access path of the PCIe device resource collection.
@odata.type	String	Type of PCIe device resource collection.
Description	String	Description of the PCIe device resource collection.

Field	Type	Description
Name	String	Name of the PCIe device resource collection.
Members@odata.count	Number	Number of PCIe device resource members.
Members	Array	PCIe device resources.

For a description of the parameters of the PCIe device resource information, refer to [Table 6-22](#).

6.13 Querying Information About the Drive Resource Collection

Function

Query information about the drive resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Chassis/chassis_id/Drives*
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the drive resource collection, refer to [Table 6-25](#).

Table 6-25 Parameter Descriptions for Querying Information About the Drive Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Drives
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#DrivesCollection.DrivesCollection",
  "@odata.id": "/redfish/v1/Chassis/1/Drives",
  "@odata.type": "#DriverCollection.DriverCollection",
  "Description": "Drivers Collection",
  "Name": "Drivers Collection",
  "Members@odata.count": 4,
  "Members": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk16"
    },
    {
      "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk17"
    },
    {
      "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk19"
    },
    {
      "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk21"
    }
  ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the drive resource collection, refer to [Table 6-26](#).

Table 6-26 Output Descriptions for Querying Information About the Drive Resource Collection

Field	Type	Description
@odata.context	String	OData description of the drive resource collection model.
@odata.id	String	Access path of the drive resource collection.
@odata.type	String	Type of drive resource collection.
Description	String	Description of the drive resource collection.
Name	String	Name of the drive resource collection.
Members@odata.count	Number	Number of drive resource members.
Members	Array	Drive resource list.
@odata.id	String	Access path of the drive resource node.

6.14 Querying Information About a Specified Drive Resource

Function

Query information about a specified drive resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/Drives/drives_id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified drive resource, refer to [Table 6-27](#).

Table 6-27 Parameter Descriptions for Querying Information About the Specified Drive Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
drives_id	ID of the specified disk.	It can be obtained from the drive list managed by the current specified controllers

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Drives/HDDPlaneDisk17
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Drives.Drives",
  "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk17",
  "@odata.type": "#Drive.v1_1_0.Drive",
  "CapableSpeedGbs": 12,
  "CapacityBytes": 644245094400,
  "FailurePredicted": null,
  "HotspareType": null,
  "Id": "HDDPlaneDisk17",
  "IndicatorLED": "Off",
  "Location": [
    {
      "Info": "Disk17",
      "InfoFormat": "DeviceName"
    }
  ],
  "Manufacturer": "TOSHIBA",
```

```

    "MediaType": "HDD",
    "Model": "AL14SEB060N",
    "Name": "Disk17",
    "NegotiatedSpeedGbs": 12,
    "Oem": {
      "Public": {
        "SASAddress": "30015EBE04B2B93F",
        "RotationSpeedRPM": null,
        "SATAPort": {
          "BelongCPU": null,
          "ControllerBDF": null,
          "ControllerPortNum": null
        },
        "TemperatureCelsius": 30
      }
    },
    "PartNumber": null,
    "PredictedMediaLifeLeftPercent": null,
    "Protocol": "SAS",
    "Revision": "0103",
    "SerialNumber": "38Q0A03LFV7B",
    "SlotNumber": 17,
    "Status": {
      "Health": "OK",
      "State": "Enabled"
    }
  }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified drive resource, refer to [Table 6-28](#).

Table 6-28 Output Descriptions for Querying Information About the Specified Drive Resource

Field	Type	Description
@odata.context	String	OData description of the specified drive resource model.
@odata.id	String	Access path of the specified drive resource.
@odata.type	String	Type of the specified drive resource.
Id	String	ID of the specified drive resource.

Field	Type	Description
Name	String	Name of the specified drive resource.
Model	String	Model of the specified drive.
Revision	String	Version information about the specified drive.
Status	Object	Status of the specified drive, including: ● State: whether drives are enabled ● Health: health status of the drives
CapableSpeedGbs	Number	Maximum interface speed of the specified drive.
NegotiatedSpeedGbs	Number	Negotiated rate of the specified drive. The value for NVMe is null.
Oem.Public	Object	-
TemperatureCelsius	Number	Temperature unit (Celsius) of the specified drive.
BackplaneId	Number	Backplane ID of the specified drive.
BackPanelLocation	String	Backplane position of the specified drive.
SASAddress	String	-
CapacityBytes	Number	Capacity of the specified drive, in bytes.
FailurePredicted	Boolean	Pre-failure status of the specified drive, including: ● true ● false
Protocol	String	Compliant protocol of the specified drive: ● SPI ● PCIe ● AHCI ● UHCI ● SAS ● SATA ● USB ● NVMe ● FC ● iSCSI ● FCoE ● NVMeOverFabrics ● SMB ● NFSv3

Field	Type	Description
		• NFSv4 • HTTP • HTTPS • FTP • SFTP
MediaType	String	Media type of the specified drive: • HDD • SSD • SMR
Manufacturer	String	Manufacturer of the specified drive.
PredictedMediaLifeLeftPercent	Number	Percentage of the remaining service life of the specified drive.
SerialNumber	String	Serial number of the specified drive.
PartNumber	String	Part number of the specified drive.
SlotNumber	Number	Slot number of the specified drive.
IndicatorLED	String	Positioning indicator status of the specified drive: • Lit • Off • UnKnown
Location	Array	Screen printing of the specified drive.
Info	String	Screen printing information about the specified drive.
InfoFormat	String	Screen printing format of the specified drive.
RotationSpeedRPM	Number	Rotation speed of the specified drive, unit: RPM.
BelongCPU	String	CPU of the controller of the specified drive.
ControllerBDF	String	Controller BDF of the specified drive.
ControllerPortNum	Number	Controller port number of the specified drive.

6.15 Querying Information About All Drive Resources

Function

Query information about the drive resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Chassis/chassis_id/Drives?$expand=.`
- Request Header: None

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about all drive resources, refer to [Table 6-29](#).

Table 6-29 Parameter Descriptions for Querying Information About All Drive Resources

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Chassis/1/Drives?\$expand=.

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None

- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#DrivesCollection.DrivesCollection",
  "@odata.id": "/redfish/v1/Chassis/Self/Drives",
  "@odata.type": "#DriverCollection.DriverCollection",
  "Description": "Drivers Collection",
  "Name": "Drivers Collection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Chassis/Self/Drives/HDDPlaneDisk30",
      "@odata.type": "#Drive.v1_1_0.Drive",
      "CapableSpeedGbs": 3,
      "CapacityBytes": 2000000000000,
      "FailurePredicted": null,
      "HotspareType": null,
      "Id": "HDDPlaneDisk30",
      "IndicatorLED": null,
      "Location": [
        {
          "Info": "",
          "InfoFormat": "DeviceName"
        }
      ],
      "Manufacturer": "ATA",
      "MediaType": "HDD",
      "Model": "WDC WD2000FYYZ-01UL1B0",
      "Name": "Disk30",
      "NegotiatedSpeedGbs": 3,
      "Oem": {
        "Public": {
          "SASAddress": null,
          "SATAPort": {
            "BelongCPU": "CPU0",
            "ControllerBDF": "0000:00:17.0",
            "ControllerPortNum": 2
          },
          "RotationSpeedRPM": 7200,
          "TemperatureCelsius": 30
        }
      },
      "PartNumber": null,
      "PredictedMediaLifeLeftPercent": null,
      "Protocol": "SATA",
    }
  ]
}
```

```
        "Revision": "01.x1kx2",
        "SerialNumber": "WD-WCC1P0458212",
        "SlotNumber": 30,
        "Status": {
            "Health": null,
            "State": null
        }
    },
    {
        "@odata.id": "/redfish/v1/Chassis/Self/Drives/HDDPlaneDisk9",
        "@odata.type": "#Drive.v1_1_0.Drive",
        "CapableSpeedGbs": 8,
        "CapacityBytes": 3840755982336,
        "FailurePredicted": false,
        "HotspareType": null,
        "Id": "HDDPlaneDisk9",
        "IndicatorLED": "Off",
        "Location": [
            {
                "Info": "Disk9",
                "InfoFormat": "DeviceName"
            }
        ],
        "Manufacturer": "Intel",
        "MediaType": "SSD",
        "Model": "INTEL SSDPF2KX038T1",
        "Name": "Disk9",
        "NegotiatedSpeedGbs": null,
        "Oem": {
            "Public": {
                "BackpanelId": 10,
                "BackPanelLocation": "Front",
                "TemperatureCelsius": 30
            }
        },
        "PartNumber": null,
        "PredictedMediaLifeLeftPercent": 100,
        "Protocol": "NVMe",
        "Revision": "9CV10200",
        "SerialNumber": "PHAX2170001D3P8CGN",
        "SlotNumber": 9,
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        }
    }
}
```

```
    }
  }
],
  "Members@odata.count": 2
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all drive resources, refer to [Table 6-30](#).

Table 6-30 Output Descriptions for Querying Information About All Drive Resources

Field	Type	Description
@odata.context	String	OData description of the drive resource collection model.
@odata.id	String	Access path of the drive resource collection.
@odata.type	String	Type of drive resource collection.
Description	String	Description of the drive resource collection.
Name	String	Name of the drive resource collection.
Members@odata.count	Number	Number of drive resource members.
Members	Array	All drive resources.

For a description of the parameters of the drive resource information, refer to [Table 6-28](#).

6.16 Querying the Power Supply Information About a Specified Chassis

Function

Query power supply information about a specified Chassis.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Chassis/Chassis_id/Power*
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the power supply information about the specified Chassis, refer to [Table 6-31](#).

Table 6-31 Parameter Descriptions for Querying Information About the Specified Chassis Power Supply

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Chassis/1/Power

- Request Header:

x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Power.Power",
  "@odata.id": "/redfish/v1/Chassis/1/Power",
  "@odata.type": "#Power.v1_5_4.Power",
  "Description": "Power sensor readings",
  "Id": "Power",
  "Name": "Power",
  "PowerControl": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerControl/1",
      "MemberId": "1",
      "Name": "Chassis Power Control",
      "PowerLimit": {
```

```

        "LimitInWatts": null,
        "PowerLimitEnable": false,
        "LimitException": "NoAction"
    },
    "PowerMetrics": {
        "AverageConsumedWatts": 0,
        "IntervalInMin": 0,
        "MaxConsumedWatts": 0,
        "MinConsumedWatts": 0
    },
    "PowerConsumedWatts": 29,
    "Oem": {
        "Public": {
            "ExpectedActivePSU": [
                {
                    "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/1"
                },
                {
                    "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/4"
                }
            ],
            "CurrentCPUPowerWatts": 0,
            "CurrentFanPowerWatts": 0,
            "CurrentMemoryPowerWatts": 0,
            "CurrentHDDPowerWatts": 0
        }
    }
},
],
"PowerControl@odata.count": 1,
"PowerSupplies": [
    {
        "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/1",
        "FirmwareVersion": "DC:1.01 PFC:1.00",
        "LineInputVoltage": 217,
        "Manufacturer": "Great Wall",
        "Model": "CRPS1200D",
        "Name": "PSU1",
        "PowerCapacityWatts": 1200,
        "PowerInputWatts": 26,
        "PowerOutputWatts": 5,
        "PowerSupplyType": "AC",
        "ProductionDate": "190123",
        "SerialNumber": "22M010020400",
    }
]

```

```
    "Status": {
      "Health": "OK",
      "State": "Enabled"
    },
    "Oem": {
      "Public": {
        "SlotNumber": 1,
        "ActiveStandby": "Active"
      }
    },
    "MemberId": "1"
  },
  {
    "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/2",
    "FirmwareVersion": null,
    "LineInputVoltage": 0,
    "Manufacturer": null,
    "Model": null,
    "Name": "PSU2",
    "PowerCapacityWatts": null,
    "PowerInputWatts": null,
    "PowerOutputWatts": null,
    "PowerSupplyType": null,
    "ProductionDate": "190123",
    "SerialNumber": null,
    "Status": {
      "Health": "Warning",
      "State": "Disabled"
    },
    "Oem": {
      "Public": {
        "SlotNumber": 2,
        "ActiveStandby": "Standby"
      }
    },
    "MemberId": "2"
  }
],
"PowerSupplies@odata.count": 2,
"Actions": {
  "#Power.CollectHistoryData": {
    "target": "/redfish/v1/Chassis/1/Power/Actions/Power.CollectHistoryData"
  }
},
```

```
"voltages": [  
  {  
    "@odata.id": "/redfish/v1/Chassis/1/Power#/voltages/1",  
    "LowerThresholdCritical": 2.643,  
    "LowerThresholdFatal": 0,  
    "LowerThresholdNonCritical": 0,  
    "MaxReadingRange": 4.463,  
    "MemberId": "1",  
    "MinReadingRange": 0,  
    "Name": "RGM_VCC3.3V",  
    "PhysicalContext": "VoltageRegulator",  
    "SensorNumber": 1,  
    "Status": {  
      "State": "Absent"  
    },  
    "UpperThresholdCritical": 3.955,  
    "UpperThresholdFatal": 0,  
    "UpperThresholdNonCritical": 0  
  },  
  {  
    "@odata.id": "/redfish/v1/Chassis/1/Power#/voltages/2",  
    "LowerThresholdCritical": 0.802,  
    "LowerThresholdFatal": 0,  
    "LowerThresholdNonCritical": 0,  
    "MaxReadingRange": 1.811,  
    "MemberId": "2",  
    "MinReadingRange": 0,  
    "Name": "CPU1_PVNN_MAIN",  
    "PhysicalContext": "VoltageRegulator",  
    "ReadingVolts": 0.014,  
    "SensorNumber": 2,  
    "Status": {  
      "Health": "Critical",  
      "State": "Enabled"  
    },  
    "UpperThresholdCritical": 1.2,  
    "UpperThresholdFatal": 0,  
    "UpperThresholdNonCritical": 0  
  },  
  {  
    "@odata.id": "/redfish/v1/Chassis/1/Power#/voltages/3",  
    "LowerThresholdCritical": 0.802,  
    "LowerThresholdFatal": 0,  
    "LowerThresholdNonCritical": 0,  
  }  
]
```



```

        "MaxReadingRange": 1.811,
        "MemberId": "3",
        "MinReadingRange": 0,
        "Name": "CPU0_PVNN_MAIN",
        "PhysicalContext": "VoltageRegulator",
        "SensorNumber": 3,
        "Status": {
            "State": "Absent"
        },
        "UpperThresholdCritical": 1.2,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Power#/voltages/4",
        "LowerThresholdCritical": 2.3,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 3.621,
        "MemberId": "4",
        "MinReadingRange": 0,
        "Name": "CPU1_PVPP_HBM",
        "PhysicalContext": "VoltageRegulator",
        "SensorNumber": 4,
        "Status": {
            "State": "Absent"
        },
        "UpperThresholdCritical": 2.797,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    }
],
"Redundancy": [
    {
        "@odata.id": "/redfish/v1/Chassis/1/Power#/Redundancy/1",
        "Mode": "Sharing",
        "Name": "PowerSupply Redundancy Group 1"
    }
]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the power supply information about the specified Chassis, refer to [Table 6-32](#).

Table 6-32 Output Descriptions for Querying the Power Supply Information About the Specified Chassis

Field	Type	Description
@odata.context	String	OData description of the power supply resource model.
@odata.id	String	Access path of the power resource.
@odata.type	String	Type of power supply resource.
Description	String	Description.
Id	String	ID of the power supply resource.
Name	String	Name of the power supply resource.
PowerControl	Array	Power control list.
PowerControl.@odata.id	String	Access path of the specified power control.
PowerControl.MemberId	String	ID of the specified power control. The ID is the unique identifier of the power control in the power control list.
PowerControl.Name	String	Name of the specified power control.
PowerLimit	Object	Power capping information.
PowerControl.PowerLimit.PowerLimitEnable	Boolean	Whether power capping is enabled.
PowerControl.PowerLimit.LimitInWatts	Number	Server power limit: - Value: Power capping is enabled. The value indicates the currently valid configuration value. - null: Power capping is disabled.
PowerControl.PowerLimit.LimitException	String	Action to be taken when power capping becomes invalid. Value: NoAction (no action).
PowerControl.PowerMetrics.AverageConsumedWatts	Number	Average power in the latest measurement interval.
PowerControl.PowerMetrics.IntervalInMin	Number	Measurement interval.
PowerControl.PowerMetrics.MaxConsumedWatts	Number	Highest power consumption level.

Field	Type	Description
PowerControl.PowerMetrics.MinConsumedWatts	Number	Lowest power consumption level.
PowerControl.PowerLimit.PowerConsumedWatts	Number	Current power of the device.
PowerControl.PowerLimit.Oem.Public	Object	Customized properties.
PowerControl.ExpectedActivePSU.@odata.id	String	Access path of a specified power supply.
PowerControl.CurrentCPUPowerWatts	Number	Current CPU power consumption.
PowerControl.CurrentFanPowerWatts	Number	Current fan power consumption.
PowerControl.CurrentMemoryPowerWatts	Number	Current memory power consumption.
CurrentHDDPowerWatts	Number	Current hard disk power consumption.
PowerControl@odata.count	Number	Array size of the power control list.
PowerSupplies	Array	Power supply list. The Status field indicates whether or not the corresponding power module is present.
PowerSupplies.FirmwareVersion	String	Firmware version of the specified power supply.
PowerSupplies.LineInputVoltage	Number	Input voltage of the specified power supply.
PowerSupplies.Manufacturer	String	Manufacturer of the specified power supply.
PowerSupplies.Model	String	Model of the specified power supply.
PowerSupplies.Name	String	Name of the specified power supply.
PowerSupplies.PowerCapacityWatts	Number	Rated power of the specified power supply.
PowerSupplies.PowerInputWatts	Number	Input power of the specified power supply.
PowerSupplies.PowerOutputWatts	Number	Output power of the specified power supply.
PowerSupplies.PowerSupplyType	String	Type of the specified power supply.
PowerSupplies.ProductionDate	String	Production date of the specified power module.

Field	Type	Description
PowerSupplies.SerialNumber	String	Serial number of the specified power supply.
PowerSupplies.Status	Object	Power supply status, including: ● State: whether the power supply is enabled. ● Health: health status of the power supply.
Oem.Public	Object	Customized properties.
PowerSupplies.Oem.Public.SlotNumber	Number	Slot number of the specified power supply.
PowerSupplies.Oem.Public.ActiveStandby	String	Active or standby power supply mode. Active: active mode. Standby: standby mode.
PowerSupplies.MemberId	String	ID of the specified power supply. The ID is the unique identifier of the power supply in the power supply list.
PowerSupplies@odata.count	Number	Number of power supplies.
Voltages.LowerThresholdCritical	Number	Critical warning threshold for low voltage of the specified voltage sensor.
Voltages.LowerThresholdFatal	Number	Fatal warning threshold for low voltage of the specified voltage sensor.
Voltages.LowerThresholdNonCritical	Number	Noncritical warning threshold for low voltage of the specified voltage sensor.
Voltages.MaxReadingRange	Number	Maximum voltage reading for the specified voltage sensor.
Voltages.MemberId	String	ID of the specified voltage sensor.
Voltages.MinReadingRange	Number	Minimum voltage reading for the specified voltage sensor.
Voltages.Name	String	Name of the specified voltage sensor.
Voltages.ReadingVolts	Number	Current reading of the specified voltage sensor. If no voltage value is obtained from the current voltage sensor, this field will be not displayed.
Voltages.SensorNumber	Number	Serial number of the specified voltage sensor.
Voltages.Status.State	String	Status of the specified voltage sensor.
Voltages.Status.Health	String	Health status of the specified voltage sensor.
Voltages.UpperThresholdCritical	Number	Critical warning threshold for high voltage of the specified voltage sensor.

Field	Type	Description
Voltages.UpperThresholdFatal	Number	Fatal warning threshold for high voltage of the specified voltage sensor.
Voltages.LowerThresholdNon-Critical	Number	Noncritical warning threshold for low voltage of the specified voltage sensor.
Voltages.@odata.id	String	Access path of the specified voltage sensor.
Redundancy.@odata.id	String	Access path of a specified power redundancy group.
Redundancy.Name	String	Name of the specified power redundancy group.
Redundancy.Mode	String	Redundancy mode of the specified power redundancy group: ● Sharing: load balancing mode. ● Failover: active-standby mode.
Actions	Object	Power operations.
#Power.CollectHistoryData.target	String	Operation path for collecting historical power statistics.

6.17 Collecting Information About Power Statistics

Function

Collect the information about the power statistics of the last 24 hours.

Permission Required

Query.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/Chassis/Chassis_id/Power/Actions/Power.CollectHistoryData`
- Request Header: None

```
X-Auth-Token: auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "Range": range_value,
  "Cycle": cycle_value
}
```

Parameters

For a description of the parameters for collecting the information about the power statistics of the last 24 hours, refer to [Table 6-33](#).

Table 6-33 Parameter Descriptions for Querying Information About Power Statistics

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self .
auth_value	When the post request is executed, the "X-Auth-Token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
range_value	Power statistics collection range.	- Day: daily statistics. - Week: weekly statistics.
cycle_value	Power statistics collection period.	- Hour: Statistics are collected once an hour (applicable to daily statistics). - Day: Statistics are collected once a day (applicable to weekly statistics).

Usage Guidelines

When the TFTP protocol is used for transmission, the TFTP server needs to be enabled on the server end, for example, through the 3CD software.

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Chassis/1/Power/Actions/Power.CollectHistoryData
```

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type: application/json
```

- Request message body:

```
{
  "Range": "Day",
  "Cycle": "Hour"
}
```

- Response Example 1: Refer to the CSV file.
Perform the following steps to get the CSV file:

Click **Send and Download** on the Postman. Select a path to save the CSV file.

- Response code: 200

Output Description

None.

6.18 Modifying Properties of a Specified Power Supply

Function

Modify properties of a specified power supply of a server.

Permission Required

Power control

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/Chassis/Chassis_id/Power*
- Request Header:

```
x-auth-token:auth_value  
Content-Type: header_type
```

- Request message body:
 - Power capping parameter configuration:

```
{  
  "PowerControl": [  
    {  
      "PowerLimit": {  
        "LimitInWatts": limit_value  
      }  
    }  
  ]  
}
```

- Active power supply configuration:

```
{  
  "Redundancy": [  
    {  
      "Mode": redundancy_type  
    }  
  ],  
  "PowerControl": [  
    {  
      "PowerLimit": {  
        "LimitInWatts": limit_value  
      }  
    }  
  ]  
}
```

```

{
  "Oem": {
    "Public": {
      "ExpectedActivePSU": [
        {
          "@odata.id":
            "/redfish/v1/Chassis/1/Power#/PowerSupplies/power_id"
        }
      ],
      "ExpectedRedundancy": [
        {
          "@odata.id":
            "/redfish/v1/Chassis/1/Power#/Redundancy/redundancy_id"
        }
      ]
    }
  }
}

```

Parameters

For a description of the parameters for modifying properties of the specified power supply, refer to [Table 6-34](#).

Table 6-34 Parameter Descriptions for Modifying Properties of the Specified Power Supply

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
limit_value	Server power capping value	- Integer: Power capping is enabled and the capping values are set. Range: 1–32767 - null: Power capping is disabled
power_id	Slot number of the power supply.	Set it in accordance with the number of power supplies of different models. Range: 1–4.

Parameter	Description	Value
redundancy_id	Power group ID.	Set it as required.
redundancy_type	Power redundancy type.	Power redundancy type. Options: ● Sharing: If redundancy_type is set to Sharing, Oem does not need to be configured. ● Failover

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Chassis/1/Power
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=  
Content-Type: application/json
```

- Request Message Body1:

```
{  
  "PowerControl": [  
    {  
      "PowerLimit": {  
        "LimitInWatts": 700  
      }  
    }  
  ]  
}
```

- Request Message Body2:

```
{  
  "Redundancy": [  
    {  
      "Mode": "Failover"  
    }  
  ],  
  "PowerControl": [  
    {  
      "Oem": {  
        "Public": {  
          "ExpectedActivePSU": [  

```

```

        {
            "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/1"
        }
    ],
    "ExpectedRedundancy": [
        {
            "@odata.id": "/redfish/v1/Chassis/1/Power#/Redundancy/1"
        }
    ]
}
}
}
]
}

```

- Response Example:

```

{
  "@odata.context": "/redfish/v1/$metadata#Power.Power",
  "@odata.id": "/redfish/v1/Chassis/1/Power",
  "@odata.type": "#Power.v1_5_4.Power",
  "Description": "Power sensor readings",
  "Id": "Power",
  "Name": "Power",
  "PowerControl": [
    {
      "Name": "Chassis Power Control",
      "PowerLimit": {
        "LimitInWatts": 550,
        "PowerLimitEnable": true,
        "LimitException": "NoAction"
      },
      "PowerMetrics": {
        "AverageConsumedWatts": 0,
        "IntervalInMin": 0,
        "MaxConsumedWatts": 0,
        "MinConsumedWatts": 0
      },
      "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerControl/1",
      "MemberId": "1",
      "PowerConsumedWatts": 29,
      "Oem": {
        "Public": {
          "ExpectedActivePSU": [
            {

```

```

        "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/1"
      },
      {
        "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/4"
      }
    ],
    "CurrentCPUPowerWatts": 0,
    "CurrentFanPowerWatts": 0,
    "CurrentMemoryPowerWatts": 0,
    "CurrentHDDPowerWatts": 0
  }
}

],
"PowerControl@odata.count": 1,
"PowerSupplies": [
  {
    "FirmwareVersion": "DC:1.01 PFC:1.00",
    "LineInputVoltage": 217,
    "Manufacturer": "Great wall",
    "Model": "CRPS1200D",
    "Name": "PSU1",
    "PowerCapacityWatts": 1200,
    "PowerInputWatts": 26,
    "PowerOutputWatts": 5,
    "PowerSupplyType": "AC",
    "SerialNumber": "22M010020400",
    "Status": {
      "Health": "OK",
      "State": "Enabled"
    },
    "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/1",
    "Oem": {
      "Public": {
        "SlotNumber": 1,
        "ActiveStandby": "Active"
      }
    },
    "MemberId": "1"
  },
  {
    "FirmwareVersion": "N/A",
    "LineInputVoltage": 0,
    "Manufacturer": "N/A",

```

```
"Model": "N/A",
"Name": "PSU2",
"PowerCapacityWatts": 65535,
"PowerInputWatts": 65535,
"PowerOutputWatts": 65535,
"PowerSupplyType": "N/A",
"SerialNumber": "N/A",
"Status": {
  "Health": "Warning",
  "State": "Disabled"
},
"@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/2",
"Oem": {
  "Public": {
    "SlotNumber": 2,
    "ActiveStandby": "Standby"
  }
},
"MemberId": "2"
},
{
  "FirmwareVersion": "N/A",
  "LineInputVoltage": 0,
  "Manufacturer": "N/A",
  "Model": "N/A",
  "Name": "PSU3",
  "PowerCapacityWatts": 65535,
  "PowerInputWatts": 65535,
  "PowerOutputWatts": 65535,
  "PowerSupplyType": "N/A",
  "SerialNumber": "N/A",
  "Status": {
    "Health": "Warning",
    "State": "Disabled"
  },
  "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/3",
  "Oem": {
    "Public": {
      "SlotNumber": 3,
      "ActiveStandby": "Standby"
    }
  },
  "MemberId": "3"
},
```

```

    {
      "FirmwareVersion": "DC:1.01 PFC:1.00",
      "LineInputVoltage": 0,
      "Manufacturer": "Great wall",
      "Model": "CRPS1200D",
      "Name": "PSU4",
      "PowerCapacityWatts": 1200,
      "PowerInputWatts": 0,
      "PowerOutputWatts": 0,
      "PowerSupplyType": "AC",
      "SerialNumber": "22M010020399",
      "Status": {
        "Health": "Warning",
        "State": "Enabled"
      },
      "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/4",
      "Oem": {
        "Public": {
          "SlotNumber": 4,
          "ActiveStandby": "Active"
        }
      },
      "MemberId": "4"
    }
  ],
  "PowerSupplies@odata.count": 4,
  "Actions": {
    "#Power.CollectHistoryData": {
      "target": "/redfish/v1/Chassis/1/Power/Actions/Power.CollectHistoryData"
    }
  },
  "Voltages": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/1",
      "LowerThresholdCritical": 2.643,
      "LowerThresholdFatal": 0,
      "LowerThresholdNonCritical": 0,
      "MaxReadingRange": 4.463,
      "MemberId": "1",
      "MinReadingRange": 0,
      "Name": "RGM_VCC3.3V",
      "PhysicalContext": "VoltageRegulator",
      "SensorNumber": 1,
      "Status": {

```

```
        "State": "Absent"
    },
    "UpperThresholdCritical": 3.955,
    "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
},
{
    "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/2",
    "LowerThresholdCritical": 0.802,
    "LowerThresholdFatal": 0,
    "LowerThresholdNonCritical": 0,
    "MaxReadingRange": 1.811,
    "MemberId": "2",
    "MinReadingRange": 0,
    "Name": "CPU1_PVNN_MAIN",
    "PhysicalContext": "VoltageRegulator",
    "ReadingVolts": 0.014,
    "SensorNumber": 2,
    "Status": {
        "Health": "Critical",
        "State": "Enabled"
    },
    "UpperThresholdCritical": 1.2,
    "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
},
{
    "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/3",
    "LowerThresholdCritical": 0.802,
    "LowerThresholdFatal": 0,
    "LowerThresholdNonCritical": 0,
    "MaxReadingRange": 1.811,
    "MemberId": "3",
    "MinReadingRange": 0,
    "Name": "CPU0_PVNN_MAIN",
    "PhysicalContext": "VoltageRegulator",
    "SensorNumber": 3,
    "Status": {
        "State": "Absent"
    },
    "UpperThresholdCritical": 1.2,
    "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
},
```

```

    {
      "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/4",
      "LowerThresholdCritical": 2.3,
      "LowerThresholdFatal": 0,
      "LowerThresholdNonCritical": 0,
      "MaxReadingRange": 3.621,
      "MemberId": "4",
      "MinReadingRange": 0,
      "Name": "CPU1_PVPP_HBM",
      "PhysicalContext": "VoltageRegulator",
      "SensorNumber": 4,
      "Status": {
        "State": "Absent"
      },
      "UpperThresholdCritical": 2.797,
      "UpperThresholdFatal": 0,
      "UpperThresholdNonCritical": 0
    }
  ],
  "Redundancy": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Power#/Redundancy/1",
      "Mode": "Sharing",
      "Name": "PowerSupply Redundancy Group 1"
    }
  ]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you modify properties of the specified power supply, refer to [Table 6-35](#).

Table 6-35 Output Descriptions for Modifying Properties of the Specified Power Supply

Field	Type	Description
@odata.context	String	OData description of the power supply resource model.
@odata.id	String	Access path of the power resource.
@odata.type	String	Type of power supply resource.
Description	String	Description.
Id	String	ID of the power supply resource.

Field	Type	Description
Name	String	Name of the power supply resource.
PowerControl	Array	Power control list.
PowerControl.@odata.id	String	Access path of the specified power control.
PowerControl.MemberId	String	ID of the specified power control. The ID is the unique identifier of the power control in the power control list.
PowerControl.Name	String	Name of the specified power control.
PowerLimit	Object	Power capping information.
PowerControl.PowerLimit.PowerLimitEnable	Boolean	Whether power capping is enabled.
PowerControl.PowerLimit.LimitInWatts	Number	Server power limit: - Value: Power capping is enabled. The value indicates the currently valid configuration value. - null: Power capping is disabled.
PowerControl.PowerLimit.LimitException	String	Action to be taken when power capping becomes invalid. Value: NoAction (no action).
PowerControl.PowerMetrics.AverageConsumedWatts	Number	Average power in the latest measurement interval.
PowerControl.PowerMetrics.IntervalInMin	Number	Measurement interval.
PowerControl.PowerMetrics.MaxConsumedWatts	Number	Highest power consumption level.
PowerControl.PowerMetrics.MinConsumedWatts	Number	Lowest power consumption level.
PowerControl.PowerLimit.PowerConsumedWatts	Number	Current power of the device.
PowerControl.PowerLimit.Oem.Public	Object	Customized properties.
PowerControl.ExpectedActivePSU.@odata.id	String	Access path of a specified power supply.
PowerControl.CurrentCPUPowerWatts	Number	Current CPU power consumption.
PowerControl.CurrentFanPowerWatts	Number	Current fan power consumption.

Field	Type	Description
PowerControl.CurrentMemory-PowerWatts	Number	Current memory power consumption.
CurrentHDDPowerWatts	Number	Current hard disk power consumption.
PowerControl@odata.count	Number	Array size of the power control list.
PowerSupplies	Array	Power supply list. The Status field indicates whether or not the corresponding power module is present.
PowerSupplies.FirmwareVersion	String	Firmware version of the specified power supply.
PowerSupplies.LineInputVoltage	Number	Input voltage of the specified power supply.
PowerSupplies.Manufacturer	String	Manufacturer of the specified power supply.
PowerSupplies.Model	String	Model of the specified power supply.
PowerSupplies.Name	String	Name of the specified power supply.
PowerSupplies.PowerCapacity-Watts	Number	Rated power of the specified power supply.
PowerSupplies.PowerInput-Watts	Number	Input power of the specified power supply.
PowerSupplies.PowerOutput-Watts	Number	Output power of the specified power supply.
PowerSupplies.PowerSupply-Type	String	Type of the specified power supply.
PowerSupplies.ProductionDate	String	Production date of the specified power module.
PowerSupplies.SerialNumber	String	Serial number of the specified power supply.
PowerSupplies.Status	Object	Power supply status, including: ● State: whether the power supply is enabled. ● Health: health status of the power supply.
Oem.Public	Object	Customized properties.
PowerSupplies.Oem.Public.SlotNumber	Number	Slot number of the specified power supply.
PowerSupplies.Oem.Public.ActiveStandby	String	Active or standby power supply mode. Active: active mode. Standby: standby mode.
PowerSupplies.MemberId	String	ID of the specified power supply. The ID is the unique identifier of the power supply in the power supply list.

Field	Type	Description
PowerSupplies@odata.count	Number	Number of power supplies.
Voltages.LowerThresholdCritical	Number	Critical warning threshold for low voltage of the specified voltage sensor.
Voltages.LowerThresholdFatal	Number	Fatal warning threshold for low voltage of the specified voltage sensor.
Voltages.LowerThresholdNon-Critical	Number	Noncritical warning threshold for low voltage of the specified voltage sensor.
Voltages.MaxReadingRange	Number	Maximum voltage reading for the specified voltage sensor.
Voltages.MemberId	String	ID of the specified voltage sensor.
Voltages.MinReadingRange	Number	Minimum voltage reading for the specified voltage sensor.
Voltages.Name	String	Name of the specified voltage sensor.
Voltages.ReadingVolts	Number	Current reading of the specified voltage sensor. If no voltage value is obtained from the current voltage sensor, this field will be not displayed.
Voltages.SensorNumber	Number	Serial number of the specified voltage sensor.
Voltages.Status.State	String	Status of the specified voltage sensor.
Voltages.Status.Health	String	Health status of the specified voltage sensor.
Voltages.UpperThresholdCritical	Number	Critical warning threshold for high voltage of the specified voltage sensor.
Voltages.UpperThresholdFatal	Number	Fatal warning threshold for high voltage of the specified voltage sensor.
Voltages.LowerThresholdNon-Critical	Number	Noncritical warning threshold for low voltage of the specified voltage sensor.
Voltages.@odata.id	String	Access path of the specified voltage sensor.
Redundancy.@odata.id	String	Access path of a specified power redundancy group.
Redundancy.Name	String	Name of the specified power redundancy group.
Redundancy.Mode	String	Redundancy mode of the specified power redundancy group: ● Sharing: load balancing mode. ● Failover: active-standby mode.
Actions	Object	Power operations.

Field	Type	Description
#Power.CollectHistoryData.target	String	Operation path for collecting historical power statistics.

6.19 Querying Cooling Resource Information About a Specified Chassis

Function

Query the temperature and fan sensor information about a specified Chassis.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/Chassis_id/Thermal`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the temperature and fan sensor information about a specified Chassis, refer to [Table 6-36](#).

Table 6-36 Parameter Descriptions for Querying the Temperature and Fan Sensor Resource Information About the Specified Chassis

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Thermal
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Thermal.Thermal",
  "@odata.id": "/redfish/v1/Chassis/1/Thermal",
  "@odata.type": "#Thermal.v1_5_3.Thermal",
  "Description": "Thermal sensor readings",
  "Oem": {
    "Public": {
      "FanSpeedAdjustmentMode": "Manual",
      "SpeedRatio": 24
    }
  },
  "FanSummary": {
    "Count": 4
  },
  "Fans": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/0",
      "MemberId": "0",
      "Name": "FAN_SPEED_01",
      "LowerThresholdCritical": 1000,
      "LowerThresholdFatal": null,
      "LowerThresholdNonCritical": null,
      "UpperThresholdCritical": 16500,
      "UpperThresholdFatal": null,
      "UpperThresholdNonCritical": null,
      "SerialNumber": "20150305",
      "Status": {
        "Health": "OK",
        "State": "Enabled"
      },
      "Oem": {
        "Public": {
          "SlotNumber": 1,
          "FanName": "FAN1",
          "SpeedRatio": 24
        }
      }
    }
  ],
}
```

```
    "Reading": 3600,
    "ReadingUnits": "RPM",
    "MinReadingRange": 1000,
    "MaxReadingRange": 16500,
    "Model": "8038"
  },
  {
    "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/1",
    "MemberId": "1",
    "Name": "FAN_SPEED_02",
    "LowerThresholdCritical": 1000,
    "LowerThresholdFatal": null,
    "LowerThresholdNonCritical": null,
    "UpperThresholdCritical": 16500,
    "UpperThresholdFatal": null,
    "UpperThresholdNonCritical": null,
    "SerialNumber": "20150305",
    "Status": {
      "Health": "OK",
      "State": "Enabled"
    },
    "Oem": {
      "Public": {
        "SlotNumber": 2,
        "FanName": "FAN2",
        "SpeedRatio": 24
      }
    },
    "Reading": 3600,
    "ReadingUnits": "RPM",
    "MinReadingRange": 1000,
    "MaxReadingRange": 16500,
    "Model": "8038"
  },
  {
    "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/2",
    "MemberId": "2",
    "Name": "FAN_SPEED_03",
    "LowerThresholdCritical": 1000,
    "LowerThresholdFatal": null,
    "LowerThresholdNonCritical": null,
    "UpperThresholdCritical": 16500,
    "UpperThresholdFatal": null,
    "UpperThresholdNonCritical": null,
```

```
"SerialNumber": "20150305",
"Status": {
  "Health": "OK",
  "State": "Enabled"
},
"Oem": {
  "Public": {
    "SlotNumber": 3,
    "FanName": "FAN3",
    "SpeedRatio": 24
  }
},
"Reading": 3600,
"ReadingUnits": "RPM",
"MinReadingRange": 1000,
"MaxReadingRange": 16500,
"Model": "8038"
},
{
  "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/3",
  "MemberId": "3",
  "Name": "FAN_SPEED_04",
  "LowerThresholdCritical": 1000,
  "LowerThresholdFatal": null,
  "LowerThresholdNonCritical": null,
  "UpperThresholdCritical": 16500,
  "UpperThresholdFatal": null,
  "UpperThresholdNonCritical": null,
  "SerialNumber": "20150305",
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  },
  "Oem": {
    "Public": {
      "SlotNumber": 4,
      "FanName": "FAN4",
      "SpeedRatio": 24
    }
  },
  "Reading": 3600,
  "ReadingUnits": "RPM",
  "MinReadingRange": 1000,
  "MaxReadingRange": 16500,
```

```
        "Model": "8038"
      }
    ],
    "Id": "Thermal",
    "Name": "Thermal",
    "Temperatures": [
      {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/0",
        "LowerThresholdCritical": null,
        "LowerThresholdFatal": null,
        "LowerThresholdNonCritical": null,
        "MinReadingRangeTemp": -128,
        "MaxReadingRangeTemp": 127,
        "MemberId": "0",
        "Name": "INPUT_TEMP",
        "PhysicalContext": "Intake",
        "ReadingCelsius": 30,
        "SensorNumber": 31,
        "Status": {
          "Health": "OK",
          "State": "Enabled"
        },
        "UpperThresholdCritical": 50,
        "UpperThresholdFatal": 52,
        "UpperThresholdNonCritical": 45
      },
      {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/1",
        "LowerThresholdCritical": null,
        "LowerThresholdFatal": null,
        "LowerThresholdNonCritical": null,
        "MinReadingRangeTemp": -128,
        "MaxReadingRangeTemp": 127,
        "MemberId": "1",
        "Name": "OUTPUT_TEMP",
        "PhysicalContext": "Intake",
        "ReadingCelsius": 39,
        "SensorNumber": 32,
        "Status": {
          "Health": "OK",
          "State": "Enabled"
        },
        "UpperThresholdCritical": null,
        "UpperThresholdFatal": null,

```

```
        "UpperThresholdNonCritical": null
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/2",
        "LowerThresholdCritical": null,
        "LowerThresholdFatal": null,
        "LowerThresholdNonCritical": null,
        "MinReadingRangeTemp": -128,
        "MaxReadingRangeTemp": 127,
        "MemberId": "2",
        "Name": "CPU1_TEMP",
        "PhysicalContext": "Intake",
        "ReadingCelsius": 62,
        "SensorNumber": 40,
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        },
        "UpperThresholdCritical": 90,
        "UpperThresholdFatal": null,
        "UpperThresholdNonCritical": null
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/3",
        "LowerThresholdCritical": null,
        "LowerThresholdFatal": null,
        "LowerThresholdNonCritical": null,
        "MinReadingRangeTemp": -128,
        "MaxReadingRangeTemp": 127,
        "MemberId": "3",
        "Name": "CPU2_TEMP",
        "PhysicalContext": "Intake",
        "ReadingCelsius": 59,
        "SensorNumber": 43,
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        },
        "UpperThresholdCritical": 90,
        "UpperThresholdFatal": null,
        "UpperThresholdNonCritical": null
    }
]
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query the temperature and fan sensor resource information about the specified Chassis, refer to [Table 6-37](#).

Table 6-37 Output Descriptions for Querying the Temperature and Fan Sensor Resource Information About the Specified Chassis

Field	Type	Description
@odata.context	String	OData description of the cooling resource.
@odata.id	String	Access path of the cooling resource.
@odata.type	String	Type of cooling resource.
Description	String	Description of the cooling resource.
Id	String	ID of the cooling resource.
Name	String	Name of the cooling resource.
Oem.Public.FanSpeedAdjustmentMode	String	This field is displayed when Oem.Public.FanSpeedAdjustmentMode is set to Automatic . Fan speed adjustment mode, including: • Automatic mode • Manual mode
Oem.Public.FanSmartCoolingMode	String	Fan speed smart-adjustment mode, including: • NormalMode: balance mode • LowNoiseMode: low noise mode • HighPerformanceMode: high-performance mode
Oem.Public.SpeedRatio	Number	Fan rotation speed ratio in percentage terms.
Temperatures.@odata.id	String	Access path of the specified temperature sensor.
Temperatures.LowerThreshold-Critical	Number	Critical warning threshold for low speed rotation of the specified fan sensor.
Temperatures.LowerThreshold-Fatal	Number	Fatal warning threshold for high speed rotation of the specified fan sensor.
Temperatures.LowerThreshold-NonCritical	Number	Noncritical warning threshold for low speed rotation of the specified fan sensor.
Temperatures.MemberId	String	ID of the specified temperature sensor.
Temperatures.Name	String	Name of the specified temperature sensor.
Temperatures.PhysicalContext	String	Area or device to which the temperature measurement applies.

Field	Type	Description
Temperatures.ReadingCelsius	Number	Current reading of the specified temperature sensor.
Temperatures.SensorNumber	String	Serial number of the specified temperature sensor.
Temperatures.Status.State	String	Status of the specified temperature sensor.
Temperatures.Status.Health	String	Health status of the specified temperature sensor.
Temperatures.UpperThreshold-Critical	Number	Critical warning threshold for high speed rotation of the specified fan sensor.
Temperatures.UpperThreshold-Fatal	Number	Fatal warning threshold for high speed rotation of the specified fan sensor.
Temperatures.UpperThreshold-NonCritical	Number	Noncritical warning threshold for low speed rotation of the specified fan sensor.
Temperatures.MinReadingRange	Number	Minimum rotation speed reading for the specified fan sensor.
Temperatures.MaxReadingRange	Number	Maximum rotation speed reading for the specified fan sensor.
FanSummary.Count	Number	Number of fan sensors.
Fans.Name	String	Name of the specified fan sensor.
Fans.LowerThresholdCritical	Number	Critical alarm threshold for the low temperature of the specified fan sensor.
Fans.LowerThresholdFatal	Number	Fatal alarm threshold for the low temperature of the specified fan sensor.
Fans.LowerThresholdNonCritical	Number	Noncritical alarm threshold for the low temperature of the specified fan sensor.
Fans.UpperThresholdCritical	Number	Critical alarm threshold for overtemperature of the specified fan sensor.
Fans.UpperThresholdFatal	Number	Fatal alarm threshold for overtemperature of the specified fan sensor.
Fans.UpperThresholdNonCritical	Number	Noncritical alarm threshold for overtemperature of the specified fan sensor.
Fans.SerialNumber	Number	Serial number of the specified fan sensor.
Fans.Status.State	String	Status of the specified fan sensor.
Fans.Status.Health	String	Health status of the specified fan sensor.
Fans.Oem.Public.SlotNumber	Number	Slot number of the specified fan sensor.

Field	Type	Description
Fans.Oem.Public.FanName	String	Name of the fan that the specified fan sensor belongs to.
Fans.Oem.Public.SpeedRatio	Number	Current reading of the specified fan sensor, in percentage.
Fans.Reading	Number	Current reading of the specified fan sensor.
Fans.ReadingUnits	String	Unit of the fan rotation speed reading for the fan sensor, including: • RPM • Percent
Fans.MinReadingRange	Number	Minimum rotation speed reading for the specified fan sensor.
Fans.MaxReadingRange	Number	Maximum rotation speed reading for the specified fan sensor.
Fans.Model	String	Model of the specified fan sensor.
Fans.@odata.id	String	Access path of the specified fan sensor.

6.20 Querying Information About the Expansion Board Resource Collection

Function

Query the information about the expansion board resource collection.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/Boards`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the information about the expansion board resource collection, refer to [Table 6-38](#).

Table 6-38 Parameter Descriptions for Querying Information About the Expansion Board Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self .
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Boards
```

- Request Header:

```
X-Auth-Token: 8574621db1284756218c7564821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#BoardInformation.BoardInformation",
  "@odata.id": "/redfish/v1/Chassis/1/Boards",
  "@odata.type": "#BoardInformation.BoardInformation",
  "Description": "Board Information",
  "DiskBackplanes": {
    "@odata.id": "/redfish/v1/Chassis/1/Boards/DiskBackplanes"
  },
  "Risercard": {
    "@odata.id": "/redfish/v1/Chassis/1/Boards/Risercard"
  },
  "Id": "Boards",
  "Name": "Board Information"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the expansion board resource collection, refer to [Table 6-39](#).

Table 6-39 Output Descriptions for Querying Information About the Expansion Board Resource Collection

Field	Type	Description
@odata.context	String	OData description of the expansion board resource collection module.
@odata.id	String	Access path of the expansion board resource collection.
@odata.type	String	Type of expansion board resource collection.
Description	String	Description of the expansion board resource collection.
DiskBackplanes	Object	Information about hard disk backplanes.
Risercard	Object	Riser card collection information.
Id	String	ID of the expansion board resource collection.
@odata.id	String	Access path of the riser card.
Name	String	Board name.

6.21 Querying Information About the Hard Disk Backplane Resource Collection

Function

Query the information about the hard disk backplane resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/Chassis_id/Boards/DiskBackplanes`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the information about the hard disk backplane resource collection, refer to [Table 6-40](#).

Table 6-40 Parameter Descriptions for Querying Information About the Hard Disk Backplane Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self .
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Boards/DiskBackplanes
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#DiskBackplanesCollection.DiskBackplanesCollection",
  "@odata.id": "/redfish/v1/Chassis/1/Boards/DiskBackplanes",
  "@odata.type": "#DiskBackplanesCollection.DiskBackplanesCollection",
  "Description": "DiskBackplanes Collection",
  "Name": "DiskBackplanes Collection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Boards/DiskBackplanes/DiskBackplanes10"
    },
    {
      "@odata.id": "/redfish/v1/Chassis/1/Boards/DiskBackplanes/DiskBackplanes11"
    }
  ],
  "Members@odata.count": 2
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the hard disk backplane resource collection, refer to [Table 6-41](#).

Table 6-41 Output Descriptions for Querying Information About the Hard Disk Backplane Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the hard disk backplane resource collection model.
@odata.id	Character string	Access path of the hard disk backplane resource collection.
@odata.type	Character string	Type of hard disk backplane resource collection.
Description	String	Description of the hard disk backplane resource collection.
Name	Character string	Name of the hard disk backplane resource collection.
Members@odata.count	Number	Current number of hard disk backplane resources.
Members	Array	Hard disk backplane resources list.
@odata.id	Character string	Access path of a hard disk backplane resource node.

6.22 Querying Information About a Specified Hard Disk Backplane Resource

Function

Query information about a specified hard disk backplane resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/Chassis_id/Boards/DiskBackplanes/DiskBackplaneId`
- Request Header:

x-auth-token:auth_value
- Request Message Body: None

Parameters

For a description of the parameters for querying the information about the specified hard disk backplane resource, refer to [Table 6-42](#).

Table 6-42 Parameter Descriptions for Querying Information About the Specified Hard Disk Backplane Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self .
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
DiskBackplaneId	ID of the specified hard disk backplane.	Obtained from the information about the slot of the hard disk backplane.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Boards/DiskBackplanes/DiskBackplane8
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#DiskBackplane.DiskBackplane",
  "@odata.id": "/redfish/v1/Chassis/1/Boards/DiskBackplanes/DiskBackplanes8",
  "@odata.type": "#DiskBackplane.v1_0_0.DiskBackplane",
  "Name": "SBF24MB",
  "CPLDVersion": null,
  "MaxDiskCountSupported": 24,
  "PartNumber": "19020100",
  "Location": "Front",
  "Manufacturer": "VANTAGEO",
  "PortCount": "SLIMSAS*2 + SLIMLINE*4",
  "SerialNumber": null,
  "Type": "3.5 SAS/SATA*24,U.2*8,Expander",
}
```



```

    "OnlineDiskCount": 0,
    "ID": 10,
    "PcbID": 1
  }

```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the specified hard disk backplane resource, refer to [Table 6-43](#).

Table 6-43 Output Descriptions for Querying Information About the Specified Hard Disk Backplane Resource

Field	Type	Description
@odata.context	String	OData description of the hard disk backplane resource collection model.
@odata.id	String	Access path of the hard disk backplane resource collection.
@odata.type	String	Type of hard disk backplane resource collection.
Name	String	Name of the hard disk backplane resource collection.
CPLDVersion	String	CPLD version of the specified hard disk backplane.
MaxDiskCountSupported	Number	Maximum number of hard disks supported by the specified hard disk backplane.
PartNumber	String	Part number of the specified hard disk backplane.
Location	String	Location of the specified hard disk backplane.
Manufacturer	String	Manufacturer of the specified hard disk backplane.
PortCount	String	Number of ports supported by the specified hard disk backplane.
SerialNumber	String	Serial number of the specified hard disk backplane.
Type	String	Type of the specified hard disk backplane.
OnlineDiskCount	Number	Number of present hard disks supported by the specified hard disk backplane.
ID	Number	Serial number of the specified hard disk backplane.
PcbID	Number	PCB ID of the specified hard disk backplane.

6.23 Querying Information About the Riser Card Resource Collection

Function

Query information about the Riser card resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Chassis/Chassis_id/Boards/Riser-card*
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the Riser card resource collection, refer to [Table 6-44](#).

Table 6-44 Parameter Descriptions for Querying Information About the Riser Card Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self .
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Chassis/1/Boards/Risercard

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#RisercardCollection.RisercardCollection",
  "@odata.id": "/redfish/v1/Chassis/1/Boards/Risercard",
  "@odata.type": "#RisercardCollection.RisercardCollection",
  "Description": "Risercard Collection",
  "Name": "Risercard Collection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Boards/Risercard/Risercard6"
    }
  ],
  "Members@odata.count": 1
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the riser card resource collection, refer to [Table 6-45](#).

Table 6-45 Output Descriptions for Querying Information About the Riser Card Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the riser card resource collection model.
@odata.id	Character string	Access path of the riser card resource collection.
@odata.type	Character string	Type of riser card resource collection.
Description	Character string	Description of the riser card resource collection.
Name	Character string	Name of the riser card resource collection.
Members@odata.count	Number	Current number of riser card resources.
Members	Object array	Riser card resource list.
@odata.id	Character string	Access path of a riser card resource node.

6.24 Querying Information About a Specified Riser Card Resource

Function

Query the information about a specified riser card resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Chassis/Chassis_id/Boards/Risercard/RisercardId*
- Request Header:

x-auth-token:auth_value Content-Type:header_type

- Request Message Body: None

Parameters

For a description of the parameters for querying the information about the specified riser card resource, refer to [Table 6-46](#).

Table 6-46 Parameter Descriptions for Querying Information About the Specified Riser Card Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self .
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
RisercardId	ID of the specified riser card.	Obtained from the information about the slot of the riser card.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Boards/Risercard/Risercard6
```

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Risercard.Risercard",
  "@odata.id": "/redfish/v1/Chassis/1/Boards/Risercard/Risercard6",
  "@odata.type": "#Risercard.v1_0_0.Risercard",
  "Manufacturer": "VANTAGEO",
  "Name": "Risercard6",
  "PartNumber": "",
  "SerialNumber": "208540654320"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the specified riser card resource, refer to [Table 6-47](#).

Table 6-47 Output Descriptions for Querying Information About the Specified Riser Card Resource

Field	Type	Description
@odata.context	String	OData description of the specified riser card resource.
@odata.id	String	Access path of the specified riser card resource.
@odata.type	String	Type of the specified riser card resource.
Manufacturer	String	Manufacturer of the specified riser card.
Name	String	Name of the specified riser card resource.
PartNumber	String	Part number of the specified riser card resource.
SerialNumber	String	Serial number of the specified riser card resource.

6.25 Modifying the Cooling Resource Information About a Specified Chassis

Function

Modify the cooling resource information about a specified chassis of a server.

Permission Required

Basic management.

Syntax

- Operation Type: PATCH
- URL: `https://device_ip/redfish/v1/Chassis/Chassis_id/Thermal`
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "oem": {
    "Public": {
      "FanSpeedAdjustmentMode": fan_speed_adjustment_mode_value,
      "FanSmartCoolingMode": smart_cool_mode_value,
      "SpeedRatio": speed_ratio_value
    }
  }
}
```

Parameters

For a description of the parameters for modifying the cooling information about the specified chassis, refer to [Table 6-48](#).

Table 6-48 Parameter Descriptions for Modifying the Cooling Resource Information About a Specified Chassis

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the chassis resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
fan_speed_adjustment_mode_value	Fan speed adjustment mode.	• Automatic • Manual
smart_cool_mode_value	Smart fan speed adjustment mode.	• NormalMode: balance mode. • LowNoiseMode: low noise mode.

Parameter	Description	Value
	This parameter is required when model_value is set to Automatic .	● HighPerformanceMode: high performance mode.
speed_ratio_value	Fan rotation speed ratio. This parameter is required when model_value is set to Manual .	10~100

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Chassis/1/Thermal
```

- Request Header:

```
X-Auth-Token: LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=  
Content-Type: application/json
```

- Request Message Body:

```
{  
  "Oem": {  
    "Public": {  
      "FanSpeedAdjustmentMode": "Manual",  
      "SpeedRatio": 50  
    }  
  }  
}
```

- Response Example:

```
{  
  "@odata.context": "/redfish/v1/$metadata#Thermal.Thermal",  
  "@odata.id": "/redfish/v1/Chassis/1/Thermal",  
  "@odata.type": "#Thermal.v1_5_3.Thermal",  
  "Description": "Thermal sensor readings",  
  "Oem": {  
    "Public": {  
      "FanSpeedAdjustmentMode": "Manual",  
      "SpeedRatio": 50  
    }  
  },  
  "FanSummary": {
```

```
    "Count": 4
  },
  "Fans": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/0",
      "MemberId": "0",
      "Name": "FAN_SPEED_01",
      "LowerThresholdCritical": 1000,
      "LowerThresholdFatal": null,
      "LowerThresholdNonCritical": null,
      "UpperThresholdCritical": 16500,
      "UpperThresholdFatal": null,
      "UpperThresholdNonCritical": null,
      "SerialNumber": "20150305",
      "Status": {
        "Health": "OK",
        "State": "Enabled"
      },
      "Oem": {
        "Public": {
          "SlotNumber": 1,
          "FanName": "FAN1",
          "SpeedRatio": 50
        }
      },
      "Reading": 7500,
      "ReadingUnits": "RPM",
      "MinReadingRange": 1000,
      "MaxReadingRange": 16500,
      "Model": "8038"
    },
    {
      "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/1",
      "MemberId": "1",
      "Name": "FAN_SPEED_02",
      "LowerThresholdCritical": 1000,
      "LowerThresholdFatal": null,
      "LowerThresholdNonCritical": null,
      "UpperThresholdCritical": 16500,
      "UpperThresholdFatal": null,
      "UpperThresholdNonCritical": null,
      "SerialNumber": "20150305",
      "Status": {
        "Health": "OK",
```



```
        "State": "Enabled"
    },
    "Oem": {
        "Public": {
            "SlotNumber": 2,
            "FanName": "FAN2",
            "SpeedRatio": 50
        }
    },
    "Reading": 7500,
    "ReadingUnits": "RPM",
    "MinReadingRange": 1000,
    "MaxReadingRange": 16500,
    "Model": "8038"
},
{
    "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/2",
    "MemberId": "2",
    "Name": "FAN_SPEED_03",
    "LowerThresholdCritical": 1000,
    "LowerThresholdFatal": null,
    "LowerThresholdNonCritical": null,
    "UpperThresholdCritical": 16500,
    "UpperThresholdFatal": null,
    "UpperThresholdNonCritical": null,
    "SerialNumber": "20150305",
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "Oem": {
        "Public": {
            "SlotNumber": 3,
            "FanName": "FAN3",
            "SpeedRatio": 50
        }
    },
    "Reading": 7500,
    "ReadingUnits": "RPM",
    "MinReadingRange": 1000,
    "MaxReadingRange": 16500,
    "Model": "8038"
},
{
```

```
"@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/3",
"MemberId": "3",
"Name": "FAN_SPEED_04",
"LowerThresholdCritical": 1000,
"LowerThresholdFatal": null,
"LowerThresholdNonCritical": null,
"UpperThresholdCritical": 16500,
"UpperThresholdFatal": null,
"UpperThresholdNonCritical": null,
"SerialNumber": "20150305",
"Status": {
  "Health": "OK",
  "State": "Enabled"
},
"Oem": {
  "Public": {
    "SlotNumber": 4,
    "FanName": "FAN4",
    "SpeedRatio": 50
  }
},
"Reading": 7500,
"ReadingUnits": "RPM",
"MinReadingRange": 1000,
"MaxReadingRange": 16500,
"Model": "8038"
},
"Id": "Thermal",
"Name": "Thermal",
"Temperatures": [
  {
    "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/0",
    "LowerThresholdCritical": null,
    "LowerThresholdFatal": null,
    "LowerThresholdNonCritical": null,
    "MinReadingRangeTemp": -128,
    "MaxReadingRangeTemp": 127,
    "MemberId": "0",
    "Name": "INPUT_TEMP",
    "PhysicalContext": "Intake",
    "ReadingCelsius": 30,
    "SensorNumber": 31,
    "Status": {
```

```
        "Health": "OK",
        "State": "Enabled"
    },
    "UpperThresholdCritical": 50,
    "UpperThresholdFatal": 52,
    "UpperThresholdNonCritical": 45
},
{
    "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/1",
    "LowerThresholdCritical": null,
    "LowerThresholdFatal": null,
    "LowerThresholdNonCritical": null,
    "MinReadingRangeTemp": -128,
    "MaxReadingRangeTemp": 127,
    "MemberId": "1",
    "Name": "OUTPUT_TEMP",
    "PhysicalContext": "Intake",
    "ReadingCelsius": 39,
    "SensorNumber": 32,
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "UpperThresholdCritical": null,
    "UpperThresholdFatal": null,
    "UpperThresholdNonCritical": null
},
{
    "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/2",
    "LowerThresholdCritical": null,
    "LowerThresholdFatal": null,
    "LowerThresholdNonCritical": null,
    "MinReadingRangeTemp": -128,
    "MaxReadingRangeTemp": 127,
    "MemberId": "2",
    "Name": "CPU1_TEMP",
    "PhysicalContext": "Intake",
    "ReadingCelsius": 66,
    "SensorNumber": 40,
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "UpperThresholdCritical": 90,
```

```

        "UpperThresholdFatal": null,
        "UpperThresholdNonCritical": null
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/3",
        "LowerThresholdCritical": null,
        "LowerThresholdFatal": null,
        "LowerThresholdNonCritical": null,
        "MinReadingRangeTemp": -128,
        "MaxReadingRangeTemp": 127,
        "MemberId": "3",
        "Name": "CPU2_TEMP",
        "PhysicalContext": "Intake",
        "ReadingCelsius": 64,
        "SensorNumber": 43,
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        },
        "UpperThresholdCritical": 90,
        "UpperThresholdFatal": null,
        "UpperThresholdNonCritical": null
    }
]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you modify the cooling information about the specified chassis, refer to [Table 6-49](#).

Table 6-49 Output Descriptions for Modifying the Cooling Information About the Specified Chassis

Field	Type	Description
@odata.context	String	OData description of the cooling resource.
@odata.id	String	Access path of the cooling resource.
@odata.type	String	Type of cooling resource.
Description	String	Description of the cooling resource.
Id	String	ID of the cooling resource.
Name	String	Name of the cooling resource.

Field	Type	Description
Oem.Public.FanSpeedAdjustmentMode	String	Fan speed adjustment mode, including: ● Automatic ● Manual
Oem.Public.FanSmartCoolingMode	String	This field is displayed when Oem.Public.FanSpeedAdjustmentMode is set to Automatic . Smart fan speed adjustment mode, including: ● NormalMode: balance mode ● LowNoiseMode: low noise mode ● HighPerformanceMode: high-performance mode
Oem.Public.SpeedRatio	Number	Fan rotation speed ratio.
Temperatures.@odata.id	String	Access path of the specified temperature sensor.
Temperatures.LowerThreshold-Critical	Number	Critical alarm threshold for the low rotation speed of the specified fan sensor.
Temperatures.LowerThreshold-Fatal	Number	Fatal alarm threshold for the high rotation speed of the specified fan sensor.
Temperatures.LowerThreshold-NonCritical	Number	Noncritical alarm threshold for the low rotation speed of the specified fan sensor.
Temperatures.MemberId	String	ID of the specified temperature sensor.
Temperatures.Name	String	Name of the specified temperature sensor.
Temperatures.PhysicalContext	String	Area or device to which the temperature measurement applies.
Temperatures.ReadingCelsius	Number	Current reading of the specified temperature sensor.
Temperatures.SensorNumber	String	Serial number of the specified temperature sensor.
Temperatures.Status.State	String	Status of the specified temperature sensor.
Temperatures.Status.Health	String	Health status of the specified temperature sensor.
Temperatures.UpperThreshold-Critical	Number	Critical alarm threshold for overtemperature of the specified temperature sensor.
Temperatures.UpperThreshold-Fatal	Number	Fatal alarm threshold for overtemperature of the specified temperature sensor.
Temperatures.UpperThreshold-NonCritical	Number	Noncritical alarm threshold for overtemperature of the specified temperature sensor.
Temperatures.MinReadingRangeTemp	Number	Minimum temperature reading for the specified temperature sensor.

Field	Type	Description
Temperatures.MaxReadingRangeTemp	Number	Maximum temperature reading for the specified temperature sensor.
FanSummary.Count	Number	Number of present fans.
Fans.MemberId	String	ID of the specified fan sensor.
Fans.Name	String	Name of the specified fan sensor.
Fans.LowerThresholdCritical	Number	Critical alarm threshold for the low temperature of the specified fan sensor.
Fans.LowerThresholdFatal	Number	Fatal alarm threshold for the low temperature of the specified fan sensor.
Fans.LowerThresholdNonCritical	Number	Noncritical alarm threshold for the low temperature of the specified fan sensor.
Fans.UpperThresholdCritical	Number	Critical alarm threshold for overtemperature of the specified fan sensor.
Fans.UpperThresholdFatal	Number	Fatal alarm threshold for overtemperature of the specified fan sensor.
Fans.UpperThresholdNonCritical	Number	Noncritical alarm threshold for overtemperature of the specified fan sensor.
Fans.SerialNumber	Number	Serial number of the specified fan sensor.
Fans.Status.State	String	Status of the specified fan sensor.
Fans.Status.Health	String	Health status of the specified fan sensor.
Fans.Oem.Public.SlotNumber	Number	Slot number of the specified fan sensor.
Fans.Oem.Public.FanName	String	Name of the fan that the specified fan sensor belongs to.
Fans.Oem.Public.SpeedRatio	Number	Current reading of the specified fan sensor, in percentage.
Fans.Reading	Number	Current reading of the specified fan sensor.
Fans.ReadingUnits	String	Unit of the fan rotation speed read by the fan sensor, including: ● RPM ● Percent
Fans.MinReadingRange	Number	Minimum rotation speed reading for the specified fan sensor.
Fans.MaxReadingRange	Number	Maximum rotation speed reading for the specified fan sensor.

Field	Type	Description
Fans.Model	String	Model of the specified fan sensor.
Fans.@odata.id	String	Access path of the specified fan sensor.

6.26 Querying Information About a Specified PCIe Device Function Resource

Function

Query information about a specified [PCIe](#) device function resource of a server.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Chassis/chassis_id/PCIeDevices/pciedevices_id/Functions/functions_id`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the information about the specified PCIe device function resource, refer to [Table 6-50](#).

Table 6-50 Parameter Descriptions for Querying Information About the Specified PCIe Device Function Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self .
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
pciedevices_id	ID of the specified PCIe device resource.	This parameter can be queried through the specified resource set.
functions_id	ID of the PCIe device function resource.	This parameter can be queried through the specified resource set.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/PCleDevices/PCleCard64/Functions/1
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#PCIEFunction.PCIEFunction",
  "@odata.id": "/redfish/v1/Chassis/1/PCleDevices/PCleCard64/Functions/1",
  "@odata.type": "##PCIEFunction.v1_2_3.PCIEFunction",
  "DeviceClass": "NetworkController",
  "DeviceId": "0x1017",
  "Id": "1",
  "Links": {
    "PCIEDevice": [
      {
        "@odata.id": "/redfish/v1/Chassis/1/PCleDevices/PCleCard64"
      }
    ]
  },
  "Name": "Function1",
  "Oem": {
    "Public": {
      "AssociatedResource": "CPU1",
      "BusNumber": "0xb8",
      "DeviceNumber": "0x00",
      "FunctionNumber": "0x00"
    }
  },
  "SubsystemId": "0x0052",
  "SubsystemVendorId": "0x15b3",
  "VendorId": "0x15b3",
  "@odata.etag": "W/\"1ae394128c6b9056e8d6da3cde35c220\""
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the specified PCIe device function resource, refer to [Table 6-51](#).

Table 6-51 Output Descriptions for Querying Information About the Specified PCIe Device Function Resource

Field	Type	Description
@odata.context	String	OData description of the specified PCIe device function resource.
@odata.id	String	Access path of the specified PCIe device function resource.
@odata.type	String	Type of the specified PCIe device function resource.
DeviceClass	String	Class of the specified PCIe device function resource, including: ● UnclassifiedDevice ● MassStorageController ● NetworkController ● DisplayController ● MultimediaController ● MemoryController ● Bridge ● CommunicationController ● GenericSystemPeripheral ● InputDeviceController ● DockingStation ● Processor ● SerialBusController ● WirelessController ● IntelligentController ● SatelliteCommunicationsController ● EncryptionController ● SignalProcessingController ● ProcessingAccelerators ● NonEssentialInstrumentation ● Coprocessor ● UnassignedClass ● Other
DeviceId	String	DID of the specified PCIe device.
Id	String	UID of the specified PCIe device function resource in the iBMC system.

Field	Type	Description
Links	Object	Links to the related resources.
PCleDevice	Array	PCle device resource list.
Name	String	Name of the specified PCle device function resource.
Oem	Object	Customized properties.
Public	Object	Customized properties.
AssociatedResource	String	Associated resource of the specified PCle device function resource.
BusNumber	String	Bus number of the specified PCle device root port.
DeviceNumber	String	Device number of the specified PCle device root port.
FunctionNumber	String	Function number of the specified PCle device root port.
SubsystemId	String	SDID of the specified PCle device root port.
SubsystemVendorId	String	SVID of the specified PCle device root port.
VendorId	String	VID of the specified PCle device root port.

6.27 Querying Information About the Collection of Leak Detection Device Resources

Function

Query information about the collection of leak detection device resources of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Chassis/chassis_id/ThermalSubsystem/LeakDetection`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Description

For a description of the parameters for querying information about the collection of leak detection device resources, refer to [Table 6-52](#).

Table 6-52 Parameter Descriptions for Querying the Information About the Collection of Leak Detection Device Resources

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the chassis resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Chassis/LeakDetection.LeakDetection",
  "@odata.id": "/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection",
  "@odata.type": "#LeakDetection.v1_0_0.LeakDetection",
  "Id": "LeakDetection",
  "Name":
    "LeakDetection",
  "LeakDetectors": {
    "@odata.id": "/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection/LeakDetectors"
  }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the collection of leak detection device resources, refer to [Table 6-53](#).

Table 6-53 Output Descriptions for Querying Information About Leak Detection Device Resources

Field	Type	Description
@odata.context	String	OData description of the model of the collection of leak detection device resources.
@odata.id	String	Access path of the collection of leak detection device resources.
@odata.type	String	Type of collection of leak detection device resources.
Id	String	ID of the collection of leak detection device resources.
Name	String	Name of the collection of leak detection device resources.
LeakDetectors	Object	Collection of leak detectors.
@odata.id	String	Access path of the leak detector resource node.

6.28 Querying Information About the Leak Detector Resource Collection

Function

Query the information about the leak detector resource collection.

Permission Required

This example shows how to query modules.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/ThermalSubsystem/LeakDetection/LeakDetectors`
- Request Header:

X-Auth-Token: auth_value
- Request Message Body: None

Description

For a description of the parameters for querying information about the leak detector resource collection, refer to [Table 6-54](#).

Table 6-54 Parameter Descriptions for Querying Information About the Leak Detector Resource Collection

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the chassis resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection/LeakDetectors
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#LeakDetectorCollection.LeakDetectorCollection",
  "@odata.id": "/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection/LeakDetectors",
  "@odata.type": "#LeakDetectorCollection.LeakDetectorCollection",
  "Name": "Leak Detector Collection",
  "Members@odata.count": 2,
  "Members": [
    {
      "@odata.id":
        "/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection/LeakDetectors/1"
    },
    {
      "@odata.id":
        "/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection/LeakDetectors/2"
    }
  ]
}
```

```
}
]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the leak detector resource collection, refer to [Table 6-55](#).

Table 6-55 Output Descriptions for Querying Information About the Leak Detector Resource Collection

Field	Type	Description
@odata.context	String	OData description of the leak detector collection model.
@odata.id	String	Access path of the leak detector resource collection.
@odata.type	String	Type of leak detector resource collection.
Name	String	Name of the leak detector resource collection.
Members@odata.count	Number	Number of leak detector resources.
Members	Array	List of leak detector resources.
@odata.count	String	Access path of a specified leak detector resource node.

6.29 Querying Information About a Specified Leak Detector

Function

Query information about a specified detector of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Chassis/chassis_id/ThermalSubsystem/LeakDetection/LeakDetectors/LeakDetector_id*

- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Description

For a description of the parameters for querying information about the specified detector, refer to [Table 6-56](#).

Table 6-56 Parameter Descriptions for Querying Information About the Specified Detector

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the chassis resource.	For a rack server, the value is 1 or Self .
LeakDetector_id	ID of the leak detector.	ID of the leak detector.
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection/LeakDetectors/1
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#LeakDetector.LeakDetector",
  "@odata.id": "/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection/LeakDetectors/1",
  "@odata.type": "#LeakDetector.v1_0_0.LeakDetector",
  "Id": "1",
  "Name": "Moisture-type Leak Detector",
  "DetectorState": "OK",
  "Status": {
    "State": "Enabled",
    "Health": "OK"
  }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified leak detector, refer to [Table 6-57](#).

Table 6-57 Output Descriptions for Querying Information About the Specified Leak Detector

Field	Type	Description
@odata.context	String	OData description of the specified leak detector model.
@odata.id	String	Access path of the specified leak detector resource.
@odata.type	String	Type of the specified leak detector resource.
Id	String	Unique ID of the specified leakage detector resource.
Name	String	Name of the specified leak detector resource.
DetectorState	String	Liquid leakage status of the liquid cooling server: ● OK: indicates that is no leak. ● Warning: indicates tat there is a warning-level leak alarm, which needs to be given attention. ● Critical: indicates that there is a critical-level leak alarm, which needs immediate action.
Status	Object	Status of the specified leakage sensor, including: ● State: whether the leakage sensor is enabled. ● Health: Health status of the leakage sensor: → OK: indicates that is no leak. → Critical: indicates that there is a leak.

6.30 Modifying Information About a Specified Drive Resource

Function

Modify the indicator status of a specified drive resource.

Permission Required

Basic management.

Syntax

- Operation Type: PATCH
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/Drives/drives_id`
- Request Header:

Content-Type: header_type
X-Auth-Token: auth_value

● Request Message Body:

```
{
  "IndicatorLED": state
}
```

Description

For a description of the parameters for modifying information about the specified drive resource, refer to [Table 6-58](#).

Table 6-58 Parameter Descriptions for Modifying Information About the Specified Drive Resource

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the chassis resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
drives_id	ID of the specified drive.	It can be obtained from the drive list managed by the current specified controller.
state	Indicator status of the specified drive resource.	● Lit ● Blinking ● Off

Usage Guidelines

After configuration, you can view the result through *GET https://device_ip/redfish/v1/Chassis/1/Drives/drives_id*.

Example

● Request Example:

PATCH https://device_ip/redfish/v1/Chassis/1/Drives/drives_id

● Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json

- Request Message Body:

```
{
  "IndicatorLED": "Lit"
}
```

- Response Example: None
- Status Code: 204

Output Description

None

6.31 Querying Information About the Network Port Resource Collection of a Specified Network Adapter

Function

Query information about the network port resource collection of a specified network adapter of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/NetworkPorts`
- Request Header:

```
X-Auth-Token: auth_value
```

- Request Message Body: None

Description

For a description of the parameters for querying information about the network port resource collection of the specified network adapter, refer to [Table 6-59](#).

Table 6-59 Parameter Descriptions for Querying Information About the Network Port Resource Collection of the Specified Network Adapter

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the chassis resource.	For a rack server, the value is 1 or Self .

Parameter	Setting	Value
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
networkadapters_id	ID of the specified network adapter resource.	It can be obtained by querying the information about the network adapter resource collection.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1/NetworkPorts
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None

- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#NetworkAdapter.NetworkAdapter",
  "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard4/NetworkPorts",
  "@odata.type": "#NetworkPortCollection.NetworkPortCollection",
  "Description": "Collection of Ethernet Interfaces for this Manager",
  "Members": [
    {
      "@odata.id":
        "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard4/NetworkPorts/1"
    },
    {
      "@odata.id":
        "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard4/NetworkPorts/2"
    }
  ],
  "Members@odata.count": 2,
  "Name": "Ethernet Network Interface Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the network port resource collection of the specified network adapter, refer to [Table 6-60](#).

Table 6-60 Output Descriptions for Querying Information About the Network Port Resource Collection of the Specified Network Adapter

Field	Type	Description
@odata.context	String	OData description of the network port resource collection of the specified network adapter.
@odata.id	String	Access path of the network port resource collection of the specified network adapter.
@odata.type	String	Type of the network port resource collection of the specified network adapter.
Name	String	Name of the network port resource collection of the specified network adapter.
Description	String	Description of the network port resource collection of the specified network adapter.
Members	Array	Members of the network port resource collection of the specified network adapter.
@odata.id	String	Access path of a single network port resource.
Members@odata.count	Number	Number of network port resources.

6.32 Querying Historical Environmental Humidity Information About a Chassis

Function

Query historical environmental humidity information about a specified chassis of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/EnvironmentHistoryHumidity`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Description

For a description of the parameters for querying historical environmental humidity information about the specified chassis, refer to [Table 6-61](#).

Table 6-61 Parameter Descriptions for Querying Historical Environmental Humidity Information About the Chassis

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the chassis resource.	For a rack server, the value is 1 or Self .
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Chassis/1/EnvironmentHistoryHumidity

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

{
 "@odata.context":
 "/redfish/v1/\$metadata#Chassis.Chassis/Members/1/EnvironmentHistoryHumidity",
 "@odata.id": "/redfish/v1/Chassis/1/EnvironmentHistoryHumidity",
 "@odata.type": "#EnvironmentHistoryHumidity.v1_1_0.EnvironmentHistoryHumidity",
 "Id": "EnvironmentHistoryHumidity",
 "Name": "EnvironmentHistoryHumidity",
 "Description": "System History Humidity",
 "Data": [
 {
 "Time": "2024-08-09 15:38:33",
 "HumidityPercent": 75
 }
]
}

```
    },
    .....
    {
        "Time": "2024-08-08 15:43:35",
        "HumidityPercent": 76
    }
]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query historical environmental humidity information about the chassis, refer to [Table 6-62](#).

Table 6-62 Output Descriptions for Querying Historical Environmental Humidity Information About the Chassis

Field	Type	Description
@odata.context	String	OData description of the environmental humidity information about the specified chassis.
@odata.id	String	Access path of the environmental humidity information about the specified chassis.
@odata.type	String	Type of historical environmental humidity information about the specified chassis.
Id	String	ID of the historical environmental humidity information about the specified chassis.
Name	String	Name of the historical environmental humidity information about the specified chassis.
Description	String	Description of the historical environmental humidity information about the specified chassis.
Data	Array	Data array of the historical environmental humidity information about the specified chassis.
Time	String	Humidity information collection time.
HumidityPercent	Number	Humidity value.

Chapter 7

Operations on SessionService Resources

Table of Contents

Querying Information About the Session Service	460
Modifying Information About the Session Service	462
Creating Information About a Session	464
Querying Information About the Session Resource Collection	466
Querying Information About a Specified Session Resource	467
Deleting Information About a Specified Session Resource	469

Figure 7-1 shows the path requirements for the SessionService resources supported by VANTAGEO servers.

Figure 7-1 SessionService Resource Path Requirements



For a description of properties of SessionService resources and operations supported by the properties, refer to Table 7-1.

Table 7-1 Descriptions of SessionService Resources Properties

URL	Property	Description	Operation
/redfish/v1/SessionService	Id	ID of the SessionService resource.	GET
	Name	Name of the SessionService resource.	GET
	SessionTimeout	Session service timeout period.	GET/PATCH
	Sessions	Access path of the session list.	GET

URL	Property	Description	Operation
/redfish/v1/SessionService/Sessions	Name	Name of the session resource.	GET
	Members@odata.count	Number of session members.	GET
	Members	Session resource list, which provides references for all session resource URLs .	GET
/redfish/v1/SessionService/Sessions/session_id	-	Specified session resource.	DELETE
	Id	UID of the specified session resource.	GET
	Name	Name of the specified session.	GET
	UserName	Account information about the specified session.	GET

6.33 Querying Information About the Session Service

Function

Query information about the current session service of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/SessionService`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the session service, refer to [Table 7-2](#).

Table 7-2 Parameter Descriptions for Querying Information About the Session Service

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/SessionService
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#SessionService.SessionService",
  "@odata.id": "/redfish/v1/SessionService",
  "@odata.type": "#SessionService.v1_1_3.SessionService",
  "Description": "Session Service",
  "Id": "SessionService",
  "Name": "Session Service",
  "ServiceEnabled": true,
  "SessionTimeout": 180,
  "Sessions": {
    "@odata.id": "/redfish/v1/SessionService/Sessions"
  },
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the session service, refer to [Table 7-3](#).

Table 7-3 Output Descriptions for Querying Information About the Session Service

Field	Type	Description
@odata.context	String	OData description of the SessionService resource model.
@odata.id	String	Access path of the SessionService resource node.
@odata.type	String	Type of SessionService resource.
Description	String	Description of the SessionService resource.
Id	String	ID of the SessionService resource.
Name	String	Name of the SessionService resource.
ServiceEnabled	Boolean	Whether the SessionService resource is enabled.
SessionTimeout	Number	Redfish session timeout period.
Sessions	Object	Session list.
@odata.id	String	Access path of the session list.
Status.Health	String	Health status of the SessionService resource.
Status.State	String	Status of the SessionService resource.

6.34 Modifying Information About the Session Service

Function

Modify the timeout period of the current session service of a server.

Permission Required

Basic management.

Syntax

- Operation Type: PATCH
- URL: `https://device_ip/redfish/v1/SessionService`
- Request Header:

X-Auth-Token: auth_value Content-Type: header_type

- Request Message Body:

```
{
  "SessionTimeout": time
}
```

Parameters

For a description of the parameters for modifying information about the session service, refer to [Table 7-4](#).

Table 7-4 Parameter Descriptions for Modifying Information About the Session Service

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
time	Redfish session timeout period.	Integer, range: 30–86400, unit: seconds.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/SessionService
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body:

```
{
  "SessionTimeout": 300
}
```

- Response Example: None
- Status Code: 204

Output Description

None

6.35 Creating Information About a Session

Function

Create a session.

Permission Required

Basic management.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/SessionService/Sessions`
- Request Header:

Content-Type: header_type

- Request Message Body:

```
{
  "UserName": name,
  "Password": password
}
```

Parameters

For a description of the parameters for creating a session, refer to [Table 7-5](#).

Table 7-5 Parameter Descriptions for Creating a Session

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
header_type	Format of the request message.	application/json
name	User for the new session.	User of the BMC system.
password	Password the user for the new session.	Password of the user for the BMC system.

Usage Guidelines

In the Redfish operations on the server, this POST operation is performed first. Because most follow-up operations need the "X-Auth-Token" value in "Headers" for authentication, the "X-Auth-Token" value can be obtained through this operation.

Example

- Request Example:

POST https://device_ip/redfish/v1/SessionService/Sessions

- Request Header:

```
Content-Type: application/json
```

- Request Message Body:

```
{
  "UserName": "username",
  "Password": "password"
}
```

- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#SessionService.Sessions",
  "@odata.id": "/redfish/v1/SessionService/Sessions/q1xUU91KqyADxiLlJcq9jdygxuz",
  "@odata.type": "#Session.v1_1_0.Session",
  "Name": "User Session",
  "Id": "q1xUU91KqyADxiLlJcq9jdygxUZr0Hwe",
  "UserName": "Administrator"
}
```

- Response Header Example:

```
Location: /redfish/v1/SessionService/Sessions/1
X-Auth-Token: YzAhv2WCq5ZMDJUq7JJ3ELEpNF3eoOab
```

- Status Code: 201

Output Description

For a description of the output returned when you create a session, refer to [Table 7-6](#).

Table 7-6 Output Descriptions for Session Creation

Field	Type	Description
@odata.context	String	OData description of the newly created session resource model.
@odata.id	String	Access path of the newly created session resource. The detailed information about the session can be obtained.
@odata.type	String	Type of the newly created session resource.
Id	String	UID of the newly created session resource.
Name	String	Name of the newly created session.
Description	String	Description of the new session.
UserName	String	Account information about newly created session.

6.36 Querying Information About the Session Resource Collection

Function

Query information about the current session resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/SessionService/Sessions*
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the session resource collection, refer to [Table 7-7](#).

Table 7-7 Parameter Descriptions for Querying Information About the Session Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

GET *https://device_ip/redfish/v1/SessionService/Sessions*

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#SessionCollection.SessionCollection",
  "@odata.id": "/redfish/v1/SessionService/Sessions",
  "@odata.type": "#SessionCollection.SessionCollection",
  "Name": "Session Collection",
  "Members": [
    {
      "@odata.id":
        "/redfish/v1/SessionService/Sessions/iZoEEcrx8c2u0zFefkA8pFD0XnSqDqaG"
    },
    {
      "@odata.id":
        "/redfish/v1/SessionService/Sessions/sf3I8CJsQrpwCumCR9niUTcpFVeaz2wx"
    }
  ],
  "Members@odata.count": 2
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the session resource collection, refer to [Table 7-8](#).

Table 7-8 Output Descriptions for Querying Information About the Session Resource Collection

Field	Type	Description
@odata.context	String	OData description of the session resource model.
@odata.id	String	Access path of the session resource node.
@odata.type	String	Type of session resource.
Name	String	Name of the session resource.
Members@odata.count	Number	Number of session members.
Members	Array	Session list
@odata.id	String	Access path of a single session resource node.

6.37 Querying Information About a Specified Session Resource

Function

Query information about a specified session resource.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/SessionService/Sessions/Session_id`
- Request Header:

```
X-Auth-Token: auth_value
```

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified session resource, refer to [Table 7-9](#).

Table 7-9 Parameter Descriptions for Querying Information About the Specified Session Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
Session_id	ID of the specified session.	It can be obtained from the session resource collection.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/SessionService/Sessions/57f5ff2105218ad2df694ab94cbeba90
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Session.Session",

```



```

"@odata.id":
"/redfish/v1/SessionService/Sessions/izOEEcrx8c2uOzFefkA8pFD0XnSqDqaG",
"@odata.type": "#Session.v1_1_0.Session",
"Description": "Session for user Administrator",
"UserName": "Administrator",
"Name": "Session",
"Id": "izOEEcrx8c2uOzFefkA8pFD0XnSqDqaG"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified session resource, refer to [Table 7-10](#).

Table 7-10 Output Descriptions for Querying Information About the Specified Session Resource

Field	Type	Description
@odata.context	String	OData description of the specified session resource model.
@odata.id	String	Access path of the specified session resource node.
@odata.type	String	Type of the specified session resource.
Description	String	Description of the specified session resource.
Id	String	UID of the specified session resource.
Name	String	Name of the session resource.
UserName	String	Username for the specified session.

6.38 Deleting Information About a Specified Session Resource

Function

Delete information about a specified session resource of a server.

Permission Required

Basic management.

Syntax

- Operation Type: DELETE
- URL: https://device_ip/redfish/v1/SessionService/Sessions/Session_id
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for deleting information about the specified session resource, refer to [Table 7-11](#).

Table 7-11 Parameter Descriptions for Deleting Information About the Specified Session Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
Session_id	Session ID to be deleted	The session_id of each session is contained in the session list query result. The ID can be used when the information about the corresponding session needs to be deleted.
auth_value	X-Auth-Token value contained in Request Header in the DELETE request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

DELETE https://device_ip/redfish/v1/SessionService/Sessions/57f5ff2105218ad2df694ab94cbeba90

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example: None
- Status Code: 204

Output Description

None

Chapter 8

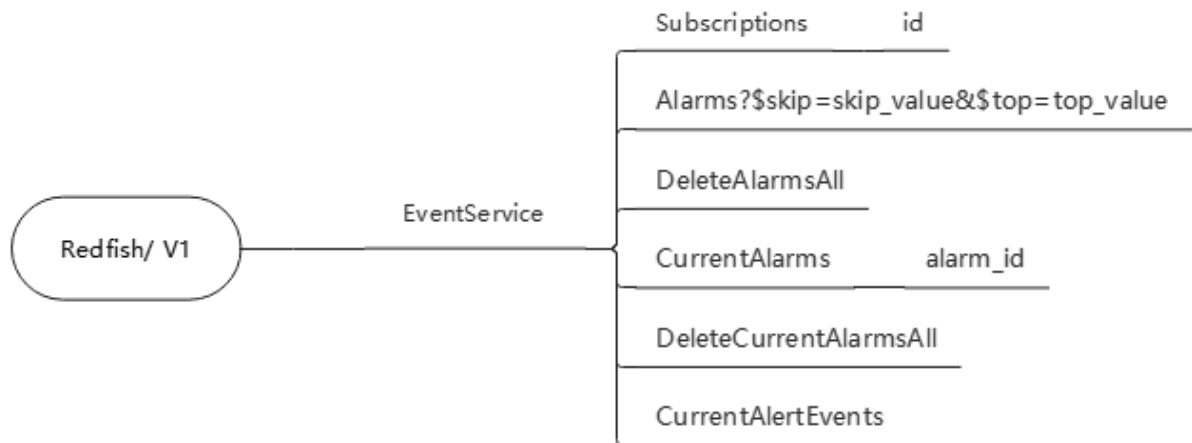
Operations on EventService Resources

Table of Contents

Querying Information About the EventService Resource	477
Querying Information About the Event Subscription Resource Collection	480
Creating an Event Subscription Resource	482
Querying Information About an Event Subscription Resource.....	486
Modifying Information About an Event Subscription Resource.....	489
Deleting an Event Subscription Resource	492
Resuming Event Subscription	494
Reporting an Event.....	495
Querying Information About the Event Resource Collection.....	498
Deleting All Event Resources	500
Querying Information About the Current Alarm Resource Collection.....	501
Querying Information About the Current Alarm Resource.....	504
Deleting the Current Alarm Resource	506
Deleting All Current Alarm Resource.....	507
Querying Information About the Current Alarm Event Resource Collection.....	508
Modifying Event Service Resource Information	512

Figure 8-1 shows the path requirements for the EventService resources supported by VANTAGEO servers.

Figure 8-1 EventService Resource Path Requirements



For a description of properties of EventService resources and operations supported by the properties, refer to [Table 8-1](#).

Table 8-1 Descriptions of EventService Resources Properties

URL	Property	Description	Operation
/redfish/v1/EventService	Id	ID of an event resource.	GET
	Name	Name of the event resource.	GET
	Status	Whether the EventService resource is enabled.	GET
	ServiceEnabled	Whether event reporting is enabled.	GET
	DeliveryRetryAttempts	Maximum number of retries for delivering event subscriptions.	GET
	DeliveryRetryIntervalSeconds	Interval (in seconds) at which an event is resent upon a failure.	GET
	EventTypesForSubscription	Type of events that can be subscribed to.	GET
	Subscriptions	Navigation resource of the event target resource collection.	GET
/redfish/v1/EventService/Subscriptions	Name	Name of the event subscription resource collection.	GET
	Members@odata.count	Number of event subscription resource members.	GET
	Members	Event subscription resource list.	GET

URL	Property	Description	Operation
	Id	ID of the specified event subscription resource.	PATCH
	Destination	Valid HTTPS destination address.	PATCH
	EventTypes	Types of monitored events.	PATCH
	context	String	PATCH
	protocol	It must be Redfish.	PATCH
	MessageIds	Optional parameter. Combination of valid message IDs defined in the event registry.	PATCH
	OriginResources	Combination of valid resource URIs .	PATCH
	OriginResources@odata.count	Number of event sources.	PATCH
	HttpHeaders	It is displayed as "null" in the query result.	PATCH
/redfish/v1/EventService/Subscriptions/subscription/id	Id	ID of the event subscription resource.	GET/ PATCH
	Name	Name of the event subscription resource.	GET/ PATCH
	Destination	Destination event service URI .	GET/ PATCH
	EventTypes	Type of event to be submitted.	GET/ PATCH
	Context	String provided by the client and stored together with the event target subscription.	GET/ PATCH
	Protocol	Protocol connected to the event.	GET/ PATCH
	MessageIds	Submitted message ID list.	GET/ PATCH
	OriginResources	Submits the event-related resource list.	GET/ PATCH
	OriginResources@odata.count	Number of event sources.	GET/ PATCH

URL	Property	Description	Operation
	HttpHeaders	HTTP Headers, for example, GET Object is empty for an authentication message.	GET
	Status	Status of the specified vent subscription. - Enabled - Disabled - StandbyOffline: suspended when the number of times that an event is reported exceeds the threshold.	GET
	DeliveryRetryPolicy	Event delivery retry policy. Options: - SuspendRetries (required): suspends subscription information if the number of retries exceeds the threshold. Default. - TerminateAfterRetries (optional): deletes subscription information if the number of retries exceeds the threshold. - RetryForever (optional): always retries delivery.	GET
	Actions	Actions.	GET
	EventDestination.ResumeSubscription	Resumes event subscription.	GET
	target	Operation path for event subscription resumption.	GET
/redfish/v1/EventService/Alarms?\$skip=skip_value&\$top=top_value	Description	Description of the event resource collection.	GET
	Id	ID of the event resource collection.	GET
	Name	Name of the event resource collection.	GET
	Members@odata.count	Number of members in the event resource collection.	GET
	Members	List of members in the event resource collection.	GET

URL	Property	Description	Operation
	AlarmCode	Event code.	GET
	AlarmLevel	Event level.	GET
	TimeStamp	Event generation time.	GET
	Message	Event information.	GET
/redfish/v1/EventService/CurrentAlarms	Description	Description of the current alarm resource collection.	GET
	Actions	Operations that can be performed on the current alarm resource collection.	GET
	Oem	Customized properties.	GET
	EventService.DeleteCurrentAlarmsAll	Deletes all current alarms.	GET
	target	Operation path.	GET
	Name	Name of the current alarm resource collection.	GET
	Members@odata.count	Number of members in the current alarm resource collection.	GET
	Members	-	GET
	AlarmId	ID of the current alarm.	GET
	AlarmCode	Code of the current alarm.	GET
	AlarmLevel	Level of the current alarm.	GET
	TimeStamp	Alarm generation timestamp.	GET
	Message	Information about the current alarm.	GET
/redfish/v1/EventService/CurrentAlarms/alarm_id	Id	ID of the current alarm resource.	GET
	Name	Name of the current alarm resource.	GET
	Description	Description of the current alarm resource.	GET
	AlarmCode	Code of the current alarm.	GET
	AlarmLevel	Level of the current alarm.	GET
	TimeStamp	Alarm generation timestamp.	GET
	Message	Information about the current alarm.	GET

URL	Property	Description	Operation
/redfish/v1/EventService/CurrentAlertEvents	Description	Description of the current alarm event resource collection.	GET
	Id	ID of the current alert alarm resource collection.	GET
	Name	Name of the current alarm event resource collection.	GET
	Members@odata.count	Number of members in the current alarm event resource collection.	GET
	Members	-	GET
	EventId	Alarm event ID.	GET
	EventType	Alarm event type.	GET
	EventTimestamp	Alarm event generation timestamp.	GET
	Severity	Alarm event severity level.	GET
	Message	Alarm event message.	GET
	Oem.Public	-	GET
	alarmStatus	Alarm status.	GET
	specificProblemID	Alarm classification ID (alarm code).	GET
	specificProblem	Alarm classification description (alarm name).	GET
	neUID	Alarm server ID (serial number of the server).	GET
	neName	Alarm server name (asset code of the server)	GET
	neType	Type of device where the alarm is raised.	GET
	objectUID	ID of the alarm part.	GET
	objectName	Name of the alarm part.	GET
	objectType	Type of alarm part.	GET
	locationInfo	Alarm positioning information.	GET
	Addinfo	Additional alarm information.	GET

8.1 Querying Information About the EventService Resource

Function

Query the information about the EventService resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/EventService`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For the parameter descriptions for querying the event service resource, refer to [Table 8-2](#).

Table 8-2 Parameter Descriptions for Querying the Event Service Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET `https://device_ip/redfish/v1/EventService`

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#EventService.EventService",

```

```

"@odata.id": "/redfish/v1/EventService",
"@odata.type": "#EventService.v1_5_0.EventService",
"Actions": {
  "#EventService.SubmitTestEvent": {
    "EventType@Redfish.AllowableValues": [
      "StatusChange",
      "ResourceUpdated",
      "ResourceAdded",
      "ResourceRemoved",
      "Alert"
    ],
    "target": "/redfish/v1/EventService/Actions/EventService.SubmitTestEvent"
  },
  "Oem": {
    "Public": {
      "#EventService.ClearHistoryAlarm": {
        "target":
          "/redfish/v1/EventService/Actions/EventService.ClearHistoryAlarm"
      }
    }
  }
},
"DeliveryRetryAttempts": 3,
"DeliveryRetryIntervalSeconds": 60,
"Description": "Event Service",
"EventTypesForSubscription": [
  "StatusChange",
  "ResourceUpdated",
  "ResourceAdded",
  "ResourceRemoved",
  "Alert"
],
"Id": "EventService",
"Name": "Event Service",
"Oem": {
  "Public": {
    "Alarms": {
      "@odata.id": "/redfish/v1/EventService/Alarms"
    },
    "CurrentAlarms": {
      "@odata.id": "/redfish/v1/EventService/CurrentAlarms"
    },
    "CurrentAlertEvents": {
      "@odata.id": "/redfish/v1/EventService/CurrentAlertEvents"
    }
  }
}

```

```

    }
  }
},
"ServiceEnabled": true,
"Status": {
  "State": "Enabled"
},
"Subscriptions": {
  "@odata.id": "/redfish/v1/EventService/Subscriptions"
}
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the event service resource, refer to [Table 8-3](#).

Table 8-3 Output Descriptions for Querying the Event Service Resource

Field	Type	Description
@odata.context	String	OData description of the EventService resource model.
@odata.id	String	Access path of the EventService resource node.
@odata.type	String	Type of EventService resource.
Actions.#EventService.SubmitTestEvent.EventType@Redfish.AllowableValues	Array	EventService resource ID.
Actions.#EventService.SubmitTestEvent.target	String	URL for executing the operation.
Actions.Oem.Public.#EventService.ClearHistoryAlarm.target	String	URL for executing the operation.
DeliveryRetryAttempts	Number	Maximum number of retries for delivering event subscriptions.
DeliveryRetryIntervalSeconds	Number	Interval (in seconds) at which an event is resent upon a failure.
Description	String	Description of the EventService resource.
EventTypesForSubscription	Array	Type of events that can be subscribed to. The ranges are the combinations of the following valid values:

Field	Type	Description
		● StatusChange: resource status change event ● ResourceUpdated: resource update event ● ResourceAdded: resource addition event ● ResourceRemoved: resource removal event ● Alert: alarming event
Id	String	ID of the EventService resource.
Name	String	Name of the EventService resource.
Oem.Public.Alarms.@odata.id	String	Access path of the alarm resource collection.
Oem.Public.CurrentAlarms.@odata.id	String	Access path of the current alarm resource collection.
Oem.Public.CurrentAlertEvents.@odata.id	String	Access path of the current alarm event resource collection.
ServiceEnabled	Boolean	Whether event reporting is enabled.
Status.State	String	Whether the EventService resource is enabled.
Subscriptions.@odata.id	String	Access path of the specified event object resource.

8.2 Querying Information About the Event Subscription Resource Collection

Function

Query the information about the event subscription resource collection.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/EventService/Subscriptions`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For the parameter descriptions for querying the event subscription resource collection, refer to [Table 8-4](#).

Table 8-4 Parameter Descriptions for Querying the Event Subscription Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
member_id	User ID	It can be obtained by querying the user list.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/EventService/Subscriptions
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#EventDestinationCollection.EventDestinationCollection",
  "@odata.id": "/redfish/v1/EventService/Subscriptions",
  "@odata.type": "#EventDestinationCollection.EventDestinationCollection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/EventService/Subscriptions/1"
    }
  ],
  "Members@odata.count": 1,
  "Name": "Event Subscriptions Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the event subscription resource collection, refer to [Table 8-5](#).

Table 8-5 Output Descriptions for Querying the Event Subscription Resource Collection

Field	Type	Description
@odata.context	String	OData description of the event subscription resource collection model.
@odata.id	String	Type of event subscription resource collection.
@odata.type	String	Access path of the event subscription resource collection.
Name	String	Name of the event subscription resource collection.
Members@odata.count	Number	Number of event subscription resource members.
Members	Array	Event subscription resource list.
@odata.id	String	Access path of a single event subscription resource node.

8.3 Creating an Event Subscription Resource

Function

Create an event subscription resource.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/EventService/Subscriptions`
- Request Header:

```
X-Auth-Token: auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "Destination": event_destination,
  "EventTypes": event_types,
  "HttpHeaders": http_headers,
  "Context": context,
  "Protocol": protocol,
  "MessageIds": message_ids,
  "OriginResources": origin_resources,
```

```

    "deliveryRetryPolicy":delivery_retry_policy
  }

```

Parameters

For the parameter descriptions for creating an event subscription resource, refer to [Table 8-6](#).

Table 8-6 Parameter Descriptions for Creating the Event Subscription Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
header_type	Format of the request message.	application/json
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
event_destination	Event subscription destination address.	Valid HTTPS destination address.
event_types	Event type for event subscription monitoring.	A combination of the following values: ● StatusChange: resource status change event ● ResourceUpdated: resource update event ● ResourceAdded: resource addition event ● ResourceRemoved: resource removal event ● Alert: alarming event
http_headers	Event subscription HTTP header parameters, which are carried when an event is reported.	Optional parameter. The value shall comply with the key:value format, and is displayed as null when being queried.
context	Event subscription context information.	String
protocol	Protocol used by the event subscription.	It must be Redfish.
message_ids	Message ID matching list of the event subscription.	Optional parameter. Combination of valid message IDs defined in the event registry.
origin_resources	Event source list.	Combination of valid resource URIs.
delivery_retry_policy	Event delivery retry policy.	Options: ● SuspendRetries (required): suspends subscription information if the number of retries exceeds the threshold. Default. ● TerminateAfterRetries (optional): deletes subscription information if the

Parameter	Description	Value
		number of retries exceeds the threshold. ● RetryForever (optional): always retries delivery.

Usage Guidelines

The specified event destination address used for creating a subscription cannot be the same as any existing subscription destination address.

Example

- Request Example:

```
POST https://device_ip/redfish/v1/EventService/Subscriptions
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body:

```
{
  "Destination": "https://10.228.34.200/redfish/test/",
  "EventTypes": [ "Alert" ],
  "HttpHeaders": {
    "Content-Type":
      "Application/JSON",
    "OData-Version": "4.0",
    "X-Auth-Token": "5ac44e4c36db20ee69f661f42239b6f5"
  },
  "Context": "event subscription context string",
  "Protocol": "Redfish",
  "MessageIds": [
    "iBMCEvents.2.0.PsPredicFailureInfo"
  ],
  "OriginResources": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/0"
    }
  ],
  "DeliveryRetryPolicy": "TerminateAfterRetries"
}
```

- Response Example:


```
{
  "@odata.context": "/redfish/v1/$metadata#EventDestination.EventDestination",
  "@odata.id": "/redfish/v1/EventService/Subscriptions",
  "@odata.type": "#EventDestination.v1_7_0.EventDestination",
  "Context": "event subscription context string",
  "Destination": "https://10.228.34.200/redfish/test/",
  "EventTypes": [
    "Alert"
  ],
  "Id": 1,
  "MessageIds": [
    "iBMCEvents.2.0.PsPredicFailureInfo"
  ],
  "Name": "Subscription 1",
  "OriginResources": [
    "/redfish/v1/Chassis/1/Power#/PowerSupplies/0"
  ],
  "OriginResources@odata.count": 1,
  "Protocol": "Redfish",
  "HttpHeaders": null
}
```

- Status Code: 201

Output Description

For a description of the output returned when you create the event subscription resource, refer to [Table 8-7](#).

Table 8-7 Output Descriptions for Creating the Event Subscription Resource

Field	Type	Description
@odata.context	String	OData description of the event subscription resource model.
@odata.id	String	Access path of the event subscription resource node.
@odata.type	String	Type of event subscription resource.
Id	String	ID of the event subscription resource.
Context	String	Event subscription context information.
Destination	String	Event subscription destination address.
EventTypes	Array	Event type for event subscription monitoring. A combination of the following values:

Field	Type	Description
		● StatusChange: resource status change event ● ResourceUpdated: resource update event ● ResourceAdded: resource addition event ● ResourceRemoved: resource removal event ● Alert: alarming event
Id	String	ID of the event subscription resource.
MessageIds	String	Message ID matching list of the event subscription.
Name	String	Name of the event subscription resource.
Protocol	String	Protocol used by the event subscription.
OriginResources	Array	Event source list.
OriginResources@odata.count	Number	Number of event sources.
HttpHeaders	String	Event subscription HTTP header.

8.4 Querying Information About an Event Subscription Resource

Function

Query the information about an event subscription resource.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/EventService/Subscriptions/id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For the parameter descriptions for querying an event subscription resource, refer to [Table 8-8](#).

Table 8-8 Parameter Descriptions for Querying the Event Subscription Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
id	ID of the valid event subscription.	-
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/EventService/Subscriptions/1
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#EventDestination.EventDestination",
  "@odata.id": "/redfish/v1/EventService/Subscriptions/1",
  "@odata.type": "#EventDestination.v1_7_0.EventDestination",
  "Context": "event subscription context string",
  "Destination": "https://10.228.34.200/redfish/test/",
  "EventTypes": [
    "Alert"
  ],
  "Id": "1",
  "MessageIds": [
    "iBMCEvents.2.0.PsPredicFailureInfo"
  ],
  "Name": "Subscription 1",
  "OriginResources": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/0"
    }
  ],
  "OriginResources@odata.count": 1,
  "Protocol": "Redfish",
}
```

```

    "SubscriptionType": "RedfishEvent",
    "HttpHeaders": null,
    "Status": "Enabled",
    "DeliveryRetryPolicy": "TerminateAfterRetries",
    "Actions": {
        "#EventDestination.ResumeSubscription": {
            "target":
                "/redfish/v1/EventService/Subscriptions/1/Actions/
                EventDestination.ResumeSubscription"
        }
    }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the event subscription resource, refer to [Table 8-9](#).

Table 8-9 Output Descriptions for Querying the Event Subscription Resource

Field	Type	Description
@odata.context	String	OData description of the event subscription resource model.
@odata.id	String	Access path of the event subscription resource node.
@odata.type	String	Type of event subscription resource.
Id	String	ID of the specified event subscription resource.
Name	String	Name of the event subscription resource.
Destination	String	Valid HTTP/HTTPS destination address.
EventTypes	Array	Types of events to which a client can subscribe. ● StatusChange: resource status change event ● ResourceUpdated: resource update event ● ResourceAdded: resource addition event ● ResourceRemoved: resource removal event ● Alert: alarming event
Context	String	Event subscription context information.
Protocol	String	Protocol used for event subscription.
SubscriptionType	String	Event subscription type.
MessageIds	Array	Message ID matching list of the event subscription.
OriginResources	Array	Event source list.

Field	Type	Description
OriginResources@odata.count	Number	Number of event sources.
HttpHeaders	Object	Event subscription HTTP header, which is displayed as "null" when being queried.
Status	String	Status of the specified vent subscription. • Enabled • Disabled • StandbyOffline: suspended when the number of times that an event is reported exceeds the threshold.
DeliveryRetryPolicy	String	Event delivery retry policy. Options: • SuspendRetries (required): suspends subscription information if the number of retries exceeds the threshold. Default. • TerminateAfterRetries (optional): deletes subscription information if the number of retries exceeds the threshold. • RetryForever (optional): always retries delivery.
Actions	Object	Actions.
#EventDestination.ResumeSubscription.target	String	Operation path for event subscription resumption.

8.5 Modifying Information About an Event Subscription Resource

Function

Modify an event subscription resource.

Permission Required

Basic management.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/EventService/Subscriptions/id*
- Request Header:

```
X-Auth-Token: auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
```

```

    "HttpHeaders": http_headers,
    "Context": context,
    "DeliveryRetryPolicy": delivery_retry_policy
  }

```

Parameters

For the parameter descriptions for modifying an event subscription resource, refer to [Table 8-10](#).

Table 8-10 Parameter Descriptions for Modifying the Event Subscription Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
id	ID of the valid event subscription.	-
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
http_headers	Event subscription HTTP header parameters, which are carried when an event is reported.	The value shall comply with the <code>key:value</code> format. During configuration, the previous information can be replaced directly.
context	Event subscription context information.	String
delivery_retry_policy	Event delivery retry policy.	● SuspendRetries (required): suspends subscription information if the number of retries exceeds the threshold. Default. ● TerminateAfterRetries (optional): deletes subscription information if the number of retries exceeds the threshold. ● RetryForever (optional): always retries delivery.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/EventService/Subscriptions/1
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body:

```
{
  "HttpHeaders":
  {
    "Content-Type": "Application/JSON",
    "OData-Version": "4.0",
    "X-Auth-Token": "5ac44e4c36db20ee69f661f42239b6f5"
  },
  "Context": "event subscription context string",
  "DeliveryRetryPolicy": "TerminateAfterRetries"
}
```

- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#EventDestination.EventDestination",
  "@odata.id": "/redfish/v1/EventService/Subscriptions/2",
  "@odata.type": "#EventDestination.v1_7_0.EventDestination",
  "Context": "Event_2",
  "Destination": "https://10.228.34.158:9002/redfish/test/",
  "EventTypes": [
    "Alert"
  ],
  "Id": "2",
  "MessageIds": [
    "iBMCEvents.2.0.PsPredicFailureInfo"
  ],
  "Name": "Subscription 2",
  "OriginResources": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/4"
    }
  ],
  "OriginResources@odata.count": 1,
  "Protocol": "Redfish",
  "SubscriptionType": "RedfishEvent",
  "HttpHeaders": null
}
```

- Status Code: 200

Output Description

For a description of the output returned when you modify an event subscription resource, refer to [Table 8-11](#).

Table 8-11 Output Descriptions for Modifying the Event Subscription Resource

Field	Type	Description
@odata.context	String	OData description of the event subscription resource model.
@odata.id	String	Access path of the event subscription resource node.
@odata.type	String	Type of event subscription resource.
Id	String	ID of the specified event subscription resource.
Name	String	Name of the event subscription resource.
Destination	String	Valid HTTP/HTTPS destination address.
EventTypes	Array	Types of events to which a client can subscribe. ● StatusChange: resource status change event ● ResourceUpdated: resource update event ● ResourceAdded: resource addition event ● ResourceRemoved: resource removal event ● Alert: alarming event
Context	String	Event subscription context information.
Protocol	String	Protocol used for event subscription, It must be Redfish in this version.
SubscriptionType	String	Event subscription type.
MessageIds	Array	(Optional) Message ID matching list of the event subscription. Combination of valid message IDs defined in the event registry.
OriginResources	Array	Mapping between event subscriptions and event sources.
OriginResources@odata.count	Number	Number of event sources.
HttpHeaders	Object	Event subscription HTTP header, which is displayed as "null" when being queried.

8.6 Deleting an Event Subscription Resource

Function

Delete an event subscription resource.

Permission Required

Basic management.

Syntax

- Operation Type: DELETE
- URL: `https://device_ip/redfish/v1/EventService/Subscriptions/id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for deleting an event subscription resource, refer to [Table 8-12](#).

Table 8-12 Parameter Descriptions for Deleting the Event Subscription Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
id	User ID	-
auth_value	X-Auth-Token value contained in Request Header in the DELETE request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

DELETE https://device_ip/redfish/v1/EventService/Subscriptions/1

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example: None
- Status Code: 204

Output Description

None

8.7 Resuming Event Subscription

Function

Resumes event subscription.

Permission Required

Basic management.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/EventService/Subscriptions/id/Actions/EventDestination.ResumeSubscription`
- Request Header:

```
X-Auth-Token: auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "DeliverBufferedEventDuration": deliver_buffered_event_duration
}
```

Description

For a description of the parameters for resuming event subscription, refer to [Table 8-13](#).

Table 8-13 Parameter Descriptions for Resuming Event Subscription

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
id	ID of the valid event subscription.	-
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
deliver_buffered_event_duration	After the subscription is resumed, the server resends the unsent events buffered for the subscription. Only those that are within the time range specified by this parameter can be resent.	Time expression that complies with the ISO-8601 specifications. For example, PT8H indicates that those that occurred within the last eight hours from the current time are sent.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/EventService/Subscriptions/13/Actions/EventDestination.ResumeSubscription
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body:

```
{
  "DeliverBufferedEventDuration": "PT8H"
}
```

- Response Example: None
- Response code: 204

Output Description

None

8.8 Reporting an Event

Function

Report an event.

Permission Required

Basic management.

Syntax

- Operation Type: POST
- **URL:** *https://event_destination*

Parameters

For the parameter descriptions for reporting an event, refer to [Table 8-14](#).

Table 8-14 Parameter Descriptions for Reporting an Event Parameters

Field	Type	Description
@odata.context	String	OData description of the root service resource model.
@odata.id	String	Access path of the root service resource node.
@odata.type	String	Type of root service resource.
Id	String	ID of the root service resource. Set it to alert_id.
Name	String	Root service resource name, which is fixed to Event Array.
Events	Object	Set of events.
EventType	String	Event type. Options: ● StatusChange: resource status change event ● ResourceUpdated: resource update event ● ResourceAdded: resource addition event ● ResourceRemoved: resource removal event ● Alert: alarm event
EventId	String	ID of this alarm event, that is, the serial number of the alarm event. The ID is incremented when a new alarm caused by the same fault is raised. The ID of the active alarm is the same as that of the cleared alarm.
EventTimestamp	String	Event occurrence time. ● Active alarm: alarm occurrence time. ● Cleared alarm: time when the alarm is cleared.
Severity	String	Alarm severity level. ● 1: Critical ● 2: Major ● 3: Minor ● 4: Warning. The OrigSeverity value of an active alarm is the same as that of the corresponding cleared alarm. This field does not need to be specified for notifications of event type, and needs to be set to Inform for notifications of internal alarm type.
Message	Object	Manufacturer-customized alarm event or title.
Oem	Object	Customized properties.
alarmStatus	String	Alarm status. ● 1: active. ● 0: cleared.

Field	Type	Description
specificProblemID	String	Alarm event code, which is displayed in decimal format.
specificProblem	String	Alarm classification description.
specificProblemID	String	Alarm classification description.
neUID	String	Alarm server ID, which is set to the SerialNumber value of the server.
neName	String	Alarm server name, which is set to the asset number of the server.
neType	String	Type of alarm device, which is set to server.
objectUID	String	Alarm object ID, which is defined by the manufacturer.
objectName	String	Alarm object name, which is defined by the manufacturer.
objectType	String	Alarm object type, which corresponds to the manufacturer-customized tAlarmPublic.DeviceType. ● {ALARM_DEVICE_TYPE_MAINBOARD, "Main-Board"} ● {ALARM_DEVICE_TYPE_PSU, "PSU"} ● {ALARM_DEVICE_TYPE_FAN, "Fan"} ● {ALARM_DEVICE_TYPE_CPU, "CPU"} ● {ALARM_DEVICE_TYPE_DISK, "Disk"} ● {ALARM_DEVICE_TYPE_MEMORY, "Memory"} ● {ALARM_DEVICE_TYPE_IOMODULE, "IOModule"} ● {ALARM_DEVICE_TYPE_GPU, "GPU"} ● {ALARM_DEVICE_TYPE_NIC_CARD, "NIC_Card"}
locationInfo	String	Alarm positioning information, which is defined by the manufacturer.
Addinfo	String	Detailed information about the alarm, including multiple Key-Value pairs, which are defined by the manufacturer. A key and its value are separated by a colon. Multiple Key-Value pairs are separated by semicolons. Keys and values cannot include colons or semicolons.
Name	String	Name of the alarm event, format: Log entry

8.9 Querying Information About the Event Resource Collection

Function

Query the information about the event resource collection.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/EventService/Alarms?`
`$skip=skip_value&$top=top_value`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the event resource collection, refer to [Table 8-15](#).

Table 8-15 Parameter Descriptions for Querying the Event Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
skip_value	Integer that indicates the number of members in the resource collection to be skipped before the first resource is retrieved.	0 and positive integers
top_value	Integer that indicates the maximum number of members to be included in the response.	0-100

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/EventService/Alarms?$skip=10&$top=3
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#AlarmsCollection.AlarmsCollection",
  "@odata.id": "/redfish/v1/EventService/Alarms",
  "@odata.type": "#AlarmsCollection.v1_0_0.AlarmsCollection",
  "Description": "Collection of Alarms",
  "Id": "Alarms",
  "Members": [
    {
      "AlarmCode": "0x1a000016",
      "AlarmLevel": "Major",
      "Message": "Disk22 is missing assert.",
      "Timestamp": "2010-05-23 02:56:09"
    },
    {
      "AlarmCode": "0x1a000016",
      "AlarmLevel": "Major",
      "Message": "Disk20 is missing assert.",
      "Timestamp": "2010-05-23 02:56:09"
    },
    {
      "AlarmCode": "0x1a000016",
      "AlarmLevel": "Major",
      "Message": "Disk18 is missing assert.",
      "Timestamp": "2010-05-23 02:56:09"
    }
  ],
  "Members@odata.count": 131,
  "Name": "Alarms Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the event resource collection, refer to [Table 8-16](#).

Table 8-16 Output Descriptions for Querying the Event Resource Collection

Field	Type	Description
@odata.context	String	OData description of the event resource collection.
@odata.id	String	Access path of the event resource collection.
@odata.type	String	Type of event resource collection.
Description	String	Description of the event resource collection.
Id	String	ID of the event resource collection.
Name	String	Name of the event resource collection.
Members@odata.count	Number	Number of event resources.
Members	Array	Event resource list.
AlarmCode	String	Event Code
AlarmLevel	String	Event level.
TimeStamp	String	Event generation time.
Message	String	Event information.

8.10 Deleting All Event Resources

Function

Delete all event resources.

Syntax

- Operation Type: DELETE
- URL: `https://device_ip/redfish/v1/EventService/DeleteAlarmsAll`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for deleting all event resources, refer to [Table 8-17](#).

Table 8-17 Parameter Descriptions for Deleting All Event Resources

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	When the DELETE request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
DELETE https://device_ip/redfish/v1/EventService/DeleteAlarmsAll
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example: None
- Response Code: 204

Output Description

None

8.11 Querying Information About the Current Alarm Resource Collection

Function

Query the information about the current alarm resource collection.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/EventService/CurrentAlarms`
- Request Header:

```
X-Auth-Token: auth_value
```

- Request Message Body: None

Parameters

For the parameter descriptions for querying the current alarm resource collection, refer to [Table 8-18](#).

Table 8-18 Parameter Descriptions for Querying the Current Alarm Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/EventService/CurrentAlarms

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#CurrentAlarmsCollection.CurrentAlarmsCollection",
  "@odata.id": "/redfish/v1/EventService/CurrentAlarms",
  "@odata.type": "#CurrentAlarmsCollection.v1_0_0.CurrentAlarmsCollection",
  "Description": "Collection of CurrentAlarms",
  "Id": "CurrentAlarms",
  "Actions": {
    "Oem": {
      "#EventService.DeleteCurrentAlarmsAll": {
        "target": "/redfish/v1/EventService/DeleteCurrentAlarmsAll"
      }
    }
  },
  "Members": [
```

```

    {
      "@odata.id": "/redfish/v1/EventService/CurrentAlarms/93",
      "AlarmCode": "0x03010109",
      "AlarmId": 93,
      "AlarmLevel": "Major",
      "Message": "CPU1_Temp CPU Temperature (86.000 degrees C)
Upper Critical - Going High (86.000 degrees C) assert.",
      "Timestamp": "2010-05-23 03:01:07"
    }
  ],
  "Members@odata.count": 2,
  "Name": "CurrentAlarms Collection"
}

```

- Status Code: 200

Output Description

a description of the output returned when you query the current alarm resource collection, refer to [Table 8-19](#).

Table 8-19 Output Descriptions for Querying the Current Alarm Resource Collection

Field	Type	Description
@odata.context	String	OData description of the current alarm resource collection model.
@odata.id	String	Access path of the current alarm resource collection.
@odata.type	String	Type of alarm resource collection.
Description	String	Description of the current alarm resource collection.
Id	String	ID of the current alarm resource collection.
Actions	Object	Operations that can be performed on the current alarm resource collection.
Oem	Object	Customized properties.
#EventService.DeleteCurrentAlarmsAll.target	String	Operation path.
Name	String	Name of the current alarm resource collection.
Members@odata.count	Number	Number of alarm resource members.
Members	Array	Event subscription resource list.

Field	Type	Description
@odata.id	String	Access path of the specified alarm resource.
AlarmId	Number	ID of the current alarm.
AlarmCode	String	Code of the current alarm.
AlarmLevel	String	Level of the current alarm.
TimeStamp	String	Alarm generation timestamp.
Message	String	Information about the current alarm.

8.12 Querying Information About the Current Alarm Resource

Function

Query the information about the current alarm resource.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/EventService/CurrentAlarms/alarm_id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For the parameter descriptions for querying the current alarm resource, refer to [Table 8-20](#).

Table 8-20 Parameter Descriptions for Querying the Current Alarm Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
alarm_id	alarm_id of the current alarm	Obtained through the upper-layer collection interface.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/EventService/CurrentAlarms/2152
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#CurrentAlarm.CurrentAlarm",
  "@odata.id": "/redfish/v1/EventService/CurrentAlarms/2152",
  "@odata.type": "#CurrentAlarm.v1_0_0.CurrentAlarm",
  "AlarmCode": 30839,
  "AlarmLevel": "Major",
  "Description": "Current Alarm",
  "Id": "2152",
  "Message": "Abnormal reading of ambient temperature (location:INPUT_TEMP).",
  "Name": "CurrentAlarm",
  "Timestamp": 1607004276
}
```

- Status Code: 200

Output Description

a description of the output returned when you query the current alarm resource, refer to [Table 8-21](#).

Table 8-21 Output Descriptions for Querying the Current Alarm Resource

Field	Type	Description
@odata.context	String	OData description of the current alarm resource model.
@odata.id	String	Access path of the current alarm resource.
@odata.type	String	Type of alarm resource.
Id	Number	ID of the current alarm resource.
Name	String	Name of the current alarm resource.

Field	Type	Description
Description	String	Description of the current alarm resource.
AlarmCode	String	Code of the current alarm.
AlarmLevel	String	Level of the current alarm.
TimeStamp	String	Alarm generation timestamp.
Message	String	Information about the current alarm.

8.13 Deleting the Current Alarm Resource

Function

Delete the current alarm resource.

Permission Required

Security management.

Syntax

- Operation Type: DELETE
- URL: `https://device_ip/redfish/v1/EventService/CurrentAlarms/alarm_id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For the parameter descriptions for deleting the current alarm resource, refer to [Table 8-22](#).

Table 8-22 Parameter Descriptions for Deleting an Active Alarm Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
alarm_id	ID of the current alarms	-
auth_value	When the DELETE request is executed, the "X-Auth-Token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

DELETE https://device_ip/redfish/v1/EventService/CurrentAlarms/2152

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example: None
- Response Code: 204

Output Description

None

8.14 Deleting All Current Alarm Resource

Function

Delete all current alarm resources.

Permission Required

Security management.

Syntax

- Operation Type: DELETE
- URL: *https://device_ip/redfish/v1/EventService/DeleteCurrentAlarmsAll*
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For the parameter descriptions for deleting all current alarm resources, refer to [Table 8-23](#).

Table 8-23 Parameter Descriptions for Deleting All Current Alarm Resources

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.

Parameter	Description	Value
auth_value	When the DELETE request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
DELETE https://device_ip/redfish/v1/EventService/DeleteCurrentAlarmsAll
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example: None
- Response Code: 204

Output Description

None

8.15 Querying Information About the Current Alarm Event Resource Collection

Function

Query the information about the current alarm event resource collection.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/EventService/CurrentAlertEvents`
- Request Header:

```
X-Auth-Token: auth_value
```
- Request Message Body: None

Parameters

For the parameter descriptions for querying the current alarm event resource collection, refer to [Table 8-24](#).

Table 8-24 Parameter Descriptions for Querying the Current Alarm Event Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/EventService/CurrentAlertEvents
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#CurrentAlertsCollection.CurrentAlertEventsCollection",
  "@odata.id": "/redfish/v1/EventService/CurrentAlertEvents",
  "@odata.type": "#CurrentAlertEventsCollection.v1_0_0.CurrentAlertEventsCollection",
  "Description": "Collection of CurrentAlertEvents",
  "Id": "CurrentAlertEvents",
  "Members": [
    {
      "EventId": "1513",
      "EventTimestamp": "2024-05-07T19:37:36+0800",
      "EventType": "Alert",
      "Message": "Hard disk is missing",
      "Oem": {
        "Public": {
          "Addinfo": "Disk20 is missing assert.",
          "alarmStatus": 1,
```

```

        "locationInfo": "Disk_20",
        "neName": "6666",
        "neType": "server",
        "neUID": null,
        "objectName": "Disk_20",
        "objectType": "Disk",
        "objectUID": "20",
        "specificProblem": "Hard disk is missing",
        "specificProblemID": "570623745"
    }
},
"Severity": "Major"
},
{
    "EventId": "1512",
    "EventTimestamp": "2024-05-07T19:37:36+0800",
    "EventType": "Alert",
    "Message": "Hard disk is missing",
    "Oem": {
        "Public": {
            "Addinfo": "Disk18 is missing assert.",
            "alarmStatus": 1,
            "locationInfo": "Disk_18",
            "neName": "6666",
            "neType": "server",
            "neUID": null,
            "objectName": "Disk_18",
            "objectType": "Disk",
            "objectUID": "18",
            "specificProblem": "Hard disk is missing",
            "specificProblemID": "570623745"
        }
    },
    "Severity": "Major"
}
],
"Members@odata.count": 2,
"Name": "CurrentAlertEvents Collection"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the current alarm event resource collection, refer to [Table 8-25](#).

Table 8-25 Output Descriptions for Querying the Current Alarm Event Resource Collection

Field	Type	Description
@odata.context	String	OData description of the current alarm event resource collection model.
@odata.id	String	Access path of the current alarm event resource collection.
@odata.type	String	Type of alarm event resource collection.
Description	String	Description of the current alarm event resource collection.
Id	String	ID of the current alarm event resource collection.
Name	String	Name of the current alarm event resource collection.
Members@odata.count	Number	Number of alarm event resource members.
Members	Array	Event subscription resource list
EventId	String	Alarm event ID.
EventType	String	Alarm type.
EventTimestamp	String	Event occurrence time.
Severity	String	Alarm level.
Message	String	Alert event message.
Oem.Public	Object	-
alarmStatus	Number	Alarm status.
specificProblemID	String	Alarm classification ID (alarm code).
specificProblem	String	Alarm classification description (alarm name).
neUID	String	Alarm server ID (serial number of the server).
neName	String	Alarm server name (asset number of the server).

Field	Type	Description
neType	String	Type of the device where the alarm is raised.
objectUID	Number	ID of the alarm part.
objectName	String	Name of the alarm part.
objectType	String	Type of alarm part.
locationInfo	String	Alarm positioning information.
Addinfo	String	Additional alarm information.

8.16 Modifying Event Service Resource Information

Function

Modify event service resource information.

Permission Required

Basic management.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/EventService*
- Request Header:

```
x-auth-token:auth_value
Content-Type:header_type
```

- Request Message Body:

```
{
  "DeliveryRetryAttempts" : retry_attempts,
  "DeliveryRetryIntervalSeconds" : retry_seconds
}
```

Parameters

For a description of the parameters for modifying event service resource information, refer to [Table 8-26](#).

Table 8-26 Parameter Descriptions for Modifying Event Service Resource Information

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.

Parameter	Description	Value
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
retry_attempts	Maximum number of event subscription retries upon a failure.	Number, range: 3–1440.
retry_seconds	Interval (in seconds) at which an event is resent upon a failure.	Number, range: 60–3600.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/EventService
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body:

```
{
  "DeliveryRetryAttempts" : 40,
  "DeliveryRetryIntervalSeconds" : 60
}
```

- Response Example: None
- Response Code: 204

Output Description

None

Chapter 9

Operations on Up- dateService Resources

Table of Contents

Querying Information About an UpdateService Resource.....

518

Querying Information About an Updateable Firmware Resource Collection.....

520

Querying Information About a Specified Updateable Firmware Resource.....

523

Updating Firmware.....

525

Querying Information About PCIe Switch Firmware Update.....

529

Updating Third-Party Module Firmware

531

Uploading a Firmware File to a Server.....

534

Updating the Firmware of a Server

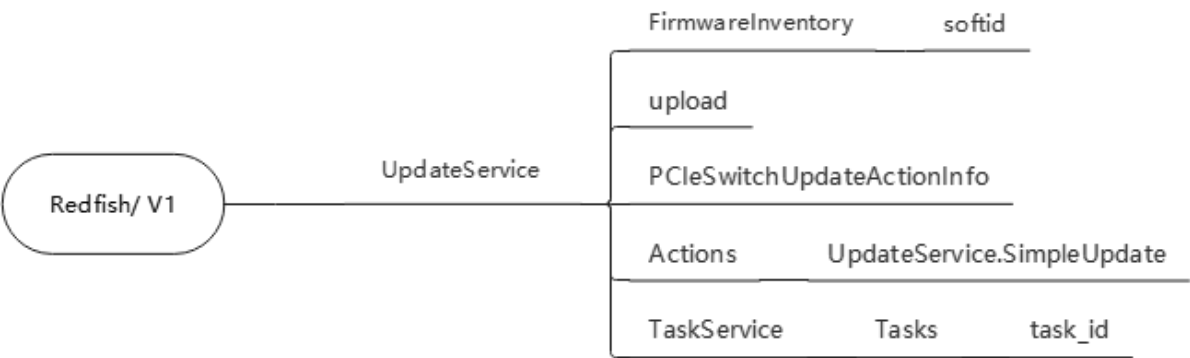
535

Querying Information About a Specified Task.....

539

Figure 9-1 shows the path requirements for the UpdateService resources supported by VANTAGEO servers.

Figure 9-1 UpdateService Resource Path Requirements



For a description of the properties of UpdateService resources and the operations supported by the properties, refer to Table 9-1.

Table 9-1 Descriptions of UpdateService Resources Properties

URL	Property	Description	Operation
/redfish/v1/UpdateService	Id	ID of an UpdateService resource.	GET

URL	Property	Description	Operation
	Name	Name of the UpdateService resource.	GET
	ServiceEnabled	Whether the UpdateService resource is enabled.	GET
	Actions	Available actions for the UpdateService resource.	GET/POST
	#UpdateService.SimpleUpdate	Update operation.	GET
	@Redfish.ActionInfo	Path to query the information about the update operation.	GET
	target	Update operation path.	GET
	FirmwareInventory	Access path of the firmware information resource node.	GET
/redfish/v1/UpdateService/FirmwareInventory	Description	Description of the updateable firmware resource collection.	GET
	Name	Name of the updateable firmware resource collection.	GET
	Members@odata.count	Number of updateable firmware resources.	GET
	Members	List of updateable firmware resources.	GET
/redfish/v1/UpdateService/FirmwareInventory/softid	Description	Description of the updateable firmware resource.	GET
	Id	ID of the specified updateable firmware resource.	GET
	Name	Name of the specified updateable firmware resource.	GET
	Status	Status of the specified updateable firmware resource.	GET

URL	Property	Description	Operation
	Version	Version of the specified updateable firmware resource.	GET
	Updateable	Update status of the specified updateable firmware resource.	GET
	BuildTime	Compilation time of the updateable firmware resource.	GET
/redfish/v1/UpdateService/Actions/UpdateService.SimpleUpdate	imageuri	Update package path.	POST
	protocol	Protocol used to download the update package.	POST
	Oem	Customized network services.	POST
	Public	Vantageo-defined services.	POST
	FlashItem	Update package type.	POST
	BMCFlash	Location for saving updated BMC firmware.	POST
	BiosFlash	Location for saving updated BIOS firmware.	POST
	PreserveConf	Whether to BMC and BIOS settings are retained.	POST
redfish/v1/UpdateService/PCleSwitchUpdateActionInfo	Id	Unique ID of the specified update service resource.	GET
	Name	Name of the resource for PCIe switch firmware update.	GET
	SupportedMode	Modes supported by the resource for PCIe switch firmware update.	GET
	Mode	Mode of the resource for PCIe switch firmware update.	GET

URL	Property	Description	Operation
/redfish/v1/UpdateService/Actions/UpdateService.ThirdPartyUpload	Messages	Collection of descriptions for third-party module firmware update.	POST
	Messages.@odata.type	Type of message for third-party module firmware update.	POST
	Messages.Message	Information about third-party module firmware update.	POST
	Messages.MessageArgs	Message arguments of third-party module firmware update.	POST
	Messages.MessageId	Message ID of third-party module firmware update.	POST
	Messages.Resolution	Recommended solution.	POST
	Messages.Severity	Severity level.	POST
/redfish/v1/UpdateService/Actions/UpdateService.SimpleUpdate	Messages	Collection of descriptions for server firmware update.	POST
	Messages.@odata.type	Type of message for server firmware update.	POST
	Messages.Message	Message for server firmware update.	POST
	Messages.MessageArgs	Message arguments for server firmware update.	POST
	Messages.MessageId	Message ID for server firmware update.	POST
	Messages.Resolution	Recommended solution.	POST
	Messages.Severity	Severity level.	POST
/redfish/v1/TaskService/Tasks/task_id	Description	Task description.	POST
	Id	Task ID.	POST
	Messages	Collection of descriptions for task details.	POST
	Messages.@odata.type	Message type for the task.	POST

URL	Property	Description	Operation
	Messages.Message	Message for the task.	POST
	Messages.MessageArgs	Message arguments of the task.	POST
	Messages.MessageId	Message ID of the task.	POST
	Messages.Resolution	Recommended solution.	POST
	Messages.Severity	Severity level.	POST
	Name	Task name.	POST
	PercentComplete	Task progress in percentage.	POST
	StartTime	Task start time.	POST
	TaskState	Task execution status.	POST
	TaskStatus	Task execution result.	POST

9.1 Querying Information About an UpdateService Resource

Function

Query information about an UpdateService resource.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/UpdateService*
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the UpdateService resource, refer to [Table 9-2](#).

Table 9-2 Parameter Descriptions for Querying Information About the UpdateService Resource

Parameter	Parameter	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/UpdateService
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#UpdateService.UpdateService",
  "@odata.id": "/redfish/v1/UpdateService",
  "@odata.type": "#UpdateService.v1_6_0.UpdateService",
  "Actions": {
    "#UpdateService.SimpleUpdate": {
      "@Redfish.ActionInfo": "/redfish/v1/UpdateService/
UpdateService.SimpleUpdateActionInfo",
      "target": "/redfish/v1/UpdateService/Actions/SimpleUpdate"
    }
  },
  "Description": "Redfish Update Service",
  "FirmwareInventory": {
    "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory"
  },
  "Id": "UpdateService",
  "Name": "Update Service",
  "ServiceEnabled": true,
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  }
}
```

```
}
}
```

- Response Code: 200

Output Description

For a description of the output returned when you query information about the UpdateService resource, refer to [Table 9-3](#).

Table 9-3 Output Descriptions for Querying Information About the UpdateService Resource

Field	Type	Description
@odata.context	String	OData description of a specified UpdateService resource model.
@odata.id	String	Access path of the specified UpdateService resource.
@odata.type	String	Type of the specified UpdateService resource.
Description	String	Description of the specified update service resource.
Id	String	ID of the specified UpdateService resource.
Name	String	Name of the specified UpdateService resource.
Status.Health	String	Status of the specified UpdateService resource.
Status.State	String	Health of the specified UpdateService resource.
ServiceEnabled	Boolean	Whether the UpdateService is enabled.
Actions	Object	Available actions for the UpdateService resource.
#UpdateService.SimpleUpdate.target	String	Update operation path.
#UpdateService.SimpleUpdate.@Redfish.ActionInfo	String	Path to query the information about the update operation.
FirmwareInventory	Object	Link to the updateable firmware resource list.
@odata.id	String	Access path of the updateable firmware resource list.

9.2 Querying Information About an Updateable Firmware Resource Collection

Function

Query information about an updateable firmware resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/UpdateService/FirmwareInventory*
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the updateable firmware resource collection, refer to [Table 9-4](#).

Table 9-4 Parameter Descriptions for Querying Information About the Updateable Firmware Resource Collection

Parameter	Parameters	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/UpdateService/FirmwareInventory

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

{
 "@odata.context":
 "/redfish/v1/\$metadata#SoftwareInventoryCollection.SoftwareInventoryCollection",
 "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory",
 "@odata.type": "#SoftwareInventoryCollection.SoftwareInventoryCollection",
 "Description": "Collection of Firmware Inventory resources available to the
UpdateService",
 "Members": [

```

    {
      "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/ActiveBMC"
    },
    {
      "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/ActiveBIOS"
    },
    {
      "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/EPLD"
    },
    {
      "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/MainBoardFRU"
    },
    {
      "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/SubCardFRU2"
    }
  ],
  "Members@odata.count": 5,
  "Name": "Firmware Inventory Collection"
}

```

- Response Code: 200

Output Description

For a description of the output returned when you query information about the updateable firmware resource collection, refer to [Table 9-5](#).

Table 9-5 Output Descriptions for Querying Information About the Updateable Firmware Resource Collection

Field	Type	Description
@odata.context	String	OData description of the updateable firmware resource collection model.
@odata.id	String	Access path of the updateable firmware resource collection model.
@odata.type	String	Type of updateable firmware resource collection model.
Description	String	Description of the updateable firmware resource collection.
Name	String	Name of the updateable firmware resource collection.
Members@odata.count	Number	Number of updateable firmware resources.
Members	Array	Session list.
@odata.id	String	Access path of an updateable firmware resource.

9.3 Querying Information About a Specified Updateable Firmware Resource

Function

Query information about a specified updateable firmware resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/UpdateService/FirmwareInventory/softid*
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about a specified updateable firmware resource of a server, refer to [Table 9-6](#).

Table 9-6 Parameter Descriptions for Querying Information About a Specified Updateable Firmware Resource

Parameter	Parameters	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
softid	ID of the updateable firmware resource.	It can be obtained from the updateable firmware resource collection.

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/UpdateService/FirmwareInventory/ActiveBMC

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#SoftwareInventory.SoftwareInventory",
  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/ActiveBMC",
  "@odata.type": "#SoftwareInventory.v1_2_3.SoftwareInventory",
  "Description": "ActiveBMC",
  "Id": "ActiveBMC",
  "Name": "ActiveBMC",
  "Oem": {
    "Public": {
      "BuildTime": "Jun 28 2023"
    }
  },
  "SoftwareId": "ActiveBMC",
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  },
  "Updateable": true,
  "Version": "04.22.01.93"
}
```

- Response Code: 200

Output Description

For a description of the output returned when you query information about a specified updateable firmware resource of a server, refer to [Table 9-7](#).

Table 9-7 Output Descriptions for Querying Information About a Specified Updateable Firmware Resource

Field	Type	Description
@odata.context	String	OData description of the updateable firmware resource.
@odata.id	String	Access path of the updateable firmware resource.
@odata.type	String	Type of updateable firmware resource.
Description	String	Description of the updateable firmware resource.
Id	String	ID of the updateable firmware resource.

Field	Type	Description
Name	String	Name of the updateable firmware resource.
SoftwareId	String	Firmware ID.
Status.Health	String	Health status of the updateable firmware resource.
Status.State	String	Status of the updateable firmware resource.
Version	String	Firmware version.
Updateable	Boolean	Whether the Update Service can update this software • true • false
BuildTime	String	Compilation time of the updateable firmware resource.

9.4 Updating Firmware

Function

Update the firmware of a server.

Permission Required

Query.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/UpdateService/Actions/UpdateService/upload`
- Request Header:

```
X-Auth-Token: auth_value
Content-Type: header_type
```

- Request Message Body: In the **VALUE** column for the **UpdateFile** parameter, select the firmware update file to be uploaded. In the **VALUE** column for **OemParameters**, select the OEM parameter JSON file to be uploaded. In the **VALUE** column for **UpdateParameters**, select the update parameter JSON file to be uploaded.

Parameters

For a description of the parameters for updating server firmware, refer to [Table 9-8](#).

Table 9-8 Parameter Descriptions for Updating Server Firmware

Field	Type	Description
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
UpdateFile	File	Firmware update file.
OemParameters	File	OEM parameter file in JSON format, including the following content: {"ImageType":"BMC","Action":"3"}
UpdateParameters	File	Content: - Update the active BMC: ["/redfish/v1/UpdateService/FirmwareInventory/BMC"] or {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/ActiveBMC"]} - Update the standby BMC: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/BackupBMC"]}
ImageType	String	Options: - BMC - BIOS - EPLD - FRU - BOOT - EXPANDER The file type is verified but not by file extension.
Action	String	Range: When ImageType is set to BMC: 1: Only the BMC BOOT is retained. 2: Only the BMC configuration is retained. 3: Both BMC BOOT and configuration are retained. 4: Neither BMC BOOT nor configuration is retained. Actions supported by the BMC: 1, 2, 3, and 4. When ImageType is set to BIOS:

Field	Type	Description
		● 3: NVRAM is retained. ● 4: NVRAM is not retained. Actions supported by the BIOS: 3 and 4. When ImageType is set to others, the Redfish interface does not parse the action setting.
Targets	Array	Active and standby BMCs and BIOSs can be updated simultaneously or separately. ● BMC update: → Update the active BMC: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/ActiveBMC"]} → Update the standby BMC: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/BackupBMC"]} → Update both the active and standby BMCs: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/ActiveBMC","/redfish/v1/UpdateService/FirmwareInventory/BackupBMC"]} ● BIOS update: → JSON parameters in the <i>UpdateParameters</i> file for updating a single-chip BIOS are as follows: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/BIOS"]} → Update the active BIOS: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/ActiveBIOS"]} → Update the standby BIOS: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/BackupBIOS"]} → Update both the active and standby BIOSs: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/ActiveBIOS","/redfish/v1/UpdateService/FirmwareInventory/BackupBIOS"]}

Usage Guidelines

None

Example

- Request Example:

POST https://device_ip/redfish/v1/UpdateService/Actions/UpdateService/upload

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

Content-Type: multipart/form-data

- Request Message Body: In the **VALUE** column for the **UpdateFile** parameter, select the firmware update file to be uploaded. In the **VALUE** column for **OemParameters**, select the OEM parameter JSON file to be uploaded. In the **VALUE** column for **UpdateParameters**, select the update parameter JSON file to be uploaded.
- Response Example:

```
{
  "@odata.type": "#UpdateService.v1_6_0.UpdateService",
  "Messages": [
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message": "A new task /redfish/v1/TaskService/Tasks/1 was created.",
      "MessageArgs":
        [
          "/redfish/v1/TaskService/Tasks/1"
        ],
      "MessageId": "Task.1.0.New",
      "Resolution": "None",
      "Severity": "OK"
    },
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message": "Device is preparing flash firmware for action
        UpdateService.MultipartPush.",
      "MessageArgs":
        [
          "UpdateService.MultipartPush"
        ],
      "MessageId": "UpdateService.1.0.PrepareUpdate",
      "Resolution": "None",
      "Severity": "OK"
    }
  ]
}
```

- Response Code: 202

Output Description

None

9.5 Querying Information About PCIe Switch Firmware Update

Function

Query information about PCIe switch firmware update.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/UpdateService/PCISwitchUpdateActionInfo`
- Request Header:

X-Auth-Token: auth_value
- Request Message Body: None

Description

For a description of the parameters for querying information about PCIe switch firmware update, refer to [Table 9-9](#).

Table 9-9 Parameter Descriptions for Querying Information About PCIe Switch Firmware Update

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/UpdateService/PCISwitchUpdateActionInfo

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#UpdateService.PCIESwitchUpdateActionInfo",
  "@odata.id": "/redfish/v1/UpdateService/PCIESwitchUpdateActionInfo",
  "@odata.type": "PCIESwitchUpdateActionInfo.v1_0_0.PCIESwitchUpdateActionInfo",
  "Id": "PCIESwitchUpdateActionInfo",
  "Name": "Pcie Switch Update Service",
  "SupportedMode": ["Balance", "Cascade", "Normal"],
  "Mode": "Cascade"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query PCIe switch firmware update, refer to [Table 9-10](#).

Table 9-10 Output Descriptions for Querying Information About PCIe Switch Firmware Update

Field	Type	Description
@odata.context	String	OData description of the PCIe-switch-firmware-update service model.
@odata.id	String	Access path of the service for PCIe switch firmware update.
@odata.type	String	Type of service for PCIe switch firmware update.
Id	String	Unique ID of the service for PCIe switch firmware update.
Name	String	Name of the service for PCIe switch firmware update.
Mode	String	Mode used by the service for PCIe switch firmware update. • Cascade • Balance • Normal

9.6 Updating Third-Party Module Firmware

Function

Update third-party module firmware.

Permission Required

Query.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/UpdateService/Actions/UpdateService.ThirdPartyUpload`
- Request Header:

```
X-Auth-Token: auth_value
Content-Type: header_type
```

- Request Message Body:

```
UpdateFile: file_value,
UpdateParameters: update_parameters_file_value,
OemParameters: oem_parameters_file_value
```

Description

For a description of the parameters for updating third-party module firmware, refer to [Table 9-11](#).

Table 9-11 Parameter Descriptions for Updating Third-Party Module Firmware

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
file_value	Firmware update file to be uploaded.	Only the firmware type is checked. No applicable model is checked.

Parameter	Setting	Value
oem_parameter-s_flie_value	JSON file for the OEM parameters to be uploaded.	Contents: {"ImageType":"UBB_E-PLD"}, {"ImageType":"UBB_RETIMER"}, {"ImageType":"UBB_OAM"}, {"ImageType":"UBB_BMC"}
update_parameter-s_flie_value	JSON file for firmware update parameters to be uploaded.	Content: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/UBB_E-PLD"]} {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/UBB_RETIMER"]} {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/UBB_OAM"]} {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/UBB_BMC"]}
ImageType	String	Range: • UBB_EPLD • UBB_RETIMER • UBB_OAM • UBB_BMC
Targets	Array	EPLD of the third-party module to be updated. {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/UBB_EPLD"]} Retimer of the third-party module to be updated. {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/UBB_RETIMER"]} {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/UBB_OAM"]} {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/UBB_BMC"]}

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/UpdateService/Actions/UpdateService.ThirdPartyUpload
```

- Request Header:

```
POST https://device_ip/redfish/v1/UpdateService/Actions/UpdateService.ThirdPartyUpload
```


- Request Message Body: In the **VALUE** column for the **UpdateFile** parameter, select the firmware update file to be uploaded. In the **VALUE** column for **OemParameters**, select the OEM parameter JSON file to be uploaded. In the **VALUE** column for **UpdateParameters**, select the update parameter JSON file to be uploaded.

```
UpdateFile: pt516_x16_reversed_usp_p8_dspp_p9_icc0-SDPP_FORCE_G5_P9_ACS-816_v2.json,
UpdateParameters: UpdateParameters2.json,
OemParameters: OemParameters2.json
```

- Response Example:

```
{
  "@odata.type": "#UpdateService.v1_6_0.UpdateService",
  "Messages": [
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message": "A new task /redfish/v1/TaskService/Tasks/1 was created.",
      "MessageArgs": [
        "/redfish/v1/TaskService/Tasks/1"
      ],
      "MessageId": "Task.1.0.New",
      "Resolution": "None",
      "Severity": "OK"
    },
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message":
        "Device is preparing flash firmware for action updateService.MultipartPush.",
      "MessageArgs": [
        "UpdateService.MultipartPush"
      ],
      "MessageId": "UpdateService.1.0.PrepareUpdate",
      "Resolution": "None",
      "Severity": "OK"
    }
  ]
}
```

- Response code: 202

Output Description

For a description of the output returned when you update third-party module firmware, refer to [Table 9-12](#).

Table 9-12 Output Descriptions for Updating Third-Party Module Firmware

Field	Type	Description
@odata.type	String	Type of message for third-party module firmware update.
Messages	Array	Collection of descriptions for third-party module firmware update.
Messages.@odata.type	String	Type of message for third-party module firmware update.
Messages.Message	String	Information about third-party module firmware update.
Messages.MessageArgs	Array	Message arguments of third-party module firmware update.
Messages.MessageId	String	Message ID of third-party module firmware update.
Messages.Resolution	String	Recommended solution.
Messages.Severity	String	Severity level. Options: • OK • Warning • Critical

9.7 Uploading a Firmware File to a Server

Function

Upload a firmware file to a specified server.

Permission Required

Basic management.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/UpdateService/FirmwareInventory*
- Request Header:

```
X-Auth-Token: auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "fwimage" : fwimage_file
}
```

Parameters

For a description of the parameters for uploading a firmware file to the server, refer to [Table 9-13](#).

Table 9-13 Parameter Descriptions for Uploading a Firmware File to the Server

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
fwimage_file	Firmware update file to be uploaded.	Only the firmware type is checked. No applicable model is checked.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/UpdateService/FirmwareInventory
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: multipart/form-data
```

- Request Message Body: In the **VALUE** column for the **fwimage** parameter, select the firmware update file to be uploaded.
- Response Example: None
- Response code: 204

Output Description

None

9.8 Updating the Firmware of a Server

Function

Update the firmware of a server.

Permission Required

Basic management.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/UpdateService/Actions/UpdateService.SimpleUpdate`
- Request Header:

```
X-Auth-Token: auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "TransferProtocol": TransferProtocol_value,
  "ImageURI": ImageURI_value,
  "Oem": {
    "Public": {
      "FlashItem": FlashItem_value,
      "BMCFirmware": BMCFirmware_value,
      "BiosFirmware": BiosFirmware_value,
      "PreserveConf": PreserveConf_value
    }
  }
}
```

Parameters

For a description of the parameters for updating the firmware of the specified server, refer to [Table 9-14](#).

Table 9-14 Parameter Descriptions for Updating the Firmware of the Specified Server

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
TransferProtocol_value	String	Protocol used to download the update package: HTTPS

Parameter	Setting	Value
		Note: For local update, this parameter does not need to be set.
ImageURI_value	String	URI for the firmware update file. Note: This parameter is used for remote update. For local update, this parameter does not need to be set.
FlashItem_value	String	Update package type, which is not required for the default user for PCIe switch firmware update. Range: • BMC • BIOS • EPLD • FRU • BOOT • EXPANDER • VR • PSU
BMCFlash_value	String	BMC flash update option. BMCFlash_value and BiosFlash_value cannot be both configured. Options: • Flash1: active BMC • Flash2: standby BMC • Both: active and standby BMCs
BiosFlash_value	String	BIOS flash update option. BMCFlash_value and BiosFlash_value cannot be both configured. Options: • Flash1: active BIOS • Flash2: standby BIOS • Both: active and standby BIOSs
PreserveConf_value	Boolean	Whether the original configuration is kept during the update process: • true: yes • false: no

Usage Guidelines

None

Example

- Request Example:

POST https://device_ip/redfish/v1/UpdateService/Actions/UpdateService.SimpleUpdate

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json

- Request Message Body:

```
{
  "TransferProtocol": "HTTPS",
  "ImageURI":
    "https://192.168.1.5/bmcdata/
    BMC_2240-RE_A6_R_V04.23.01.01T1_20230516085914.UBF", "Oem": {
    "Public": {
      "FlashItem": "BMC",
      "BMCFlash": "Flash1",
      "PreserveConf": true
    }
  }
}
```

- Response Example:

```
{
  "@odata.type": "#UpdateService.v1_6_0.UpdateService",
  "Messages": [
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message": "A new task /redfish/v1/TaskService/Tasks/1 was created.",
      "MessageArgs": [
        "/redfish/v1/TaskService/Tasks/1"
      ],
      "MessageId": "Task.1.0.New",
      "Resolution": "None",
      "Severity": "OK"
    },
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message":
        "Device is preparing flash firmware for action UpdateService.SimpleUpdate.",
      "MessageArgs": [
        "UpdateService.SimpleUpdate"
      ],
      "MessageId": "UpdateService.1.0.PrepareUpdate",
      "Resolution": "None",
    }
  ]
}
```

```
        "Severity": "OK"
      }
    ]
  }
}
```

- Response code: 202

Output Description

For a description of the output returned when you update the firmware of the server, refer to [Table 9-15](#).

Table 9-15 Output Descriptions for Updating the Firmware of the Server

Field	Type	Description
@odata.type	String	Type of the server firmware update resource.
Messages	Array	Collection of descriptions for server firmware update.
Messages.@odata.type	String	Type of message for server firmware update.
Messages.Message	String	Message for server firmware update.
Messages.MessageArgs	Array	Message arguments for server firmware update.
Messages.MessageId	String	Message ID for server firmware update.
Messages.Resolution	String	Recommended solution.
Messages.Severity	String	Severity level. Options: • OK • Warning • Critical

9.9 Querying Information About a Specified Task

Function

Query information about a specified task.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/TaskService/Tasks/task_id`
- Request Header:

```
X-Auth-Token: auth_value
```

- Request Message Body: None

Description

For a description of the parameters for querying information about the specified task, refer to [Table 9-16](#).

Table 9-16 Parameter Descriptions for Querying Information About the Specified Task

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
task_id	Task ID.	Included in the response message body returned when the task was created successfully.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/TaskService/Tasks/1
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Task.Task",
  "@odata.id": "/redfish/v1/TaskService/Tasks/1",
  "@odata.type": "#Task.v1_4_2.Task",
  "Description": "Task for update Service Task",
  "Id": "1",
  "Messages": [
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message": "Task /redfish/v1/UpdateService/upload is running normally.",
      "MessageArgs": [
        "/redfish/v1/UpdateService/upload"
      ],
    }
  ],
}
```



```

        "MessageId": "Task.1.0.Running",
        "Resolution": "None",
        "Severity": "OK"
    },
    {
        "@odata.type": "#Message.v1_0_8.Message",
        "Message": "Device is flashing firmware for action /redfish/v1/UpdateService/upload.",
        "MessageArgs": [
            "/redfish/v1/UpdateService/upload"
        ],
        "MessageId": "UpdateService.1.0.FlashFirmware",
        "Resolution": "None",
        "Severity": "OK"
    }
],
"Name": "Update Service Task",
"PercentComplete": 21,
"StartTime": "2024-09-13T17:59:34+08:00",
"TaskState": "Running",
"TaskStatus": "OK"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified task, refer to [Table 9-17](#).

Table 9-17 Output Descriptions for Querying Information About the Specified Task

Field	Type	Description
@odata.context	String	OData description of the task resource model.
@odata.id	String	Access path of the task resource.
@odata.type	String	Type of task resource.
Description	String	Description.
Id	String	Task ID.
Messages	Array	Collection of descriptions for task details.
Messages.@odata.type	String	Message type for the task.
Messages.Message	String	Message for the task.
Messages.MessageArgs	Array	Message arguments of the task.

Field	Type	Description
Messages.MessageId	String	Message ID of the task.
Messages.Resolution	String	Recommended solution.
Messages.Severity	String	Severity level. Options: • OK • Warning • Critical
Name	String	Task name.
PercentComplete	Number	Task progress in percentage.
StartTime	String	Task start time.
TaskState	String	Task execution status.
TaskStatus	String	Task execution result.

Chapter 10

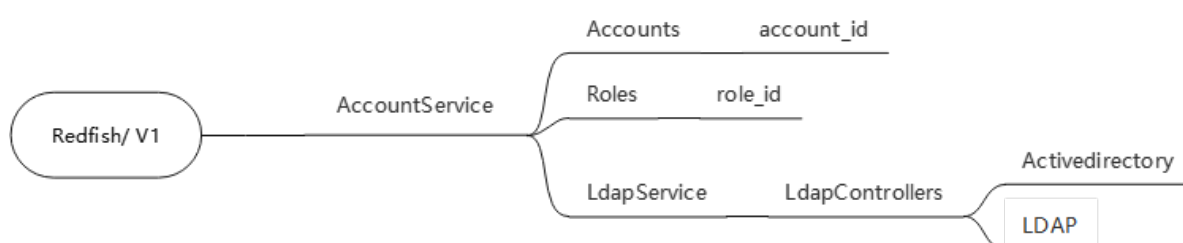
Operations on AccountService Resources

Table of Contents

Querying User Service Information	546
Modifying User Service Information	549
Querying Information About the User Resource Collection	552
Querying Information About a Specified Account Resource	554
Creating an Account	556
Deleting an Account	559
Modifying Information About a Specified Account	560
Querying Information About the Role Resource Collection	563
Querying Information About a Specified Role Resource	565
Querying Information About the LDAP Service Resource	567
Querying Information About the Collection of LDAP Domain Controller Resources	569
Querying the Active Directory Information	571
Modifying the Active Directory Information	574
Querying LDAP Information	580
Modifying the LDAP Information	583

Figure 10-1 shows the path requirements for the AccountService resources supported by VANTAGEO servers

Figure 10-1 AccountService Resource Path Requirements



For a description of properties of AccountService resources and operations supported by the properties, refer to [Table 10-1](#).

Table 10-1 Descriptions of AccountService Resources Properties

URL	Property	Description	Operation
/redfish/v1/AccountService	Id	ID of the AccountService resource.	GET
	Name	Name of the AccountService resource.	GET
	MinPasswordLength	Minimum password length.	GET
	MaxPasswordLength	Maximum password length.	GET
	AccountLockoutThreshold	Maximum number of incorrect password attempts.	GET
	AccountLockoutDuration	Account lockout duration after a user login failure.	GET
	AccountLockoutCounterResetAfter	Time after which account lockout counter is reset.	GET
	Roles	Role resources.	GET
	Accounts	User resources.	GET
	Status	Status of the specified resource, including: ● Status: enabling status ● Health: health status	GET
	SSHAdministratorUserName	Username of the SSH administrator.	GET
	OSUserManagementEnabled	Whether permission to inband management is enabled.	GET
/redfish/v1/AccountService/Accounts	Name	Name of the account resource.	GET
	Members@odata.count	Number of account members.	GET
	Members	User list, which provides references to all user URLs.	GET
	Id	ID of the specified user resource.	POST
/redfish/v1/AccountService/Accounts/account_id	Id	ID of the specified user resource.	GET
	Name	Name of the account resource.	GET
	UserName	Username of the account.	GET/PATCH
	Password	User password.	GET/PATCH
	RoleId	Role resource ID in the account configuration.	GET/PATCH

URL	Property	Description	Operation
	Locked	Locked state of the account.	GET/PATCH
	Enabled	Whether the account is enabled.	GET/PATCH
	Links	Links to the user resource.	GET
	Roles	Links to the roles corresponding to the user.	GET
/redfish/v1/AccountService/Roles	Name	Name of the role resource.	GET
	Members@odata.count	Number of current roles.	GET
	Members	-	GET
/redfish/v1/AccountService/Roles/role_id	Id	ID of the specified role resource.	GET
	Name	Name of the specified role resource.	GET
	IsPredefined	Whether the specified role is pre-defined.	GET
	AssignedPrivileges	Privileges assigned to the specified role.	GET
	OemPrivileges	Customized privileges assigned to the specified role.	GET
/redfish/v1/AccountService/LdapService	Id	ID of the LDAP service resource.	GET
	Name	Name of the LDAP service resource.	GET
redfish/v1/AccountService/LdapService/Ldap-Controllers	Name	Name of the LDAP domain controller set.	GET
	Members	LDAP controller member list.	GET
/AccountService/LdapService/Ldap-Controllers/Activedirectory	Id	ID of the Active Directory information resource.	GET/PATCH
	Name	Name of the Active Directory information resource.	GET/PATCH
	GroupLoginInterface	Access permission.	GET/PATCH
	GroupRole	Role group permission.	GET/PATCH
	MemberId	Role group ID: 0-4	GET/PATCH
	GroupDomain	Group domain	GET/PATCH
/redfish/v1/AccountService/LdapService/Ldap-Controllers/LDAP	BindDN	Bound DN.	GET/PATCH
	CommonNameType	Common name types, including: IP	GET/PATCH

URL	Property	Description	Operation
		FQDN	
	EncryptionType	Encryption type. Options: - NoEncryption - SSL - StartTLS	GET/PATCH
	LDAPAuthenticationEnable	Whether LDAP authentication is enabled.	GET/PATCH
	LDAPRoleGroups	LDAP role group.	GET/PATCH
	GroupName	Group name.	GET/PATCH
	GroupDomain	Group domain.	GET/PATCH
	GroupLoginInterface	Access permission, options: - KVM - VMedia	GET/PATCH
	GroupRole	Role group permission, options: - Administrator - Operator - ReadOnly	GET/PATCH
	MemberId	Role group ID.	GET/PATCH
	Name	Name of the LDAP information resource.	GET/PATCH
	Password	Password, which is displayed as null.	GET/PATCH
	Port	Port number.	GET/PATCH
	SearchBase	Search base.	GET/PATCH
	ServerAddress	Server address.	GET/PATCH
	UserLoginAttribute	User login attributes, options: - uid - cn	GET/PATCH

10.1 Querying User Service Information

Function

Query the current user service information about a server, including the password length, the maximum number of incorrect password attempts, and the lockout duration.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/AccountService`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameter Descriptions

For a description of the parameters for querying the user service information, refer to [Table 10-2](#).

Table 10-2 Parameter Descriptions for Querying User Service Information

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET `https://device_ip/redfish/v1/AccountService`

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#AccountService.AccountService",
  "@odata.id": "/redfish/v1/AccountService",
  "@odata.type": "#AccountService.v1_2_2.AccountService",
  "AccountLockoutDuration": 180,
```

```

    "AccountLockoutThreshold": 3,
    "Accounts": {
        "@odata.id": "/redfish/v1/AccountService/Accounts"
    },
    "Description": "BMC User Accounts",
    "Id": "AccountService",
    "MaxPasswordLength": 20,
    "MinPasswordLength": 5,
    "Name": "Account Service",
    "Roles": {
        "@odata.id": "/redfish/v1/AccountService/Roles"
    },
    "ServiceEnabled": true,
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    }
    "Oem":{
        "Public":{
            "SSHAdministratorUserName":"sysadmin",
            "OSUserManagementEnabled": true
        }
    }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query user service information, refer to [Table 10-3](#).

Table 10-3 Output Descriptions for Querying User Service Information

Field	Type	Description
@odata.context	String	OData description of the AccountService resource model.
@odata.id	String	Access path of the AccountService resource node.
@odata.type	String	Type of AccountService resource.
Description	String	Description of the AccountService resource.
Id	String	ID of the AccountService resource.
Name	String	Name of the AccountService resource.

Field	Type	Description
MinPasswordLength	Number	Minimum password length.
MaxPasswordLength	Number	Maximum password length.
AccountLockoutThreshold	Number	Maximum number of incorrect password attempts, range: 1–10.
AccountLockoutDuration	Number	Lockout duration after a login failure, range: 60-3600 (It must be a multiple of 60), in seconds.
AccountLockoutCounterResetAfter	Number	Time after which account lockout counter is reset.
Roles	Object	Role resources.
@odata.id	String	Access path of the role resource node.
ServiceEnabled	Boolean	Whether the AccountService resource is enabled.
Accounts	Object	User resources.
@odata.id	String	Access path of the Account resource node.
Status.Health	String	Health status of the AccountService resource resource.
Status.State	String	Status of the AccountService resource.
SSHAdministratorUserName	String	Username of the SSH administrator.
OSUserManagementEnabled	Boolean	Whether permission to inband management is enabled.

10.2 Modifying User Service Information

Function

Modify the current user service information about a server, including the maximum number of incorrect password attempts, and the lockout duration.

Permission Required

User Configuration

Syntax

- Operation Type: PATCH
- **URL:** `https://device_ip/redfish/v1/AccountService`

- Request Header:

X-Auth-Token: auth_value

Content-Type: header_type

If-Match: ifmatch_value

- Request Message Body:

→ User information modification:

```
{
  "AccountLockoutThreshold":count,
  "AccountLockoutDuration":time
}
```

→ [SSH](#) administrator password modification:

```
{
  "Oem":{
    "Public":{
      "SSHAdministratorPassword": password
    }
  }
}
```

→ Modification of the inband management permission flag:

```
{
  "Oem":{
    "Public":{
      "OSUserManagementEnabled": flag
    }
  }
}
```

Parameter Descriptions

For a description of the parameters for modifying user service information, refer to [Table 10-4](#).

Table 10-4 Parameter Descriptions for Modifying User Service Information

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	Authentication parameters of the request message.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json

Parameter	Description	Value
ifmatch_value	Parameters matching the request message.	Perform the GET operation on the related resource and obtain the value from the ETag parameter in the header of the response message.
count	Maximum number of incorrect password attempts.	Integer, range: 0–10.
time	Duration for which a user is locked upon a login failure.	Range: 60–3600 (It must be a multiple of 60), unit: seconds.
password	SSH administrator password.	8–64 characters.
flag	Whether permission to inband management is enabled.	• true • false

Usage Guidelines

For a specified user, multiple properties in the request message body can be modified at the same time.

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/AccountService
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body:

```
{
  "AccountLockoutThreshold":8,
  "AccountLockoutDuration": 3
}
```

→ SSH administrator password modification:

```
{
  "oem":{
    "Public":{
      "SSHAdministratorPassword": "Superuser9!"
    }
  }
}
```

→ Modification of the inband management permission flag:

```
{
  "oem": {
    "Public": {
      "OSUserManagementEnabled": true
    }
  }
}
```

- Response Example: None
- Response Code: 204

Output Description

None

10.3 Querying Information About the User Resource Collection

Function

Query information about the user resource collection of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/AccountService/Accounts*
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the user resource collection, refer to [Table 10-5](#).

Table 10-5 Parameter Descriptions for Querying Information About the User Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.

Parameter	Description	Value
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/Accounts
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#ManagerAccountCollection.ManagerAccountCollection",
  "@odata.id": "/redfish/v1/AccountService/Accounts",
  "@odata.type": "#ManagerAccountCollection.ManagerAccountCollection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/AccountService/Accounts/2"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Accounts/3"
    }
  ],
  "Members@odata.count": 2,
  "Name": "Accounts Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the user resource collection, refer to [Table 10-6](#).

Table 10-6 Output Descriptions for Querying Information About the User Resource Collection

Field	Type	Description
@odata.context	String	OData description of the account resource model.
@odata.id	String	Access path of the account resource node.
@odata.type	String	Type of account resource.
Name	String	Name of the account resource.
Members@odata.count	Number	Number of account members.
Members	Array	User list.
@odata.id	String	Access path of a single account resource node.

10.4 Querying Information About a Specified Account Resource

Function

Query information about a specified account resource of a server.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/AccountService/Accounts/account_id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified account resource, refer to [Table 10-7](#).

Table 10-7 Parameter Descriptions for Querying Information About the Specified Account Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Parameter	Description	Value
account_id	Subscriber ID .	It can obtained by querying the user list.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/Accounts/2
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#ManagerAccount.ManagerAccount",
  "@odata.id": "/redfish/v1/AccountService/Accounts/2",
  "@odata.type": "/redfish/v1/$metadata#ManagerAccount.ManagerAccount",
  "Name": "User Account",
  "Id": "2",
  "Enabled": true,
  "Links": {
    "Roles": {
      "@odata.id": "/redfish/v1/AccountService/Roles/Administrator"
    }
  },
  "RoleId": "Administrator",
  "UserName": "Administrator",
  "Locked": false
}
```

- Status Code: 200

Output Description

a description of the output returned when you query information about the specified account resource, refer to [Table 10-8](#).

Table 10-8 Output Descriptions for Querying Information About the Specified Account Resource

Field	Type	Description
@odata.context	String	OData description of the specified account resource model.
@odata.id	String	Access path of the specified account resource node.
@odata.type	String	Type of the specified account resource.
Id	String	ID of the specified account resource.
Name	String	Name of the account resource.
Enabled	Boolean	Whether the account is enabled resource.
Links	Object	Links to the account resource.
Roles	Object	Links to the roles corresponding to the account resource.
Locked	Boolean	Locked state of the account resource.
RoleId	String	Role resource ID in the account configuration.
UserName	String	Username of the account resource.
@odata.id	String	Access path of the role corresponding to the account resource.

10.5 Creating an Account

Function

Create an account.

Permission Required

User management.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/AccountService/Accounts`
- Request Header:

```
X-Auth-Token: auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
```



```

    "UserName": name,
    "Password": password,
    "RoleId": role,
    "Id" : id
  }

```

Parameters

For the parameter descriptions for creating an account, refer to [Table 10-9](#).

Table 10-9 Parameter Descriptions for Creating an Account

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
header_type	Format of the request message.	application/json
auth_value	When the post request is executed, the "X-Auth-Token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through / <i>redfish/v1/SessionService/Sessions</i> .
name	Username of the new account.	A string of 4–16 characters.
password	Password of the new account.	A string of 8–16 characters.
role	Role of the new account.	Available role types include: ● Administrator ● Operator ● User ● OEM1 ● OEM2 ● OEM3 ● OEM4
id	Account ID.	String, range: 2–16 characters.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/AccountService/Accounts
```

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json

● Request Message Body:

```
{
  "Id": "7",
  "UserName": "test77",
  "Password": "Superuser9!",
  "RoleId": "Administrator"
}
```

● Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#ManagerAccount.ManagerAccount",
  "@odata.id": "/redfish/v1/AccountService/Accounts/7",
  "@odata.type": "#ManagerAccount.v1_1_1.ManagerAccount",
  "Name": "User Account",
  "Enabled": true,
  "Id": "7",
  "Links": {
    "Roles": {
      "@odata.id": "/redfish/v1/AccountService/Roles/Administrator"
    }
  },
  "Locked": false,
  "RoleId": "Administrator",
  "UserName": "test77"
}
```

● Response code: 201

Output Description

a description of the output returned when you create an account, refer to [Table 10-10](#).

Table 10-10 Output Descriptions for Creating an Account

Field	Type	Description
@odata.context	String	OData description of the specified account resource model.
@odata.id	String	Access path of the specified account resource node.
@odata.type	String	Type of the specified account resource.
Id	String	ID of the specified user resource.
Name	String	Name of the account resource.

Field	Type	Description
Enabled	Boolean	Whether the account is enabled.
Links	Object	Links to the account resource.
Roles	Object	Links to the roles corresponding to the account.
Locked	Boolean	Locked state of the account.
RoleId	String	Role name, including: • Administrator • Operator • User • OEM1 • OEM2 • OEM3 • OEM4
UserName	String	Username
@odata.id	String	Access path of the role resource corresponding to the user.

10.6 Deleting an Account

Function

Delete a specified account.

Permission Required

User management.

Syntax

- Operation Type: DELETE
- URL: *https://device_ip/redfish/v1/AccountService/Accounts/account_id*
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for deleting a specified account, refer to [Table 10-11](#).

Table 10-11 Parameter Descriptions for Deleting a Specified Account

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
account_id	Subscriber ID.	It can be obtained by querying the account list.
auth_value	When the DELETE request is executed, the "X-Auth-Token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
DELETE https://device_ip/redfish/v1/AccountService/Accounts/1
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example: None
- Response Code: 204

Output Description

None

10.7 Modifying Information About a Specified Account

Function

Modify the username, password, permission, lockout status, enabling status, and login interface of a specified account.

Permission Required

User management.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/AccountService/Accounts/account_id*
- Request Header:

X-Auth-Token: auth_value
Content-Type: header_type

● Request Message Body:

```
{
  "UserName": name,
  "Password": password,
  "RoleId": role,
  "Enabled": flag,
  "Oem": {
    "Public": {
      "snmpAuthentication": authprotocol,
      "snmpPrivacy": privprotocol
    }
  }
}
```

Parameters

For the parameter descriptions for modifying information about the specified account, refer to [Table 10-12](#).

Table 10-12 Parameter Descriptions for Modifying Information About the Specified account

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	Authentication parameters of the request message.	It can be obtained by creating a session through / <i>redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
name	Username of the account whose information is to be modified.	A string of 4–16 characters.
password	Password of the account whose information is to be modified.	The maximum length of the string is 20 characters.
role	Role of the account whose information is to be modified.	Available role types include: ● Administrator ● Operator ● User ● OEM1 ● OEM2

Parameter	Description	Value
		• OEM3 • OEM4
flag	Whether the account is enabled.	Range: • true • false
authprotocol	SNMPv3 authentication algorithm.	String, range: • SHA • MD5 • SHA256 • SHA384 • SHA512
privprotocol	SNMPv3 encryption algorithm.	String, range: • DES • AES • AES256

Usage Guidelines

For a specified account, one or more properties in the requested message body can be modified at the same time.



Note

The Oem parameter is optional. If no Oem is added, this parameter is not modified.

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/AccountService/Accounts/1
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234e
Content-Type: application/json
```

- Request Message Body:

```
{
  "UserName": "username",
  "Password": "superuser9!",
  "RoleId": "Administrator",
  "Oem": {
    "Public": {
      "snmpAuthentication": "SHA",
```

```
        "snmpPrivacy": "DES"
      }
    }
  }
```

- Response Example: None
- Response Code: 204

Output Description

None

10.8 Querying Information About the Role Resource Collection

Function

Query information about the role resource collection of a server.

Permission Required

User management.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/AccountService/Roles*
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For the parameter description for querying information about the role resource collection, refer to [Table 10-13](#).

Table 10-13 Parameter Descriptions for Querying Information About the Role Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/Roles
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#RoleCollection.RoleCollection",
  "@odata.id": "/redfish/v1/AccountService/Roles",
  "@odata.type": "#RoleCollection.RoleCollection",
  "Name": "Roles Collection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/Administrator"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/Operator"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/User"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/OEM1"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/OEM2"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/OEM3"
    },
    {
      "@odata.id": "/redfish/v1/AccountService/Roles/OEM4"
    }
  ],
  "Members@odata.count": 7
}
```

- Status Code: 200

Output Description

a description of the output returned when you query information about the role resource collection, refer to [Table 10-14](#).

Table 10-14 Output Description for Querying Information About the Role Resource Collection

Field	Type	Description
@odata.context	String	OData description of the role resource model.
@odata.id	String	Access path of the role resource node.
@odata.type	String	Type of role resource.
Name	String	Name of the role resource.
Members@odata.count	Number	Number of role members.
Members	Array	Session List.
@odata.id	String	Access path of a single role resource node.

10.9 Querying Information About a Specified Role Resource

Function

Query information about a specified role resource of a server.

Permission Required

User management.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/AccountService/Roles/role_id*
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified role resource, refer to [Table 10-15](#).

Table 10-15 Parameter Descriptions for Querying Information About the Specified Role Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
role_id	Role ID.	It can be obtained from the role resource collection.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/Roles/Administrator
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Role.Role",
  "@odata.id": "/redfish/v1/AccountService/Roles/Administrator",
  "@odata.type": "#Role.v1_2_1.Role",
  "IsPredefined": true,
  "Name": "User Role",
  "Id": "Administrator",
  "AssignedPrivileges": [
    "ConfigureUsers",
    "ConfigureComponents",
    "ConfigureManager",
    "ConfigureSelf",
    "Login"
  ],
  "OemPrivileges": [
    "OEMSecureConfig",
    "OEMRemoteControl",
    "OEMTelecommunicationsMedium",
    "OEMPowerControl",
  ]
}
```

```
    "OEMDebugDiagnostics"  
  ]  
}
```

- Status Code: 200

Output Description

a description of the output returned when you query information about the specified role resource, refer to [Table 10-16](#).

Table 10-16 Output Descriptions for Querying Information About the Specified Role Resource

Field	Type	Description
@odata.context	String	OData description of the specified role resource model.
@odata.id	String	Access path of the specified role resource node.
@odata.type	String	Type of the specified role resource.
Id	String	ID of the specified role resource.
Name	String	Name of the specified role resource.
IsPredefined	Boolean	Whether the specified role is pre-defined.
AssignedPrivileges	Array	Privileges assigned to the specified role.
OemPrivileges	Array	Customized privileges assigned to the specified role.

10.10 Querying Information About the LDAP Service Resource

Function

Query the [LDAP](#) about the LDAP service resource.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/AccountService/LdapService`
- Request Header:

```
x-auth-token:auth_value
```

- Request Message Body: None

Parameters

For a description of the parameters for querying the LDAP about the LDAP service resource, refer to [Table 10-17](#).

Table 10-17 Parameter Descriptions for Querying Information About the LDAP Service Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/LdapService
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#AccountService.LdapService",
  "@odata.id": "/redfish/v1/AccountService/LdapService",
  "@odata.type": "#LdapCollection.LdapServiceCollection",
  "Id": "Ldap Service",
  "LdapControllers": [
    {
      "@odata.id": "/redfish/v1/AccountService/LdapService/LdapControllers"
    }
  ],
  "Name": "Ldap Service"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the LDAP about the LDAP service resource, refer to [Table 10-18](#).

Table 10-18 Output Descriptions for Querying Information About the LDAP Service Resource

Field	Type	Description
@odata.context	String	OData description of the LDAP service resource model.
@odata.id	String	Access path of the LDAP service resource node.
@odata.type	String	Type of LDAP service resource.
Id	String	ID of the LDAP service resource.
Name	String	Name of the LDAP service resource.
LdapControllers	Array	Controller list.
@odata.id	String	LDAP controller information.

10.11 Querying Information About the Collection of LDAP Domain Controller Resources

Function

Query information about the collection of LDAP domain controller resources.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/AccountService/LdapService/Ldap-Controllers`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the collection of LDAP domain controller resources, refer to [Table 10-19](#).

Table 10-19 Parameter Descriptions for Querying Information About the Collection of LDAP Domain Controller Resources

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#AccountService.LdapService.LdapControllers",
  "@odata.id":
    "/redfish/v1/AccountService/LdapService/LdapControllers",
  "@odata.type":
    "#AccountService.LdapService.LdapControllers.Activedirectory",
  "Members": [
    {
      "@odata.id":
        "/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory"
    },
    {
      "@odata.id":
        "/redfish/v1/AccountService/LdapService/LdapControllers/LDAP"
    }
  ],
  "Members@odata.count": 2,
  "Name": "Ldap Controller collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the collection of LDAP domain controller resources, refer to [Table 10-20](#).

Table 10-20 Output Descriptions for Querying Information About the Collection of LDAP Controller Resources

Field	Type	Description
@odata.context	String	OData description of the LDAP domain controller collection model.
@odata.id	String	Access path of the LDAP domain controller collection node.
@odata.type	String	Type of LDAP domain controller collection.
Name	String	Name of the LDAP domain controller collection.
Members	Array	LDAP controller member list.
@odata.id	String	ID of an LDAP controller member.
Members@odata.count	Number	Number of LDAP controller members.

10.12 Querying the Active Directory Information

Function

Query the Active Directory information.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the Active Directory information, refer to [Table 10-21](#).

Table 10-21 Parameter Descriptions for Querying the Active Directory Information

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#AccountService.LdapService.LdapControllers.Activedirectory",
  "@odata.id":
    "/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory",
  "@odata.type": "#LdapCollection.LdapControllers.Activedirectory",
  "ADAuthenticationEnable": true,
  "ADRoleGroups": [
    {
      "GroupDomain": "",
      "GroupLoginInterface": [],
      "GroupName": "",
      "GroupRole": null,
      "MemberId": 0
    },
    {
      "GroupDomain": "",
      "GroupLoginInterface": [],
      "GroupName": "",
      "GroupRole": null,
      "MemberId": 1
    }
  ],
}
```



```

    {
      "GroupDomain": "",
      "GroupLoginInterface": [],
      "GroupName": "",
      "GroupRole": null,
      "MemberId": 2
    },
    {
      "GroupDomain": "",
      "GroupLoginInterface": [],
      "GroupName": "",
      "GroupRole": null,
      "MemberId": 3
    },
    {
      "GroupDomain": "",
      "GroupLoginInterface": [],
      "GroupName": "",
      "GroupRole": null,
      "MemberId": 4
    }
  ],
  "ADSSLEnable": false,
  "DomainControllerServerAddress1": "192.168.5.3",
  "DomainControllerServerAddress2": null,
  "DomainControllerServerAddress3": null,
  "Name": "Activedirectory",
  "Password": null,
  "UserDomain": null,
  "UserName": null
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the Active Directory information, refer to [Table 10-22](#).

Table 10-22 Output Descriptions for Querying the Active Directory Information

Field	Type	Description
@odata.context	String	OData description of the Active Directory information resource model.
@odata.id	String	Access path of Active Directory information resource node.

Field	Type	Description
@odata.type	String	Type of Active Directory information resource.
Id	String	ID of the Active Directory information resource.
Name	String	Name of the Active Directory information resource.
Password	String	Displayed as null.
ADAuthenticationEnable	Boolean	Whether Active Directory authentication is enabled.
ADSSLEnable	Boolean	Whether SSL encryption is enabled.
DomainControllerServerAddress1	String	Domain controller server address 1.
DomainControllerServerAddress2	String	Domain controller server address 2.
DomainControllerServerAddress3	String	Domain controller server address 3.
UserDomain	String	User domain.
ADRoleGroups	Array	AD role group.
GroupName	String	Group name.
GroupDomain	String	Group domain.
GroupLoginInterface	Array	Access permission: ● KVM ● VMedia
GroupRole	String	Role group permission: ● Administrator ● Operator ● ReadOnly
MemberId	Number	Role group ID: 0-4
UserName	String	Username

10.13 Modifying the Active Directory Information

Function

Modify the Active Directory information.

Permission Required

User management.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/AccountService/LdapService/Ldap-Controllers/Activedirectory*

- Request Header:

```
x-auth-token:auth_value
Content-Type: header_type
```

- Request Message Body:

```
{
  "ADAuthenticationEnable": ad_authentication_enable_value,
  "DomainControllerServerAddress1": DomainControllerServerAddress1_value ,
  "DomainControllerServerAddress2": DomainControllerServerAddress2_value ,
  "DomainControllerServerAddress3": DomainControllerServerAddress3_value ,
  "Password": password_value,
  "UserDomain": user_domain_value,
  "UserName": user_name_value,
  "ADSSLEnable": adssl_enable_value,
  "ADRoleGroups": [
    {
      "GroupDomain": group_domain_value,
      "GroupName": group_name_value,
      "GroupRole": group_role_value,
      "MemberId": member_id_value
    }
  ]
}
```

Parameters

For a description of the parameters for modifying the Active Directory information, refer to [Table 10-23](#).

Table 10-23 Parameter Descriptions for Modifying the Active Directory Information

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json

Parameter	Description	Value
ad_authenticationEnable_value	Boolean	Whether Active Directory authentication is enabled. ● true: enabled. ● false: disabled.
omainControllerServerAddress1_value	String	Domain controller server address 1.
DomainControllerServerAddress2_value	String	Domain controller server address 2.
DomainControllerServerAddress3_value	String	Domain controller server address 3.
adssl_enable_value	Boolean	SSL encryption enabled: ● true ● false
password_value	String	Password
user_domain_value	String	User domain.
user_name_value	String	Username The following requirements must be met: ● Range: 1–64 characters. ● Consists of letters, digits, spaces, and hyphens (-). ● Must begin with a letter. ● Case-sensitive.
group_domain_value	String	Group domain. The following requirements must be met: ● Range: 2–255 characters. ● Consists of letters, digits, spaces, hyphens (-), and periods (.).
group_name_value	String	Group name. If this parameter is set to null, the role group is deleted. The following requirements must be met: ● Range: 1–64 characters. ● Consists of case-sensitive letters, digits, spaces, hyphens (-), and underscores (_). ● Must not consist of only spaces.

Parameter	Description	Value
		● If this parameter is set to null, the role group is deleted.
group_role_value	String	Role group permission: ● Administrator ● Operator ● ReadOnly
member_id_value	Number	Role group ID: 0-4

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body:

```
{
  "ADAuthenticationEnable": true,
  "DomainControllerServerAddress1": "2.4.3.5",
  "Password": "superuser7!",
  "UserDomain": "MyDddidntest.com",
  "UserName": "teseddst", "ADRoleGroups": [
    {
      "GroupDomain": "example.com",
      "GroupName": "bsp",
      "GroupRole": "ReadOnly",
      "MemberId": 1
    },
    {
      "GroupDomain": "exampdle.com",
      "GroupName": "testd",
      "GroupRole": "Administrator",
      "MemberId": 3
    }
  ]
}
```

- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#AccountService.LdapService.LdapControllers.Activedirectory",
  "@odata.id":
    "/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory",
  "@odata.type": "#LdapCollection.LdapControllers.Activedirectory",
  "ADAuthenticationEnable": true,
  "ADRoleGroups": [
    {
      "GroupDomain": "",
      "GroupLoginInterface": [],
      "GroupName": "",
      "GroupRole": null,
      "MemberId": 0
    },
    {
      "GroupDomain": "",
      "GroupLoginInterface": [],
      "GroupName": "",
      "GroupRole": null,
      "MemberId": 1
    },
    {
      "GroupDomain": "",
      "GroupLoginInterface": [],
      "GroupName": "",
      "GroupRole": null,
      "MemberId": 2
    },
    {
      "GroupDomain": "",
      "GroupLoginInterface": [],
      "GroupName": "",
      "GroupRole": null,
      "MemberId": 3
    },
    {
      "GroupDomain": "",
      "GroupLoginInterface": [],
      "GroupName": "",
      "GroupRole": null,
      "MemberId": 4
    }
  ]
}
```

```

    }
  ],
  "ADSSLEnable": false,
  "DomainControllerServerAddress1": "192.168.5.3",
  "DomainControllerServerAddress2": null,
  "DomainControllerServerAddress3": null,
  "Name": "Activedirectory",
  "Password": null,
  "UserDomain": null,
  "UserName": null
}

```

- Status Code: 200

Output Description

For a description of the output returned when you modify the Active Directory information, refer to [Table 10-24](#).

Table 10-24 Output Descriptions for Modifying the Active Directory Information

Field	Type	Description
@odata.context	String	OData description of the Active Directory information resource model.
@odata.id	String	Access path of Active Directory information resource node.
@odata.type	String	Type of Active Directory information resource.
Id	String	ID of the Active Directory information resource.
Name	String	Name of the Active Directory information resource.
Password	String	Displayed as null.
ADAuthenticationEnable	Boolean	Whether Active Directory authentication is enabled.
DomainControllerServerAddress1	String	Domain controller server address 1.
DomainControllerServerAddress2	String	Domain controller server address 2.
DomainControllerServerAddress3	String	Domain controller server address 3.
UserDomain	String	User domain.
ADRoleGroups	Array	AD role group.
GroupName	String	Group name.

Field	Type	Description
GroupDomain	String	Group domain.
GroupLoginInterface	Array	Access permission: • KVM • VMedia
GroupRole	String	Role group permission: • Administrator • Operator • ReadOnly
MemberId	Number	Role group ID: 0-4
UserName	String	Username

10.14 Querying LDAP Information

Function

Query LDAP information.

Permission Required

Query.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/AccountService/LdapService/Ldap-Controllers/LDAP`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Description

For a description of the parameters for querying LDAP information, refer to [Table 10-25](#).

Table 10-25 Parameter Descriptions for Querying LDAP Information

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Parameter	Setting	Value
	the GET request for authentication.	

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers/LDAP
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#AccountService.LdapService.LdapControllers.LDAP",
  "@odata.id": "/redfish/v1/AccountService/LdapService/LdapControllers/LDAP",
  "@odata.type": "#LdapCollection.LdapControllers.LDAP",
  "LDAPRoleGroups": [
    {
      "GroupDomain": "cn=manager",
      "GroupLoginInterface": [
        "KVM",
        "VMedia"
      ],
      "GroupName": "testAdmin",
      "GroupRole": "Administrator",
      "MemberId": 0
    },
    {
      "GroupDomain": "ou=login",
      "GroupLoginInterface": [],
      "GroupName": "testUser",
      "GroupRole": "ReadOnly",
      "MemberId": 1
    }
  ],
  "BindDN": "cn=manager",
  "CommonNameType": "IP",
}
```

```

    "EncryptionType": "NoEncryption",
    "LDAPAuthenticationEnable": true,
    "Name": "LDAP",
    "Password": null,
    "Port": 389,
    "SearchBase": "dc=com",
    "ServerAddress": "192.168.1.5",
    "UserLoginAttribute": "cn"
  }

```

- Status Code: 200

Output Description

For a description of the output returned when you query LDAP information, refer to [Table 10-26](#).

Table 10-26 Output Descriptions for Querying LDAP Information

Field	Type	Description
@odata.context	String	OData description of the LDAP resource model.
@odata.id	String	Access path of the LDAP resource node.
@odata.type	String	Type of LDAP resource.
BindDN	String	Bound DN.
CommonNameType	String	Common name type. Options: • IP • FQDN
EncryptionType	String	Encryption type. Options: • NoEncryption • SSL • StartTLS
LDAPAuthenticationEnable	Boolean	Whether LDAP authentication is enabled.
LDAPRoleGroups	Array	LDAP role group.
GroupName	String	Group name.
GroupDomain	String	Group domain
GroupLoginInterface	Array	Access permission, options: • KVM • VMedia
GroupRole	String	Role group permission, options: • Administrator • Operator • ReadOnly

Field	Type	Description
MemberId	Number	Role group ID, range: 0–4.
Name	String	Name of the LDAP information resource.
Password	String	Password, which is displayed as null in the query result.
Port	Number	Port number.
SearchBase	String	Search base.
ServerAddress	String	Server address.
UserLoginAttribute	String	User login attribute, options: • uid • cn

10.15 Modifying the LDAP Information

Function

Modify the LDAP information.

Permission Required

User management.

Syntax

- Operation Type: PATCH
- URL: `https://device_ip/redfish/v1/AccountService/LdapService/Ldap-Controllers/LDAP`
- Request Header:

X-Auth-Token: auth_value
Content-Type: header_type

- Request Message Body:

```
{
  "LDAPRoleGroups": [
    {
      "GroupDomain": group_domain_value,
      "GroupName": group_name_value,
      "GroupRole": group_role_value,
      "MemberId": member_id_value
    }
  ],
}
```

```

    "BindDN": bind_dn_value,
    "EncryptionType": encryption_type_value,
    "LDAPAuthenticationEnable": ldap_authentication_enable_value,
    "Name": name_value,
    "Password": password_value,
    "Port": port_value,
    "SearchBase": search_base_value,
    "ServerAddress": server_address_value,
    "UserLoginAttribute": user_login_attribute_value
  }

```

Description

For a description of the parameters for modifying the LDAP information, refer to [Table 10-27](#).

Table 10-27 Parameter Descriptions for Modifying the LDAP Information

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
group_domain_value	String	Group domain name (which consists of 4–253 letters and digits, and starts with a letter. The following special characters are allowed: ".", ",", "_", "-", and "=~". Before "=", only the following characters are allowed: "cn", "uid", "ou", "dc", and "o". Two examples are as follows: "cn=login", and "dc=domain")
group_name_value	String	Group name. If this parameter is set to null, the role group is deleted.
group_role_value	String	Role group permission: ● Administrator ● Operator ● ReadOnly
member_id_value	Number	Role Group ID: 0–4.
bind_dn_value	Bound DN.	The following requirements must be met: ● Range: 4–64 characters.

Parameter	Setting	Value
		- Consists of letters and digits. - Supported special characters: ".", ",", "-", ".", and "=". - It must start with a letter and cannot end with ",", or "=". - The value before "=" must be "cn", "uid", "ou", "dc", or "o", and the first segment must start with "cn" or "uid". Examples: "cn=manager", "ou=login", "dc=domain", or "dc=com".
encryption_type_value	String	Encryption type, options: - NoEncryption - SSL - StartTLS You can set the encryption type to SSL or Start TLS. This interface is not used for uploading certificates.
ldap_authentication_enabled_value	Whether LDAP authentication is enabled.	- true - false
name_value	Name of the LDAP information resource.	Name of the LDAP information resource.
password_value	Password	The following requirements must be met: - Range: 1–47 characters. - There is no space in the middle.
port_value	Port number.	Number, range: 1–65535.
server_address_value	Server address.	IPv4 address, IP v6 address, or domain name format.
user_login_attribute_value	User login attribute.	Supports cn and uid , which must be the same as the LDAP user information of the bound DN.
search_base_value	Search base.	The following requirements must be met: - Range: 4–253 characters. - Consists of letters and digits. - Supported special characters: ".", ",", "-", ".", and "=". - It must start with a letter.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers/LDAP
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body:

```
{
  "BindDN": "cn=admin,dc=ldapdomain,dc=com",
  "EncryptionType": "NoEncryption",
  "LDAPAuthenticationEnable": true,
  "LDAPRoleGroups": [
    {
      "GroupDomain": "ou=testgroup,dc=ldapdomain,dc=com",
      "GroupName": "sdf",
      "GroupRole": "Operator",
      "MemberId": 0
    }
  ],
  "Password": "Superuser9!",
  "Port": 392,
  "SearchBase": "ou=login,dc=domain,dc=com",
  "ServerAddress": "192.168.1.5",
  "UserLoginAttribute": "uid"
}
```

- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#AccountService.LdapService.LdapControllers.LDAP",
  "@odata.id": "/redfish/v1/AccountService/LdapService/LdapControllers/LDAP",
  "@odata.type": "#LdapCollection.LdapControllers.LDAP",
  "LDAPRoleGroups": [
    {
      "GroupDomain": "cn=manager",
      "GroupLoginInterface": [
        "KVM",
        "VMedia"
      ],
      "GroupName": "sdf",
    }
  ]
}
```

```

        "GroupRole": "operator",
        "MemberId": 0
    }
],
"BindDN": "cn=manager",
"CommonNameType": "IP",
"EncryptionType": "NoEncryption",
"LDAPAuthenticationEnable": true,
"Name": "LDAP",
"Password": null,
"Port": 389,
"SearchBase": "dc=com",
"ServerAddress": "192.168.1.5",
"UserLoginAttribute": "cn"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you modify the LDAP information, refer to [Table 10-28](#).

Table 10-28 Output Descriptions for Modifying the LDAP Information

Field	Type	Description
@odata.context	String	OData description of the LDAP resource model.
@odata.id	String	Access path of the LDAP information resource node.
@odata.type	String	Type of LDAP resource.
BindDN	String	Bound DN..
CommonNameType	String	Common name type. Options: • IP • FQDN
EncryptionType	String	Encryption type. Options: • NoEncryption • SSL • StartTLS
LDAPAuthenticationEnable	Boolean	Whether LDAP authentication is enabled.
LDAPRoleGroups	Array	LDAP role group.
GroupName	String	Group name.
GroupDomain	String	Group domain
GroupLoginInterface	Array	Access permission, options:

Field	Type	Description
		• KVM • VMedia
GroupRole	String	Role group permission, options: • Administrator • Operator • ReadOnly
MemberId	Number	Role group ID, range: 0–4.
Name	String	Name of the LDAP information resource.
Password	String	Password, which is displayed as null in the query result.
Port	Number	Port number.
SearchBase	String	Search base.
ServerAddress	String	Server address.
UserLoginAttribute	String	User login attribute, options: • uid • cn

Chapter 11

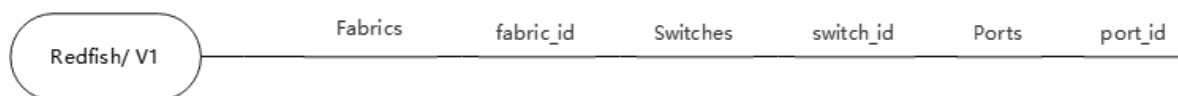
Operations on Fabric Resources

Table of Contents

Querying Information About the Fabrics Resource Collection	591
Querying Information About a Specified Fabrics Resource	593
Querying Information About the Switch Resource Collection	594
Querying Information About a Specified Switch Resource	596
Querying Information About the Port Resource Collection of a Specified Switch	598
Querying Information About a Specified Port of a Specified Switch	600

Figure 11-1 shows the path requirements for the Fabric resources supported by for VANTAGEO servers.

Figure 11-1 Fabric Resource Path Requirements



For a description of properties of Fabric resources and operations supported by the properties, refer to [Table 11-1](#)

Table 11-1 Descriptions of Fabric Resources Properties

URL	Attribute	Description	Command
/redfish/v1/Fabrics	Name	Name of the Fabric resource.	GET
	Members@odata.count	Number of Fabric resources.	GET
	Members	List of Fabric resources.	GET
/redfish/v1/Fabrics/fabric_id	Id	ID of the Fabric resource.	GET
	Name	Name of the Fabric resource.	GET
	FabricType	Type of Fabric resource.	GET
	Switchs	Collection of switch resources.	GET

URL	Attribute	Description	Command
/redfish/v1/Fabrics/fabric_id/Switches	Description	Description of the switch resource collection.	GET
	Name	Name of the switch resource collection.	GET
	Members@odata.count	Number of members in the switch resource collection.	GET
	Members	List of switch resources.	GET
/redfish/v1/Fabrics/fabric_id/Switches/switch_id	Id	ID of a switch resource.	GET
	Name	Name of the switch resource.	GET
	Ports	List of port resources of a specified switch.	GET
/redfish/v1/Fabrics/fabric_id/Switches/switch_id/Ports	Description	Description of the port resource collection of a specified switch.	GET
	Members@odata.count	Number of members in the port resource collection of the specified switch.	GET
	Members	List of port resources of the specified switch.	GET
	Name	Name of the port resource collection of the specified switch.	GET
/redfish/v1/Fabrics/fabric_id/Switches/switch_id/Ports/port_id	Id	Access path of the specified port resource of the specified switch.	GET
	PortProtocol	Protocol used by the port resource.	GET
	Name	Name of the port resource.	GET
	ActiveWidth	Number of active channels of the port.	GET
	LinkStatus	Link status of the port.	GET
	CurrentSpeedGbps	Current speed of the port.	GET
	SFP.PartNumber	Part number the SFP.	GET
	SFP.SerialNumber	Optical module sequence number	GET
	SFP.Manufacturer	Manufacturer of the SFP.	GET

URL	Attribute	Description	Command
	SFP.MediumType	Data transmission media type of SFP.	GET

11.1 Querying Information About the Fabrics Resource Collection

Function

Query the information about the Fabrics resource collection.

Permission Required

Query.

Syntax



Operation Type: GET



URL: `https://device_ip/redfish/v1/Fabrics`



Request Header:

x-auth-token:auth_value



Request Message Body: None

Parameters

For a description of the parameters for querying information about the Fabrics resource collection, refer to [Table 11-2](#).

Table 11-2 Parameter Descriptions for Querying Information About the Fabrics Resource Collection

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

Only servers with GPUs support this function.

Example



Request Example:

GET https://device_ip/redfish/v1/Fabrics



Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234



Request Message Body: None



Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#FabricCollection.FabricCollection",
  "@odata.id": "/redfish/v1/Fabrics",
  "@odata.type": "#FabricCollection.FabricCollection",
  "Description": "The Collection of Fabric",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Fabrics/PCIE"
    },
    {
      "@odata.id": "/redfish/v1/Fabrics/Serdes"
    }
  ],
  "Members@odata.count": 2,
  "Name": "FabricCollection"
}
```



Status Code: 200

Output Description

For a description of the output returned when you query information about the Fabrics resource collection, refer to [Table 11-3](#).

Table 11-3 Output Descriptions for Querying Information About the Fabrics Resource Collection

Field	Type	Description
@odata.context	String	OData description of the Fabrics resource collection.
@odata.id	String	Access path of the Fabric resource collection.
@odata.type	String	Type of Fabric resource collection.
Description	String	Description of the Fabric resource collection.
Name	String	Name of the Fabric resource collection.
Members@odata.count	Number	Number of Fabric resources.
Members	Array	List of Fabric resources.
@odata.id	String	Access path of a single Fabric resource node.

11.2 Querying Information About a Specified Fabrics Resource

Function

Query the information about a specified Fabrics resource.

Permission Required

Query.

Syntax



Operation Type: GET



URL: *https://device_ip/redfish/v1/Fabrics/fabric_id*



Request Header:

x-auth-token:auth_value



Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified Fabrics resource, refer to [Table 11-4](#).

Table 11-4 Parameter Descriptions for Querying Information About the Specified Fabrics Resource

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
fabric_id	ID of the Fabric resource.	PCIe or SerDes.

Usage Guidelines

Only servers with GPUs support this function.

Example



Request Example:

GET https://device_ip/redfish/v1/Fabrics/PCIe



Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234



Request Message Body: None



Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Fabric.Fabric",
  "@odata.id": "/redfish/v1/Fabrics/PCie",
  "@odata.type": "#Fabric.v1_2_2.Fabric",
  "FabricType": "PCie",
  "Name": "PCie Fabric",
  "Id": "PCie",
  "Switches": {
    "@odata.id": "/redfish/v1/Fabrics/PCie/Switches"
  }
}
```



Status Code: 200

Output Description

For a description of the output returned when you query information about the specified Fabrics resource, refer to [Table 11-5](#).

Table 11-5 Output Descriptions for Querying Information About the Specified Fabrics Resource

Field	Type	Description
@odata.context	String	OData description of the Fabrics resource.
@odata.id	String	Access path of the Fabric resource.
@odata.type	String	Type of Fabric resource.
Id	String	ID of the Fabric resource.
Name	String	Name of the Fabric resource.
FabricType	String	Type of Fabric resource.
Switchs	Object	Collection of switch resources.
@odata.id	String	Access path of the switch resource collection node.

11.3 Querying Information About the Switch Resource Collection

Function

Query the information about the switch resource collection.

Permission Required

Query.

Syntax



Operation Type: GET



URL:

`https://device_ip/redfish/v1/Fabrics/fabric_id/Switches`



Request Header:

`x-auth-token:auth_value`



Request Message Body: None

Parameters

For a description of the parameters for querying information about the switch resource collection, refer to [Table 11-6](#).

Table 11-6 Parameter Descriptions for Querying Information About the Switch Resource Collection

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
fabric_id	ID of the Fabric resource.	PCIe or SerDes.

Usage Guidelines

Only servers with GPUs support this function.

Example



Request Example:

`GET https://device_ip/redfish/v1/Fabrics/PCIe/Switches`



Request Header:

`X-Auth-Token: 8574621d21b84756218c7456821c234`



Request Message Body: None



Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#SwitchCollection.SwitchCollection",
  "@odata.id": "/redfish/v1/Fabrics/PCIe/Switches",
  "@odata.type": "#SwitchCollection.SwitchCollection",
  "Description": "The collection of switch",
  "Name": "Switch Collection",
```

```
"Members": [
  {
    "@odata.id": "/redfish/v1/Fabrics/PCIE/Switches/PCIERetimer0"
  }
],
"Members@odata.count": 1
}
```

 Status Code: 200

Output Description

For a description of the output returned when you query the information about the switch resource collection, refer to [Table 11-7](#).

Table 11-7 Output Descriptions for Querying Information About the Switch Resource Collection

Field	Type	Description
@odata.context	String	OData description of the switch resource collection.
@odata.id	String	Access path of the switch resource collection.
@odata.type	String	Type of switch resource collection.
Name	String	Name of the switch resource collection.
Members@odata.count	Number	Number of members in the switch resource collection.
Members	Array	List of switch resources.
@odata.id	String	Access path of a single switch resource node.

11.4 Querying Information About a Specified Switch Resource

Function

Query information about a specified switch resource.

Permission Required

Query.

Syntax

 Operation Type: GET

 URL:

`https://device_ip/redfish/v1/Fabrics/fabric_id/Switches/switch_id`

 Request Header:

x-auth-token:auth_value



Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified switch resource, refer to [Table 11-8](#).

Table 11-8 Parameter Descriptions for Querying Information About the Specified Switch Resource

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
fabric_id	ID of the Fabric resource.	PCIe or SerDes.
switch_id	Switch resource ID.	Obtained from the upper-level URL.

Usage Guidelines

Only servers with GPUs support this function.

Example



Request Example:

GET https://device_ip/redfish/v1/Fabrics/PCIe/Switches/PCIeRetimer0



Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234



Request Message Body: None



Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Switch.Switch",
  "@odata.id": "/redfish/v1/Fabrics/PCIe/Switches/PCIeRetimer0",
  "@odata.type": "#Switch.v1_6_0.Switch",
  "Id": "PCIeRetimer0",
  "Name": "PCIeRetimer0",
  "Ports": {
    "@odata.id": "/redfish/v1/Fabrics/PCIe/Switches/PCIeRetimer0/Ports"
  }
}
```



Status Code: 200

Output Description

For a description of the output returned when you query information about the specified switch resource, refer to [Table 11-9](#).

Table 11-9 Output Descriptions for Querying Information About the Specified Switch Resource

Field	Type	Description
@odata.context	String	OData description of the switch resource model.
@odata.id	String	Access path of the switch resource.
@odata.type	String	Type of switch resource.
Id	String	ID of the switch resource.
Name	String	Name of the switch resource.
Ports	Object	Port resources.
@odata.id	String	Access path of a specified port resource node.

11.5 Querying Information About the Port Resource Collection of a Specified Switch

Function

Query the information about the port resource collection of a specified switch.

Permission Required

Query.

Syntax



Operation Type: GET

 URL:

`https://device_ip/redfish/v1/Fabrics/fabric_id/Switches/switch_id/Ports`



Request Header:

x-auth-token:auth_value



Request Message Body: None

Parameters

For a description of the parameters for querying information about the port resource collection of the specified switch, refer to [Table 11-10](#).

Table 11-10 Querying Information About the Port Resource Collection of a Specified Switch

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
fabric_id	ID of the Fabric resource.	PCIe or SerDes.
switch_id	Switch resource ID.	Obtained from the upper-level URL.

Usage Guidelines

Only servers with GPUs support this function.

Example



Request Example:

```
GET https://device_ip/redfish/v1/Fabrics/PCIe/Switches/PCIeRetimer0/Ports
```



Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```



Request Message Body: None



Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#PortCollection.PortCollection",
  "@odata.id": "/redfish/v1/Fabrics/PCIe/Switches/PCIeRetimer0/Ports",
  "@odata.type": "#PortCollection.PortCollection",
  "Description": "The Collection of Port",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Fabrics/PCIe/Switches/PCIeRetimer0/Ports/0"
    }
  ],
  "Members@odata.count": 1,
  "Name": "Port Collection"
}
```



Status Code: 200

Output Description

For a description of the output returned when you query information about the port resource collection of the specified switch, refer to [Table 11-11](#).

Table 11-11 Output Descriptions for Querying Information About the Port Resource Collection of the Specified Switch

Field	Type	Description
@odata.context	String	OData description of the port resource collection model.
@odata.id	String	Access path of the port resource collection.
@odata.type	String	Type of port resource collection.
Description	String	Description of the port resource collection.
Members@odata.count	Number	Number of members in the port resources collection of the specified switch.
Members	Array	List of port resources of the specified switch.
@odata.id	String	Access path of a single port resource node of the specified switch.
Name	String	Name of the switching port resource collection.

11.6 Querying Information About a Specified Port of a Specified Switch

Function

Query information about a specified port of a specified switch.

Permission Required

Query.

Syntax

Table 11-12 Parameter Descriptions for Querying LDAP Service Resources

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
fabric_id	ID of the Fabric resource.	PCIe or SerDes.
switch_id	ID of the switch resource.	Obtained from the upper-level URL.
port_id	ID of the port resource.	The port number can be obtained by querying the specified port resource collection.

Usage Guidelines

Only servers with GPUs support this function.

Example

Request Example:

```
GET https://device_ip/redfish/v1/Fabrics/PCIe/Switches/PCIeRetimer0/Ports/0
```



Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
```



Request Message Body: None



Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Ports.Ports",
  "@odata.id": "/redfish/v1/Fabrics/PCIe/Switches/PCIeRetimer0/Ports/0",
  "@odata.type": "#Port.v1_5_0.Port",
  "PortProtocol": "PCIe",
  "Id": "0",
  "Name": "PCIeRetimer0 Port 0",
  "Activewidth": "0",
  "LinkStatus": "Starting",
  "CurrentSpeedGbps": 0,
  "SFP": {
    "PartNumber": null,
    "SerialNumber": null,
    "Manufacturer": null,
    "MediumType": null
  }
}
```

}

Status Code: 200

Output Description

For a description of the output returned when you query the specified port of the specified switch, refer to [Table 11-13](#).

Table 11-13 Output Descriptions for Querying the Specified Port of the Specified Switch

Field	Type	Description
@odata.context	String	OData description of the port resource model.
@odata.id	String	Access path of the port resource.
@odata.type	String	Type of port resource.
PortProtocol	String	Protocol used by the port resource.
Id	String	ID of the port resource.
Name	String	Name of the port resource.
ActiveWidth	String	Number of active channels of the port.
LinkStatus	String	Link status of the port.
CurrentSpeedGbps	Number	Current speed of the port.
SFP.PartNumber	String	Part number the SFP.
SFP.SerialNumber	String	Sequence number of the SFP.
SFP.Manufacturer	String	Manufacturer of the SFP.
SFP.MediumType	String	Data transmission media type of SFP.

Chapter 12

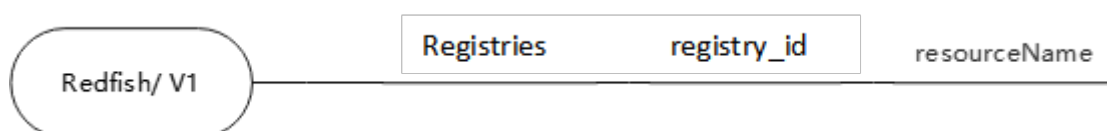
Operations on Registry Resources

Table of Contents

Querying Information About the Registry Resource Collection.....	605
Querying Information About a Specified Registry Resource.....	606
Querying Information About a Specified Registry Resource File	609

Figure 12-1 shows the Redfish registry resource path requirements applicable to VANTAGEO servers.

Figure 12-1 Redfish Registry Resource Path Requirements



For a description of the properties of registry resources and the operations supported by the properties, refer to [Table 12-1](#).

Table 12-1 Descriptions for Properties of Registry Resources

URL	Property	Description	Command
/redfish/v1/Registries	Name	Name of the registry resource collection.	GET
	Description	Description of the registry resource collection.	GET
	Members@odata.count	Number of members in the registry resource collection.	GET
	Members	List of registry resources.	GET
/redfish/v1/Registries/registry_id	Description	Description of the specified registry resource.	GET
	Id	ID of the specified registry resource.	GET
	Name	Name of the specified registry resource.	GET

URL	Property	Description	Command
	Languages	RFC5646-compliant languages for the specified registry resource.	GET
	Languages@odata.count	Number of languages for the specified registry resource.	GET
	Location	Location of the specified registry resource file.	GET
	Language	RFC5646-compliant language for the specified registry resource file.	GET
	Uri	URI of the specified registry resource file.	GET
	Location@odata.count	Number of locations for the specified registry resource file.	GET
	Registry	Registry name and version.	GET
/redfish/v1/Registries/registries_id/resourceName	RegistryVersion	Registry version.	GET
	OwningEntity	Entity that the specified registry belongs to.	GET
	Name	Name of the specified registry file.	GET
	RegistryEntries	List of all attributes and their metadata for the specified register file.	GET
	Attributes	Attributes of the specified registry file.	GET
	Language	RFC5646-compliant language for the specified registry resource file.	GET
	Id	ID of the specified registry file.	GET
	Description	Description of the specified registry file.	GET

12.1 Querying Information About the Registry Resource Collection

Function

Query the information about the registry resource collection.

Permission Required

Query.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Registries`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the registry resource collection, refer to [Table 12-2](#).

Table 12-2 Parameter Descriptions for Querying Information About the Registry Resource Collection

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Registries

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None



Response Example:

```
{
  "@odata.id": "/redfish/v1/Registries",
  "@odata.type": "#MessageRegistryFileCollection.MessageRegistryFileCollection",
  "Name": "Registry File Collection",
  "Description": "Registry Repository",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Registries/BiosAttributeRegistryResource"
    }
  ],
  "Members@odata.count": 1
}
```



Status Code: 200

Output Description

For a description of the output returned when you query information about the registry resource collection, refer to [Table 12-3](#).

Table 12-3 Output Descriptions for Querying Information About the Registry Resource Collection

Field	Type	Description
@odata.id	String	Access path of the registry resource collection model.
@odata.type	String	Type of registry resource collection.
Name	String	Name of the registry resource collection.
Description	String	Description of the registry resource collection.
Members@odata.count	Number	Number of members in the registry resource collection.
Members	Array	List of registry resources.
@odata.id	String	Access path of a specified registry resource.

12.2 Querying Information About a Specified Registry Resource

Function

Query information about a specified registry resource.

Permission Required

Query.

Syntax



Operation Type: GET



URL: *https://device_ip/redfish/v1/Registries/registries_id*



Request Header:

x-auth-token:auth_value



Request Message Body: None

Parameters

For a description of the parameters for querying the information about of the specified registry resource, refer to [Table 12-4](#).

Table 12-4 Parameter Descriptions for Querying Information About a Specified Registry Resource

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
registries_id	ID of the specified registry resource.	BiosAttributeRegistryResource

Usage Guidelines

None

Example



Request Example:

GET *https://device_ip/redfish/v1/Registries/BiosAttributeRegistryResource*



Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234



Request Message Body: None



Response Example:

{
 "@odata.id": "/redfish/v1/Registries/BiosAttributeRegistryResource",
 "@odata.type": "#MessageRegistryFile.v1_1_0.MessageRegistryFile",
 "Description": "BiosAttributeRegistryResource Message Registry File Location",
 "Id": "BiosAttributeRegistryResource",
 "Name": "BiosAttributeRegistryResource",
}

```

    "Languages": [
      "en"
    ],
    "Languages@odata.count": 1,
    "Location": [
      {
        "Language": "en",
        "Uri": "/redfish/v1/Registries/BiosAttributeRegistryResource/
        BiosAttributeRegistry"
      }
    ],
    "Location@odata.count": 1,
    "Registry": "BiosAttributeRegistryResource.0.71.0"
  }

```



Status Code: 200

Output Description

For a description of the output returned when you query the information about the specified registry resource, refer to [Table 12-5](#).

Table 12-5 Output Descriptions for Querying Information About the Specified Registry Resource

Field	Type	Description
@odata.id	String	Access path of a specified registry resource.
@odata.type	String	Type of the specified registry resource.
Description	String	Description of the specified registry resource.
Id	String	ID of the specified registry resource.
Name	String	Name of the specified registry resource.
Languages	Array	RFC5646-compliant languages for the specified registry resource.
Languages@odata.count	Number	Number of languages for the specified registry resource.
Location	Array	Location of the specified registry resource file.
Language	String	RFC5646-compliant language for the specified registry resource file.
Uri	String	URI of the specified registry resource file.
Location@odata.count	Number	Number of locations for the specified registry resource file.

Field	Type	Description
Registry	String	Registry name and version.

12.3 Querying Information About a Specified Registry Resource File

Function

Query the information about a specified registry resource file.

Permission Required

Query.

Syntax

 Operation Type: GET

 **URL:** `https://device_ip/redfish/v1/Registries/registries_id/resource-Name`

 Request Header:

`x-auth-token:auth_value`

 Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified registry resource file, refer to [Table 12-6](#).

Table 12-6 Parameter Descriptions for Querying Information About the Specified Registry Resource File

Parameter	Setting	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
registries_id	ID of the specified registry resource.	BiosAttributeRegistryResource
resourceName	Name of the resource file to be queried.	Obtained by querying the resource file name based on the upper-level registry ID.

Usage Guidelines

None

Example



Request Example:

GET https://device_ip/redfish/v1/Registries/BiosAttributeRegistryResource/BiosAttributeRegistry



Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234



Request Message Body: None



Response Example:

```
{
  "RegistryVersion": "0.71.0",
  "OwningEntity": "VANTGAE0",
  "Name": "BIOS Attribute Registry",
  "RegistryEntries": {
    "Attributes": [
      {
        ....
      },
      {
        ....
      }
    ]
  },
  "@odata.type": "#AttributeRegistry.v1_3_1.AttributeRegistry",
  "Language": "en",
  "Id": "BiosAttributeRegistry",
  "Description": "This registry defines a representation of BIOS Attribute instances"
}
```



Status Code: 200

Output Description

For a description of the output returned when you query information about the specified registry resource file, refer to [Table 12-7](#).

Table 12-7 Output Descriptions for Querying Information About the Specified Registry Resource File

Field	Type	Description
RegistryVersion	String	Registry version.
OwningEntity	String	Entity that the specified registry belongs to.
Name	String	Name of the specified registry resource.

Field	Type	Description
RegistryEntries	Object	List of all attributes and their metadata for the specified register file.
Attributes	Array	Attributes of the specified registry file.
@odata.type	String	Type of the specified registry file.
Language	String	RFC5646-compliant language for the specified registry resource file.
Id	String	ID of the specified registry file.
Description	String	Description of the specified registry file.

Chapter 13

Redfish Installation and Use

Table of Contents

Environment Installation	612
Use Case.....	612

13.1 Environment Installation

Redfish supports environment installation in the following two ways:

- (Recommended) Use the Postman tool to manage the Redfish interface. The download link is <https://www.postman.com/>.
- Use the *httprequester-2.2-fx.xpi* plug-in for Firefox earlier than 56.0b3 (64 bits).

13.2 Use Case

Abstract

This procedure uses querying the current service root resources as an example to describe how to use the Postman tool. For other resource operation methods, refer to this procedure.



Note

For details on how to query the current root service resources, refer to [3.2 Querying the Current Root Service Resources](#).

Steps

1. Open the Postman tool, create a request on the main page, and select a request action, see [Figure 13-1](#).

Figure 13-1 Selecting a Request Action

GET https://192.168.5.7/redfish/v1. GET https://192.168.5.7/redfish/v1. GET Untitled Request

Untitled Request

GET Enter request URL

Headers Body Pre-request Script Tests

VALUE	DESCRIPTION
Value	Description

Send

Hit the Send button to get a response.

2. On the **Params** tab, set the **URL** of the Redfish interface, see [Figure 13-2](#).

Figure 13-2 Setting the URL

https://192.168.5.7/redfish/v1/

GET

https://192.168.5.7/redfish/v1/

Send

Params

Authorization

Headers

Body

Pre-request Script

Tests

Cookies

Code

KEY	VALUE	DESCRIPTION
Key	Value	Description

Response

Hit the Send button to get a response.

3. Select **Authorization > TYPE**. Select **Basic Auth**, see [Figure 13-3](#).

Figure 13-3 Selecting an Authentication Type

The screenshot shows a REST client interface with the URL `https://192.168.5.7/redfish/v1/`. The **Authorization** tab is selected. A dropdown menu for **TYPE** is open, showing options: **Inherit auth from parent**, **No Auth**, **Bearer Token**, **Basic Auth**, **Digest Auth**, **OAuth 1.0**, **OAuth 2.0**, **Hawk Authentication**, **AWS Signature**, and **NTLM Authentication [Beta]**. The **Send** button is visible in the top right.

4. On the **Authorization** tab, enter the BMC username and password, see [Figure 13-4](#).

Figure 13-4 Entering the BMC Username and Password

The screenshot shows the REST client interface with the **Authorization** tab selected. The **TYPE** dropdown is set to **Basic Auth**. A message states: "The authorization header will be automatically generated when you send the request. [Learn more about authorization](#)". Below this is a **Preview Request** button. To the right, there are input fields for **Username** (containing "admin") and **Password** (masked with "*****"). A checkbox for **Show Password** is present. A warning message at the top of the right pane says: "Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)".

5. Click **Send** to send a request through the Redfish interface, see [Figure 13-5](#).

Figure 13-5 Sending a Request

https://192.168.5.7/redfish/v1/

GEThttps://192.168.5.7/redfish/v1/

Send

ParamsAuthorizationHeaders (1)BodyPre-request ScriptTestsCookiesCode

TYPEBasic Auth

The authorization header will be automatically generated when you send the request. [Learn more about authorization](#)

Preview Request

Usernameadmin

Password*****

Show Password

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)

BodyCookiesHeaders (13)Test ResultsStatus: 200 OKTime: 331 msSize: 1.37 KB

PrettyRawPreviewJSON

```
1 {
2   "@odata.context": "/redfish/v1/$metadata#ServiceRoot.ServiceRoot",
3   "@odata.etag": "W/\"1558746422\"",
4   "@odata.id": "/redfish/v1/",
5   "@odata.type": "#ServiceRoot.v1_1_1.ServiceRoot",
6   "AccountService": {
7     "@odata.id": "/redfish/v1/AccountService"
8   },
9   "Chassis": {
10    "@odata.id": "/redfish/v1/Chassis"
11  },
12  "Description": "The service root for all Redfish requests on this host",
13  "EventService": {
14    "@odata.id": "/redfish/v1/EventService"
15  },
16  "Id": "RootService",
17  "Links": {
18    "Sessions": {
19      "@odata.id": "/redfish/v1/SessionService/Sessions"
20    }
21  }
22 }
```

Glossary

AD

- Active Directory

AHCI

- Advanced Host Controller Interface

API

- Application Program Interface

ARM

- Asynchronous Response Mode

BBU

- Battery Backup Unit

BDF

- Bus/Device/Function

BIOS

- Basic Input/Output System

BMC

- Baseboard Management Controller

BMC

- Baseboard Management Controller

CD

- Compact Disk

CIFS

- Common Internet File System

CPLD

- Complex Programmable Logic Device

CPU

- Central Processing Unit

CSRF

- Cross-Site Request Forgery

DDR

- Double Data Rate

DHCP

- Dynamic Host Configuration Protocol

DNS

- Domain Name System

ECC

- Error Check and Correction

EPLD

- Erasable Programmable Logic Device

FC

- Fiber Channel

FCoE

- Fibre Channel Over Ethernet

FPGA

- Field Programmable Gate Array

FQDN

- Fully Qualified Domain Name

FRU

- Field Replaceable Unit

FTP

- File Transfer Protocol

GPU

- Graphics Processing Unit

HDD

- Hard Disk Drive

HDM

- Handoff Direction Message

HTTP

- Hypertext Transfer Protocol

HTTPS

- Hypertext Transfer Protocol Secure

I/O

- Input/Output

IB

- InfiniBand

ID

- Identification

IO

- Input & Output

IP

- Internet Protocol

IPv4

- Internet Protocol Version 4

IPv6

- Internet Protocol Version 6

JSON

- Java Script Object Notation

KVM

- Keyboard, Video and Mouse

SMTP

- Simple Message Transfer Protocol

LDAP

- Lightweight Directory Access Protocol

LLDP

- Link Layer Discovery Protocol

MAC

- Media Access Control

MTU

- Maximum Transfer Unit

NAT

- Network Address Translation

NFS

- Network File System

NTP

- Network Time Protocol

NVMe

- Non-Volatile Memory Express

OEM

- Original Equipment Manufacturer

OPA

- Optical Pre-Amplifier

OS

- Operating System

PCB

- Printed Circuit Board

PCIe

- Peripheral Component Interconnect Express

PSU

- Power Supply Unit

PXE

- Preboot eXecution Environment

RAID

- Redundant Array of Independent Disks

RPM

- Rotations Per Minute

SAS

- Serial Attached SCSI

SATA

- Serial ATA

SEL

- System Event Log

SFTP

- Secure File Transfer Protocol

SMB

- Server Message Block

SMR

- Switching Mode Rectifier

SMTP

- Simple Message Transfer Protocol

SN

- Serial Number

SNMP

- Simple Network Management Protocol

SPI

- Serial Peripheral Interface

SSD

- Solid State Drive

SSDP

- Simple Service Discovery Protocol

SSH

- Secure Shell

SSL

- Secure Sockets Layer

TCP

- Transmission Control Protocol

TDP

- Thermal Design Power

TLS

- Transport Layer Security

UDP

- User Datagram Protocol

UHCI

- Universal Host Controller Interface

UID

- User Identifier

UID

- Unique Identifier

URI

- Uniform Resource Identifier

URL

- Uniform Resource Locator

USB

- Universal Serial Bus

UUID

- Universal Unique Identifier

VID

- VLAN Identifier

VLAN

- Virtual Local Area Network

VNC

- Virtual Network Computing

VR

- Voltage Regulator

XML

- Extensible Markup Language

iBMC

- intelligent Board Management Controller

iSCSI

- Internet Small Computer System Interface