VANTAGEO Server

Redfish Interface Description (for BMC Version 3)

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	2024-10-22	Updated "Chapter 4, Operations on Manager Resources" .
R1.2	2023-12-20	Updated "Chapter 4, Operations on Manager Resources" .
R1.1	2023-04-29	Updated "Chapter 4, Operations on Manager Resources" and "Chapter 5, Operations on System Resources".
R1.0	2022-06-01	First edition.

Serial Number: VT20230307

Publishing Date: 2024-10-22 (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 23

2.1 Querying the Redfish Version Information 24

2.2 Querying the Current Root Service Resources 25

4. Operations on Manager Resources 28

4.1 Querying Information About the Manager Resource Collection 52

4.2 Querying Information About a Specified Manager Resource 53

4.3 Modifying Information About a Specified Manager Resource 60

4.4 Querying Information About the Syslog Configuration 65

4.5 Configuring Information About the Syslog Server 68

4.6 Submitting a Syslog Test Log 73

4.7 Querying Information About the NtpService Configuration Resource 74

4.8 Modifying Properties of the NTP Resource 76

4.9 Querying Information About the BMC Service 80

4.10 Modifying Information About a Specified BMC Service 83

4.11 Querying the Virtual Media Resource Collection 87

4.12 Querying a Virtual Media Resource 89

4.13 Connecting to the Virtual Media 92

4.14 Disconnecting the Virtual Media 94

4.15 Querying Information About the LLDP Service Configuration Resource 96

4.16 Modifying Properties of the LLDP Service Resource 98

4.17 Querying Information About the SNMP Resource 100

4.18 Modifying Properties of the SNMP Resource 105

4.19 Submitting an SNMP Trap Test Event 110

4.20 Querying the Management Interface Collection of the BMC 111

4.21 Querying Information About a Specified Management Interface Resource of the BMC 113

4.22 Modifying a Specified Management Interface Resource of the BMC 120

4.23 Querying the KVM Service Resource 127

4.24 Modifying Information About the KVM Resource 129

4.25 Changing the BMC Firmware Version 132

4.26 Importing a Configuration File 134

4.27 Exporting Configurations 137

4.28 Validating Configurations 140
4.29 Restarting the BMC 142
4.30 Querying Information About the Log Service Resource Collection 144
4.31 Querying Information About a Specified Log Service Re- source 146
4.32 Querying Information About the SEL Log Service Resource Collection 148
4.33 Querying Information About the SEL Log Service Resource Collection by Specifying a Parameter 150
4.34 Querying Information About a Specified SEL Log Service Re- source 152
4.35 Querying the Import and Export Progress 155
4.36 Performing One-Click Collection 157
4.37 Exporting Logs 159
4.38 Querying Information About the NAT Resource 162
4.39 Setting Information About the NAT Resource 164
4.40 Performing One-Click Configuration Solidification 167
4.41 Performing One-Click Configuration Information Export 169
4.42 Performing One-Click Configuration Restoration 172
4.43 Querying Information About the SMTP Resource 175
4.44 Modifying Properties of the SMTP Resource 178
4.45 Sending an SMTP Test Email 182
4.46 Querying Information About the DNS Resource 183
4.47 Modifying Properties of the DNS Resource 187
4.48 Setting the BMC Time and Time Zone 190
4.49 Downloading a BMC File 193
4.50 Querying Information About the SDM Service Resource 195
4.51 Querying the Component Early-Warning Information About the SDM Service Resource 197
4.52 Clearing System Logs 199
4.53 Exporting a Screenshot 200
4.54 Triggering a Screenshot 202
4.55 Querying Information About the Firewall Service Resource 203
4.56 Adding a Firewall Rule 207
4.57 Deleting a Firewall Rule 209
4.58 Querying the One-Click Collection Progress 211
4.59 Querying Information About the HDM Service Resource Collection 213
4.60 Querying Information About HDM Resource Health Status 215
4.61 Querying Information About the SecurityService Resource 218
4.62 Querying Information About the SSL Certificate Resource 220

4.63 Importing an SSL Certificate ... 223
5. Operations on System Resources ... 228
5.1 Querying Information About the System Resource Collection ... 243
5.2 Querying Information About a Specified System Resource ... 245
5.3 Performing Remote Power-On, Remote Power-Off, and Remote Reset ... 254
5.4 Modifying Properties of a Specified System Resource ... 256
5.5 Setting the System Boot Mode ... 263
5.6 Querying Information About the CPU Resource Collection ... 266
5.7 Querying Information About a Specified CPU Resource ... 268
5.8 Querying Information About All CPU Resources ... 271
5.9 Querying Information About the Memory Resource Collection ... 274
5.10 Querying Information About a Specified Memory Resource ... 276
5.11 Querying Information About All Memory Resources ... 279
5.12 Querying Information About the Storage Resource Collection ... 282
5.13 Querying Information About a Specified Storage Resource ... 284
5.14 Querying Information About All Storage Resources ... 288
5.15 Querying Information About the Logical Volume Resource Collection ... 291
5.16 Querying Information About a Specified Logical Volume Resource ... 293
5.17 Creating a Logical Volume ... 297
5.18 Deleting a Logical Volume ... 302
5.19 Querying Properties of the BIOS Resource ... 304
5.20 Querying BIOS Settings ... 339
5.21 Modifying the BIOS Settings ... 344
5.22 Setting the BIOS Password ... 348
5.23 Restoring Manufacturer-Specified BIOS Configurations ... 350
5.24 Deleting All Logical Volumes ... 352
5.25 Setting Whether a Logical Disk Is a Boot Disk ... 353
6. Operations on Chassis Resources ... 359
6.1 Querying Information About the Chassis Resource Collection ... 381
6.2 Querying Information About the Specified Chassis Resource ... 382
6.3 Modifying the Position Indicator Status of a Chassis ... 387
6.4 Querying Information About the Network Adapter Resource Collection ... 389
6.5 Querying Information About a Specified Network Adapter Resource ... 391
6.6 Querying Information About All Network Adapter Resources ... 401
6.7 Querying Information About the Network Port Resource Collection ... 408
6.8 Querying Information About a Specified Network Port Resource ... 410
6.9 Modifying the LLDP Switch of a Network Port ... 414

6.10 Querying Information About the PCIe Device Resource Collection 418
6.11 Querying Information About a Specified PCIe Device Resource 420
6.12 Querying Information About a Specified PCIe Function Resource 425
6.13 Querying Information About All PCIe Device Resources 428
6.14 Querying Information About the Drive Resource Collection 433
6.15 Querying Information About a Specified Drive Resource 435
6.16 Querying Information About All Drive Resources 440
6.17 Querying Information About a Specified Chassis Power Supply 445
6.18 Modifying Properties of a Specified Power Supply 454
6.19 Querying the Cooling Resource Information About a Specified Chassis 463
6.20 Modifying the Cooling Resource Information About a Specified Chassis 471
6.21 Modifying the Status of a Specified Drive 481
6.22 Querying the Information About the Optical Module Resources Connected to a Specified Network Port 486
6.23 Querying Information About Extended Boards 490
6.24 Querying Information About the Disk Backplane Resource Collection 492
6.25 Querying Information About a Specified Disk Backplane Resource 494
6.26 Modifying Information About a Specified NEO Card 497
6.27 Querying Power Statistics 503
6.28 Querying Information About the Leak Detection System 504
6.29 Querying Information About the Leak Detector Resource Collection 506
6.30 Querying Information About a Specified Leak Detector Resource 508
7. Operations on SessionService Resources 511
7.1 Creating a Session 512
7.2 Querying Information About the Session Service 514
7.3 Modifying Information About the Session Service 516
7.4 Querying Information About the Session Resource Collection 518
7.5 Querying Information About a Specified Session Resource 519
7.6 Deleting Information About a Specified Session Resource 521
8. Operations on AccountService Resources 523
8.1 Querying User Service Information 528
8.2 Modifying User Service Information 531
8.3 Querying Information About the User Resource Collection 533
8.4 Querying Information About a Specified User Resource 534
8.5 Creating an Account 537
8.6 Deleting a User 541
8.7 Modifying Information About a Specified User 542

8.8 Querying Information About the Role Resource Collection 544
8.9 Querying Information About the Specified Role Resource 546
8.10 Querying Information about the LDAP Service Resource 548
8.11 Querying Information About the LDAP Domain Controller Collection 550
8.12 Querying Active Directory Information 552
8.13 Modifying Active Directory Information 555
8.14 Querying the LDAP Information 560
8.15 Modifying the LDAP Information 562
9. Operations on EventService Resources 568
9.1 Querying the EventService Resource 574
9.2 Querying the Event Subscription Resource Collection 577
9.3 Creating an Event Subscription Resource 579
9.4 Querying an Event Subscription Resource 583
9.5 Modifying an Event Subscription Resource 585
9.6 Deleting an Event Subscription Resource 589
9.7 Querying the Alarm Resource Collection 590
9.8 Querying the Current Alarm Resource Collection 593
9.9 Querying the Current Alarm Resource 595
9.10 Deleting the Current Alarm Resource 597
9.11 Querying the Current Alarm Event Resource Collection 598
9.12 Modifying an Event Service Resource 602
9.13 Resuming an Event Subscription Resource 604
9.14 Clearing Historical Alarms in Batches 607
10. Operations on UpdateService Resources 609
10.1 Querying Information About the UpdateService Resource 613
10.2 Querying Information About the Updatable Firmware Resource Collection 616
10.3 Querying Information About a Specified Updatable Firmware Resource 618
10.4 Updating Firmware 621
10.5 Uploading a File 624
10.6 Canceling the Activation of the BIOS Changes 625
10.7 Querying Information About the Internal Firmware Resource Collection 627
10.8 Querying Information About a Specified Internal Firmware Resource of a Server 629
10.9 Querying the Information About the Hotfix Resource Collection 631
10.10 Loading or Removing Hotfixes 634
11. Redfish Installation and Use 637
11.1 Environment Installation 637
11.2 Use Case 637

Glossary 641

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 on a Redfish interface.
Chapter 4, Operations on Manager Resources	Describes the operations on Manager resources on a Redfish interface.
Chapter 5, Operations on System Resources	Describes the operations on System resources on a Redfish interface.
Chapter 6, Operations on Chassis Resources	Describes the operations on Chassis resources on a Redfish interface.
Chapter 7, Operations on SessionService Resources	Describes the operations on SessionService resources on a Redfish interface.
Chapter 8, Operations on AccountService Resources	Describes the operations on AccountService resources on a Redfish interface.
Chapter 9, Operations on EventService Resources	Describes the operations on EventService resources on a Redfish interface.
Chapter 10, Operations on UpdateService Resources	Describes the operations on UpdateService resources on a Redfish interface.
Chapter 11, Redfish Installation and Use	Describes how to install the environment and use the 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, ease of implementation and use, and high scalability, and is 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.
AccountService	Used for managing BMC users.
EventService	Used for reporting and managing BMC SEL events.
UpdateService	Used for managing updatable 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.

Request Header	Description
	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.
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.

Response Header	Description
Content-Type	Describes the media type used in the message body. ● Services shall set **Content-Type** to **application/json** when returning resources as JSON. ● 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 information about 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 **ManagerAccount** 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.

Status Code	Description
400	The request is illegal. An error occurs on the client and an error message is returned.
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.
428	The ETag check is enabled on the server, but the request does not include the **ETag** header.
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/VirtualMedia	GET
/redfish/v1/Managers/manager_id/VirtualMedia/Media_type	GET
/redfish/v1/Managers/manager_id/VirtualMedia/Media_type/Oem/VANTAGEO/Actions/VirtualMedia.VmmControl	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/EthernetInterfaces	GET
/redfish/v1/Managers/manager_id/EthernetInterfaces/id	GET/PATCH

URL	Operation
/redfish/v1/Managers/manager_id/KvmService	GET/PATCH
/redfish/v1/Managers/manager_id/Actions/Manager.RollBack	POST
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.ImportConfiguration	POST
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.ExportConfiguration	POST
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.EffectFactory	POST
/redfish/v1/Managers/manager_id/Actions/Manager.Reset	POST
/redfish/v1/Managers/manager_id/LogServices	GET
/redfish/v1/Managers/manager_id/LogServices/SEL	GET
/redfish/v1/Managers/manager_id/LogServices/SEL/Entries	GET
/redfish/v1/Managers/manager_id/LogServices/SEL/Entries?$skip=a	GET
/redfish/v1/Managers/manager_id/LogServices/SEL/Entries/entries_id	GET
/redfish/v1/Managers/managers_id/Actions/Oem/VANTAGEO/Manager.Configuration/Progress	GET
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.Dump	POST
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.ExportLogs	POST
/redfish/v1/Managers/manager_id/EthernetInterfaces/usb0/Oem/VANTAGEO/NAT	GET/PATCH
/redfish/v1/Managers/manager_id/EthernetInterfaces/usb0/Oem/VANTAGEO/NAT	GET/PATCH
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.CompressFile	POST
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.ExportCompressFile	POST
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.ResetFactory	POST
/redfish/v1/Managers/manager_id/SmtpService	GET/PATCH
/redfish/v1/Managers/manager_id/SmtpService/Actions/SmtpService.SubmitTestEvent	POST
/redfish/v1/Managers/manager_id/DnsService	GET/PATCH
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.SetBMCTimes	POST
/redfish/v1/Managers/manager_id/Actions/Oem/Public/Manager.GeneralDownload	POST
/redfish/v1/Managers/manager_id/SDMService	GET
/redfish/v1/Managers/manager_id/SDMService/alias_id/EventReports	GET
/redfish/v1/Managers/manager_id/TestService/Actions/ClearSystemLog	POST
/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.AutoScreenCap	POST
/redfish/v1/Managers/manager_id/SecurityService/FirewallRules	GET

URL	Operation
/redfish/v1/Managers/manager_id/SecurityService/FirewallRules/Actions/Firewall-Rule.AddRules	POST
/redfish/v1/Managers/managers_id/Actions/Oem/VANTAGEO/Manager.Dump/Progres	GET
/redfish/v1/Managers/managers_id/HDMService	GET
/redfish/v1/Managers/managers_id/HDMService/module_type	GET
/redfish/v1/Managers/manager_id/SecurityService	GET
/redfish/v1/Managers/managers_id/SecurityService/HttpsCert	GET
/redfish/v1/Managers/manager_id/SecurityService/HttpsCert/Actions/HttpsCert.Im-portServerCertificate	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/Settings	GET/PATCH
/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/Chassis	GET
/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?$expand=.	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/NetworkPorts	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapteras_id/Network-Ports/networkports_id	GET/PATCH
/redfish/v1/Chassis/chassis_id/PCIeDevices	GET
/redfish/v1/Chassis/chassis_id/PCIeDevices/pciedevices_id	GET
/redfish/v1/Chassis/chassis_id/PCIeDevices/pciedevices_id/Functions/functions_id	GET
/redfish/v1/Chassis/chassis_id/PCIeDevices?$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/Thermal	GET/PATCH
/redfish/v1/Chassis/Chassis_id/NetworkAdapters/networkadapteras_id/Network-Ports/networkports_id/OpticalModule	GET
/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/Power/NetworkAdapters/NetworkAdapters_id	PATCH
/redfish/v1/Chassis/chassis_id/Power/Actions/Power.CollectHistoryData	POST
/redfish/v1/Chassis/chassis_id/ThermalSubsystem/LeakDetection	GET
/redfish/v1/Chassis/chassis_id/ThermalSubsystem/LeakDetection/LeakDetectors	GET
/redfish/v1/Chassis/chassis_id/ThermalSubsystem/LeakDetection/Lea kDetec-tors/leakdetector_id	GET
SessionService resources	
/redfish/v1/SessionService	GET/PATCH

URL	Operation
/redfish/v1/SessionService/Sessions	GET/POST
/redfish/v1/SessionService/Sessions/Session_id	GET/DELETE
AccountService resources	
/redfish/v1/AccountService	GET/PATCH
/redfish/v1/AccountService/Accounts	GET/POST
/redfish/v1/AccountService/Accounts/member_id	GET/DELETE
/redfish/v1/AccountService/Accounts/account_id	GET/PATCH/ DELETE
/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
/redfish//v1/AccountService/LdapService/LdapControllers/LDAP	GET/PATCH
EventService resources	
/redfish/v1/EventService	GET
/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/CurrentAlarms	GET
/redfish/v1/EventService/CurrentAlarms/alarm_id	GET/DELETE
/redfish/v1/EventService/CurrentAlertEvents	GET
/redfish/v1/EventService/Subscriptions/subscriptions_id/Actions/EventDestination.Re-sumeSubscription	POST
/redfish/v1/EventService/Actions/EventService.ClearHistoryAlarm	POST
UpdateService resourcess	
/redfish/v1/UpdateService	GET
/redfish/v1/UpdateService/FirmwareInventory	GET
/redfish/v1/UpdateService/FirmwareInventory/softid	GET

URL	Operation
/redfish/v1/UpdateService/Actions/UpdateService.SimpleUpdate	POST
/redfish/v1/UpdateService/upload	POST
/redfish/v1/UpdateService/Actions/Oem/VANTAGEO/ UpdateService.CancelBiosActive	POST
/redfish/v1/UpdateService/InsideFirmwareInventory	GET
/redfish/v1/UpdateService/InsideFirmwareInventory/softid	GET
/redfish/v1/UpdateService/HotFix	GET/POST

Chapter 3
Operations on Public Fixed Resources

Table of Contents

Querying the Redfish Version Information 24
Querying the Current Root Service Resources 25

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

Figure 3-1 Path Requirements for Public Fixed Resources

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	Redfish Version	Detailed Redfish version information.	GET
	UUID	UUID of the device.	GET
	Systems	System resources.	GET
	Chassis	Chassis resources.	GET
	Managers	Manager resources.	GET
	SessionService	SessionService resources.	GET
	AccountService	AccountService resources.	GET
	UpdateService	UpdateService resources.	GET
	EventService	EventService resources.	GET

2.1 Querying the Redfish Version Information

Function

Query the current version of the Redfish protocol.

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.

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": "W/\"1577215941\"",
    "@odata.id": "/redfish/v1/",
    "@odata.type": "#ServiceRoot.v1_3_0.ServiceRoot",
```

```
    "AccountService":
{
    "@odata.id": "/redfish/v1/AccountService"
},
"Chassis":
{
    "@odata.id": "/redfish/v1/Chassis"
},
"Description": "The service root for all Redfish requests on this host",
"EventService":
{
"@odata.id": "/redfish/v1/EventService"
},
"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",
"RedfishVersion": "1.5.0",
"Registries":
{
    "@odata.id": "/redfish/v1/Registries"
},
"SessionService":
{
    "@odata.id": "/redfish/v1/SessionService"
},
"Systems":
{
    "@odata.id": "/redfish/v1/Systems"
},
"Tasks":
```

```
    {
        "@odata.id": "/redfish/v1/TaskService"
    },
    "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.
Id	String	ID of the root service.
Name	String	Name of the root service resource.
RedfishVersion	String	Detailed Redfish version information.
UUID	String	UUID of the device.
Systems	Object	System resources.
Chassis	Object	Chassis resources.
Managers	Object	Manager resources.
Tasks	Object	TaskService resources.
SessionService	Object	SessionService resources.
AccountService	Object	AccountService resources.
EventService	Object	EventService resources.
UpdateService	Object	UpdateService resources.
Registries	Object	Message registry resources.
Description	String	Root service description.
Links	Object	-
Sessions	Object	SessionService resources.

Chapter 4
Operations on Manager Resources

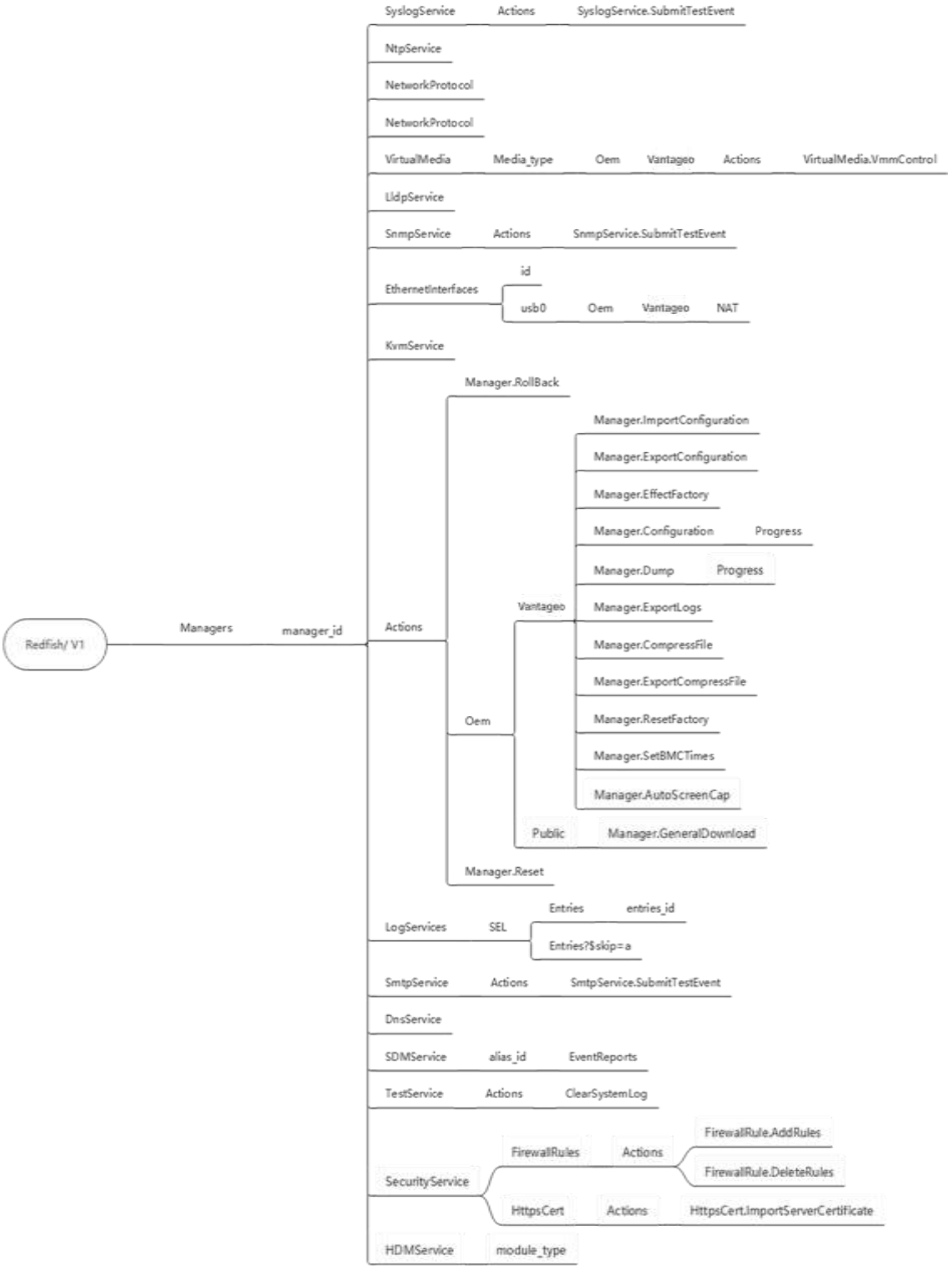
Table of Contents

Querying Information About the Manager Resource Collection 52
Querying Information About a Specified Manager Resource 53
Modifying Information About a Specified Manager Resource 60
Querying Information About the Syslog Configuration 65
Configuring Information About the Syslog Server 68
Submitting a Syslog Test Log 73
Querying Information About the NtpService Configuration Resource 74
Modifying Properties of the NTP Resource 76
Querying Information About the BMC Service 80
Modifying Information About a Specified BMC Service 83
Querying the Virtual Media Resource Collection 87
Querying a Virtual Media Resource 89
Connecting to the Virtual Media 92
Disconnecting the Virtual Media 94
Querying Information About the LLDP Service Configuration Resource 96
Modifying Properties of the LLDP Service Resource 98
Querying Information About the SNMP Resource 100
Modifying Properties of the SNMP Resource 105
Submitting an SNMP Trap Test Event 110
Querying the Management Interface Collection of the BMC 111
Querying Information About a Specified Management Interface Resource of the BMC 113
Modifying a Specified Management Interface Resource of the BMC 120
Querying the KVM Service Resource 127
Modifying Information About the KVM Resource 129
Changing the BMC Firmware Version 132
Importing a Configuration File 134
Exporting Configurations 137

Validating Configurations 140
Restarting the BMC 142
Querying Information About the Log Service Resource Collection 144
Querying Information About a Specified Log Service Resource 146
Querying Information About the SEL Log Service Resource Collection 148
Querying Information About the SEL Log Service Resource Collection by Specifying a Parameter 150
Querying Information About a Specified SEL Log Service Resource 152
Querying the Import and Export Progress 155
Performing One-Click Collection 157
Exporting Logs 159
Querying Information About the NAT Resource 162
Setting Information About the NAT Resource 164
Performing One-Click Configuration Solidification 167
Performing One-Click Configuration Information Export 169
Performing One-Click Configuration Restoration 172
Querying Information About the SMTP Resource 175
Modifying Properties of the SMTP Resource 178
Sending an SMTP Test Email 182
Querying Information About the DNS Resource 183
Modifying Properties of the DNS Resource 187
Setting the BMC Time and Time Zone 190
Downloading a BMC File 193
Querying Information About the SDM Service Resource 195
Querying the Component Early-Warning Information About the SDM Service Resource 197
Clearing System Logs 199
Exporting a Screenshot 200
Triggering a Screenshot 202
Querying Information About the Firewall Service Resource 203
Adding a Firewall Rule 207
Deleting a Firewall Rule 209
Querying the One-Click Collection Progress 211
Querying Information About the HDM Service Resource Collection 213
Querying Information About HDM Resource Health Status 215
Querying Information About the SecurityService Resource 218
Querying Information About the SSL Certificate Resource 220
Importing an SSL Certificate 223

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
	Members@odata.count	Number of Manager resource members.	GET
	Members	Manager resource list.	GET
	@odata.id	Access path of a single Manager resource node.	GET
/redfish/v1/Managers/manager_id	Id	ID of the Manager resource.	GET/PATCH
	Name	Name of the Manager resource.	GET/PATCH
	ManagerType	Type of Manager resource.	GET/PATCH
	Manufacturer	Specifies the manufacturer of the management resource chip.	GET
	FirmwareVersion	Firmware version of the Manager resource.	GET/PATCH
	FirmwareVersionDate	Time of the BMC version.	GET
	UUID	UUID of the Manager resource.	GET/PATCH
	Model	Model of the Manager resource.	GET
	DateTime	System time of the Manager resource.	GET/PATCH
	DateTimeLocalOffset	Time zone of the Manager resource.	GET/PATCH
	NetworkProtocol	Access path of the network protocol supported by the specified Manager resource.	GET/PATCH
	EthernetInterfaces	Access path of the Ethernet interface information about the specified Manager resource.	GET/PATCH
	EthernetInterfaces	Access path of the Ethernet interface information about the specified Manager resource.	GET/PATCH
	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

URL	Property	Description	Operation
	KvmService	Access path of the KVM service of the specified Manager resource.	GET
	SnmpService	Access path of the SNMP service of the specified Manager resource.	GET
	SmtpService	Access path of the SMTP service of the specified Manager resource.	GET
	HDMService	Access path of the HDM service of the specified Manager resource.	GET
	LldpService	Access path of the LLDP service of the specified Manager resource.	GET
	VirtualMedia	Access path of the virtual media service of the specified Manager resource.	GET
	DnsService	Access path of the DNS service of the specified Manager resource.	GET
	FirewallService	Access path of the firewall 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 configurations.	GET
	Manager.ExportConfiguration	Exports configurations.	GET
	Manager.FactoryReset	Restores the factory default settings.	GET
/redfish/v1/Managers/1/SyslogService	Id	ID of the syslog service.	GET/PATCH
	Name	Name of the syslog service.	GET/PATCH
	ServiceEnabled	Syslog service enabled.	GET/PATCH
	ServerIdentitySource	● Board serial number: BoardSN	GET/PATCH

URL	Property	Description	Operation
		• Asset tag: ProductAssetTag • Host name: HostName	
	TransmissionProtocol	Transmission protocol: • UDP • TCP	GET/PATCH
	SyslogServers	Syslog servers.	GET/PATCH
	MemberId	• 0 • 1 • 2 • 3	GET/PATCH
	Enabled	Channel enabled.	GET/PATCH
	Address	Server address.	GET/PATCH
	Port	Server port number.	GET/PATCH
	LogType	Log type.	GET/PATCH
	Actions	Available actions for the specified Syslog resource.	GET/PATCH
	SyslogService.SubmitTestEvent	Submit the test event.	GET/PATCH
/redfish/v1/Managers/1/NtpService	ServiceEnabled	NTP service enabled.	GET/PATCH
	AlternateNtpServer	Alternate NTP server address.	GET/PATCH
	PreferredNtpServer	Preferred NTP server address.	GET/PATCH
	ExtraNtpServer	Address of the extra NTP server.	GET/PATCH
	MinPollingInterval	Minimum polling interval.	GET/PATCH
	MaxPollingInterval	Maximum polling interval.	GET/PATCH
	CurrentPollingInterval	Current polling interval.	GET/PATCH
	NtpAddressOrigin	Select the NTP mode: • static • IPv4 • IPv6	GET/PATCH
	ServerAuthenticationEnabled	Whether the server authentication is enabled.	GET/PATCH
	NtpSynResult	Result of NTP synchronization: • successful: The synchronization is successful.	GET/PATCH

URL	Property	Description	Operation
		• fail: The synchronization is unsuccessful. • NULL: The configuration file is empty. • mode is not NTP: The mode is not NTP. • get NTP result fail: The configuration file cannot be read.	
/redfish/v1/Managers/manager_id/NetworkProtocol	Id	BMC network protocol resource ID.	GET
	Name	BMC network protocol resource name.	GET
	HostName	BMC host name.	GET
	HTTPS/KVMIP/SNMP/SSH/VirtualMedia	Service information supported by BMC.	GET/PATCH
	ProtocolEnabled	Whether the protocol is enabled.	GET/PATCH
	Port	Service port number.	GET/PATCH
	NotifyIPv6Scope	IPV6 multicast address scope for SSDP service messages: • Link: Link local scope. • Site: Site local scope. • Organization: Organization local scope.	GET/PATCH
	NotifyMulticastIntervalSeconds	SSDP service message multicast interval time.	GET/PATCH
	Oem.Public	-	GET/PATCH
	VirtualMedia-CD/VirtualMedia-HD/SSDP	-	GET/PATCH
	Instance	Number of Instances.	GET/PATCH
	NotifyEnabled	Whether the SSDP service message multicast is enabled: • true • false	GET/PATCH
/redfish/v1/Managers/manager_id/VirtualMedia	Description	Description.	GET
	Members	Virtual media resource list.	GET
	@odata.id	Access path of the virtual media resource collection.	GET

URL	Property	Description	Operation
	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 of the virtual media resource.	GET
	Id	ID of the virtual media resource.	GET
	Name	Name of the virtual media resource.	GET
	MediaTypes	Media types.	GET
	TransferProtocolType	Transfer protocol type.	GET
	TransferMethod	Transfer method: stream.	GET
	Image	Image path.	GET
	ImageName	Image name.	GET
	ConnectedVia	Connection method.	GET
	Inserted	Connection status.	GET
	Oem	Customized properties of a specified session.	GET/POST
/redfish/v1/Managers/manager_id/VirtualMedia/Media_type/Oem/VANTAGEO/ Actions/VirtualMedia.VmmControl	Information	-	POST
	target	Access path of the virtual media resource.	POST
/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	Operational mode of the LLDP resource.	GET
/redfish/v1/Managers/manager_id/SnmpService	Actions	Operations that can be performed on the SNMP resource.	GET

URL	Property	Description	Operation
	#SnmpService.SubmitTestEvent	Submits an SNMP Trap Test Event.	GET
	Id	ID of the SNMP resource.	GET
	Name	Name of the SNMP resource.	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
	TrapVersion	Global SNMP Trap version number.	GET
	SnmpV3AuthUser	● For administrators, this array lists all users with the SNMP permission. ● For non-administrators, it is displayed as null.	GET
	UserName	Username with the SNMP permission.	GET
	SnmpV3AuthProtocol	SNMPv3 user authentication algorithm: MD5 SHA	GET
	SnmpV3PrivProtocol	NMPv3 user encryption algorithm: DES AES	GET
	SnmpV3AuthUser@odata.count	Number of current users with the SNMP permission. For non-administrators, the number of current users with the SNMP permission is displayed as null.	GET
	SnmpV3EngineID	SNMPv3 Engine ID.	GET
	SnmpTrapNotification	SNMP Trap properties.	GET
	TrapServer	SNMP Trap server information.	GET
	MemberId	SNMP Trap group member number.	GET
	TrapVersion	SNMP Trap version number.	GET
	TrapV3User	SNMPv3 username.	GET

URL	Property	Description	Operation
	TrapServerAddress	SNMP Trap server address.	GET
	TrapServerPort	SNMP Trap server port number.	GET
	TrapServerEnable	Whether to a single SNMP trap channel is enabled.	GET
	TrapServer@odata.count	Number of SNMP Trap servers.	GET
	snmpTrapCommunity	SNMP trap community name. This property contains sensitive information and is displayed as null. The PATCH operation is available.	GET
	AlarmSeverity	Alarm severity level.	GET
	snmpTrapEnable	Whether SNMP Trap is enabled.	GET
	TrapMode	● EventOIDMode event OID mode. ● ModuleOIDMode module OID mode.	GET
	SnmpV1V2Enable	Whether SNMPv1/v2C Set/Get is enabled.	GET
/redfish/v1/Managers/manager_id/EthernetInterfaces	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
	Description	Description of the specified BMC management interface resource.	GET
	AutoNeg	Whether auto-negotiation is enabled.	GET
	FullDuplex	Whether full-duplex mode is used.	GET
	HostName	DNS hostname, which does not contain any domain information.	GET
	PermanentMACAddress	Permanent MAC address assigned to the interface.	GET

URL	Property	Description	Operation
	MTUSize	MTU (in bytes) configured on the current interface.	GET
	SpeedMbps	Current rate (in Mbps).	GET
	InterfaceEnabled	Whether the interface is enabled.	GET
	IPv4Addresses	IPv4 information object.	GET
	Address	IPv4 address.	GET
	AddressOrigin	Source of the IPv4 address.	GET
	Gateway	Gateway of the IPv4 address.	GET
	SubnetMask	IPv4 subnet mask.	GET
	IPv6Addresses	IPv6 information object.	GET
	Address	IPv6 address.	GET
	AddressOrigin	Source of the IPv6 address.	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
	Pv6StaticAddresses	Static IPv6 information object.	GET
	Address	Static IPv6 address.	GET
	PrefixLength	Prefix length of the static IPv6 address.	GET
	IPv6DefaultGateway	Default IPv6 gateway.	GET
	NameServers	Domain name server list.	GET
	VLAN	VLAN information object.	GET
	VLANEnable	Whether VLAN is enabled.	GET
	VLANId	Configured VLAN ID.	GET
	Oem.Public	OEM object.	GET
	DNSDhcpEnabled	Whether DNS DHCP is enabled.	GET
	DNSServiceEnabled	Whether the DNS service is enabled.	GET
	IPStacks	Whether IPv4 and IPv6 are enabled: ● null: interface not enabled	GET

URL	Property	Description	Operation
		• IPv4: IPv4 enabled only • IPv6: IPv6 enabled only • IPv4AndIPv6: IPv4 and IPv6 both enabled	
	PatchInProgress	Configuration validity flag: • true: being configured • false: configured completely and applied successfully.	GET
/redfish/v1/Managers/manager_id/KvmService	MaximumNumberOfSessions	Maximum number of KVM sessions.	GET/PATCH
	KvmUrl	URL for logging in to the KVM. When you log in through this URL, the Web session is automatically logged out.	GET
	NumberOfActivatedSessions	Number of current KVM sessions.	GET
	ActivatedSessionsType	Type of KVM session.	GET
	AutoScreenCapEnable	Whether the automatic screen cap is enabled.	GET/PATCH
	EncryptionEnabled	KVM encryption enabled.	GET/PATCH
	SessionTimeoutMinutes	Session timeout minutes.	GET/PATCH
/redfish/v1/Managers/manager_id/Actions/Manager.RollBack	ode	String indicating the specified message ID in the message registry.	POST
	message	Readable error message corresponding to the one in the message registry.	POST
	@odata.type	OData description of the message resource.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity level.	POST
	Resolution	Recommended solution.	POST
/redfish/v1/Managers/manager_id/Actions/Oem/	code	ID of the specified message in the message registry.	POST

URL	Property	Description	Operation
VANTAGEO/Manager.ImportConfiguration	message	Readable error message corresponding to the one in the message registry.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity levels supported by the Redfish interface.	POST
	Resolution	Recommended solution.	POST
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.ExportConfiguration	code	String indicating the specified message ID in the message registry.	POST
	message	Readable error message corresponding to the one in the message registry.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity levels supported by the Redfish interface.	POST
	Resolution	Recommended solution.	POST
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.EffectFactory	code	String indicating the specified message ID in the message registry.	POST
	message	Readable error message corresponding to the one in the message registry.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity levels supported by the Redfish interface.	POST

URL	Property	Description	Operation
	Resolution	Recommended solution.	POST
	message	Readable error message corresponding to the one in the message registry.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity levels supported by the Redfish interface.	POST
	Resolution	Recommended solution.	POST
/redfish/v1/Managers/manager_id/LogServices	Name	Name of the log service resource collection.	GET
	Members@odata.count	Number of current log service resources.	GET
	Members	List of log service resources.	GET
/redfish/v1/Managers/manager_id/LogServices/SEL	Entries	Access path of the SEL log resource collection.	GET
	MaxNumberOfRecords	Maximum number of log records of the specified log service resource.	GET
/redfish/v1/Managers/manager_id/LogServices/SEL/Entries	Name	Name of the SEL log resource collection.	GET
	Members@odata.count	Number of SEL logs.	GET
	Members	List of SEL log resources.	GET
/redfish/v1/Managers/manager_id/LogServices/SEL/Entries?$skip=a	Name	Name of the SEL log resource collection.	GET
	Members@odata.count	Number of SEL logs.	GET
	Members	List of SEL log resources.	GET
/redfish/v1/Managers/manager_id/LogServices/SEL/Entries/entries_id	Name	Name of the specified SEL log instance.	GET
	id	ID of the specified SEL log instance.	GET
	EntryType	Type of SEL log instance.	GET

URL	Property	Description	Operation
	Description	Description of the specified SEL log instance.	GET
	SensorType	Sensor type for generating SEL log instance information.	GET
	SensorNumber	Sensor ID for generating SEL log instance information.	GET
	EventTimestamp	Timestamp of the SEL log instance information.	GET
	Created	Generation time of the SEL log instance information.	GET
	Severity	Log severity level of the SEL log instance information.	GET
	EntryCode	Entry code of SEL log instance information.	GET
	Message	Message content of the SEL log instance information.	GET
/redfish/v1/Managers/manager-s_id/Actions/Oem/VANTAGEO/Manager.Configuration/P-rogress	Detail	Detailed information. Options: ● ImortConfiguration ● ExportConfiguration	GET
	Percentage	Percentage.	GET
	State	State. Options: ● STATE_FAILED ● STATE_SUCCESSED ● STATE_RUNNING ● STATE_SILENT	GET
	Type	Type. Options: ● BMC ● BIOS ● Logs ● BMC_BIOS	GET
	Message	Message description.	GET
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.Dump	code	ID of the specified message in the message registry.	GET
	message	Readable error message corresponding to the one in the message registry.	GET

URL	Property	Description	Operation
	@odata.type	OData description of the message resource.	GET
	MessageId	Message ID.	GET
	RelatedProperties	Message-related properties.	GET
	Message	Details.	GET
	MessageArgs	Message arguments.	GET
	Severity	Severity levels supported by the Redfish interface.	GET
	Resolution	Recommended solution.	GET
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.ExportLogs	code	String indicating the specified message ID in the message registry.	POST
	message	Readable error message corresponding to the one in the message registry.	POST
	@odata.type	OData description of the message resource.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity levels supported by the Redfish interface.	POST
	Resolution	Recommended solution.	POST
/redfish/v1/Managers/manager_id/EthernetInterfaces/usb0/Oem/VANTAGEO/NAT	Oem.Public	OEM object of the usb0 resource node.	GET
	BmcIpaddress	IPv4 address of the BMC.	GET/PATCH
	BmcPort	Port of the BMC.	GET/PATCH
	HostIpaddress	IP address of the host.	GET/PATCH
	HostPort	Port number of the host.	GET/PATCH
	NATEnabled	Whether NAT is enabled.	GET/PATCH
	code	ID of the specified message in the message registry.	PATCH

URL	Property	Description	Operation
	message	Readable error message corre-sponding to the one in the message registry.	PATCH
	MessageId	Message ID.	PATCH
	NATDefault	Default NAT configuration.	PATCH
/redfish/v1/Man-agers/manag-er_id/Actions/Oem/VANTAGEO/Manag er.Com- pressFile	code	ID of the specified message in the message registry.	POST
	message	Readable error message corre-sponding to the one 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
	Resolution	Recommended solution.	POST
/redfish/v1/Man-agers/manag-er_id/Actions/Oem/VANTAGEO/Mana ger.ExportCompres -sFile	code	ID of the specified message in the message registry.	POST
	message	Readable error message corre-sponding to the one 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
	Resolution	Recommended solution.	POST
/redfish/v1/Man-agers/manag-er_id/Actions/Oem/VANTAGEO/Mana-ger.ResetFactory	code	ID of the specified message in the message registry.	POST
	message	Readable error message corre-sponding to the one in the message registry.	POST

URL	Property	Description	Operation
	@odata.type	OData description of the message resource.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity level.	POST
	Resolution	Recommended solution.	POST
/redfish/v1/Managers/manager_id/SmtpService	Actions	Operations that can be performed on the SNMP resource.	GET
	#SmtpService.SubmitTestEvent	Sends an SMTP test email.	GET
	AttachAssettag	Whether an asset tag is attached to the email subject.	GET
	AttachHostname	Whether the hostname is attached to the email subject.	GET
	EmailSubject	Email subject.	GET
	ReciverEmailId	Receiving mailbox address collection.	GET
	EmailAddress	Receiving email address.	GET
	SenderEmailId	Sender's email address.	GET
	SmtpAuthEnable	Whether SMTP identity authentication is enabled.	GET
	SmtpEnable	Whether alarms are sent to the mailbox.	GET
	SmtpPassword	SMTP password.	GET
	SmtpServerIp	Address of the SMTP server.	GET
	SmtpServerPort	Port number of the SMTP server.	GET
	SmtpTlsEnable	Whether the TLS function is enabled.	GET
	SmtpUsername	SMTP username.	GET

URL	Property	Description	Operation
/redfish/v1/Managers/manager_id/DnsService	DnsIpConfig	DNS Server IP configurations.	GET
	DnsDhcpEnable	Method for obtaining the DNS server address: ● true: The address is obtained automatically. ● false: The address is configured manually.	GET
	DnsEnable	Whether the DNS service is enabled.	GET
	DnsInterface	Network interface name. ● eth0 ● eth1 ● bond0	GET
	IpPriority	IP priority. ● ipv4 ● ipv6	GET
	NameServers	Domain name server list.	GET
	DomainConfig	Domain configuration.	GET
	DhcpEnable	Method for obtaining the domain information. ● true: automatic ● false: manual	GET
	DomainInterface	Network interface name. ● eth0 ● eth1 ● bond0	GET
	DomainPriority	Domain type. ● ipv4 ● ipv6	GET
	DomainName	Domain name.	GET
	HostNameConfig	Hostname setting.	GET
	HostSetting	Hostname setting mode. ● Automatic ● Manual	GET
	HostName	Hostname.	GET
	PatchInProgress	Configuration validity flag: ● true: being configured	GET

URL	Property	Description	Operation
		• false: configured completely and applied successfully.	
	RegisterBMC	Registration configurations of the BMC.	GET
	Eth0Reg	Eth0 registration mode: • nsupdate • fqdn • hostname • null	GET
	Eth1Reg	Eth1 registration mode: • nsupdate • fqdn • hostname • null	GET
	Bond0Reg	Bond0 registration mode: • nsupdate • fqdn • hostname • null	GET
/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.SetBMCTimes	code	ID of the specified message in the message registry.	POST
	message	Readable error message corresponding to the one in the message registry.	POST
	@odata.type	OData description of the message resource.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity level.	POST
	Resolution	Recommended solution.	POST
/redfish/v1/Managers/manager_id/SDMService	SilkName	Silk screen of the device.	GET
	ComponentType	Component type of the device.	GET
	ComponentID	Component ID of the device.	GET

URL	Property	Description	Operation
	Alias	Unique identifier of the device in the device tree.	GET
	EventReports	Access path of the early warning report information about device faults.	GET
	DeviceInfo	Access path of device information.	GET
	OnlineTimeStamp	Timestamp when the device goes online.	GET
	Members@odata.count	Number of devices.	GET
	Name	Name of the SDM service resource collection.	GET
/redfish/v1/Managers/manager_id/SDMService/alias_id/EventReports	EventRecords	Fault analysis record generated by the SDM fault early warning system. Each object corresponds to an event.	GET
	ReportTimeStamp	Timestamp when the report is generated.	GET
	SilkName	Silk screen of the device.	GET
	ComponentType	Component type of the device.	GET
	ComponentID	Component ID of the device.	GET
	Type	Event type. ● Installation ● Replacement ● Removal	GET
	Information	Event description.	GET
/redfish/v1/Managers/manager_id/SecurityService/FirewallRules	Actions	Operations that can be performed on the resource.	GET
	#FirewallRule.AddRules	Adds a firewall rule.	GET
	#FirewallRule.DeleteRules	Deletes a firewall rule.	GET
	ActiveStrategy	Currently valid rule policy: ● Accept: enables rules that accept data, that is, the whitelist takes effect. ● Drop: enables rules that drop data, that is, the blacklist takes effect.	GET

URL	Property	Description	Operation
		● Other: **IPv4ActiveStrategy** and **IPv6ActiveStrategy** are inconsistent.	
	IPv4ActiveStrategy	Currently valid IPv4 firewall rule policy: ● Accept: enables rules that accept data, that is, the whitelist takes effect. ● Drop: enables rules that drop data, that is, the blacklist takes effect.	GET
	IPv6ActiveStrategy	Currently valid IPv6 firewall rule policy: ● Accept: enables rules that accept data, that is, the whitelist takes effect. ● Drop: enables rules that drop data, that is, the blacklist takes effect.	GET
	EndDateTime	Time when the rule becomes invalid.	GET
	EndIPAddress	End IP address corresponding to the rule.	GET
	EndMacAddress	End MAC address corresponding to the rule.	GET
	RuleType	Mode type of this rule: ● Accept ● Drop	GET
	StartDateTime	Time when the rule takes effect.	GET
	StartIPAddress	Start IP address corresponding to the rule.	GET
	StartMacAddress	Start MAC address corresponding to the rule.	GET
/redfish/v1/Managers/manager-s_id/Actions/Oem/VANTAGEO/Manager.Dump/Progre-ss	Percentage	Percentage.	GET
	State	State.	GET
	Type	Type: **Logs**.	GET
	Message	Message description.	GET

URL	Property	Description	Operation
	TarName	Name of the package containing collected log files.	GET
/redfish/v1/Managers/manager_id/HDMService	Name	Name of the HDMService resource.	GET
	Members@odata.count	Number of HDMService resources.	GET
	Members	List of HDMService resources.	GET
/redfish/v1/Managers/manager_id/HDMService/module_type	Name	Name of the specified HDMService resource.	GET
	Id	ID of the specified HDMService resource.	GET
	Count	Number of specified resources.	GET
	Records	List of HDMService resource objects.	GET
	TimeStamp	Health assessment timestamp.	GET
	ComponentID	Component ID. For a resource without this information, the parameter is set to 0 by default.	GET
	ComponentType	Component type. For a resource without this information, the parameter is set to an empty string by default.	GET
	Slot	Slot number. For a resource without this information, the parameter is set to 0 by default.	GET
	SilkName	Silk screen of the device.	GET
	HealthScore	Health score of the device.	GET
	Reasons	List of reasons why the HDMService chassis is not healthy.	GET
	ReportTimeStamp	Time when an alarm is reported.	GET
	AlarmCode	Alarm code.	GET
	Level	Alarm severity level.	GET
	ComponentType	Component type.	GET
/redfish/v1/Managers/manager_id/SecurityService	Name	Name of the SessionService resource.	GET

URL	Property	Description	Operation
	Id	Unique ID of the SecurityService resource.	GET
	FirewallRules	Lower-level firewall rule URI.	GET
	HttpsCert	URI for SSL certificate information query.	GET
/redfish/v1/Managers/manager-s_id/SecurityService/HttpsCert	Id	ID of the SSL certificate resource.	GET
	Name	Name of the SSL certificate resource.	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
	Subject	City or area.	GET
	CommonName	Common name.	GET
	Country	Country.	GET
	Organization	Organization.	GET
	OrganizationalUnit	Organizational unit.	GET
	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

4.1 Querying Information About the Manager Resource Collection

Function

Query information about the Manager resource collection of a server.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#ManagerCollection.ManagerCollection",
    "@odata.etag": "W/\"1579419263\"",
```

```
    "@odata.id": "/redfish/v1/Managers",
    "@odata.type": "#ManagerCollection.ManagerCollection",
    "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.
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.

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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#Manager.Manager",
    "@odata.etag": "W/\"1579422717\"",
    "@odata.id": "/redfish/v1/Managers/1",
    "@odata.type": "#Manager.v1_3_3.Manager",
    "Actions":{
        "#Manager.Reset": {
            "ResetType@Redfish.AllowableValues": [
                "ForceRestart"
            ],
            "target": "/redfish/v1/Managers/1/Actions/Manager.Reset"
        },
        "Oem": {
            "#Manager.CompressFile": {
                "@Redfish.ActionInfo": "/redfish/v1/Managers/1/CompressFileActionInfo",
```

```
          "target": "/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.CompressFile"
           },
           "#Manager.Dump": {
              "@Redfish.ActionInfo": "/redfish/v1/Managers/1/DumpActionInfo",
              "target": "/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.Dump"
           },
           "#Manager..EffectFactory": {
            "@Redfish.ActionInfo": "/redfish/v1/Managers/1/EffectFactoryActionInfo",
            "target": "/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.EffectFactory"
           },
           "#Manager.ExportCompressFile": {
               "@Redfish.ActionInfo": "/redfish/v1/Managers/1/
               ExportCompressFileActionInfo",
               "target": "/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/
               Manager.ExportCompressFile"
           },
           "#Manager.ExportConfiguration":{
               "@Redfish.ActionInfo": "/redfish/v1/Managers/1/
               ExportConfigurationActionInfo",
               "target": "/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/
               Manager.ExportConfiguration"
           },
           "#Manager.ExportLogs": {
             "@Redfish.ActionInfo": "/redfish/v1/Managers/1/ExportLogsActionInfo",
             "target": "/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.ExportLogs"
           },
           "#Manager.FactoryReset":{
               "FactoryResetType@Redfish.AllowableValues": ["ResetAll"],
               "target": "/redfish/v1/Managers/1/Actions/Manager.FactoryReset"
           },
           "#Manager.GeneralDownload": {
               "@Redfish.ActionInfo": "/redfish/v1/Managers/1/
               GeneralDownloadActionInfo",
               "target": "/redfish/v1/Managers/1/Actions/Oem/Public/
               Manager.GeneralDownload"
           },
           "#Manager.ImportConfiguration": {
               "@Redfish.ActionInfo": "/redfish/v1/Managers/1/
               ImportConfigurationActionInfo",
               "target": "/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/
               Manager.ImportConfiguration"
           },
           "#Manager.ResetFactory": {
               "@Redfish.ActionInfo": "/redfish/v1/Managers/1/ResetFactoryActionInfo",
```

```
            "target": "/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.ResetFactory"
          },
          "#Manager.RollBack": {
              "RollBackType@Redfish.AllowableValues": [
                  "RollBack"
              ],
              "target": "/redfish/v1/Managers/1/Actions/Manager.RollBack"
           },
           "#Manager.SetBMCTimes": {
            "@Redfish.ActionInfo": "/redfish/v1/Managers/1/SetBMCTimesActionInfo",
            "target": "/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.SetBMCTimes"
           }
      },
      "CommandShell": {
          "ConnectTypesSupported": [
              "IPMI",
              "SSH"
          ],
      "MaxConcurrentSessions": 1,
      "ServiceEnabled": true
  },
  "DateTime": "2020-01-19T16:31:55+08:00",
  "DateTimeLocalOffset": "+08:00",
  "Description": "BMC",
  "EthernetInterfaces": {
      "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces"
  },
  "FirmwareVersion": "03.07.0400",
  "FirmwareVersionDate": "Apr 2 2023,
  "GraphicalConsole": {
      "ConnectTypesSupported": [
          "KVMIP"
      ],
      "MaxConcurrentSessions": 4,
      "ServiceEnabled": true
  },
  "Id": "1",
  "KvmService": {
      "@odata.id": "/redfish/v1/Managers/1/KvmService"
  },
  "Links": {
      "ManagerForChassis": [{
          "@odata.id": "/redfish/v1/Chassis/1"
      }],
```

```
        "ManagerForServers": [{
            "@odata.id": "/redfish/v1/Systems/1"
        }],
        "ManagerInChassis": [{
            "@odata.id": "/redfish/v1/Chassis/1"
        }]
    },
    "LldpService": {
        "@odata.id": "/redfish/v1/Managers/1/LldpService"
    },
    "LogServices": {
        "@odata.id": "/redfish/v1/Managers/1/LogServices"
    },
    "ManagerType": "BMC",
    "Manufacturer": "ASPEED",
    "Model": "1257662150",
    "Name": "Manager",
    "NetworkProtocol": {
        "@odata.id": "/redfish/v1/Managers/1/NetworkProtocol"
    },
    "NtpService": {
        "@odata.id": "/redfish/v1/Managers/1/NtpService"
    },
    "Oem": {
       "DnsService": {
          "@odata.id": "/redfish/v1/Managers/1/DnsService"
        },
        "Public": {
            "FirewallService": {
                "@odata.id": "/redfish/v1/Managers/1/SecurityService"
            },
            "IfMatchEnabled": true
        }
    },
    "PowerState": "On",
    "SerialConsole": {
        "ConnectTypesSupported": [
            "IPMI"
        ],
        "ServiceEnabled": false
    },
    "ServiceEntryPointUUID":  "30e72400-0000-1000-0000-1c191516d176",
    "SnmpService": {
        "@odata.id": "/redfish/v1/Managers/1/SnmpService"
```

```
    },
    "SmtpService": {
        "@odata.id": "/redfish/v1/Managers/1/SmtpService"
    },
    "HDMService": {
       "@odata.id": "/redfish/v1/Managers/1/HDMService"
    },
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "SyslogService": {
        "@odata.id": "/redfish/v1/Managers/1/SyslogService"
    },
    "UUID": "30e72400-0000-1000-0000-1c191516d176",
    "VirtualMedia": {
        "@odata.id": "/redfish/v1/Managers/1/VirtualMedia"
    }
}
```


- 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 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.
Id	String	ID of the Manager resource.
Name	String	Name of the Manager resource.
ManagerType	String	Type of Manager resource.
Manufacturer	String	Specifies the manufacturer of the management resource chip.
FirmwareVersion	String	Firmware version of the Manager resource.
FirmwareVersionDate	String	Time of the BMC version.

Field	Type	Description
UUID	String	UUID 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.
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.
EthernetInterfaces	Object	Access path of the Ethernet interface information about the specified Manager resource.
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.
SmtpService	Object	Access path of the SMTP service of the specified Manager resource.
HDMService	Object	Access path of the HDM service of the specified Manager resource.
LldpService	Object	Access path of the LLDP service of the specified Manager resource.
VirtualMedia	Object	Access path of the virtual media service of the specified Manager resource.
DnsService	Object	Access path of the DNS service of the specified Manager resource.
FirewallService	Object	Access path of the firewall service of the specified Manager resource.
Links	Object	Links to the related resources.
Actions	Object	Available actions for the specified Manager resource.
Oem	Object	Customized properties.

Field	Type	Description
#Manager.RollBack	Object	OS operation.
RollBackType@Redfish.Allow-ableValues	Array	OS operations allowed through the Redfish interface, including: RollBack
target	String	Operation path.
Manager.RollBack	Object	Switches BMC versions.
Manager.ImportConfiguration	Object	Imports configurations.
Manager.ExportConfiguration	Object	Exports configurations.
Manager.FactoryReset	Object	Restores the factory default settings.

4.3 Modifying Information About a Specified Manager Resource

Function

Modify information about a specified Manager resource of a server.

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:
  - → Configuring the time zone:

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

  - → Configuring Etag check enable:

```
{
    "Oem":{
        "Public":{
            "IfMatchEnabled":ifmatchenabled_value
        }
    }
}
```

Description

For a description of the parameters for modifying information about the specified Manager resource, refer to Table 4-6.

Table 4-6 Parameter Descriptions for Modifying 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 PATCH request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
datetimelocaloffset_value	Time zone of the Manager resource, in two formats: ● Time offset ● Time zone name	● Time offset format: +hh:mm or -hh:mm ● Range: -12:00 through +14:00 ● Time zone name example: Asia/Shanghai or America/New_York
ifmatchenabled_value	Whether the If-Match function is enabled.	● true ● false

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
    "DateTimeLocalOffset": "+08:00",
    {
        "Oem":{
            "Public":{
                "IfMatchEnabled":true
```

```
            }
        }
    }
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#Manager.Manager",
    "@odata.etag": "W/\"1579422717\"",
    "@odata.id": "/redfish/v1/Managers/1",
    "@odata.type": "#Manager.v1_3_3.Manager",
    "Actions":
    {
        "#Manager.Reset": {
        "ResetType@Redfish.AllowableValues": ["ForceRestart"],
        "target": "/redfish/v1/Managers/1/Actions/Manager.Reset"},
        "Oem": {
        "#Manager.FactoryReset": {
        "FactoryResetType@Redfish.AllowableValues": ["ResetAll"],
        "target": "/redfish/v1/Managers/1/Actions/Manager.FactoryReset"},
        "#Manager.RollBack": {
        "RollBackType@Redfish.AllowableValues": ["RollBack"],
        "target": "/redfish/v1/Managers/1/Actions/Manager.RollBack"}
     }
},
    "CommandShell":
    {
        "ConnectTypesSupported": ["IPMI","SSH"],
        "MaxConcurrentSessions": 1,
        "ServiceEnabled": true
    },
    "DateTime": "2021-05-18T11:29:41+08:00",
    "DateTimeLocalOffset": "+08:00",
    "Description": "BMC",
    "EthernetInterfaces":
    {
        "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces"
    },
    "FirmwareVersion": "03.14.0200",
    "GraphicalConsole":
    {
        "ConnectTypesSupported": ["KVMIP"],
        "MaxConcurrentSessions": 4,
        "ServiceEnabled": true
```

```
},
"Id": "1",
"Links":
{
    "ManagerForChassis": [{"@odata.id": "/redfish/v1/Chassis/1"}],
    "ManagerForServers": [{"@odata.id": "/redfish/v1/Systems/1"}],
    "ManagerInChassis": [{"@odata.id": "/redfish/v1/Chassis/1"}]
},
"LldpService":
{
    "@odata.id": "/redfish/v1/Managers/1/LldpService"
},
"LogServices":
{
    "@odata.id": "/redfish/v1/Managers/1/LogServices"
},
"ManagerType": "BMC",
"Manufacturer": "ASPEED",
"Model": "2163162150",
"Name": "Manager",
"NetworkProtocol":
{
    "@odata.id": "/redfish/v1/Managers/1/NetworkProtocol"
},
"NtpService":
{
    "@odata.id": "/redfish/v1/Managers/1/NtpService"
},
 "Oem": {
     "DnsService": {
        "@odata.id": "/redfish/v1/Managers/1/DnsService"
   },
   "Public": {
       "FirewallService": {
           "@odata.id": "/redfish/v1/Managers/1/SecurityService"
       },
       "IfMatchEnabled": true
    }
},
"PowerState": "On",
"SerialConsole":
{
    "ConnectTypesSupported": ["IPMI"],
    "ServiceEnabled": false
```

```
    },
    "ServiceEntryPointUUID":  "6059463c-0000-1000-0000-202103230938",
    "SnmpService":
    {
        "@odata.id": "/redfish/v1/Managers/1/SnmpService"
    },
    "SmtpService": {
        "@odata.id": "/redfish/v1/Managers/1/SmtpService"
    },
    "Status":
    {
        "Health": "OK",
        "State": "Enabled"
    },
    "SyslogService":
    {
        "@odata.id": "/redfish/v1/Managers/1/SyslogService"
    },
    "UUID":  "6059463c-0000-1000-0000-202103230938",
    "VirtualMedia":
    {
        "@odata.id": "/redfish/v1/Managers/1/VirtualMedia"
    }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you modify information about the specified Manager resource, refer to Table 4-7.

Table 4-7 Output Descriptions for Modifying 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.

Field	Type	Description
FirmwareVersion	String	Firmware version of the Manager resource.
UUID	String	UUID 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. ● Time zone format, for example, +08:00. ● Time region format, for example, Asia/Shanghai and America/New_York.
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.
Links	Object	Links to the related resources.

4.4 Querying Information About the Syslog Configuration

Function

Query information about the Syslog configuration.

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

Description

For a description of the parameters for querying information about the Syslog configuration, refer to Table 4-8.

Table 4-8 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**.

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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#SyslogService.SyslogService",
    "@odata.etag": "W/\"1581179556\"",
    "@odata.id": "/redfish/v1/Managers/1/SyslogService",
    "@odata.type": "#SyslogService.v1_2_0.SyslogService",
    "Actions":
    {
        "#SyslogService.SubmitTestEvent":
        {
            "target": "/redfish/v1/Managers/1/SyslogService/Actions/SyslogService.
                       SubmitTestEvent"
         }
    },
    "Id": "SyslogService",
    "Name": "Syslog Service",
    "ServerIdentitySource": "HostName",
    "ServiceEnabled": true,
    "SyslogServers":
    [{
        "Address": "1.2.3.4",
        "Enabled": true,
        "LogType": ["SecurityLog", "OperationLog", "EventLog"],
        "MemberId": "0",
        "Port": 123
     },
```

```
    {
        "Address": "",
        "Enabled": false,
        "LogType": [],
        "MemberId": "1",
        "Port": 0
    },
    {
        "Address": "",
        "Enabled": false,
        "LogType": [],
        "MemberId": "2",
        "Port": 514
    },
    {
        "Address": "",
        "Enabled": false,
        "LogType": [],
        "MemberId": "3",
        "Port": 514
    }],
    "TransmissionProtocol": "UDP"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the Syslog configuration, refer to Table 4-9.

Table 4-9 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 node.
@odata.type	String	Type of Syslog resource.
Id	String	ID of the Syslog resource.
Name	String	Name of the Syslog resource.
ServiceEnabled	Boolean	Whether the Syslog service is enabled.
ServerIdentitySource	String	Host ID: ● Board serial number: BoardSN ● Asset tag: ProductAssetTag

Field	Type	Description
		• Host name: HostName
TransmissionProtocol	String	Transmission protocol. • UDP • TCP
SyslogServers	Object	Syslog servers.
Enabled	Boolean	Channel enabled.
Address	String	Server address.
MemberId	Member ID.	• 0 • 1 • 2 • 3
Port	Number	Server port number.
LogType	Array	Log type: • OperationLog • SecurityLog • EventLog
Actions	Object	Operations that can be performed on the Syslog resource.
SyslogService.SubmitTestEvent	Object	Submits a test event.

4.5 Configuring Information About the Syslog Server

Function

Configure information about the Syslog server.

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,
    "ServiceEnabled": ServiceEnabled,
    "SyslogServers":
    [{
        "Address": add_value,
        "Enabled": enabled_value,
        "LogType": logtype_value,
        "Port": port_value,
        "MemberId": MemberId},
        {"Address": add_value,
        "Enabled": enabled_value,
        "LogType": logtype_value,
        "Port": port_value,
        "MemberId": MemberId
    }]
}
```

Parameters

For a description of the parameters for configuring the Syslog server information, refer to Table 4-10.

Table 4-10 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 GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
ServerIdentitySource	Host ID.	Host ID: ● Board serial number: BoardSN ● Asset tag: ProductAssetTag ● Host name: HostName
TransmissionProtocol	Transmission protocol.	● UDP ● TCP
ServiceEnabled	Whether the Syslog service is enabled.	● true: enabled ● false: disabled
SyslogServers	Syslog servers.	-

Parameter	Description	Value
MemberId	Member ID.	-
enabled_value	Channel enabled.	-
add_value	Server address.	-
port_value	Server port number.	-
logtype_value	Log type.	• OperationLog • SecurityLog • EventLog

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
"ServerIdentitySource": "BoardSN",
"TransmissionProtocol": "UDP",
"SyslogServers":
[{
    "Address": "101.22.33.44",
    "Enabled": true,
    "LogType": ["EventLog","OperationLog","SecurityLog"],
    "Port": 222,
    "MemberId": "0"},
{
    "Address": "55.66.77.88",
    "Enabled": false,
    "LogType": ["EventLog","SecurityLog"],
    "Port": 333,
    "MemberId": "1"
}]
```

- Response Example:

```
{
```

```
"@odata.context": "/redfish/v1/$metadata#SyslogService.SyslogService",
"@odata.etag": "W/\"1655706366\"",
"@odata.id": "/redfish/v1/Managers/1/SyslogService",
"@odata.type": "#SyslogService.v1_2_0.SyslogService",
"Actions": {
    "#SyslogService.SubmitTestEvent": {
        "target": "/redfish/v1/Managers/1/SyslogService
                            /Actions/SyslogService.SubmitTestEvent"
    }
},
"Id": "SyslogService",
"Name": "Syslog Service",
"ServerIdentitySource": "BoardSN",
"ServiceEnabled": true,
"SyslogServers": [
    {
        "Address": "101.22.33.44",
        "Enabled": true,
        "LogType": [
            "SecurityLog",
            "OperationLog",
            "EventLog"
        ],
        "MemberId": "0",
        "Port": 222
    },
    {
        "Address": "",
        "Enabled": false,
        "LogType": [],
        "MemberId": "1",
        "Port": 514
    },
    {
        "Address": "",
        "Enabled": false,
        "LogType": [],
        "MemberId": "2",
        "Port": 514
    },
    {
        "Address": "",
        "Enabled": false,
        "LogType": [],
```

```
            "MemberId": "3",
            "Port": 514
        }
    ],
    "TransmissionProtocol": "UDP"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you configure information about the Syslog configuration, refer to Table 4-11.

Table 4-11 Output Descriptions for Configuring 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 node.
@odata.type	String	Type of Syslog resource.
Id	String	ID of the Syslog resource.
Name	String	Name of the Syslog resource.
ServiceEnabled	Boolean	Whether the Syslog service is enabled.
ServerIdentitySource	String	Host ID: ● Board serial number: BoardSN ● Asset tag: ProductAssetTag ● Host name: HostName
TransmissionProtocol	String	Transmission protocol. ● UDP ● TCP
SyslogServers	Object	Syslog servers.
Enabled	Boolean	Channel enabled.
Address	String	Server address.
MemberId	Member ID.	● 0 ● 1 ● 2 ● 3
Port	Number	Server port number.
LogType	Array	Log type: ● OperationLog

Field	Type	Description
		• SecurityLog • EventLog
Actions	Object	Operations that can be performed on the Syslog resource.
SyslogService.SubmitTestEvent	Object	Submits a test event.

4.6 Submitting a Syslog Test Log

Function

Submit a Syslog test log.

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.Subm itTestEvent
```

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/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.

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

Description

For a description of the parameters for querying information about the NtpService configuration resource, refer to Table 4-12.

Table 4-12 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1620317151\"",
    "@odata.id": "/redfish/v1/Managers/1/NtpService",
    "@odata.type": "#NtpService.v1_2_0.NtpService",
    "AlternateNtpServer": "128.0.0.63",
    "CurrentPollingInterval": 60,
    "Description": "NtpService",
    "ExtraNtpServer": "128.0.0.88",
    "MaxPollingInterval": 65535,
    "MinPollingInterval": 60,
    "NtpAddressOrigin": "static",
    "NtpSynResult": "fail",
    "PreferredNtpServer": "10.228.31.63",
    "ServerAuthenticationEnabled": false,
    "ServiceEnabled": true
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the NtpService configuration resource, refer to Table 4-13.

Table 4-13 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 node.

Field	Type	Description
@odata.type	String	Type of NTP resource.
ServiceEnabled	Boolean	NTP enabled.
AlternateNtpServer	String	Alternate NTP server address.
PreferredNtpServer	String	Preferred NTP server address.
ExtraNtpServer	String	Address of the extra NTP server.
MinPollingInterval	Number	Minimum synchronization interval.
MaxPollingInterval	Number	Maximum synchronization interval.
CurrentPollingInterval	Number	Current polling interval. Range: MinPollingInterval through MaxPollingInterval.
NtpAddressOrigin	String	NTP mode. ● static ● IPv4 ● IPv6
ServerAuthenticationEnabled	Boolean	Whether server security authentication is enabled: ● successful: Synchronization is successful. ● fail: Synchronization is unsuccessful. ● NULL: The configuration file is null. ● mode is not NTP: non-NTP mode. ● Get NTP result fail: The configuration file fails to be read.

4.8 Modifying Properties of the NTP Resource

Function

Modify properties of the NTP resource.

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
```

Note

If ETag verification is enabled in the environment, you need to add a "ETag: auth_value" line in the request header.

- Request Message Body:

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

Description

For a description of the parameters for modifying properties of the NTP resource, refer to Table 4-14.

Table 4-14 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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
ServiceEnabled	Boolean	Whether the NTP service is enabled: ● true ● false
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: MinPollingInterval through MaxPollingInterval.
NtpAddressOrigin	Address type.	● **ipv4**: The address is automatically obtained from the IPv4 protocol stack.

Parameter	Description	Value
		● **ipv6**: The address is automatically obtained from the IPv6 protocol stack. ● **static**: The address is set manually.

Usage Guidelines

Parameters of multiple services can be set at the same time. The ServiceEnabled field is required.

- When ServiceEnabled is set to true, NtpAddressOrigin is required. Default value is static.
- When ServiceEnabled is set to true and NtpAddressOrigin is set to static, PreferredNtpServer is required and CurrentPollingInterval is optional.

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
    "CurrentPollingInterval": 60,
    "NtpAddressOrigin": "ipv4",
    "ServiceEnabled": true
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#NtpService.NtpService",
    "@odata.etag": "W/\"1655706892\"",
    "@odata.id": "/redfish/v1/Managers/1/NtpService",
    "@odata.type": "#NtpService.v1_2_0.NtpService",
    "AlternateNtpServer": "time.nist.gov",
    "CurrentPollingInterval": 60,
    "Description": "NtpService",
    "ExtraNtpServer": "",
    "MaxPollingInterval": 65535,
    "MinPollingInterval": 60,
    "NtpSynResult": "mode is not NTP",
    "PreferredNtpServer": "pool.ntp.org",
```

```
    "ServerAuthenticationEnabled": false,
    "ServiceEnabled": false
}
```

- Status Code: 200

Output Description

For a description of the output returned when you modify information about the NtpService configuration resource, refer to Table 4-15.

Table 4-15 Output Descriptions for Modifying 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 node.
@odata.type	String	Type of NTP resource.
ServiceEnabled	Boolean	NTP enabled. ● true ● false
AlternateNtpServer	String	Alternate NTP server address.
PreferredNtpServer	String	Preferred NTP server address.
ExtraNtpServer	String	Address of the extra NTP server.
MinPollingInterval	Number	Minimum synchronization interval.
MaxPollingInterval	Number	Maximum synchronization interval.
CurrentPollingInterval	Number	Current polling interval. Range: MinPollingInterval through MaxPollingInterval.
NtpAddressOrigin	String	NTP mode. ● static ● IPv4 ● IPv6
ServerAuthenticationEnabled	Boolean	Whether the server authentication is enabled.
NtpSynResult	String	Whether server security authentication is enabled: ● successful: The synchronization is successful. ● fail: The synchronization is unsuccessful. ● NULL: The configuration file is empty. ● mode is not NTP: The mode is not NTP. ● get NTP result fail:The configuration file cannot be read.

4.9 Querying Information About the BMC Service

Function

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

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 4-16.

Table 4-16 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
```

```
    "@odata.context": "/redfish/v1/
         $metadata#ManagerNetworkProtocol.ManagerNetworkProtocol",
    "@odata.etag": "W/\"1597987265\"",
    "@odata.id": "/redfish/v1/Managers/1/NetworkProtocol",
    "@odata.type": "#ManagerNetworkProtocol.v1_2_0.ManagerNetworkProtocol",
    "HTTPS": {"Port": 443,"ProtocolEnabled": true},
    "HostName": "a",
    "IPMI": {"Port": 623,"ProtocolEnabled": true},
    "Id": "NetworkProtocol",
    "KVMIP": {"Port": 7855,"ProtocolEnabled": true},
    "Name": "Manager Network Protocol",
    "Oem":
    {
        "Public":
        {
            "VirtualMedia-CD":
            {
                "Instance": 1,
                "Port": 5124,
                "ProtocolEnabled": true
            },
            "VirtualMedia-HD":
            {
                "Instance": 1,
                "Port": 5127,
                "ProtocolEnabled": true
            }
        }
    },
    "SNMP":
    {
        "Port": 161,
        "ProtocolEnabled": true
    },
    "SSH":
    {
        "Port": 22,
        "ProtocolEnabled": true
    },
    "VirtualMedia": {"ProtocolEnabled": true}
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the BMC service, refer to Table 4-17.

Table 4-17 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.
Id	String	BMC network protocol resource ID.
Name	String	BMC network protocol resource name.
HostName	String	BMC host name.
HTTPS/KVMIP/SNMP/SSH/VirtualMedia/IPMI	Object	Service information supported by BMC.
ProtocolEnabled	Boolean	Service enabling status: ● true ● false
Port	Number	Service port number.
NotifyIPv6Scope	String	IPV6 multicast address range for SSDP service messages: ● Link: link local range. ● Site: Site local range. ● Organization: Organization local range.
NotifyMulticastIntervalSeconds	Number	SSDP service message multicast interval time.
Oem.Public	Customized field.	-
VirtualMedia-CD/VirtualMedia-HD/SSDP	Object	-
ProtocolEnabled	Boolean	Service enabling status: true/false

Field	Type	Description
Port	Number	Service port number.
Instance	Number	Number of instances.
NotifyEnabled	Boolean	Whether the SSDP service message multicast is enabled: • true • false

4.10 Modifying Information About a Specified BMC Service

Function

Modify the enabling status of a specified BMC service of a server.

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": notifymulticastintervalseconds_value,
    "NotifyIPv6Scope": notifyipv6scope_value
},
"Oem": {
    "Public":
    {
        "OEMServerType": {
            "Port": oem_port_value,
            "ProtocolEnabled": oem_protocolEnabled_value,
            "NotifyEnabled": oem_notifyEnabled_value
        }
    }
}
```

Parameters

For a description of the parameters for modifying information about the specified BMC service, refer to Table 4-18.

Table 4-18 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 `/redfish/v1/SessionService/Sessions`.
header_type	Format of the request message.	application/json
Service_type	Specified BMC services of the server.	• HTTPS • KVMIP • VirtualMedia • SSH • SNMP • SSDP
protocolenabled_value	Modifies the enabling status of the service.	Boolean: • true • false
port_value	Modifies the server port number.	Integer type: 1–65535.
notifymulticastintervalseconds_value	SSDP service message multicast interval time.	Number type: 0~1800
notifyipv6scope_value	IPV6 multicast address scope for SSDP service messages.	String type: • Link: Link local scope. • Site: Site local scope. • Organization: Organization local scope.
Oem.Public	Customized field.	-
OEMServerType	OEM service type to be set.	Modifiable service type: • VirtualMedia-CD • VirtualMedia-HD • SSDP
oem_notifyEnabled_value	Whether the SSDP service message multicast is enabled.	Boolean type: • true • false

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
    "KVMIP":
    {
        "Port": 7580,
        "ProtocolEnabled": true
    }
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/
         $metadata#ManagerNetworkProtocol.ManagerNetworkProtocol",
    "@odata.etag": "W/\"1597987448\"",
    "@odata.id": "/redfish/v1/Managers/1/NetworkProtocol",
    "@odata.type": "#ManagerNetworkProtocol.v1_2_0.ManagerNetworkProtocol",
    "HTTPS": {"Port": 443,"ProtocolEnabled": true},
    "HostName": "a",
    "IPMI": {"Port": 623,"ProtocolEnabled": true},
    "Id": "NetworkProtocol",
    "KVMIP": {"Port": 7580,"ProtocolEnabled": true},
    "Name": "Manager Network Protocol",
    "Oem":
    {
        "Public":
        {
            "VirtualMedia-CD": {"Instance": 1,"Port": 5124,"ProtocolEnabled": true},
            "VirtualMedia-HD": {"Instance": 1,"Port": 5127,"ProtocolEnabled": true}
        }
    },
    "SNMP": {"Port": 161,"ProtocolEnabled": true},
```

```
    "SSH": {"Port": 22, "ProtocolEnabled": true},
    "VirtualMedia": {"ProtocolEnabled": true}
}
```

- Status Code: 200

Output Description

For a description of the output returned when you modify information about the specified BMC service, refer to Table 4-19.

Table 4-19 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.
@odata.type	String	Type of BMC service resource collection.
Id	String	BMC network protocol resource ID.
Name	String	BMC network protocol resource name.
HTTPS/KVMIP/SNMP/SSH/VirtualMedia/IPMI	Object	Service information supported by BMC.
ProtocolEnabled	Boolean	Service enabling status: true/false
Port	Number	Service port number.
NotifyIPv6Scope	String	IPV6 multicast address scope for SSDP service messages: ● Link: Link local scope. ● Site: Site local scope. ● Organization: Organization local scope.
NotifyMulticastIntervalSecondsD	Number	SSDP service message multicast interval time.
Oem.Public	Customized field.	-
VirtualMedia-CD/VirtualMedia-HD/SSDP	Object	-

Field	Type	Description
ProtocolEnabled	Boolean	Service enabling status: true/ false
Port	Number	Service port number.
Instance	Number	Number of instances.
NotifyEnabled	Boolean	Whether the SSDP service message multicast is enabled: • true • false

4.11 Querying the Virtual Media Resource Collection

Function

Query the virtual media resource collection.

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

Description

For a description of the parameters for querying the virtual media resource collection, refer to Table 4-20.

Table 4-20 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	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

Usage Guidelines

In the response example, the media resource collection is displayed in Members, where the CD1 and USBStick1 resources can be queried and used only after the number of media resources is set to two.

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.etag": "W/\"1578381227\"",
    "@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": 2,
    "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 4-21.

Table 4-21 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 node.
@odata.type	String	Type of virtual media resource collection.
Description	String	Description
Members	Array	Virtual media resource list. CD1 and USBStick1 resources can be queried only when the number of entities is set to two.
@odata.id	String	Access path of the virtual media resource collection node.
Members@odata.count	Number	Number of virtual media resource members that can be connected currently.
Name	String	Name of the virtual media resource collection.

4.12 Querying a Virtual Media Resource

Function

Query a virtual media resource.

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

Description

For a description of the parameters for querying the virtual media resource, refer to Table 4-22.

Table 4-22 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	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
Media_type	Virtual media type.	Supported types: CD, CD1, USBStick, and USBStick1.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:


```
{
    "@odata.context": "/redfish/v1/$metadata#VirtualMedia.VirtualMedia",
    "@odata.etag": "W/\"1579167518\"",
    "@odata.id": "/redfish/v1/Managers/1/VirtualMedia/CD",
    "@odata.type": "#VirtualMedia.v1_2_0.VirtualMedia",
    "ConnectedVia": "NotConnected",
    "Description": "CD VirtualMedia",
    "Id": "CD",
    "Image": "",
    "ImageName": "",
    "Inserted": false,
    "MediaTypes": "",
    "Name": "VirtualMedia",
    "Oem": {
        "Public": {
            "Actions": {
                "#VirtualMedia.VmmControl": {
                    "@Redfish.ActionInfo":
```

```
                    "/redfish/v1/Managers/1/VirtualMedia/CD/VmmControlActionInfo",
                    "target":
                    "/redfish/v1/Managers/1/VirtualMedia/CD/Oem/VANTAGEO/Actions/
                        VirtualMedia.VmmControl"
                }
            }
        }
    },
    "TransferMethod": "",
    "TransferProtocolType": ""
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query the virtual media resource, refer to Table 4-23.

Table 4-23 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 node.
@odata.type	String	Type of virtual media resource.
Description	String	Description
Id	String	ID of the virtual media resource.
Name	String	Name of the virtual media resource.
MediaTypes	Object	Type of media: CD, CD1, USBStick, or USBStick1.
TransferProtocolType	String	Type of the transmission protocol: NFS/CIFS
TransferMethod	String	Transfer method: stream
Image	String	Image path.
ImageName	String	Image name.
ConnectedVia	String	Connection method.
Inserted	Boolean	Connection status: ● true: mounting (inserted) ● false: removed (removed)
Oem	Object	Customized properties of a specified session.

4.13 Connecting to the Virtual Media

Function

Connect to the virtual media.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/Managers/manager_id/VirtualMedia/Media_type/Oem/VANTAGEO/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
}
```

Description

For a description of the parameters for connecting the virtual media, refer to Table 4-24.

Table 4-24 Parameter Descriptions for Connecting 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.	Supported types: CD, CD1, USBStick, and USBStick1.
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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
Image_value	The type is string. The shared path is configured on the shared server. The maximum path length shall contain 256 characters. The format is as fol-	-

Parameter	Description	Value
	lows: *"Image":"protocol://server_ip/file_path/file_name"*.	
username_value	Username. This field is required when the CIFS protocol is used. Its maximum length is 32 characters.	The type is string. This field is not required when NFS is used as the transmission protocol.
password_value	Password. This field is required when the CIFS protocol is used. Its maximum length is 32 characters.	The type is string. This field is not required when NFS is used as the transmission protocol.
value	Virtual media operation type.	Connect: Connect to virtual media.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/VirtualMedia/CD/Oem/VANTAGEO/Actions/
VirtualMedia.Vmm- Control
```

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

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

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#VirtualMedia.VirtualMedia",
    "@odata.etag": "W/\"1593704686\"",
    "@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: 202

Output Description

For a description of the output returned when the virtual media is accessed, refer to Table 4-25.

Table 4-25 Output Descriptions for Connecting the Virtual Media

Field	Type	Description
@odata.context	String	OData description of the virtual media resource model.
@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 node.

4.14 Disconnecting the Virtual Media

Function

Disconnect the virtual media.

Syntax

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

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

- Request Message Body:

```
{
    "VmmControlType":value
}
```

Description

For the parameter descriptions for disconnecting the virtual media, refer to Table 4-26.

Table 4-26 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.	Supported types: CD, CD1, USBStick, and USBStick1.
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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
value	Disconnection.	Disconnect: Disconnecting the Virtual Media

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0= Content-Type:application/json
```

- Request Message Body:

```
{
    "VmmControlType":"Disconnect"
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#VirtualMedia.VirtualMedia",
    "@odata.etag": "W/\"1593704686\"",
    "@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: 202

Output Description

For a description of the output returned when the virtual media is disconnected, refer to Table 4-27.

Table 4-27 Output Descriptions for Disconnecting the Virtual Media

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

4.15 Querying Information About the LLDP Service Configuration Resource

Function

Query information about the LLDP service configuration resource.

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

Description

For a description of the parameters for querying information about the LLDP service configuration resource, refer to Table 4-28.

Table 4-28 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.
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 */redfish/v1/SessionService/Sessions*.

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": "W/\"1586863355\"",
    "@odata.id": "/redfish/v1/Managers/1/LldpService",
    "@odata.type": "#LldpService.v1_0_0.LldpService",
    "Description": "LLDP Service",
    "Id": "LldpService",
    "LldpEnabled": false,
    "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 4-29.

Table 4-29 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 node.
@odata.type	String	Type of LLDP resource.
Description	String	Description of the LLDP resource.
Id	String	ID of the BIOS resource.
Name	String	Name of the LLDP resource.
LldpEnabled	Boolean	Whether LLDP is enabled: ● true: enabled ● false: disabled
WorkMode	String	LLDP operation mode. ● TX: Only transmitting modes. ● TxRx: both transmitting and receiving modes. ● Rx: receiving mode. ● Disable: neither transmitting mode nor receiving mode.

4.16 Modifying Properties of the LLDP Service Resource

Function

Modify properties of the LLDP service resource.

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
}
```

Description

For a description of the parameters for modifying properties of the LLDP service resource, refer to Table 4-30.

Table 4-30 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**.
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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
enable_value	Whether LLDP is enabled.	• true: enabled • false: disabled
workmode_value	Operational mode of the LLDP resource.	• TX: only transmitting modes. • TxRx: both transmitting and receiving modes. • Rx: receiving mode. TxRx mode is the default mode used when LLDP is enabled. 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:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0= Content-Type:application/json
```

- Request Message Body:

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

- Response Example:

```
{
    "@odata.context":"/redfish/v1/$metadata#LldpService.LldpService",
    "@odata.etag": "W/\"1586863355\"",
    "@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 4-31.

Table 4-31 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 node.
@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: both transmitting and receiving ● Rx: receiving mode

4.17 Querying Information About the SNMP Resource

Function

Query information about the SNMP resource of a server.

Syntax

- Operation Type: GET

- URL: *https://device_ip/redfish/v1/Managers/manager_id/SnmpService*
- Request Header: None

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the SNMP resource, refer to Table 4-32.

Table 4-32 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#SnmpService.SnmpService",
    "@odata.etag": "W/\"946763130\"",
    "@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",
 "ReadOnlyCommunity": null,
 "ReadWriteCommunity": null,
 "SnmpTrapNotification":
 {
     "TrapServer":
     [{
         "MemberId": "0",
         "TrapServerAddress": "",
         "TrapServerPort": 162,
         "TrapV3User": "",
         "TrapVersion": "",
         "TrapServerEnable": true
    },
    {
         "MemberId": "1",
         "TrapServerAddress": "1.2.3.4",
         "TrapServerPort": 1,
         "TrapV3User": "",
         "TrapVersion": "V1".
         "TrapServerEnable": true
     },
     {
         "MemberId": "7",
         "TrapServerAddress": "2.2.2.2",
         "TrapServerPort": 65535,
         "TrapV3User": "",
         "TrapVersion": "V2C",
         "TrapServerEnable": true
     },
     {
         "MemberId": "14",
         "TrapServerAddress": "10.44.55.66",
         "TrapServerPort": 12222,
         "TrapV3User": "test_user",
         "TrapVersion": "V3",
         "TrapServerEnable": true
     }],
     "AlarmSeverity": "Critical",
     "TrapMode": "ModuleOIDMode",
     "TrapServer@odata.count": 4,
```

```
        "TrapVersion": "V2C",
        "snmpTrapCommunity": public,
        "TrapServerEnable": false
    },
    "SnmpV1V2Enable": false,
    "SnmpV3AuthUser":
    [{
        "snmpV3AuthProtocol": "md5",
        "snmpV3PrivProtocol": "des",
        "UserName": "root"
    },
    {
        "snmpV3AuthProtocol": "md5",
        "snmpV3PrivProtocol": "des",
        "UserName": "root_100"
    },
    {
        "snmpV3AuthProtocol": "sha",
        "snmpV3PrivProtocol": "aes",
        "UserName": "snmp_test"
    }],
    "SnmpV3AuthUser@odata.count": 3,
    "SnmpV3EngineID": "0x80000f3e034c09b4050022"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the SNMP resource, refer to Table 4-33.

Table 4-33 Output Descriptions for Querying Information About the SNMP Resource

Field	Type	Description
@odata.context	String	OData description of the SNMP resource model.
@odata.id	String	Access path of the SNMP resource node.
@odata.type	String	Type of SNMP resource.
Actions	Object	Operations that can be performed on the SNMP resource.
#SnmpService.SubmitTestEvent	Object	Submits an SNMP Trap Test Event.
Id	String	ID of the BIOS resource.

Field	Type	Description
Name	String	Name of the SNMP resource.
ReadOnlyCommunity	String	SNMP read-only community. Note: This property contains sensitive information and is displayed as null. The PATCH operation is available.
ReadWriteCommunity	String	SNMP readwrite community. Note: This property contains sensitive information and is displayed as null. The PATCH operation is available.
TrapVersion	String	SNMP global trap version number.
SnmpV3AuthUser	Array	• For administrators, this array lists all users with the SNMP permission. • For non-administrators, it is displayed as null.
UserName	String	Username with the SNMP permission.
SnmpV3AuthProtocol	String	SNMPv3 user authentication algorithm, including: • None • MD5 • SHA • SHA256 • SHA384 • SHA512
SnmpV3PrivProtocol	String	SNMPv3 encryption algorithm, including: • None • DES • AES • AES256
SnmpV3AuthUser@odata.count	Number	For non-administrators, the number of current users with the SNMP permission is displayed as null.
SnmpV3EngineID	String	SNMPv3 engine ID.
SnmpTrapNotification	Object	SNMP Trap properties.
TrapServer	Array	SNMP Trap server information.
MemberId	String	SNMP Trap group member number.
TrapVersion	String	SNMP Trap version number.

Field	Type	Description
TrapV3User	String	SNMPv3 username.
TrapServerAddress	String	SNMP Trap server address.
TrapServerPort	Number	SNMP Trap server port number.
TrapServerEnable	Boolean	Whether the SNMP trap for a single channel is enabled: ● true: enabled ● flase: disabled
TrapServer@odata.count	Number	Number of SNMP Trap servers.
snmpTrapCommunity	String	SNMP trap community name. This property contains sensitive information and is displayed as null. The PATCH operation is available.
AlarmSeverity	String	Alarm severity level: ● Critical ● Major ● Minor ● Normal
snmpTrapEnable	Boolean	Whether SNMP Trap is enabled: ● true: enables SNMP Trap. ● false: disables SNMP Trap.
TrapMode	String	● EventOIDMode event OID mode. ● ModuleOIDMode module OID mode.
SnmpV1V2Enable	Boolean	Whether Set and V2CGet in SNMP V1/V2C are enabled: ● True: enabled ● false: disabled

4.18 Modifying Properties of the SNMP Resource

Function

Modify properties of the SNMP resource.

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:

```
{
    "ReadWriteCommunity": ReadWriteCommunity,
    "ReadOnlyCommunity": ReadOnlyCommunity,
    "SnmpTrapNotification":
    {
        "snmpTrapCommunity": snmpTrapCommunity,
        "snmpTrapEnable": snmpTrapEnable,
        "AlarmSeverity": AlarmSeverity,
        "TrapVersion": TrapVersionGlobal,
        "TrapMode": TrapMode,
        "TrapServer":
        [{
            "MemberId": MemberId,
            "TrapVersion": TrapVersion,
            "TrapV3User": TrapV3User,
            "TrapServerAddress": TrapServerAddress,
            "TrapServerPort": TrapServerPort,
            "TrapServerEnable": TrapServerEnable
        }]
    }
}
```

Description

For a description of the parameters for modifying properties of the SNMP resource, refer to Table 4-34.

Table 4-34 Parameter Descriptions for Modifying Properties of 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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json

Parameter	Description	Value
TrapVersionGlobal	Global SNMP Trap version number.	Supported versions: ● V1 ● V2C ● V3
ReadWriteCommunity	Read-write community.	A string containing 1–18 characters, including digits, letters, and special characters. Allowed special characters: characters except for spaces, single quotes, and backslashes. The hashtag (#) symbol cannot be placed at the beginning. If double quotes are at both the beginning and end, that is, the outer double quotes enclose the inner double quotes, the server automatically removes all double quotes. To access the SNMP channel, use the field inside the two pairs of double quotes. If double quotation marks are at the beginning and in the middle, the configuration fails.
ReadOnlyCommunity	Read-Only Community.	A string containing 1–18 characters, including digits, letters, and special characters. Allowed special characters: visible characters except for spaces, single quotes, and backslashes. The hashtag (#) symbol cannot be placed at the beginning. If double quotes are at both the beginning and end, that is, the outer double quotes enclose the inner double quotes, the server automatically removes all double quotes. To access the SNMP channel, use the field inside the two pairs of double quotes. If double quotation marks are at the beginning and in the middle, the configuration fails.

Parameter	Description	Value
snmpTrapCommunity	SNMP trap community name.	String containing 1–18 characters, including digits, letters, and special characters. Special characters allowed: visible characters except for spaces, single quotes, angle brackets, and backslashes. The hashtag (#) symbol cannot be placed at the beginning.
snmpTrapEnable	Whether SNMP Trap is enabled.	• True: enabled. • false: disabled.
MemberId	Trap group member ID.	Range: 0–14.
TrapVersion	Trap version.	V1, V2C, and V3 are supported.
TrapV3User	V3 ussername.	Select a user from those with SNMP permissions as the SNMPv3 Trap user (it is valid when TrapVersion V3 is adopted).
TrapServerAddress	Server address.	IPv4 or IPv6 address or domain name. • A domain name ranges from 1 through 255 characters and cannot exceed six levels. The top-level domain name must be only letters and not exceed six characters. • If this field is "0.0.0.0", it means this Trap Server is deleted. • The Trap Server whose MemberId is "0" is the default Server and cannot be deleted. After the deletion operation is performed, the default configuration is restored.
TrapServerPort	Server port number.	Range: 1–65535.
TrapServerEnable	Whether a single SNMP trap channel is enabled. Optional.	• True (default): enabled. • false: disabled.
TrapMode	SNMP Trap mode.	• EventOIDMode event OID mode. • ModuleOIDMode module OID mode.
AlarmSeverity	Alarm severity level.	Alarm severity level: • Critical • Major • Minor • Normal

Parameter	Description	Value
SnmpV1V2Enable	Whether SNMP V1/V2C Set/ Get is enabled.	• True: enabled. • false: disabled.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
    "ReadOnlyCommunity": "testname1",
    "ReadWriteCommunity": "testname2",
    "TrapVersion": "V2C",
    "SnmpTrapNotification":
    {
        "snmpTrapCommunity": "testname3",
        "snmpTrapEnable": false,
        "TrapMode": "ModuleOIDMode",
        "TrapServer":
        [{
            "MemberId": "0",
            "TrapVersion": "V1",
            "TrapV3User": "",
            "TrapServerAddress": "10.10.10.10",
            "TrapServerPort": 162,
            "TrapServerEnable": true
        },
        {
            "MemberId": "14",
            "TrapVersion": "V3",
            "TrapV3User": "test_user",
            "TrapServerAddress": "10.10.10.11",
            "TrapServerPort": 163,
            "TrapServerEnable": true
        }]
```

```
    }
}
```

- Response Example: None
- Status Code: 204

Output Description

None

4.19 Submitting an SNMP Trap Test Event

Function

Submit an SNMP Trap test event.

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 the parameter descriptions for submitting an SNMP Trap test event, refer to Table 4-35.

Table 4-35 Parameter Descriptions for Submitting an SNMP Trap Test Event

Parameter	Description	Value
MemberId	ID of the Trap group member.	0–14, or 255. 255: submits a test event to all valid SNMP Trap servers.

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": 13
}
```

- Response Example: None
- Status Code: 204

Output Description

None

4.20 Querying the Management Interface Collection of the BMC

Function

Query the current management interface resource collection supported by the BMC of a server.

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

Description

For a description of the parameters for querying the management interface resource collection, refer to Table 4-36.

Table 4-36 Parameter Descriptions for Querying the Collection of Management Interface Resources of 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**.

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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#EthernetInterfaceCollection.
                     EthernetInterfaceCollection",
  "@odata.etag": "W/\"946772855\"",
  "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces",
  "@odata.type": "#EthernetInterfaceCollection.EthernetInterfaceCollection",
  "Description": "Collection of Ethernet Interfaces for this Manager",
  "Members": [
      {
         "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces/eth0"
      },
      {
         "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces/eth1"
      },
      {
         "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces/usb0"
      }
   ],
  "Members@odata.count": 3,
  "Name": "Ethernet Network Interface Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the management interface resource collection of the BMC, refer to Table 4-37.

Table 4-37 Output Descriptions for Querying the Collection of Management Interface Resources of the BMC

Field	Type	Description
@odata.context	String	OData description of the management interface collection model of the BMC.
@odata.id	String	Access path of the management interface collection node of the BMC.
@odata.type	String	Type of management interface resource collection of the BMC. CPU/Memory/Disk/PCIe(NIC)/PCIe(GPU)/PCIe(RAID)/PSU/Fan/NIC without RAID.
Name	String	Name of the management interface resource collection of the BMC.
Members@odata.count	Number	Number of resources in the management interface resource collection of the BMC.
Members	Array	List of resources in the management interface resource collection of the BMC.
@odata.id	String	Access path of a single management interface resource node of the BMC.

4.21 Querying Information About a Specified Management Interface Resource of the BMC

Function

Query information about a specified management interface resource of the BMC.

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

Description

For a description of the parameters for querying information about the specified management interface resource of the BMC, refer to Table 4-38.

Table 4-38 Parameter Descriptions for Querying Information About the Specified Management Interface Resource of 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**.
id	ID of the specified management interface resource of the BMC.	-
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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/EthernetInterfaces/eth0
```

- Request Header:

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

- Request Message Body: None
- Response Example (Management Interface of the BMC):


```
{
    "@odata.context": "/redfish/v1/$metadata#EthernetInterface.EthernetInterface",
    "@odata.etag": "W/\"946773488\"",
    "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces/eth0",
    "@odata.type": "#EthernetInterface.v1_4_0.EthernetInterface",
    "AutoNeg": true,
    "Description": "Ethernet Interface eth0",
    "FullDuplex": true,
    "HostName": "iSAC4C09B4052911",
    "IPv4Addresses":
    [{
        "Address": "0.0.0.0",
        "AddressOrigin": "DHCP",
```

```
        "Gateway": "0.0.0.0",
        "SubnetMask": "0.0.0.0"
    }],
    "IPv6Addresses":
    [{
        "Address": "::",
        "AddressOrigin": "LinkLocal",
        "PrefixLength": 0
    },
    {
        "Address": "1::2",
        "AddressOrigin": "Static",
        "PrefixLength": 64
    }],
    "IPv6DefaultGateway": "1::222",
    "IPv6StaticAddresses":
    [{
        "Address": "1::2",
        "PrefixLength": 64
    }],
    "Id": "eth0",
    "InterfaceEnabled": true,
    "MTUSize": 1500,
    "Name": "eth0",
    "NameServers": ["2.3.5.5", "6.7.8.9", ""],
    "Oem":
    {
        "Public":
        {
            "DNSDhcpEnabled": false,
            "DNSServiceEnabled": true,
            "IPStacks": "IPv6",
            "PatchInProgress": false
        }
    },
    "PermanentMACAddress": "4C:09:B4:05:29:11",
    "SpeedMbps": 1000,
    Status": { "Health": "OK", "State": "Enabled"},
    "VLAN": {"VLANEnable": false, "VLANId": 0}
}
```


- Response Example (usb0 virtual network interface):


```
{
    "@odata.context": "/redfish/v1/$metadata#EthernetInterface.EthernetInterface",
```

```
"@odata.etag": "W/\"946701411\"",
"@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces/usb0",
"@odata.type": "#EthernetInterface.v1_4_0.EthernetInterface",
"AutoNeg": null,
"Description": "Ethernet Interface usb0",
"FullDuplex": null,
"HostName": "iSAC4C09B4062809",
"IPv4Addresses": [
    {
        "Address": "169.254.0.19",
        "AddressOrigin": "Static",
        "Gateway": "0.0.0.0",
        "SubnetMask": "255.255.255.0"
    }
],
"IPv6Addresses": [
    {
        "Address": "::",
        "AddressOrigin": "LinkLocal",
        "PrefixLength": 0
    },
    {
        "Address": "::",
        "AddressOrigin": "DHCPv6",
        "PrefixLength": 0
    }
],
"IPv6DefaultGateway": "::",
"IPv6StaticAddresses": [
    {
        "Address": "::",
        "PrefixLength": 0
    }
],
"Id": "usb0",
"InterfaceEnabled": true,
"MTUSize": 1500,
"Members": [
    {
       "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces/usb0/Oem/VANTAGEO/NAT"
    }
],
"Members@odata.count": 1,
"Name": "usb0",
```

```
    "NameServers": [
        "",
        "",
        ""
    ],
    "Oem": {
        "Public": {
            "DNSDhcpEnabled": null,
            "DNSServiceEnabled": null,
            "IPStacks": null,
            "PatchInProgress": null
        }
    },
    "PermanentMACAddress": "E2:33:81:6D:CD:0F",
    "MACAddress": "E2:33:81:6D:CD:0F",
    "SpeedMbps": null,
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "VLAN": {
        "VLANEnable": null,
        "VLANId": null
    }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified management interface resource of the BMC, refer to Table 4-39 and Table 4-40.

Table 4-39 Output Descriptions for Querying Information About the Specified Management Interface Resource of the BMC—1

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

Field	Type	Description
Id	String	ID of the specified management interface resource of the BMC.
Name	String	Name of the specified management interface resource of the BMC.
Description	String	Description of the specified management interface resource of the BMC.
AutoNeg	Boolean	Whether auto-negotiation is enabled.
FullDuplex	Boolean	Whether full-duplex mode is used.
HostName	String	DNS hostname, which does not contain any domain information.
PermanentMACAddress	String	Permanent MAC address allocated to the interface.
MTUSize	Number	MTU (in bytes) configured on the current interface.
SpeedMbps	Number	Current rate (in Mbps).
InterfaceEnabled	Boolean	Whether the interface is enabled.
IPv4Addresses	Array	IPv4 information object.
Address	String	IPv4 address.
AddressOrigin	String	Origin of the IPv4 address.
Gateway	String	IPv4 gateway address.
SubnetMask	String	IPv4 subnet mask.
IPv6Addresses	Array	IPv6 information object.
Address	String	IPv6 address.
AddressOrigin	String	Origin of the IPv6 address.
PrefixLength	Number	Prefix length of the IPv6 address.
IPv6StaticAddresses	Array	Static IPv6 information object.
Address	String	Static IPv6 address.
PrefixLength	Number	Prefix length of the static IPv6 address.
IPv6DefaultGateway	String	Default IPv6 gateway.
NameServers	Array	Domain name server list.
VLAN	Object	VLAN information object.
VLANEnable	Boolean	VLAN enabling switch.

Field	Type	Description
VLANId	Number	Configured VLAN ID.
Oem.Public	Object	OEM object.
DNSDhcpEnabled	Boolean	Manual or automatic DNS switch: ● true: automatic ● false: manual
DNSServiceEnabled	Boolean	Whether the DNS service is enabled.
IPStacks	String	Whether to enable IPv4/IPv6: ● null: interface not enabled ● IPv4: IPv4 enabled only ● IPv6: IPv6 enabled only ● IPv4AndIPv6: IPv4 and IPv6 both enabled
PatchInProgress	Boolean	Configuration validity flag: ● true: being configured ● false: configured completely and applied successfully.

Table 4-40 Output Descriptions for Querying Information About the Specified Management Interface Resource of the BMC—2

Field	Type	Description
@odata.context	String	OData description of the model of the specified management interface resource of the BMC.
@odata.id	String	Access path of the node of the specified management interface resource of the BMC.
@odata.type	String	Type of the specified management interface resource of the BMC.
Id	String	ID of the specified management interface resource of the BMC.
Name	String	Name of the specified management interface resource of the BMC.
IPv4Address	Object	IPv4 address object
Address	String	IPv4 address of usb0.
SubnetMask	String	IPv4 address of usb0.
MACAddress	String	MAC address.
InterfaceEnabled	Boolean	Whether usb0 is enabled: ● true: enabled. ● false: disabled.

Field	Type	Description
Status	String	Interface status.
Members@odata.count	Number	Number of NAT resources.
Members	Array	NAT resource list.

4.22 Modifying a Specified Management Interface Resource of the BMC

Function

Modify information about a specified management interface resource of the BMC.

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:
  - → Enable the interface:

```
{
    "InterfaceEnabled": interface_enabled
}
```

  - → Enable IPv4/IPv6:

```
{
    "Oem":
    {
        "Public": { "IPStacks": ip_stack}
    }
}
```

  - → Configure IPv4 information:

```
{
    "IPv4Addresses":
    [{
        "Address": ipv4_address,
        "AddressOrigin": ipv4_address_origin,
        "SubnetMask": ipv4_subnet_mask,
```

```
        "Gateway": ipv4_gateway
    }]
}
```

→ Configure IPv6 information:

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

→ Configure the static IPv6 information:

```
{
    "IPv6StaticAddresses":
    [{
        "Address": ipv6_address,
        "PrefixLength": ipv6_prefix
    }]
    "IPv6DefaultGateway": Gw_value
}
```

→ Configure the VLAN information:

```
{
    "VLAN":
    {
        "VLANEnable": vlan_enable,
        "VLANId": vlan_id
    }
}
```

→ Configure the HostName information:

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

→ Configure the NameServers information:

```
{
    "NameServers": [nameserver, nameserver, nameserver]
}
```

→ Configure the usb0 virtual network interface:

```
{
    "InterfaceEnabled": enabled,
    "IPv4Addresses": {
       "Address": "address",
       "SubnetMask": "netmask"
    }
}
```

Description

For a description of the parameters for modifying the specified management interface resource of the BMC, refer to Table 4-41.

Table 4-41 Parameter Descriptions for Modifying the Specified Management Interface Resource of the BMC

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
interface_enabled	Whether to enable the interface.	• true: enables the interface. • false: disables the interface.
ip_stack	Whether to enable IPv4/IPv6.	• "IPv4": enables IPv4 only. • "IPv6": enables IPv6 only. • "IPv4AndIPv6": enables both IPv4 and IPv6.
ipv4_address	IPv4 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 IPv6 address.	• "Static": configures a static IPv6 address. • "DHCPv6": assigns the address through DHCP.

Parameter	Description	Value
ipv6_prefix	Prefix length of the IPv6 address.	Integer type, range: 1–128.
Gw_value	Default IPv6 gateway.	Character string, in IPv6 format.
vlan_enable	Whether to enable the VLAN.	● true: enables the VLAN. ● false: disables the VLAN.
hostname	Hostname.	● The hostname cannot exceed 63 characters. ● The hostname can contain only alphabetic characters (A through Z), numeric characters (0 through 9), and hyphens (-). ● The hostname cannot contain blank characters including spaces. ● The hostname is not case-sensitive. ● The first character of the hostname must be a letter, and the last character cannot be a hyphen.
vlan_id	VLAN ID.	Integer type, range: 1–4094.
nameserver	Domain name server.	String, valid IPv4 or IPv6 address.
enabled	Whether the virtual network interface is enabled.	String. Value: true or false.
address	IPv4 address.	String, valid IPv4 address.
netmask	IPv4 subnet mask.	String, valid IPv4 address.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Managers/1/EthernetInterfaces/eth0
```

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
    "IPv4Addresses":
```

```
    [{
        "Address": "128.0.0.15",
        "AddressOrigin": "Static", "Gateway": "128.0.0.1",
        "SubnetMask": "255.255.255.0"
    }],
    "IPv6Addresses":
    [{
        "Address": "1::2",
        "AddressOrigin": "Static",
        "PrefixLength": 64
    }],
    "IPv6DefaultGateway": "1::100",
    "InterfaceEnabled": true,
    "NameServers": ["1.2.3.4", "5.6.7.8", ""],
    "Oem":
    {
        "Public": {"IPStacks": "IPv4AndIPv6"}
    }
}
```


- Response Example:


```
{
        "@odata.context": "/redfish/v1/$metadata#EthernetInterface.EthernetInterface",
    "@odata.etag": "W/\"946773488\"",
    "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces/eth0",
    "@odata.type": "#EthernetInterface.v1_4_0.EthernetInterface",
    "AutoNeg": true,
    "Description": "Ethernet Interface eth0",
    "FullDuplex": true,
    "HostName": "iSAC4C09B4052911",
    "IPv4Addresses": [{
        "Address": "0.0.0.0",
        "AddressOrigin": "DHCP",
        "Gateway": "0.0.0.0",
        "SubnetMask": "0.0.0.0"
    }],
    "IPv6Addresses": [{
        "Address": "::",
        "AddressOrigin": "LinkLocal",
        "PrefixLength": 0
    }, {
        "Address": "1::2",
        "AddressOrigin": "Static",
        "PrefixLength": 64
```

```
    }],
    "IPv6DefaultGateway": "1::222",
    "IPv6StaticAddresses": [{
        "Address": "1::2",
        "PrefixLength": 64
    }],
    "Id": "eth0",
    "InterfaceEnabled": true,
    "MTUSize": 1500,
    "Name": "eth0",
    "NameServers": [
        "2.3.5.5", "6.7.8.9", ""
    ],
    "Oem": {
        "Public": {
            "DNSDhcpEnabled": false,
            "DNSServiceEnabled": true,
            "IPStacks": "IPv6",
            "PatchInProgress": false
        }
    },
    "PermanentMACAddress": "4C:09:B4:05:29:11",
    "SpeedMbps": 1000,
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "VLAN": {
        "VLANEnable": false,
        "VLANId": 0
    }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you modify the specified BMC management interface resource, refer to Table 4-42.

Table 4-42 Output Descriptions for Modifying Information About the Specified BMC Management Interface Resource

Field	Type	Description
@odata.context	Character string	OData description of the specified BMC management interface resource model.

Field	Type	Description
@odata.id	Character string	Access path of the specified BMC management interface resource node.
@odata.type	Character string	Type of the specified BMC management interface resource.
Id	Character string	ID of the specified BMC management interface resource.
Name	Character string	Name of the specified BMC management interface resource.
Description	Character string	Description of the specified BMC management interface resource.
AutoNeg	Boolean	Whether auto-negotiation is enabled.
FullDuplex	Boolean	Whether full-duplex mode is used.
HostName	Character string	DNS hostname, which does not contain any domain information.
PermanentMACAddress	Character string	Permanent MAC address assigned to the interface.
MTUSize	Number	MTU (in bytes) configured on the current interface.
SpeedMbps	Number	Current rate (in Mbps).
InterfaceEnabled	Boolean	Whether the interface is enabled.
IPv4Addresses	Array	IPv4 information object.
Address	Character string	IPv4 address.
AddressOrigin	Character string	Source of the IPv4 address.
Gateway	Character string	IPv4 gateway address.
SubnetMask	Character string	IPv4 subnet mask.
IPv6Addresses	Array	IPv6 information object.
Address	Character string	IPv6 address.
AddressOrigin	Character string	Source of the IPv6 address.
PrefixLength	Number	Prefix length of the IPv6 address.
IPv6StaticAddresses	Array	Static IPv6 information object.
Address	Character string	Static IPv6 address.
PrefixLength	Number	Prefix length of the static IPv6 address.
IPv6DefaultGateway	Character string	Default IPv6 gateway.

Field	Type	Description
NameServers	Array	Domain name server list.
VLAN	Object	VLAN information object.
VLANEnable	Boolean	Whether VLAN is enabled.
VLANId	Number	Configured VLAN ID.
Oem.Public	Object	OEM object.
DNSDhcpEnabled	Boolean	Whether DNS DHCP is enabled: ● true: automatic ● false: manual
DNSServiceEnabled	Boolean	Whether the DNS service is enabled.
IPStacks	Character string	Whether IPv4 and IPv6 are enabled: ● null: interface not enabled ● IPv4: IPv4 enabled only ● IPv6: IPv6 enabled only ● IPv4AndIPv6: IPv4 and IPv6 both enabled
PatchInProgress	Boolean	Configuration validity flag: ● true: being configured ● false: configured completely and applied successfully.

4.23 Querying the KVM Service Resource

Function

Query the KVM service resource of a server.

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

Description

For a description of the parameters for querying the KVM service resource, refer to Table 4-43.

Table 4-43 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1592392472\"",
    "@odata.id": "/redfish/v1/Managers/1/KvmService",
    "@odata.type": "#KvmService.v1_0_0.KvmService",
    "ActivatedSessionsType": "Private",
    "AutoScreenCapEnable": true,
    "EncryptionEnabled": true,
    "KvmUrl": "https://192.168.5.7/viewer.html?&token=omS8pwLE3aesgDwp",
    "MaximumNumberOfSessions": 4,
    "NumberOfActivatedSessions": 0,
    "SessionTimeoutMinutes": 5
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the KVM service resource, refer to Table 4-44.

Table 4-44 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 service resource node.
@odata.type	String	Type of KVM service resource.
MaximumNumberOfSessions	Number	Maximum number of KVM sessions.
KvmUrl	String	URL for logging in to the KVM. When you log in through this URL, the Web session is automatically logged out.
NumberOfActivatedSessions	Number	Number of current KVM sessions.
ActivatedSessionsType	String	Type of KVM session: ● "Shared": shared ● "Private": exclusive ● null: no session
AutoScreenCapEnable	Boolean	Whether automatic screen capture is enabled: ● true ● false
EncryptionEnabled	Boolean	Whether KVM encryption is enabled: ● true ● false
SessionTimeoutMinutes	Number	Session timeout minutes, range: 5–60 minutes.

4.24 Modifying Information About the KVM Resource

Function

Modify information about the KVM resource.

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,
    "AutoScreenCapEnable":AutoScreenCapEnable_value
}
```

Parameters

For a description of the parameters for modifying the KVM resource, refer to Table 4-45.

Table 4-45 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 GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
EncryptionEnabled_value	Whether KVM encryption is enabled.	• true: enabled • false: disabled
SessionTimeoutMinutes_value	Session timeout minutes.	Session timeout minutes, range: 5–60 minutes.
AutoScreenCapEnable_value	Whether automatic screen capture is enabled.	• true: Automatic screen capture is enabled. • false: Automatic screen capture is disabled.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

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

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#KvmService.KvmService",
    "@odata.etag": "W/\"1592392472\"",
    "@odata.id": "/redfish/v1/Managers/1/KvmService",
    "@odata.type": "#KvmService.v1_0_0.KvmService",
    "ActivatedSessionsType": "Private",
    "AutoScreenCapEnable": true,
    "EncryptionEnabled": true,
    "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 4-46.

Table 4-46 Output Descriptions for Modifying Information About the KVM Resource

Field	Type	Description
@odata.context	String	OData description of the KVM resource model.
@odata.id	String	Access path of the KVM resource.
@odata.type	String	Type of KVM resource.
MaximumNumberOfSessions	Number	Maximum number of KVM sessions.
NumberOfActivatedSessions	Number	Number of current KVM sessions.
ActivatedSessionsType	String	Type of KVM session: ● "Shared": shared ● "Private": exclusive ● null: no session
EncryptionEnabled	Boolean	Whether KVM encryption is enabled: ● true ● false

Field	Type	Description
SessionTimeoutMinutes	Number	Session timeout minutes, range: 5–60 minutes.

4.25 Changing the BMC Firmware Version

Function

Change the BMC firmware version.

Syntax

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

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

- Request Message Body:

```
{
    "RollBackType": value
}
```

Parameters

For the parameter descriptions for changing the BMC firmware version, refer to Table 4-47.

Table 4-47 Parameter Descriptions for Changing the BMC Firmware Version

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
value	Operation Type	RollBack: switching among BMC versions

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
    "RollBackType":"RollBack"
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1596373630\"",
    "@odata.id": "/redfish/v1/Managers/1/Actions/Manager.RollBack",
    "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"
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you change the BMC firmware version, refer to Table 4-48.

Table 4-48 Output Descriptions for Changing the BMC Firmware Version

Field	Type	Description
code	String	String indicating the specified message ID in the message registry.
message	String	The readable error message corresponding to the one 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 levels supported by the Redfish include: ● OK ● Warning ● Critical
Resolution	String	Solution.

4.26 Importing a Configuration File

Function

Import BMC/BIOS configurations to the server.

Syntax

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

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

- Request Message Body:

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

- Request Message (Form):

```
<form enctype="multipart/form-data" action=" https://device_ip/redfish/v1/manager_id/
                Actions/Oem/VANTAGEO/Manager.ImportConfiguration" method="POST">
    <input name="image_file" type="file">
    <input name="Type" type="type">
</form>
```

Description

For a description of the parameters for importing configurations, refer to Table 4-49.

Table 4-49 Parameter Descriptions for Configuration Import

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
type_value	Operation type.	• BMC • BIOS • BMC_BIOS • PCIEDEV
content_value	File path.	Configuration file import path. The file name must start with "ID_".
image_file	File	The Select the file to be imported. The file name must start with "ID_".

Usage Guidelines

None

Example

- Request Example:

```
POST https://deviceip/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.ImportConfiguration
```

- Request Header:

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

- Request Message Body:

```
{
   "Type":"BMC",
   "Content":"tftp://10.10.10.191/ID_config.tar.gz"
}
```

- Request Message (Form):

```
<form enctype="multipart/form-data" action=" https://device_ip/redfish/v1/manager_id/
                Actions/Oem/VANTAGEO/Manager.ImportConfiguration" method="POST">
    <input name="image_file" type="bmc.tar.gz">
    <input name="Type" type="BMC">
</form>
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1596373630\"",
    "@odata.id": "/redfish/v1/Managers/1/Actions/Manager.ImportConfiguration,
    "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"
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you import configurations, refer to Table 4-50.

Table 4-50 Output Descriptions for Configuration Import

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	The readable error message corresponding to the one in the message registry.

Field	Type	Description
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Detailed information.
MessageArgs	Array	Message arguments.
Severity	String	Severity levels supported by the Redfish interface. ● OK ● Warning ● Critical
Resolution	String	Solution.

4.27 Exporting Configurations

Function

Export BMC/BIOS configurations.

Syntax

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

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

- Request Message Body:

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

- Request Message (Form):

```
<form enctype="multipart/form-data" action=" https://device_ip/redfish/v1/manager_id/
                Actions/Oem/VANTAGEO/Manager.ExportConfiguration" method="POST">
<input name="Type" type="type">
</form>
```

Description

For a description of the parameters for exporting configurations, refer to Table 4-51.

Table 4-51 Parameter Descriptions for Configuration Export

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
type_value	Operation type.	BMC/BIOS
content_value	File path.	Configuration file export path.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
    "Type":"BMC",
    "Content":"tftp://10.10.10.191/ID_config.tar.gz"
}
```

- Request Message (Form):

```
<form enctype="multipart/form-data" action=" https://device_ip/redfish/v1/manager_id
            /Actions/Oem/VANTAGEO/Manager.ExportConfiguration"  method="POST">
<input name="Type" type="BMC">
</form>
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1596373630\"",
    "@odata.id": "/redfish/v1/Managers/1/Actions/Manager.ExportConfiguration",
    "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 Form Example: None
- Status Code: 200

Output Description

For a description of the output returned when you export configurations, refer to Table 4-52.

Table 4-52 Output Descriptions for Configuration Export

Field	Type	Description
code	String	String indicating the specified message ID in the message registry.
message	String	The readable error message corresponding to the one in the message registry.
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Detailed information.
MessageArgs	Array	Message arguments.
Severity	String	Severity levels supported by the Redfish interface. ● OK ● Warning

Field	Type	Description
		• Critical
Resolution	String	Solution.

4.28 Validating Configurations

Function

Validates BMC/BIOS configurations.

Syntax

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

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

- Request Message Body:

```
{
    "EffectType:type_value
}
```

Description

For a description of the parameters for validating configurations, refer to Table 4-53.

Table 4-53 Parameter Descriptions for Validating Configurations

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
type_value	Operation type.	BMC/BIOS

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
    "RollBackType":"BMC"
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1596373630\"",
    "@odata.id": "/redfish/v1/Managers/1/Actions/Manager.EffectFactory",
    "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"
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you change the BMC firmware version, refer to Table 4-54.

Table 4-54 Output Descriptions for Changing the BMC Firmware Version

Field	Type	Description
code	String	String indicating the specified message ID in the message registry.
message	String	The readable error message corresponding to the one in the message registry.
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Detailed information.
MessageArgs	Array	Message arguments.
Severity	String	Severity levels supported by the Redfish interface. ● OK ● Warning ● Critical
Resolution	String	Solution.

4.29 Restarting the BMC

Function

Restart the BMC of the server.

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
}
```

Description

For a description of the parameters for restarting the BMC, refer to Table 4-55.

Table 4-55 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 */redfish/v1/SessionService/Sessions*.
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:

```
{
    "RollBackType":"ForceRestart"
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1596373630\"",
    "@odata.id": "/redfish/v1/Managers/1/Actions/Manager.Reset",
    "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"
    }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you restart the BMC, refer to Table 4-56.

Table 4-56 Output Descriptions for Restarting the BMC

Field	Type	Description
code	String	String indicating the specified message ID in the message registry.
message	String	The readable error message corresponding to the one in the message registry.
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Detailed information.
MessageArgs	Array	Message arguments.
Severity	String	Severity levels supported by the Redfish interface. ● OK ● Warning ● Critical
Resolution	String	Solution.

4.30 Querying Information About the Log Service Resource Collection

Function

Query information about the log service resource collection of a server.

Syntax

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

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

- Request Message Body: None

Description

For a description of parameters for querying information about the log service resource collection, refer to Table 4-57.

Table 4-57 Parameter Descriptions for Querying Information About the Log Service 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#LogServiceCollection.LogServiceCollection",
    "@odata.etag": "W/\"1642939184\"",
    "@odata.id": "/redfish/v1/Managers/Self/LogServices",
    "@odata.type": "#LogServiceCollection.LogServiceCollection",
```

```
    "Description": "Collection of Log Services for this System",
    "Members": [
    {
        "@odata.id": "/redfish/v1/Managers/1/LogServices/SEL"
    }
],
    "Members@odata.count": 1,
    "Name": "Log Service Collection"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the log service resource collection, refer to Table 4-58.

Table 4-58 Output Descriptions for Querying Information About the Log Service Resource Collection

Field	Type	Description
@odata.context	String	OData description of the log service resource collection model.
@odata.id	String	Access path of the log service resource collection node.
@odata.type	String	Type of log service resource collection.
Name	String	Name of the log service resource collection.
Members@odata.count	Number	Number of current log service resources.
Members	Array	Log service resource list.
@odata.id	String	Access path of a log service resource node.

4.31 Querying Information About a Specified Log Service Resource

Function

Query information about the log service resource collection of a server.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Managers/manager_id/LogServices/SEL*

- Request Header:

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

- Request Message Body: None

Description

For a description of parameters for querying information about the specified log service resource, refer to Table 4-59.

Table 4-59 Parameter Descriptions for Querying Information About the Specified 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**.
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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#LogService.LogService",
    "@odata.etag": "W/\"1643093744\"",
    "@odata.id": "/redfish/v1/Managers/1/LogServices/SEL",
    "@odata.type": "#LogService.v1_1_0.LogService",
    "Entries":
    {
        "@odata.id": "/redfish/v1/Managers/1/LogServices/SEL/Entries"
    }
```

```
    "MaxNumberOfRecords": 200
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified log service resource, refer to Table 4-60.

Table 4-60 Output Descriptions for Querying Information About the Specified Log Service Resource

Field	Type	Description
@odata.context	String	OData description of the specified log service resource model.
@odata.id	String	Access path of the specified log service resource node.
@odata.type	String	Type of the specified log service resource.
Entries	Object	Access path of the specified log service resource node.
MaxNumberOfRecords	String	Maximum number of log records of the specified log service resource.

4.32 Querying Information About the SEL Log Service Resource Collection

Function

Query information about the SEL log service resource collection of a server.

Syntax

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

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the SEL log service resource collection, refer to Table 4-61.

Table 4-61 Parameter Descriptions for Querying Information About the SEL Log Service 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#LogEntryCollection.LogEntryCollection",
    "@odata.etag": "W/\"1642864805\"",
    "@odata.id": "/redfish/v1/Managers/Self/LogServices/SEL/Entries",
    "@odata.type": "#LogEntryCollection.LogEntryCollection",
    "Description": "Collection of entries for this log service",
    "Members":
    [{
        "@odata.id": "/redfish/v1/Managers/1/LogServices/SEL/Entries/35"
    },
    {
        "@odata.id": "/redfish/v1/Managers/1/LogServices/SEL/Entries/36"
    },
    ],
    "Members@odata.count": 2,
    "Name": "Log Service Entries Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the SEL log service resource collection, refer to Table 4-62.

Table 4-62 Output Descriptions for Querying Information About the SEL Log Service Resource Collection

Field	Type	Description
@odata.context	String	OData description of the SEL log service resource collection model.
@odata.id	String	Access path of the SEL log service resource collection node.
@odata.type	String	Type of SEL log service resource collection.
Name	String	Name of the SEL log service resource collection.
Members@odata.count	Number	Number of members in the SEL log service resource collection.
Members	Array	Member list of the SEL log service resource collection.

4.33 Querying Information About the SEL Log Service Resource Collection by Specifying a Parameter

Function

Query information about the SEL log service resource collection of a server by specifying a parameter as the query condition.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Managers/manager_id/LogServices/SEL/Entries?$skip=a*
- Request Header:

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the SEL log service resource collection by specifying a parameter as the query condition, refer to Table 4-63.

Table 4-63 Parameter Descriptions for Querying Information About the SEL Log Service Resource Collection by Specifying a Condition

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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://deviceip/redfish/v1/Managers/1/LogServices/SEL/Entries?$skip=100
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#LogEntryCollection.LogEntryCollection",
    "@odata.etag": "W/\"1642864805\"",
    "@odata.id": "/redfish/v1/Managers/Self/LogServices/SEL/Entries",
    "@odata.type": "#LogEntryCollection.LogEntryCollection",
    "Description": "Collection of entries for this log service",
    "Members": [
    {
        "@odata.id": "/redfish/v1/Managers/1/LogServices/SEL/Entries/35"
    },
    {
        "@odata.id": "/redfish/v1/Managers/1/LogServices/SEL/Entries/36"
    },
    ],
```

```
    "Members@odata.count": 2,
    "Name": "Log Service Entries Collection"
}
```

- Status Code: 200

Output Description

For a description of the output when your query information about the SEL log service resource collection by specifying a parameter as the query condition, refer to Table 4-64.

Table 4-64 Output Descriptions for Querying Information About the SEL Log Service Resource Collection by Specifying a Condition

Field	Type	Description
@odata.context	String	OData description of the SEL log service resource collection model.
@odata.id	String	Access path of the SEL log service resource collection node.
@odata.type	String	Type of SEL log service resource collection.
Name	String	Name of the SEL log service resource collection.
Members@odata.count	Number	Number of members in the SEL log service resource collection.
Members	Array	Member list of the SEL log service resource collection.

4.34 Querying Information About a Specified SEL Log Service Resource

Function

Query information about the specified SEL log service resource of a server.

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 4-65.

Table 4-65 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**.
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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GEThttps://device_ip/redfish/v1/Managers/1/LogServices/SEL/Entries/172
```

- Request Header:

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

- Request Message Body: None
- Response Example:


```
{
    "@odata.context":"/redfish/v1/$metadata#LogEntry.LogEntry",
   "@odata.etag":"W/\"1643093744\"",
   "@odata.id":"/redfish/v1/Managers/1/LogServices/SEL/Entries/172",
   "@odata.type":"#LogEntry.v1_3_0.LogEntry",
   "Created":"2022-01-25T14:57:14+08:00",
   "Description":"SELLOGINFO",
   "EntryCode":"LowerNon-recoverable-goinglow",
   "EntryType":"SEL",
   "EventTimestamp":"2022-01-25T14:57:14+08:00",
   "Id":"172",
   "Message":"LowerNon-recoverable-goinglow",
   "Name":"SEL467",
   "SensorNumber":2,
```

```
    "SensorType":"Temperature",
    "Severity":"Non-recoverable"
}
```

- 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 4-66.

Table 4-66 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.
Name	String	Name of the SEL log instance.
id	String	ID of the SEL log instance.
EntryType	String	Type of SEL log instance. ● SEL ● Oem
Description	String	Log resource description information.
SensorType	String	Sensor type for generating SEL log instance information.
SensorNumber	Number	Sensor ID for generating SEL log instance information.
EventTimestamp	String	Timestamp of the SEL log instance information.
Created	String	Generation time of the SEL log instance information.
Severity	String	Log severity level of the SEL log instance information. ● OK ● Warning ● Critical ● Non-recoverable

Field	Type	Description
EntryCode	String	Entry code of SEL log instance information.
Message	String	Message content of the SEL log instance information.

4.35 Querying the Import and Export Progress

Function

Query the import and export progress.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Managers/managers_id/Actions/Oem/VANTAGEO/Manager.Configuration/Progress*
- Request Header:

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

- Request Message Body: None

Description

For a description of the parameters for querying the import and export progress, refer to Table 4-67.

Table 4-67 Parameter Descriptions for Querying the Import and Export 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	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Import and Export Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.Configuration/Progress
```

- Log Collection Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.Dump/Progress
```

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Import and Export Response Example:

```
{
   "@odata.context": "/redfish/v1/$metadata",
   "@odata.etag": "W/\"1650013347\"",
   "@odata.id":
   "/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.Configuration/Progress",
   "Detail": "ImortConfiguration",
   "Percentage": "100",
   "State": "STATE_SUCCESSED",
   "Type": "BMC"
```

- Log Collection Response Example:

```
{
   "@odata.context": "/redfish/v1/$metadata",
   "@odata.etag": "W/\"1650013347\"",
   "@odata.id":
   "/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.Configuration/Progress",
   "Detail": "ImortConfiguration",
   "Percentage": "100",
   "State": "STATE_SUCCESSED",
   "Type": "BMC"
```

- Status Code: 200

Output Description

For a description of the output returned when you query the import and export progress, refer to Table 4-68.

Table 4-68 Output Descriptions for Querying the Import and Export Progress

Field	Type	Description
@odata.context	String	OData description of the import and export progress resource model.
@odata.id	String	Access path of the specified SEL log service resource node.

Field	Type	Description
Detail	String	Task type description. ● ImortConfiguration ● ExportConfiguration
Percentage	String	Percentage.
State	String	Import/export task status. Options: ● STATE_FAILED ● STATE_SUCCESSED ● STATE_RUNNING ● STATE_SILENT
Type	String	Type. ● BMC ● BIOS ● Logs ● BMC_BIOS

4.36 Performing One-Click Collection

Function

Perform one-click collection.

Syntax

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

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

- Request Message Body:

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

Description

For a description of the parameters for performing one-click collection, refer to Table 4-69.

Table 4-69 Parameter Descriptions for Performing One-Click 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 POST request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
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/Actions/Oem/VANTAGEO/Manager.Dump
```

- Request Header:

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

- Request Message (Form):

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

- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata",
  "@odata.etag": "W/\"1596373630\"",
  "@odata.id": "/redfish/v1/Managers/1/Actions/Manager.Dump",
  "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"
  }
}
```


- Status Code: 200

Output Description

For a description of the output when you perform one-click collection, refer to Table 4-70.

Table 4-70 Output Descriptions for Performing One-Click Collection

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Readable error message corresponding to the one in the message registry.
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Detailed information.
MessageArgs	Array	Message arguments.
Severity	String	Severity levels supported by the Redfish interface. ● OK ● Warning ● Critical
Resolution	String	Solution.

4.37 Exporting Logs

Function

Export one-click collection logs.

Syntax

- Operation Type: POST

- URL: *https://device_ip/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.ExportLogs*
- Request Header:

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

- Request Message Body:

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

- Request Message (Form):

```
<form enctype="multipart/form-data" action=" https://device_ip/redfish/v1/manager_id
               /Actions/Oem/VANTAGEO/Manager.ExportLogs"  method="POST">
<input name="Type" type="type">
</form>
```

Description

For a description of the parameters for export one-click collection logs, refer to Table 4-71.

Table 4-71 Parameter Descriptions for Exporting One-Click Collection Logs

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
type_value	Operation type.	Type: Logs
content_value	File path.	Configuration file export path.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
    "Type":"BMC",
    "Content":"tftp://10.10.10.191/ID_config.tar.gz"
}
```

- Request Message (Form):

```
<form enctype="multipart/form-data" action=" https://device_ip/redfish/v1/manager_id
               /Actions/Oem/VANTAGEO/Manager.ExportLogs"  method="POST">
<input name="Type" type="Logs">
</form>
```

- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata",
  "@odata.etag": "W/\"1596373630\"",
  "@odata.id": "/redfish/v1/Managers/1/Actions/Manager.ExportLogs",
  "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 Form Example: None
- Status Code: 200

Output Description

For a description of the output when you export one-click collection logs, refer to Table 4-72.

Table 4-72 Output Descriptions for Exporting One-Click Collection Logs

Field	Type	Description
code	String	String indicating the specified message ID in the message registry.
message	String	The readable error message corresponding to the one in the message registry.
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Detailed information.
MessageArgs	Array	Message arguments.
Severity	String	Severity level. Redfish supports the following severity levels: ● OK ● Warning ● Critical
Resolution	String	Solution.

4.38 Querying Information About the NAT Resource

Function

Query the information about the NAT resource.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Managers/manager_id/EthernetInterfaces/usb0/Oem/VANTAGEO/NAT*
- Request Header:

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the SNMP resource, refer to Table 4-73.

Table 4-73 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**.
id	ID of the management port resource supported by the BMC.	-
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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/EthernetInterfaces/usb0/Oem/VANTAGEO/NAT
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
   "@odata.context": "/redfish/v1/$metadata#EthernetInterface.EthernetInterface",
   "@odata.etag": "W/\"1652538923\"",
   "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces/usb0/Oem/VANTAGEO/usb0/NAT",
   "@odata.type": "#EthernetInterface.v1_4_0.EthernetInterface",
   "Oem": {
     "Public": {
        "BmcIpaddress": "192.168.5.52",
        "BmcPort": 2232,
        "HostIpaddress": "113.113.113.113",
        "HostPort": 22,
        "NATEnaled": true
     }
```

```
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the NAT resource, refer to Table 4-74.

Table 4-74 Output Descriptions for Querying Information About the SNMP Resource

Field	Type	Description
@odata.context	String	OData description of the specified management interface resource model of the BMC.
@odata.id	String	Access path of the node of the specified management interface resource of the BMC.
@odata.type	String	Type of the specified management interface resource of the BMC.
Oem.Public	String	OEM object of the usb0 resource node.
BmcIpaddress	String	IPv4 address of a UE
BmcPort	Number	XCAP port
HostIpaddress	String	IPv4 address of the host.
HostPort	Number	Port number of the host.
NATEnabled	Boolean	Whether VLAN is enabled: ● true: enabled. ● false: disabled.

4.39 Setting Information About the NAT Resource

Function

Set the information about the NAT resource.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/Managers/manager_id/EthernetInterfaces/usb0/Oem/VANTAGEO/NAT*
- Request Header:

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

- Request Message Body:

```
{
        "BmcIpaddress": bmc_ip,
        "BmcPort": bmc_port,
        "HostIpaddress": host_ip,
        "HostPort": host_port,
        "NATDefault": nat_default,
        "NATEnaled": nat_enable
    }
}
```

Description

For a description of the parameters for setting the information about the NAT resource, refer to Table 4-75.

Table 4-75 Parameter Descriptions for Setting Information About the NAT 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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
nat_enable	VLAN enabling switch.	• false: disabled. • true: enabled.
nat_default	Default configuration.	Whether to use the default configuration: • 0: uses the default configuration. • 1: uses the configured value.
bmc_ip	BMC address.	BMC address.
bmc_port	BMC port number.	BMC port number.
host_ip	Host address.	Host address.
host_port	Port number of the host.	Port number of the host.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Managers/1/EthernetInterfaces/usb0/Oem/VANTAGEO/NAT
```

- Request Header:

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

- Request Message Body:

```
{
      "BmcIpaddress": "192.168.5.52",
      "BmcPort": 2232,
      "HostIpaddress": "113.113.113.113",
      "HostPort": 22,
      "NATDefault": 1,
      "NATEnaled": true
}
```

- Response Example: None
- Status Code: 204

Output Description

For a description of the output when you set the information about the NAT resource, refer to Table 4-76.

Table 4-76 Output Descriptions for Setting Information About the NAT Resource

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Easy-to-read error messages corresponding to messages in the message registry.
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
NATEnabled	Boolean	VLAN enabling switch.
NATDefault	Number	Default NAT configuration.
BmcIpaddress	String	BMC IP address.

Field	Type	Description
BmcPort	Number	XCAP port
HostIpaddress	String	IP address of the host.
HostPort	Number	Port number of the host.

4.40 Performing One-Click Configuration Solidification

Function

Perform one-click configuration solidification.

Syntax

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

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

- Request Message Body:

```
{
     "Type":type_value,
     "CustomNumber":custom_value
}
```

Description

For a description of the parameters for performing one-click configuration solidification, refer to Table 4-77.

Table 4-77 Parameter Descriptions for Performing One-Click Configuration Solidification

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 */redfish/v1/SessionService/Sessions*.

Parameter	Description	Value
header_type	Format of the request message.	application/json
type_value	Target type.	• BMC • BIOS • BMC_BIOS
custom_value	Customized ID.	Maximum length: 19 characters, containing digits 0–9, lowercase characters a–z, uppercase characters A–Z, dots, underscores, and hyphens.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
    "Type": "BMC",
    "CustomNumber": "456123789"
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1656938788\"",
    "@odata.id":
    "/redfish/v1/Managers/Self/Actions/Oem/VANTAGEO/Manager.CompressFile", "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"
    }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you perform one-click configuration solidification, refer to Table 4-77.

Table 4-78 Output Descriptions for Performing One-Click Configuration Solidification

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	The readable error message corresponding to the one in the message registry.
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Detailed information.
MessageArgs	Array	Message arguments.
Severity	String	Severity level, including: ● OK ● Warning ● Critical
Resolution	String	Solution.

4.41 Performing One-Click Configuration Information Export

Function

Perform one-click configuration information export.

Syntax

- Operation Type: POST

- URL: *https://device_ip/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.ExportCompressFile*
- Request Header:

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

- Request Message Body:

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

- Request Message (Form):

```
<form enctype="multipart/form-data"
    action="https://device_ip/redfish/v1/manager_id/Actions/
    Oem/VANTAGEO/Manager.Export CompressFile"
    method="POST">
<input name="Type" type="type">
</form>
```

Description

For a description of the parameters for performing one-click configuration information export, refer to Table 4-79.

Table 4-79 Parameter Descriptions for Performing One-Click Configuration Information Export

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 POST request, the "Headers" field must carry the "X-Auth-Token" value for authentication.	It can be obtained when a session is created through */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
type_value	Target type.	• BMC • BIOS • BMC_BIOS

Parameter	Description	Value
custom_value	File path.	Configuration file export path.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
    "Type":"BMC",
    "Content":"tftp://10.10.10.191/ID_config.tar.gz"
}
```

- Request Message (Form):

```
<form enctype="multipart/form-data"
    action=" https://device_ip/redfish/v1/1/Actions/
    Oem/VANTAGEO/Manager.ExportCompressFile"
    method="POST">
<input name="Type" type="BMC">
</form>
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1656938788\"",
    "@odata.id":
    "/redfish/v1/Managers/Self/Actions/Oem/VANTAGEO/Manager.ExportCompressFile", "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"
    }
}
```


- Status Code: 200

Output Description

For a description of the output when you perform one-click configuration information export, refer to Table 4-80.

Table 4-80 Output Descriptions for Performing One-Click Configuration Information Export

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	The readable error message corresponding to the one in the message registry.
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Detailed information.
MessageArgs	Array	Message arguments.
Severity	String	Severity level, including: ● OK ● Warning ● Critical
Resolution	String	Solution.

4.42 Performing One-Click Configuration Restoration

Function

Perform one-click configuration restoration.

Syntax

- Operation Type: POST

- URL: *https://device_ip/redfish/v1/Managers/manager_id/Actions/Oem/VANTAGEO/Manager.ResetFactory*
- Request Header:

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

- Request Message Body:

```
{
    "Type":type_value,
    "ResetType":reset_value
}
```

Description

For a description of the parameters for performing one-click configuration restoration, refer to Table 4-81.

Table 4-81 Parameter Descriptions for Performing One-Click Configuration Restoration

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
type_value	Target type.	• BMC • BIOS
reset_value	Restoration mode.	• When type_value is set to BMC: → 0: one-click restoration to manufacturer-specified configurations. → 1: one-click restoration to the default board configurations. → 2: one-click restoration to manufacturer-specified configurations (excluding IP settings) → 255: one-click restoration to VANTAGEO- specified factory default configurations.

Parameter	Description	Value
		● When type_value is set to BIOS: → 0: one-click restoration to the manufacturer-customized configuration as specified in the contract. → 255: one-click restoration to VANTAGEO- specified factory default configurations.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
    "Type": "BMC",
    "ResetType":0
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1656938788\"",
    "@odata.id": "/redfish/v1/Managers/Self/Actions/Oem/VANTAGEO/Manager.ResetFactory",
    "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"
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you perform one-click configuration restoration, refer to Table 4-82.

Table 4-82 Output Descriptions for Performing One-Click Configuration Restoration

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	The readable error message corresponding to the one in the message registry.
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Detailed information.
MessageArgs	Array	Message arguments.
Severity	String	Severity level, including: ● OK ● Warning ● Critical
Resolution	String	Solution.

4.43 Querying Information About the SMTP Resource

Function

Query information about the SMTP resource of a server.

Syntax

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

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the SMTP resource, refer to Table 4-83.

Table 4-83 Parameter Descriptions for Querying Information About the SMTP 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/
    $metadata#ManagerSmtpServiceCollection.ManagerSmtpServiceCollection",
    "@odata.etag": "W/\"1669299640\"",
    "@odata.id": "/redfish/v1/Managers/1/SmtpService",
    "@odata.type": "#ManagerSmtpServiceCollection.ManagerSmtpServiceCollection",
    "Actions": {
      "#SmtpService.SubmitTestEvent": {
      "target": "/redfish/v1/Managers/1/SmtpService/Actions/SmtpService.SubmitTestEvent"
        }
    },
    "AttachAssettag": true,
    "AttachHostname": true,
```

```
    "EmailSubject": "Server Alert",
    "ReciverEmailId": [
        {
            "EmailAddress": "111111111@qq.com"
        },
        {
            "EmailAddress": "123456@163.com"
        }
    ],
    "SenderEmailId": "111111111@qq.com",
    "SmtpAuthEnable": true,
    "SmtpEnable": true,
    "SmtpPassword": null,
    "SmtpServerIp": "10.54.141.153",
    "SmtpServerPort": 25,
    "SmtpTlsEnable": true,
    "SmtpUsername": "111111111@qq.com"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the SMTP resource, refer to Table 4-84.

Table 4-84 Output Descriptions for Querying Information About the SMTP Resource

Field	Type	Description
@odata.context	String	OData description of the SMTP resource model.
@odata.id	String	Access path of the SNMP resource node.
@odata.type	String	Type of BIOS resource.
Actions	Object	Operations that can be performed on the SMTP resource.
#SmtpService.SubmitTestEvent	Object	Sending an SMTP test email.
AttachAssettag	Boolean	Whether an asset tag is attached to the email subject. ● true: yes ● false: no
AttachHostname	Boolean	Whether the hostname is attached to the email subject. ● true: yes

Field	Type	Description
		• false: no
EmailSubject	String	Mail subject.
ReciverEmailId	Array	Receiving mailbox address collection.
EmailAddress	String	Receiving email address.
SenderEmailId	String	Sender's mailbox address.
SmtpAuthEnable	Boolean	Whether SMTP identity authentication is enabled. • true: yes. • false: no.
SmtpEnable	Boolean	Whether alarms are sent to the mailbox: • True: yes. • false: disabled.
SmtpPassword	String	SMTP password.
SmtpServerIp	String	Address of the LDAP or LDAPS server.
SmtpServerPort	Number	NRF Server Port
SmtpTlsEnable	Boolean	Whether to enable the TE function. • true: enabled. • false: disabled.
SmtpUsername	String	SMTP username.

4.44 Modifying Properties of the SMTP Resource

Function

Modify properties of the SMTP resource.

Syntax

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

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

- Request Message Body:

```
{
    "SmtpEnable": SmtpEnable,
    "SmtpServerIp": SmtpServerIp,
```

```
    "SmtpServerPort": SmtpServerPort,
    "SmtpTlsEnable": SmtpTlsEnable,
    "SmtpAuthEnable": SmtpAuthEnable,
    "SmtpUsername": SmtpUsername,
    "SmtpPassword": SmtpPassword,
    "SenderEmailId": SenderEmailId,
    "ReciverEmailId": ReciverEmailId,
    "EmailSubject": EmailSubject,
    "AttachHostname": AttachHostname,
    "AttachAssettag": AttachAssettag
}
```

Description

For a description of the parameters for modifying properties of the SMTP resource, refer to Table 4-85.

Table 4-85 Parameter Descriptions for Modifying Properties of the SMTP 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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
SmtpEnable	Whether to send alarms to the mailbox:	• true: enabled. • false: no.
SmtpServerIp	Address of the LDAP or LDAPS server.	IPv4 address format or IPv6 address format
SmtpServerPort	NRF Server Port	Optional. Default: 25. Port number range: 1–65535.
SmtpTlsEnable	Whether to enable the TLS function.	Optional. Default: false. • true: enabled. • false: disabled.
SmtpAuthEnable	Whether to enable SMTP identity authentication.	Optional. Default: false. • true: enabled. • false: disabled.

Parameter	Description	Value
SmtpUsername	SMTP username.	If SMTP authentication is enabled, this parameter is required. The username rules are as follows: ● String of 1–31 characters containing letters, digits, and allowed special characters. ● The username must begin with a digit or letter. ● For special characters, only '. ',' _ ','-', and '@' are allowed.
SmtpPassword	SMTP password.	If SMTP authentication is enabled, this parameter is required. The password rules are as follows: ● String of 1–63 characters. ● The password cannot include blank characters, including spaces, tabs, and line breaks.
SenderEmailId	Sender's mailbox address.	The mailbox name has a minimum length of 6 bytes and a maximum length of 63 bytes, including the username and domain name. The mailbox name rules are as follows: ● Digits, uppercase letters, lowercase letters, underscores, an at symbol, and periods are supported. ● A mailbox name cannot start or end with an at sign or period. ● Only one at symbol is allowed. The mailbox domain name is after the at symbol. ● There is at least one period in the domain name, but two consecutive periods are not allowed.
ReciverEmailId	Receiving email address	The mailbox format must be the same as that of the sender. A maximum of four mailbox addresses are supported, which are separated by commas.

Parameter	Description	Value
EmailSubject	Email subject.	Optional. Default: Server Alert. The subject can contain 6–63 characters.
AttachHostname	Whether the hostname is attached to the email subject.	Optional. Default: false. ● true: yes ● false: no
AttachAssettag	Whether an asset tag is attached to the email subject.	Optional. Default: false. ● true: yes ● false: no

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
    "SmtpEnable": true,
    "SmtpServerIp": "10.54.141.153",
    "SmtpServerPort": 25,
    "SmtpTlsEnable": true,
    "SmtpAuthEnable": true,
    "SmtpUsername": "111111111@qq.com",
    "SmtpPassword": "123456789",
    "SenderEmailId": "111111111@qq.com",
    "ReciverEmailId": "111111@vantageo.com,123456@163.com",
    "EmailSubject": "Server Alert",
    "AttachHostname": true,
    "AttachAssettag": true
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/
```

```
    $metadata#ManagerSmtpServiceCollection.ManagerSmtpServiceCollection",
    "@odata.etag": "W/\"1669299640\"",
    "@odata.id": "/redfish/v1/Managers/1/SmtpService",
    "@odata.type": "#ManagerSmtpServiceCollection.ManagerSmtpServiceCollection",
    "Actions": {
      "#SmtpService.SubmitTestEvent": {
      "target": "/redfish/v1/Managers/1/SmtpService/Actions/SmtpService.SubmitTestEvent"
        }
    },
    "AttachAssettag": true,
    "AttachHostname": true,
    "EmailSubject": "Server Alert",
    "ReciverEmailId": [
        {
            "EmailAddress": "111111@vantageo.com"
        },
        {
            "EmailAddress": "123456@163.com"
        }
    ],
    "SenderEmailId": "111111111@qq.com",
    "SmtpAuthEnable": true,
    "SmtpEnable": true,
    "SmtpPassword": null,
    "SmtpServerIp": "10.54.141.153",
    "SmtpServerPort": 25,
    "SmtpTlsEnable": true,
    "SmtpUsername": "111111111@qq.com"
}
```


- Status Code: 202

Output Description

None

4.45 Sending an SMTP Test Email

Function

Send an SMTP test email.

Syntax

- Operation Type: POST

- URL: *https://device_ip/redfish/v1/Managers/manager_id/SmtpService/Actions/SmtpService.SubmitTestEvent*
- Request Header:

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

- Request Message Body:

```
{
}
```

Description

None

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
}
```

- Response Example: None
- Status Code: 204

Output Description

None

4.46 Querying Information About the DNS Resource

Function

Query the information about the DNS resource.

Syntax

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

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the SNMP resource, refer to Table 4-86.

Table 4-86 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#DnsService.DnsService",
    "@odata.etag": "W/\"1672892532\"",
    "@odata.id": "/redfish/v1/Managers/1/DnsService",
    "@odata.type": "#DnsService.v1_0_0.DnsService",
    "DnsIpConfig": {
        "DnsDhcpEnable": true,
```

```
        "DnsEnable": true,
        "DnsInterface": "eth1",
        "IpPriority": "ipv4"
    },
    "DomainConfig": {
        "DhcpEnable": true,
        "DomainInterface": "eth1",
        "DomainPriority": "ipv4"
    },
    "HostNameConfig": {
        "HostName": "iSACAA621D33E326",
        "HostSetting": "auto"
    },
    "PatchInProgress": false,
    "RegisterBMC": {
        "Eth0Reg": "fqdn",
        "Eth1Reg": "hostname"
    }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the DNS resource, refer to Table 4-87.

Table 4-87 Output Descriptions for Querying Information About the SNMP Resource

Field	Type	Description
@odata.context	String	OData description of the DNS resource model.
@odata.id	String	Access path of the SNMP resource node.
@odata.type	String	Type of BIOS resource.
DnsIpConfig	Object	DNS Server IP configurations.
DnsDhcpEnable	Boolean	Method used to obtain the DNS server address: ● true: The address is obtained automatically. ● false: The address is configured manually.
DnsEnable	Boolean	Whether the DNS service is enabled.
DnsInterface	String	Network interface name:

Field	Type	Description
		• eth0 • eth1 • bond0
IpPriority	String	IP priority: • ipv4 • ipv6
NameServers	Array	Domain name server list.
DomainConfig	Object	Domain configuration.
DhcpEnable	Boolean	Method used to obtain the domain information. True: automatic. False: manual.
DomainInterface	String	Network interface name: • eth0 • eth1 • bond0
DomainPriority	String	Domain type: • ipv4 • ipv6
DomainName	String	Domain name.
HostNameConfig	Object	Hostname configurations.
HostSetting	String	Hostname setting mode: • auto: • Manual
HostName	String	Hostname.
PatchInProgress	Boolean	Configuration validity flag: • true: configuration in progress • false: configuration completed
RegisterBMC	Object	Registration configurations of the BMC.
Eth0Reg	String	Eth0 registration mode: • nsupdate • fqdn • hostname • null
Eth1Reg	String	Eth1 registration mode: • nsupdate • fqdn • hostname

Field	Type	Description
		• null
Bond0Reg	String	Bond0 registration mode: • nsupdate • fqdn • hostname • null

4.47 Modifying Properties of the DNS Resource

Function

Modify properties of the DNS resource.

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:

```
{
    "HostNameConfig": {
        "HostSetting":  HostSetting
           "HostName": HostName
    },
    "DomainConfig": {
        "DhcpEnable":  dhcpEnable
          "DomainInterface": DomainIface
          "DomainPriority":Domainpriority
          "DomainName": domainname
    },
    "DnsIpConfig": {
        "NameServers": [ip, ip, ip]
         "DnsEnable":  DNSEnable
         "DnsDhcpEnable": DNSDHCP
         "DnsInterface": DnsIface
         "IpPriority": IPPriority
    },
    "RegisterBMC": {
        "Eth0Reg":  eth0reg
```

```
        "Eth1Reg": eth1reg
        "Bond0Reg": bond0reg
    }
}
```

Description

For a description of the parameters for modifying properties of the DNS resource, refer to Table 4-88.

Table 4-88 Parameter Descriptions for Modifying Properties of the DNS 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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
DnsDhcpEnable	Method used to obtain the DNS server address.	● true: The address is obtained automatically. ● false: The address is configured manually.
DnsEnable	Whether to enable the DNS service.	● true: yes ● false: no
DnsInterface	Network interface name.	● eth0 ● eth1 ● bond0
IpPriority	IP priority.	● ipv4 ● ipv6
NameServers	Domain name server list.	String, valid IPv4 or IPv6 address.
DhcpEnable	Method to obtain the domain information.	● true: The information is obtained automatically. ● false: The information is configured manually.
DomainInterface	Network interface name.	● eth0 ● eth1 ● bond0

Parameter	Description	Value
DomainPriority	Domain type.	• ipv4 • ipv6
DomainName	Domain name.	Valid domain name string. The length of a single node of the domain name cannot exceed 63 characters, and the FQDN cannot exceed 255 characters.
HostSetting	Hostname setting mode.	• auto: • Manual
HostName	Hostname.	• A hostname cannot exceed 63 characters. • The name can contain only alphabetic characters (A-Z), numeric character (0-9), and hyphens (-). • No blank characters including spaces are allowed. • The name cannot start or end with a hyphen.
Eth0Reg	Eth0 registration mode.	• nsupdate • fqdn • hostname • null
Eth1Reg	Eth1 registration mode.	• nsupdate • fqdn • hostname • null
Bond0Reg	Bond0 registration mode.	• nsupdate • fqdn • hostname • null

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
    "HostNameConfig": {
        "HostSetting": "manu",
        "HostName": "aabbcc"
    },
    "DomainConfig": {
        "DhcpEnable": true,
        "DomainInterface": "eth0",
        "DomainName": "VANTAGEO.fun.com",
        "DomainPriority": "ipv4"
    },
    "DnsIpConfig": {
        "DnsEnable": true,
        "DnsDhcpEnable": true,
        "DnsInterface": "eth0",
        "IpPriority": "ipv4",
        "NameServers": [
            "1.2.3.4",
            "",
            "2022::39"
        ]
    },
    "RegisterBMC": {
        "Eth0Reg": "fqdn",
        "Eth1Reg": "hostname"
    }
}
```

- Response Example: None
- Status Code: 204

Output Description

None

4.48 Setting the BMC Time and Time Zone

Function

Set the BMC time and time zone.

Syntax

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

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

- Request Message Body:

```
{
    "SetTimeEnabled":settime_value,
    "Times":time_value,
    "DateTimeLocalOffset":timezone_value
}
```

Description

For a description of the parameters for setting the BMC time and time zone, refer to Table 4-89.

Table 4-89 Parameter Descriptions for Setting the BMC Time and Time Zone

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
settime_value	Enables the automatic mode for obtaining time information.	• true: automatic • false: manual In this version, this parameter can be set to true only.
time_value	Time.	Times: time string. Format: YYYY-MM-DD HH:MM:SS.
timezone_value	Time zone.	Time zone of the Manager resource, in time zone format, for example, +08:00 or time zone/region

Parameter	Description	Value
		format, for example, Asia/Shanghai, America/New_York.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
    "SetTimeEnabled":true,
    "Times":"2024-05-30 13:59:59",
    "DateTimeLocalOffset":"Asia/Shanghai"
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1596373630\"",
    "@odata.id": "/redfish/v1/Managers/1/Actions/Manager.SetBMCTimes",
    "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"
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you set the BMC time and time zone, refer to Table 4-90.

Table 4-90 Output Descriptions for Setting the BMC Time and Time Zone

Field	Type	Description
code	Character string	ID of the specified message in the message registry.
message	Character string	Readable error message corresponding to the one in the message registry.
@odata.type	Character string	OData description of the message resource.
MessageId	Character string	Message ID.
RelatedProperties	Array	Message-related properties.
Message	Character string	Details.
MessageArgs	Array	Message arguments.
Severity	Character string	Severity level. Severity levels supported by Redfish, including: ● OK ● Warning ● Critical
Resolution	Character string	Recommended solution.

4.49 Downloading a BMC File

Function

Download a BMC file of a server.

Syntax

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

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

- Request Message Body:

```
{
    "TransferProtocol":protocol_value,
```

```
    "Path": path_value
}
```

Description

For a description of the parameters for downloading a BMC file, refer to Table 4-91.

Table 4-91 Parameter Descriptions for Downloading a BMC File

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
protocol_value	Protocol	Supported protocol: HTTPS
path_value	Download path	File path in the BMC, which refers to "/var/redfish" and its subdirectories. This parameter is set to **/var/redfish/filename**, where **filename** indicates the name of the file that is downloaded. The filename is obtained from the **TarName** field in the response message of the "Querying Import and Export Progress" interface.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
```

```
    "TransferProtocol":"HTTPS",
    "Path":"/var/redfish/bmcinfo_dump_UnknownProductSN_20210728-0413.tar.gz"
}
```

- Response Example: file content.
- Status Code: 200

Output Description

None

4.50 Querying Information About the SDM Service Resource

Function

Query information about the BMC SDM service resource of a server.

Syntax

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

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the SDM service resource, refer to Table 4-92.

Table 4-92 Parameter Descriptions for Querying Information About the SDM 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 POST request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:


```
{
    "@odata.context": "/redfish/v1/$metadata#SdmService.SdmService",
    "@odata.etag": "W/\"1685125323\"",
    "@odata.id": "/redfish/v1/Managers/1/SDMService",
    "@odata.type": "#SdmService.v1_0_0.SdmService",
    "Devices": [
        {
            "Alias": 65792,
            "ComponentID": 0,
            "ComponentType": "Memory",
            "DeviceInfo": "/redfish/v1/Systems/1/Memory/DIMM1",
            "EventReports": "/redfish/v1/Managers/1/SDMService/65792/EventReports",
            "OnlineTimeStamp": 1685123864,
            "SilkName": "DIMM1"
        },
        {
            "Alias": 65794,
            "ComponentID": 2,
            "ComponentType": "Memory",
            "DeviceInfo": "/redfish/v1/Systems/1/Memory/DIMM3",
            "EventReports": "/redfish/v1/Managers/1/SDMService/65794/EventReports",
            "OnlineTimeStamp": 1685123864, "SilkName": "DIMM3"
        }
    ],
    "Members@odata.count": 2,
    "Name": "SDMService Collection"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the SDM Service resource, refer to Table 4-93.

Table 4-93 Output Descriptions for Querying Information About the SDM Service Resource

Field	Type	Description
@odata.context	Character string	OData description of the SDM service resource model.
@odata.id	Character string	Access path of the SDM service resource.
@odata.type	Character string	Type of SDM service resource.
SilkName	Character string	Silk screen of the device.
ComponentType	Character string	Component type of the device.
ComponentID	Number	Component ID of the device.
Alias	Number	Unique identifier of the device in the device tree.
EventReports	Object	Access path of the early warning report information about device faults.
DeviceInfo	Object	Resource access path of device information.
OnlineTimeStamp	Number	Timestamp when the device goes online.
Members@odata.count	Number	Number of devices.
Name	Character string	Name of the SDM service resource collection.

4.51 Querying the Component Early-Warning Information About the SDM Service Resource

Function

Query the component early-warning information about the SDM service resource of a server.

Syntax

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

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

- Request Message Body: None

Description

For a description of the parameters for querying the component early-warning information about the SDM service resource, refer to Table 4-94.

Table 4-94 Parameter Descriptions for Querying the Component Early-Warning Information About the SDM 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 POST request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/SDMService/65792/EventReports
```

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#SdmService.SdmService",
    "@odata.etag": "W/\"1685189621\"",
    "@odata.id": "/redfish/v1/Managers/1/SDMService/65792/EventReports",
    "EventRecords": [
        {
            "ComponentID": 0,
            "ComponentType": 1,
            "Information": "Device Installation(SN:3939EC67)",
            "ReportTimeStamp": 1685123864,
            "SerialNumber": "3939EC67",
            "SilkName": "DIMM1",
            "Type": "Installation"
        }
    ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query component early-warning information about the SDM service resource, refer to Table 4-95.

Table 4-95 Output Descriptions for Querying Component Early-Warning Information About the SDM Service Resource

Field	Type	Description
@odata.context	Character string	OData description of the DNS resource model.
@odata.id	Character string	Access path of the SNMP resource.
@odata.type	Character string	Type of BIOS resource.
EventRecords	Array	Fault analysis record generated by the SDM fault early warning system. Each object corresponds to an event.
ReportTimeStamp	Number	Timestamp when the report is generated.
SilkName	Character string	Silk screen of the device.
ComponentType	Number	Component type of the device.
ComponentID	Number	Component ID of the device.
Type	Character string	Event type. ● Installation ● Replacement ● Removal
Information	Character string	Event description.

4.52 Clearing System Logs

Function

Clear the system logs of a server.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/Managers/manager_id/TestService/Actions/ClearSystemLog*
- Request Header:

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

- Request Message Body:

```
{
```

```
}
```

Description

For a description of the parameters for clearing system logs, refer to Table 4-96.

Table 4-96 Parameter Descriptions for Clearing System Logs

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 `/redfish/v1/SessionService/Sessions`.

Usage Guidelines

The request message needs to contain a null body, for example, {}.

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/TestService/Actions/ClearSystemLog
```

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body:

```
{
}
```

- Response Example: None
- Status Code: 204

Output Description

None

4.53 Exporting a Screenshot

Function

Export a screenhot.

Syntax

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

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

- Request Message Body:

```
{
}
```

Description

For a description of the parameters for exporting a screenshot, refer to Table 4-97.

Table 4-97 Parameter Descriptions for Exporting a Screenshot

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Managers/1/Actions/Oem/Public/Manager.CapPictureDownload
```

- Request Header:

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

- Request Message Body:

```
{
}
```

- Response Example:

  File content.

- Status Code: 200

Output Description

None

4.54 Triggering a Screenshot

Function

Trigger a screenshot.

Syntax

- Operation Type: POST
- URL:*:https://device_ip/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Ma-nager.AutoScreenCap*
- Request Header:

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

- Request Message Body:

```
{
}
```

Description

For a description of the parameters for triggering a screenshot, refer to Table 4-98.

Table 4-98 Parameter Descriptions for Trigger a Screenshot

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 */redfish/v1/SessionService/Sessions*.

Parameter	Description	Value
header_type	Format of the request message.	application/json

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234e
Content-Type: application/json
```

- Request Message Body:

```
{
}
```

- Response Example:

  File content.

- Status Code: 200

Output Description

None

4.55 Querying Information About the Firewall Service Resource

Function

Query information about the firewall service resource.

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 the firewall service resource, refer to Table 4-99.

Table 4-99 Parameter Descriptions for Querying Information About the Firewall 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#FirewallRule.FirewallRule",
    "@odata.etag": "W/\"1647265688\"",
    "@odata.id": "/redfish/v1/Managers/1/SecurityService/FirewallRules",
    "@odata.type": "#FirewallRule.v1_0_0.FirewallRule",
    "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",
    "IPv4ActiveStrategy": "Drop",
    "IPv6ActiveStrategy": "Drop",
    "Id": "FirewallRules",
    "Name": "Firewall Rules",
    "Rules": [
        {
            "@odata.id": "/redfish/v1/Managers/1/SecurityService/FirewallRules#/Rules/
            MacRules_1",
            "EndDateTime": null,
            "EndIPAddress": null,
            "EndMacAddress": "68:05:CA:F9:43:19",
            "RuleType": "Drop",
            "StartDateTime": null,
            "StartIPAddress": null,
            "StartMacAddress": "68:05:CA:F9:43:14",
            "WorkdayOnly": false
        },
        {
            "@odata.id": "/redfish/v1/Managers/1/SecurityService/FirewallRules#/Rules/
            MacRules_2",
            "EndDateTime": null,
            "EndIPAddress": null,
            "EndMacAddress": "68:05:CA:F9:43:19",
            "RuleType": "Drop",
            "StartDateTime": null,
            "StartIPAddress": null,
            "StartMacAddress": "68:05:CA:F9:43:14",
            "WorkdayOnly": false
        }
    ]
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the firewall service resource, refer to Table 4-100.

Table 4-100 Output Descriptions for Querying Information About the Firewall Service Resource

Field	Type	Description
@odata.context	Character string	OData description of the firewall service resource model.
@odata.id	Character string	Access path of the firewall service resource model.
@odata.type	Character string	Type of firewall service resource model.
Actions	Object	Operations that can be performed on the resource.
#FirewallRule.AddRules	Object	Adds a firewall rule.
#FirewallRule.DeleteRules	Object	Deletes a firewall rule.
ActiveStrategy	Character string	Currently valid rule policy: ● Accept: enables rules that accept data, that is, the whitelist takes effect. ● Drop: enables rules that drop data, that is, the blacklist takes effect. ● Other: selected when **IPv4ActiveStrategy** and **IPv6ActiveStrategy** are inconsistent.
IPv4ActiveStrategy	Character string	Currently valid IPv4 firewall rule policy: ● Accept: enables rules that accept data, that is, the whitelist takes effect. ● Drop: enables rules that drop data, that is, the blacklist takes effect.
IPv6ActiveStrategy	Character string	Current effective IPv6 firewall rule policy: ● Accept: enables rules that accept data, that is, the whitelist takes effect. ● Drop: enables rules that drop data, that is, the blacklist takes effect.
EndDateTime	Character string	Time when the rule becomes invalid.
EndIPAddress	Character string	End IP address corresponding to the rule.
EndMacAddress	Character string	End MAC address corresponding to the rule.
RuleType	Character string	Mode type of this rule: ● Accept ● Drop
StartDateTime	Character string	Time when the rule takes effect.
StartIPAddress	Character string	Start IP address corresponding to the rule.
StartMacAddress	Character string	Start MAC address corresponding to the rule.

Field	Type	Description
WorkdayOnly	Boolean	Whether a rule is effective on workdays only.

4.56 Adding a Firewall Rule

Function

Add a firewall rule.

Syntax

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

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

- Request Message Body:

```
{
    "Rules": [
        {
            "RuleType": rule_type,
            "StartDateTime": start_time,
            "EndDateTime": end_time,
            "StartIPAddress": start_ip,
            "EndIPAddress": end_ip,
            "WorkdayOnly":work_day
        },
        {
            "RuleType": rule_ip,
            "StartMacAddress": start_mac,
            "EndMacAddress": end_mac
        }
    ]
}
```

Description

For a description of the parameters for adding a firewall rule, refer to Table 4-101.

Table 4-101 Parameter Descriptions for Adding a Firewall Rule

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 `/redfish/v1/SessionService/Sessions`.
rule_type	Sets the mode type of the rule.	• Accept • Drop
start_time	Start time of the validity period of the rule. Optional.	Time string. Format • YYYY-MM-DD • HH:MM
end_time	End time of the validity period of the rule. Optional.	Time string. Format • YYYY-MM-DD • HH:MM
start_ip	Start IP address corresponding to this rule.	Either **start_ip** or **StartMacAddress** can be configured. Format: xxx.x.x.x, ::x.
end_ip	End IP address corresponding to this rule. Optional.	Either **end_ip** or **EndMacAddress** can be configured. Format: xxx.x.x.x, ::x.
start_mac	Start MAC address corresponding to the rule.	Either **start_ip** or **StartMacAddress** can be configured. Format: xx:xx:xx:xx:xx:xx.
end_mac	End MAC address corresponding to the rule. Optional.	Either **end_ip** or **EndMacAddress** can be configured. Format: xx:xx:xx:xx:xx:xx.
work_day	Whether the rule is valid only on workdays. Optional.	• true: effective on workdays only • False (default): valid 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: 8574621d21b84756218c7456821c234e
Content-Type: application/json
```

- Request Message Body:

```
{
    "Rules": [
        {
            "RuleType": "Accept",
            "StartDateTime": "2024-02-20 00:00",
            "EndDateTime": "2024-02-22 00:00",
            "StartIPAddress": "128.0.0.100"
        },
        {
            "RuleType": "Drop",
            "StartMacAddress": "11:22:33:44:55:66"
        }
    ]
}
```

- Response Example: None
- Status Code: 204

Output Description

None

4.57 Deleting a Firewall Rule

Function

Delete a firewall rule.

Syntax

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

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

- Request Message Body:

```
{
    "Rules": [
        {
            "@odata.id": ip_rule_id
        },
        {
            "@odata.id": mac_rule_id
        }
    ]
}
```

Description

For a description of the parameters for deleting a firewall rule, refer to Table 4-102.

Table 4-102 Parameter Descriptions for Deleting a Firewall Rule

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
ip_rule_id	Odataid of the IP rule to be deleted.	• Accept • Drop
mac_rule_id	Odataid of the MAC rule to be deleted. Optional.	Time string. Format: • YYYY-MM-DD • HH:MM

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: 8574621d21b84756218c7456821c234e
Content-Type: application/json
```

- Request Message Body:

```
{
    "Rules": [
        {
            "@odata.id": "/redfish/v1/Managers/1/SecurityService/FirewallRules#/Rules/IPRules_1"
        },
        {
            "@odata.id": "/redfish/v1/Managers/1/SecurityService/FirewallRules#/Rules/MacRules_1"
        }
    ]
}
```

- Response Example: None
- Status Code: 204

Output Description

None

4.58 Querying the One-Click Collection Progress

Function

Query the one-click collection progress.

Syntax

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

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

- Request Message Body: None

Description

For a description of the parameters for querying the one-click collection progress, refer to Table 4-103.

Table 4-103 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	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.Dump/Progress
```

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1653572784\"",
    "@odata.id": "/redfish/v1/Managers/1/Actions/Oem/VANTAGEO/Manager.Dump/Progress",
    "Message": "SUCCESSED",
    "Percentage": "100",
    "State": "STATE_SUCCESSED",
    "TarName": "bmcinfo_dump_UnknownProductSN_20220601-1822.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 4-104.

Table 4-104 Output Descriptions for Querying the One-Click Collection Progress

Field	Type	Description
@odata.context	Character string	OData description of the firewall service resource model.
@odata.id	Character string	Access path of the firewall resource node.
Percentage	Character string	Percentage.
State	Character string	Alarm status. ● STATE_FAILED ● STATE_SUCCESSED ● STATE_RUNNING ● STATE_SILENT
Type	Character string	Type: **Logs**.
Message	Character string	Description
TarName	Character string	Name of the package containing collected log files.

4.59 Querying Information About the HDM Service Resource Collection

Function

Query information about the BMC HDM service resource collection.

Syntax

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

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the HDM service resource collection, refer to Table 4-105.

Table 4-105 Parameter Descriptions for Querying Information About the HDM Service 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#HDMService.HDMService",
    "@odata.id": "/redfish/v1/Managers/1/HDMService",
    "@odata.type": "#HDMService.v1_0_0.HDMService",
    "Name": "HDMService Collection",
    "Members@odata.count": 1,
    "Members": [
        {
            "@odata.id": "redfish/v1/Managers/1/HDMService/Chassis",
        }
    ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the HDM service resource collection, refer to Table 4-106.

Table 4-106 Output Descriptions for Querying Information About the HDM service Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the HDM service resource collection model.
@odata.id	Character string	Access path of the HDMService resource collection node.
@odata.type	Character string	Type of HDM service resource collection.
Name	Character string	Name of the HDM service resource collection.
Members@odata.count	Number	Number of current HDM service resources.
Members	Array	List of HDM service resources.
@odata.id	Character string	Access path of a single HDM service resource.

4.60 Querying Information About HDM Resource Health Status

Function

Query information about HDM resource health status of a server.

Syntax

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

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

- Request Message Body: None

Description

For a description of the parameters for querying information about HDM resource health status, refer to Table 4-107.

Table 4-107 Output Descriptions for Querying Information About HDM Resource Health Status

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.
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 */redfish/v1/SessionService/Sessions*.
module_type	Module Type	The supported module type is Chassis.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Managers/1/HDMService/Chassis
```

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:


```
{
    "@odata.context": "/redfish/v1/$metadata#HDMService.HDMService.Chassis",
    "@odata.id": "/redfish/v1/Managers/1/HDMService/Chassis",
    "@odata.type": "#HDMChassis.v1_0_0.HDMChassis",
    "Name": "Chassis",
    "Id": "Chassis",
    "Count": 1,
    "Records": [
        {
            "TimeStamp": 1535348824,
            "ComponentID": 0,
            "ComponentType": "Chassis",
            "Slot": 0,
            "SilkName": "CHASSIS",
            "HealthScore": 90,
            "Reasons": [
                {
                    "ReportTimeStamp": 1535348824,
                    "AlarmCode": 30848,
                    "Level": "Major",
```

```
                    "ComponentType":"FAN"
                },
                {
                    "ReportTimeStamp": 1535348824,
                    "AlarmCode": 30732,
                    "Level": "Critical",
                    "ComponentType":"PSU"
                }
            ]
        }
    ]
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about HDM resource health status, refer to Table 4-108.

Table 4-108 Output Descriptions for Querying Information About the HDM Resource Health Status

Field	Type	Description
@odata.context	Character string	OData description of the specified HDM service resource model.
@odata.id	Character string	Access path of the specified HDM service resource node.
@odata.type	Character string	Type of the specified HDM service resource.
Name	Character string	Name of the specified HDMService resource.
Id	Character string	ID of the specified HDMService resource.
Count	Number	Number of specified resources.
Records	Object	List of HDM service resource objects.
TimeStamp	Number	Health assessment timestamp.
ComponentID	Number	Component ID of the device. For a resource without this information, the parameter is set to 0 by default.
ComponentType	Character string	Component type. For a resource without this information, the parameter is set to an empty string by default.
Slot	Character string	Slot number. For a resource without this information, the parameter is set to 0 by default.
SilkName	Character string	Silk screen of the device.

Field	Type	Description
HealthScore	Number	Health score of the device.
Reasons	Object	List of reasons why the HDMService chassis is not healthy.
ReportTimeStamp	Number	Time when an alarm is reported.
AlarmCode	Number	Alarm code.
Level	Character string	Alarm severity level.
ComponentType	Character string	Component type.

4.61 Querying Information About the SecurityService Resource

Function

Query information about the SecurityService resource of a server.

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 4-109.

Table 4-109 Parameter Descriptions for Querying Information About the SecurityService 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/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"
    },
    "@odata.etag": "W/\"49a2197c00fc2a182517a6bcefb388fa\""
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the SecurityService resource, refer to Table 4-110.

Table 4-110 Output Descriptions for Querying Information About the SecurityService Resource

Field	Type	Description
@odata.context	Character string	OData description of the SecurityService resource model.
@odata.id	Character string	Access path of the SecurityService resource node.
@odata.type	Character string	Type of SecurityService resource.

Field	Type	Description
Name	Character string	Name of the SecurityService resource.
Id	Character string	Unique ID of the SecurityService resource.
FirewallRules	Character string	Lower-level firewall rule URI.
HttpsCert	Character string	URI for SSL certificate information query.

4.62 Querying Information About the SSL Certificate Resource

Function

Query information about the current SSL resource of a server.

Syntax

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

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

- Request Message Body: None

Description

For a description of the parameters for querying the KVM service resource, refer to Table 4-111 .

Table 4-111 Parameter Descriptions for Querying Information About the SSL 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:


```
{
    "@odata.context": "/redfish/v1/$metadata#SecurityService.HttpsCert",
    "@odata.etag": "W/\"cb05d34b99da743a731917dfaada4b0d\"",
    "@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": "Mumbai",
                "CommonName": "Vantageo",
                "Country": "India",
                "Organization": "Vantageo Pvt Ltd",
                 "OrganizationalUnit": "Compute and Storage Product Line",
                "State": "Mumbai"
            },
            "IssuerAddress": "support@vantageo.com",
```

```
            "KeyUsage": "Digital Signature, Non Repudiation, Key Encipherment",
            "PublicKeyLengthBits": "2048",
            "SerialNumber": "4FF5D2D1B5A683DE8616801FAE92BA0D888DA5F9",
            "SignatureAlgorithm": "sha256WithRSAEncryption",
            "Subject": {
                "City": "Mumbai",
                "CommonName": "Vantageo",
                "Country": "India",
                "Organization": "Vantageo Pvt Ltd",
                "OrganizationalUnit": "Compute and Storage Product Line",
                "State": "Mumbai"
            },
            "SubjectAddress": "support@vantageo.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 information about the SSL certificate resource, refer to Table 4-112.

Table 4-112 Output Descriptions for Querying Information About the SSL Certificate Resource

Field	Type	Description
@odata.context	Character string	OData description of the SSL certificate resource model.
@odata.id	Character string	Access path of the SSL certificate resource node.
@odata.type	Character string	Type of SSL certificate service resource.
Id	Character string	ID of the SSL certificate resource.
Name	Character string	Name of the SSL certificate resource.
Version	Character string	Version
IssuerAddress	Character string	Issuer's email address.
KeyUsage	Character string	Certificate used for
PublicKey	Character string	Public Key
PublicKeyLengthBits	Character string	Public key length.

Field	Type	Description
SerialNumber	Character string	Serial number.
SignatureAlgorithm	Character string	Signature algorithm.
Issuer	Character string	Certificate issuer
Subject	Character string	Certificate receiver.
City	Character string	City or area.
CommonName	Character string	Common name.
Country	Character string	Country.
Organization	Character string	Organization.
OrganizationalUnit	Character string	Organizational unit.
State	Character string	Province (state).
SubjectAddress	Character string	Recipient's email address.
ValidNotAfter	Character string	End time of the validity period of the certificate.
ValidNotBefore	Character string	Start time of the validity period of the certificate.

4.63 Importing an SSL Certificate

Function

Import an SSL certificate.

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 4-113.

Table 4-113 Parameter Descriptions for Importing an SSL Certificate

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 via `/redfish/v1/SessionService/Sessions`.
header_type	Format of the request message.	application/json
Certificate	Server certificate.	Certificate file, which can be a file uploaded to a temporary directory of the BMC, a file that can be accessed through HTTPS from a remote server, or the contents of a certificate file.
Privatekey	SSL private key.	Private key file, which can be a file path uploaded to the temporary directory of the BMC, an https remote file, or the content of a certificate 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:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

→ Local import: You need to upload the file to the */tmp/sslcert/* directory of the BMC, and then invoke the interface.

```
{
    "Certificate": "/tmp/sslcert/server.pem",
    "Privatekey": "/tmp/sslcert/privkey.pem"
}
```

→ Remote import:

```
{
    "Certificate": "https://192.168.170.57/server.pem",
    "Privatekey": "https://192.168.170.57/privkey.pem"
}
```

→ Upload text contents directly.

```
{
    "Certificate": "-----BEGIN CERTIFICATE-----
MIIDODCCAiACFHB4CIcZ84cto99USIMDZJ5GPMJaMA0GCSqGSIb3DQEBCwUAMFgx
CzAJBgNVBAYTAkNOMRIwEAYDVQQIDAlHdWFuZ2RvbmcxCzAJBgNVBAcMAlNaMQww
CgYDVQQKDANaVEUxDDAKBgNVBAsMA0JNQzEMMAoGA1UEAwwDVVNBMB4XDTI0MDUy
NzAyNTQzNloXDTI1MDUyNzAyNTQzNlowWTELMAkGA1UEBhMCQ04xEjAQBgNVBAgM
CUd1YW5nZG9uZzELMAkGA1UEBwwCU1oxDDAKBgNVBAoMA1pURTEMMAoGA1UECwwD
Qk1DMQ0wCwYDVQQDDARKYXAuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA2OIk2Y4nY1fNgvTqilHYfDwcR3+71MilpfQUOKRQgy1s+T1tMiKd2cIhnFQT
lozOP53oECznbN8XzTszxuWUpEXOu6Oj6FTN1T7QCiUq/b3W2BZ9wM1K6Wq7Ok72
ZX+0VXDMT4FPoQZrb9dI1MrzHOCWgE0LZgqHuxOur51L+xKrpVqMh8fx+lBGFrhG
pB9Z2jcnZkUTLCl26Fu/L3jLOfQ7vv7kruZi8omOLqLzk0xYneOSHj+3+AWYO2u4
LWI4k/XWWVAnFsSHkBU3EVqTHT2Q0x5PxRBCEkFg/o8DSMgrEehADbSP00xUpHUo
45gHG+j291ELtNMGzTTVvP6WswIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQATZ7IR
maUAYLs3f69+tFREYtr4yyoCmu46QMAn5eFO079jLXwvQnQU7fNZmxwo0yo65m2x
Hs6EgegfHrEFf5ecjPoTV5GfgfKyW76aYsVxfoYx2dp4Tr1BQm7LTdC+pKqikMqz
u5ri3kxz+7k5fsFsSo+FeeMWnMPHiobYDb4F8MsPpwTNfPAev1ZvAVjNzXLLoB+3
gzsRGT2/98BY1Rd8PhMKVaHofXeM/Xkkd/6iNfjsPbZQgaU4IrQAvXfplvQ697Q+
AVwj/prIVOI7p8XGyoJI1v5mTq8w3JkdK3zs+T4uxdSrlacu/g0EcBPL/bmQ4KuW
P6pshnQq2/0TmbuN
-----END CERTIFICATE-------- ",
"Privatekey": "-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA2OIk2Y4nY1fNgvTqilHYfDwcR3+71MilpfQUOKRQgy1s+T1t
MiKd2cIhnFQTlozOP53oECznbN8XzTszxuWUpEXOu6Oj6FTN1T7QCiUq/b3W2BZ9
wM1K6Wq7Ok72ZX+0VXDMT4FPoQZrb9dI1MrzHOCWgE0LZgqHuxOur51L+xKrpVqM
h8fx+lBGFrhGpB9Z2jcnZkUTLCl26Fu/L3jLOfQ7vv7kruZi8omOLqLzk0xYneOS
Hj+3+AWYO2u4LWI4k/XWWVAnFsSHkBU3EVqTHT2Q0x5PxRBCEkFg/o8DSMgrEehA
DbSP00xUpHUo45gHG+j291ELtNMGzTTVvP6WswIDAQABAoIBAQDSfw/tpWH/J95v
aT56iNTzgKoNon3rbK5LQqbfMjDxnvzN08EvrrgoxQ2LjdQ4ZvnjbW/Lh7CufwfU
```

```
yo+M1f/8LeCpmBLWDASIQ4NrGf/KFyVZO03reav/p64T7pbzHsU8ecxMT/LovscK
Wn7be/Qmtx8GEfFth5KDcgP1KWg2oxEoV2a9pvOQSoo4pbb6P4I9zOGfQwA3lvp+
hC/fC78PnbgRtcUY/JOmRJm6xV8xZLc9p1HE34r5U8O8PIqo2MxUQXluoEsSCHNM
ZruBhaqsY8HTnSHO8fJ5e6Er6hnqT49cvaQkj/mYABz7beTPdcSrYlCqHWmhv4Af
JyFvy2XxAoGBAO5oiGwgjAqjvZoW3CorNuuXzLs4TxyOydcUu9fSmAOdRPzUXrL/
y4KP8PpH8SnxNxVH1L1/e3NPMxdLMOUNZ9gZFX5WXg6verZZpAtdUCMRmoLaLAti
KoJi8XuYyAgFHY34pbIiyHZ8EbitAfYjEhyuO3ZO1UcghGCUwS8OhjGfAoGBAOtv
36nAzBk9n+8dBFpiFH5h/jpLrTsxoTA89ng/UM4D9ZzXvTWabcFP+/6YcGcAqp4V
vHsKfI99M62jWlzABZ5DqeeZP3G4XW53xTlflZCk9IsbREmaKP3uc3y3t6zn6tx0
5KSlJF6j84Ha4Bo6X3DVAOes1MLuSbXXjXPOzMptAoGBANVvYDLtMHKWBLhentxh
s9lXHUK/NpRMhia3uTOOpfGXsptmxSEbP+azVtm6bn1OJjI3DI5aAvtIfETuW+e0
CLO+QS/JwosDLqjxt5s0/vlmWR2slKHcUJJKYkZOkSAc9EiVwkGoQi9RA8yBlq/0
1dI3aaSzE/2JbvnIMus/6qOhAoGAQpmcEJ4cXkuDcZWoxJSYLYQO8XKO51jLuyST
qEJo7k5KbXrN6FruD1A7/bJLoaebnCqT7c5ym/iT5Nuf1Trwm+uSJZTBUL8Rlw1E
ek1its8i6jLlZ1i3ndWVT8N8runQE1rxzu1OU11XpfUvjdvTYcywJ9dpPFdB/LGk
Lw1h+yUCgYEAORNvBTLTu8dZwtaeUFUan93r5o/VHvw9OJkTIVvTIMTvDsF6cedJ
kUJPzLVfcVa8MHm4nYU5GzrDyVhH333Juo3JaBhfZadFfS8w+xqDzvHRYOIBmLAD
ebvNBeuXgkf6vjlY1m519dVza3/FV///8DhEfOVLXqg6/hej1XWL2jI=
-----END RSA PRIVATE KEY---------"
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"310ebf6c4d296427ee158442a6b71357\"",
    "@odata.id": "/redfish/v1/Managers/1/SecurityService/HttpsCert/Actions/
    HttpsCert.ImportServerCertificate",
    "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"
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you import an SSL certificate, refer to Table 4-114 .

Table 4-114 Output Descriptions for Importing an SSL Certificate

Field	Type	Description
code	Character string	String indicating the specified message ID in the message registry.
message	Character string	Readable error message corresponding to the one in the message registry.
@odata.type	Character string	OData description of the message resource.
MessageId	Character string	Message ID.
RelatedProperties	Array	Message-related properties.
Message	Character string	Details.
MessageArgs	Array	Message arguments.
Severity	Character string	Severity levels supported by the Redfish, including: ● OK ● Warning ● Critical
Resolution	Character string	Recommended solution.

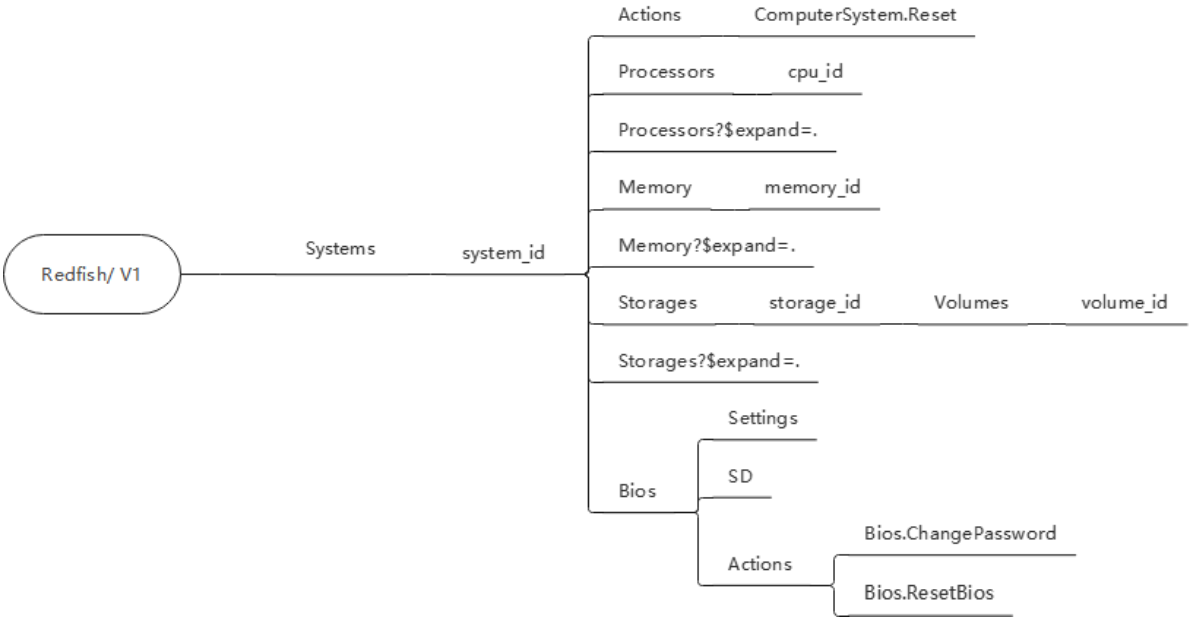
Chapter 5
Operations on System Resources

Table of Contents

Querying Information About the System Resource Collection 243
Querying Information About a Specified System Resource 245
Performing Remote Power-On, Remote Power-Off, and Remote Reset 254
Modifying Properties of a Specified System Resource 256
Setting the System Boot Mode 263
Querying Information About the CPU Resource Collection 266
Querying Information About a Specified CPU Resource 268
Querying Information About All CPU Resources 271
Querying Information About the Memory Resource Collection 274
Querying Information About a Specified Memory Resource 276
Querying Information About All Memory Resources 279
Querying Information About the Storage Resource Collection 282
Querying Information About a Specified Storage Resource 284
Querying Information About All Storage Resources 278
Querying Information About the Logical Volume Resource Collection 291
Querying Information About a Specified Logical Volume Resource 293
Creating a Logical Volume 297
Deleting a Logical Volume 302
Querying Properties of the BIOS Resource 304
Querying BIOS Settings 339
Modifying the BIOS Settings 344
Setting the BIOS Password 348
Restoring Manufacturer-Specified BIOS Configurations 350
Deleting All Logical Volumes 352
Setting Whether a Logical Disk Is a Boot Disk 353

Figure 5-1 shows the path requirements for the Redfish 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	Id	ID of a specified System resource.	GET
	Name	Name of the specified System resource.	GET
	AssetTag	Asset tag of the specified System resource.	GET/PATCH
	Manufacturer	Manufacturer of the specified System resource.	GET
	Model	Model of the specified System resource.	GET
	SerialNumber	Serial number of the specified System resource.	GET

URL	Property	Description	Operation
	UUID	UID of the specified System resource.	GET
	HostName	Name of the specified System resource.	GET/PATCH
	Status	Status of the specified System resource.	GET
	PowerState	Power-on status of the specified System resource.	GET
	IndicatorLED	Position indicator status of the specified drive.	GET/PATCH
	HostName	Name of the specified System resource.	GET
	PartNumber	Component ID of the specified System resource.	GET
	Status	Status of the specified System resource.	GET
	PowerState	Power-on status of the specified System resource.	GET/PATCH
	Boot	Boot parameters of the specified System resource.	GET
	BootSourceOverrideEnabled	Mode for applying the current boot settings of the System.	GET
	BootSourceOverrideEnabled@Redfish.AllowableValues	Options of the mode for applying the current boot settings of the System, including: ● Once: effective only once ● Continuous: effective permanently	GET
	BootSourceOverrideTarget	Current boot settings of the System.	GET
	BootSourceOverrideTarget@Redfish.AllowableValues	Range of the boot devices defined by Redfish, including: ● None ● PXE ● Floppy ● CD ● HDD	GET

URL	Property	Description	Operation
		• BiosSetup	
	BootSourceOverrideMode	System boot mode.	GET
	BootSourceOverrideMode@Redfish.AllowableValues	System boot mode, options: • Legacy only • UEFI only	GET
	BiosVersion	BIOS versions of the specified System resource.	GET
	Actions	Operations that can be performed for the specified System resource through the Redfish interface.	GET
	#ComputerSystem.Reset	OS operation.	GET
	ResetType@Redfish. AllowableValues	OS operations allowed through the Redfish interface, including: • On • ForceOff • GracefulShutdown • ForceRestart • ForcePowerCycle	GET
	target	Access path of properties of the the restart operation.	GET
	Processors	CPU properties of the specified System resource.	GET
	Memory	Memory properties of the specified System resource.	GET
	Storage	Access path of the storage resource node.	GET
	LogServices	Access path of the log service resource node.	GET
	Bios	Access path of the BIOS function resource node.	GET
	Links	Resources link.	GET
	Chassis	Access path of the chassis resource node.	GET
	ManagedBy	Access path of the Manager resource node.	GET

URL	Property	Description	Operation
	PoweredBy	Access path of the power resource node.	GET
	CooledBy	Access path of the fan resource node.	GET
	Oem.Public	Custom properties.	GET
	ConfigurationModel	Year + typical configuration model. The configuration value must be in dictionary format.	GET
	CPUUsagePercent	Dynamic I/O usage detected by CUPS. ● Obtained from the iSDMA when the iSDMA is installed and started completely at the OS side of the server. ● Obtained from the Intel ME when the iSDMA is not installed at the OS side of the server or it is installed but not started completely. For a non-Intel model, the dynamic CPU usage cannot be displayed.	GET
	IOUsagePercent	Dynamic I/O usage detected by CUPS. It is obtained from the Intel ME in any case. For a non-Intel model, the dynamic I/O usage cannot be displayed.	GET
	MemoryUsagePercent	Dynamic memory usage detected by CUPS. ● Obtained from the iSDMA when the iSDMA is installed and started completely at the OS side of the server. ● Obtained from Intel ME when the iSDMA is not installed at the OS side of the server or it is installed but not started completely. For a non-Intel model, the dynamic memory usage cannot be displayed.	GET

URL	Property	Description	Operation
	PowerOnDelayEnabled	Whether power-on delay is enabled: ● true ● false	GET
	PowerOnDelayMode	Power-on delay mode: ● CustomDelay: custom delay mode. ● RandomDelay: random delay mode.	GET
	PowerOnDelaySeconds	Power-on delay in custom delay mode.	GET
	PowerButtonEnable	Whether the custom power button function is enabled: ● Enabled ● Disabled	GET
	PowerOnStrategy	Custom power-on policy: ● TurnOn: stays on. ● RestorePreviousState: same as before. ● StayOff: stays off.	GET
	BootSourceOverrideMode	System boot mode: ● Legacy ● UEFI	GET
	MaintenanceSerialNumber	Serial number of the mainboard.	GET
	ProductName	Custom product name.	GET
	ProductSpecificIdentity	Product ID, planned product name, mainboard name, and CPU manufacturer.	GET
	ProductVersion	Product version number.	GET
	DiskIndex	Disk partition number.	GET
	PartitionName	Disk partition name.	GET
	TotalCapacityGB	Total capacity of a disk partition.	GET
	UsagePercen	Usage of a disk partition in percentage.	GET
	SystemMemoryTotalGiB	Total available memory size of the system, unit: GB (valid after the iSD-	GET

URL	Property	Description	Operation
		MA 2.0 is installed on the OS side of the server and is completely started).	
	SystemMemoryUsageGiB	Used memory size of the system, unit: GB (valid after the iSDMA 2.0 is installed on the OS side of the server and is completely started).	GET
	SystemMemoryFreeGiB	Remaining memory size of the system, unit: GB (valid after the iSDMA 2.0 is installed on the OS side of the server and is completely started).	GET
	code	ID of the specified message in the message registry.	PATCH
	message	Error message corresponding to the message in the message registry.	PATCH
	MessageId	Message ID.	PATCH
	RelatedProperties	Message-related properties.	PATCH
	Message	Details.	PATCH
	Severity	Severity levels supported by Redfish, including: ● OK ● Warning ● Critical	PATCH
	Resolution	Recommended solution.	PATCH
/redfish/v1/Systems/system_id/Actions/ComputerSystem.Reset	code	ID of the specified message in the message registry.	POST
	message	Error message corresponding to the message in the message registry.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	Severity	Severity level. Severity levels supported by Redfish, including: ● OK ● Warning ● Critical	POST

URL	Property	Description	Operation
	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 URLs.	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: ● x86 ● x86-64 ● IA-64 ● ARM-A32 ● ARM-A64 ● MIPS32 ● MIPS64 ● OEM	GET
	ProcessorArchitecture	CPU architecture.	GET
	Manufacturer	CPU manufacturer.	GET
	Model	CPU type.	GET
	MaxSpeedMHz	Maximum CPU speed.	GET
	TDPWatts	CPU nominal TDP.	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.	GET
	L1CacheKiB	Level I cache of the specified CPU resource, unit: KiB.	GET
	L2CacheKiB	Level II cache of the specified CPU resource, unit: KiB.	GET

URL	Property	Description	Operation
	L3CacheKiB	Level III cache of the specified CPU resource, unit: KiB.	GET
	FrequencyMHz	Frequency of the specified CPU resource, unit: MHz.	GET
	SerialNumber	Serial number of the specified CPU resource.	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
	CapacityMiB	Capacity of the specified memory resource.	GET
	Manufacturer	Manufacturer of the specified memory resource.	GET
	AllowedSpeedsMHz	Maximum speed 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

URL	Property	Description	Operation
	DeviceLocator	Silk screen 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
/redfish/v1/Systems/system_id/Memory?$expand=.	Name	Name of the memory resource collection.	GET
	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	Id	ID of the specified storage resource.	GET
	Name	Name of the specified storage resource.	GET
	StorageControllers@odata.count	Number of storage controllers.	GET

URL	Property	Description	Operation
	StorageControllers	Information about the storage controllers.	GET
	Name	Name of a storage controller.	GET
	Status	Status of the storage controller.	GET
	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
	SerialNumber	Serial number of the storage controller.	GET
	Oem.Publicl	Manufacturer-customized properties.	GET
	MemorySizeMiBl	Memory size of the specified storage controller.	GET
	CapacitanceStatusl	BBU status of the specified storage controller.	GET
	Drives@odata.count	Number of drives managed by the storage controller.	GET
	Drives	Drive list.	GET
	Oem	Customized properties of the storage controller.	GET
	Description	Information about the specified storage controller.	GET
	PHYStatus	Physical-layer bit error status of the specified controller.	GET
	InvalidDwordCount	Number of invalid DWORDs.	GET

URL	Property	Description	Operation
	LossDwordSyncCount	Number of times that DWORD synchronization is lost.	GET
	PHYId	Customized properties of the storage controller.	GET
	PhyResetProblemCount	Number of PHY restart problems.	GET
	RunningDisparityErrorCount	Number of running disparity errors.	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.	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	Error message corresponding to the message 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
	Resolution	Recommended solution.	POST
/redfish/v1/Systems/system_id/Storages/storage_id/Volumes/volume_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

URL	Property	Description	Operation
	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
	BootEnable	Whether it is a boot disk.	GET
	IoPolicy	I/O policy of the logical volume.	GET
	VolumeName	Name of the logical volume.	GET
	Links	Resources link.	GET
	Status	Status of the logical volume.	GET
	NumDriveperspan	Number of drive members in a span.	GET
	SpanNumber	Number of spans of a volume.	GET
	code	ID of the specified message in the message registry.	DELETE
	message	Error message corresponding to the message in the message registry.	DELETE
	MessageId	Message ID.	DELETE
	RelatedProperties	Message-related properties.	DELETE
	Message	Details.	DELETE
	MessageArgs	Message arguments.	DELETE

URL	Property	Description	Operation
	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/Settings	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
	Actions	Operations that can be performed on the BIOS resource.	GET
	@Redfish.Settings	Information about BIOS settings.	GET
/redfish/v1/Systems/system_id/Bios/SD	Id	ID of the BIOS setting resource.	GET
	Name	Name of the BIOS setting resource.	GET
	Attributes	Property list of the current BIOS setting resource.	GET
	Actions	Operations that can be performed on the BIOS resource.	GET
	@Redfish.Settings	Information about BIOS settings.	GET
/redfish/v1/Systems/system_id/Bios/Actions/Bios.ChangePassword	code	ID of the specified message in the message registry.	POST
	message	Error message corresponding to the message in the message registry.	POST
	@odata.type	OData description of the message resource.	POST
	MessageId	Message ID.	POST

URL	Property	Description	Operation
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	Severity	Severity level.	POST
	Resolution	Recommended solution.	POST
/redfish/v1/Systems/system_id/Bios/Actions/Bios.ResetBios	code	ID of the specified message in the message registry.	POST
	message	Error message corresponding to the message in the message registry.	POST
	@odata.type	OData description of the message resource.	POST
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST
	Message	Details.	POST
	Severity	Severity level.	POST
	Resolution	Recommended solution.	POST
redfish/v1/Systems/system_id/Storages/storage_id/Volumes/volumes_id	ame	Name of the specified logic volume resource.	PATCH
	Id	ID of the specified logical volume ID.	PATCH
	VolumeType	Redundancy type of the logical volume.	PATCH
	CapacityBytes	Capacity of the logical volume.	PATCH
	OptimumIOSizeBytes	Stripe size of the logical volume.	PATCH
	Links	Member logical volume list.	PATCH
	Drives	Drive list managed by the specified storage controller.	PATCH
	@odata.id	Access path of the specified drive.	PATCH
	Drives@odata.count	Number of member physical disks included in the RAID.	PATCH
	Status	Status of the specified logical volume resource.	PATCH
	Oem.Public	Customized logical volume information.	PATCH

URL	Property	Description	Operation
	RaidControllerID	Controller ID of the logical volume.	PATCH
	VolumeRaidLevel	RAID level of the logical volume. The value must be in dictionary format.	PATCH
	DriveCachePolicy	Hard disk cache policy.	PATCH
	NumDrive	Number of physical disk members.	PATCH
	ReadPolicy	Read policy of the logical volume.	PATCH
	WritePolicy	Write policy of the logical volume.	PATCH
	AccessPolicy	Access policy of the logical volume.	PATCH
	BootEnable	Whether it is a boot disk.	PATCH
	IoPolicy	I/O policy of the logical volume.	PATCH
	VolumeName	Name of the logical volume.	PATCH
	State	Status of the logical volume.	PATCH
	NumDriveperspan	Number of drive members in a span.	PATCH
	SpanNumber	Number of spans of a volume.	PATCH

5.1 Querying Information About the System Resource Collection

Function

Query information about the current System resource collection of a server.

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.
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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1581093321\"",
    "@odata.id": "/redfish/v1/Systems",
    "@odata.type": "#ComputerSystemCollection.ComputerSystemCollection",
    "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.
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 a server itself can be queried.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Systems/system_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 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**.

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 */redfish/v1/SessionService/Sessions*.

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:

```
{
    "@odata.context": "/redfish/v1/$metadata#ComputerSystem.ComputerSystem",
    "@odata.etag": "W/\"1620798675\"",
    "@odata.id": "/redfish/v1/Systems/1",
    "@odata.type": "#ComputerSystem.v1_5_0.ComputerSystem",
    "Actions": {
        "#ComputerSystem.Reset": {
            "ResetType@Redfish.AllowableValues": [
                "On",
                "ForceOff",
                "GracefulShutdown",
                "ForceRestart",
                "PowerCycle",
                "ForcePowerCycle"
            ],
            "target": "/redfish/v1/Systems/1/Actions/ComputerSystem.Reset"
        }
    },
    "AssetTag": "CYMHsV3kDojd",
    "Bios": {
        "@odata.id": "/redfish/v1/Systems/1/Bios"
    },
    "BiosVersion": "03.18.0100",
    "Boot": {
        "BootSourceOverrideMode" "Legacy only",
```

```
    "BootSourceOverrideEnabled@Redfish.AllowableValues": [
        "Legacy only",
        "UEFI only"
    ],
    "BootSourceOverrideEnabled": "Once",
    "BootSourceOverrideEnabled@Redfish.AllowableValues": [
        "Once",
        "Continuous"
    ],
    "BootSourceOverrideTarget": "None",
    "BootSourceOverrideTarget@Redfish.AllowableValues": [
        "None",
        "Pxe",
        "Cd",
        "Floppy",
        "Hdd",
        "BiosSetup",
        "RemotelyHdd",
    ]
},
"Description": "System 1",
"HostName": "ZyzuOO-1dy-Xoy4-LDmoZFOiR43XYFqVX2tfwRYqdC9iJd9KDzRe",
"Id": "1",
"IndicatorLED": "Off",
"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"
},
"Model": "2230-RE",
"Name": "System",
"Oem": {
    "Public": {
        "BiosVersionDate": "Jan 1 2023",
        "CPUUsagePercent": 0,
        "CmccVersion": "2020V1",
        "Version": "2020V1",
        "ConfigurationModel": "202011031558",
        "IOUsagePercent": 0,
        "MaintenanceSerialNumber":"",
        "MemoryUsagePercent": 0,
        "PartitionLists": [
            {
                "DiskIndex": 1,
                "PartitionName": "/",
                "TotalCapacityGB": 50,
                "UsagePercent": 14
            },
            {
                "DiskIndex": 2,
                "PartitionName": "/boot",
                "TotalCapacityGB": 1,
                "UsagePercent": 17
            },
            {
                "DiskIndex": 3,
                "PartitionName": "/boot/efi",
                "TotalCapacityGB": 0.2,
                "UsagePercent": 5
            },
            {
                "DiskIndex": 4,
                "PartitionName": "/home",
                "TotalCapacityGB": 212.6,
                "UsagePercent": 1
            }
            ],
```

```
            "PowerOnDelayEnabled": false,
            "PowerOnDelayMode": "CustomDelay",
            "PowerOnDelaySeconds": 20,
            "PowerButtonEnable": "Disabled",
            "PowerOnStrategy": "TurnOn",
            "ProductName": "2230-RE",
            "ProductSpecificIdentity": "2230-RE,SPLMA,Intel"
            "ProductExtra": "SSC02-X17-25D-NA",
            "SystemMemoryFreeGiB": 41.40,
            "SystemMemoryUsageGiB": 4.60,
            "SystemMemoryTotalGiB": 46
        }
    },
    "PartNumber": "202011031446",
    "PowerState": "Off",
    "Processors": {
        "@odata.id": "/redfish/v1/Systems/1/Processors"
    },
    "SerialNumber": "202011031440",
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "Storages": {
        "@odata.id": "/redfish/v1/Systems/1/Storages"
    },
    "SystemType": "Physical",
    "UUID": "60816054-0000-1000-0000-202103221328"
    "ProductVersion": "Intel Whitley IceLake"
}
```


- 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.

Field	Type	Description
@odata.id	String	Access path of the specified System resource node.
@odata.type	String	Type of System resource.
Id	String	ID of the specified System resource.
Name	String	Name of the specified System resource.
AssetTag	String	Asset tag of the specified System resource.
Manufacturer	String	Manufacturer of the specified System resource.
Model	String	Model of the specified System resource.
SerialNumber	String	Serial number of the specified System resource.
UUID	String	Globally unique ID of the specified System resource.
IndicatorLED	String	Positioning indicator status of the specified chassis resource, options: ● Lit ● Off ● Blinking
HostName	String	Hostname of the specified System resource.
PartNumber	String	Part number of the specified System resource.
Status	Object	Status of the specified System resource, including ● Health: The System resource is healthy. ● Status: The System resource is enabled.
PowerState	String	Power-on status of the specified System resource, including ● On ● Off
Boot	Object	Boot parameters of the specified System resource.

Field	Type	Description
BootSourceOverrideEnabled	String	Mode for applying the current boot settings 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
BootSourceOverrideTarget	String	Current boot settings of the System.
BootSourceOverrideTarget@Redfish.AllowableValues	Array	Range of the boot devices defined by the Redfish, including: ● None ● PXE ● Floppy ● CD ● HDD ● BiosSetup ● RemotelyHdd
BootSourceOverrideMode	String	System boot mode.
BootSourceOverrideMode@Redfish.AllowableValues	String	System boot mode, options: ● Legacy only ● UEFI only
BiosVersion	String	BIOS version of the specified System resource.
Actions	Object	Operations that can be performed for the specified System resource through the Redfish interface.
#ComputerSystem.Reset	Object	OS operation.
ResetType@Redfish. Allowa bleValues	Array	OS operations allowed through the Redfish interface, including: ● On ● ForceOff ● GracefulShutdown ● ForceRestart ● ForcePowerCycle
target	String	Access path of the restart operation properties.
Processors	Array	Access path of the processor resource node.

Field	Type	Description
Memory	Array	Access path of the memory resource node.
Storages	Array	Access path of the storage resource node.
Bios	Array	Access path of the BIOS resource node.
Links	Array	System resource links.
Chassis	Array	Access path of the chassis resource node.
ManagedBy	Array	Access path of the Manager resource node.
PoweredBy	Array	Access path of the power resource.
CooledBy	Array	Access path of the fan resource node.
Oem.Public	Object	Customized properties.
ConfigurationModel	String	Year + typical configuration model. The configuration value must be in dictionary format.
CPUUsagePercent	Number	Dynamic CPU usage detected by CUPS. ● Obtained from the iSDMA when the iSDMA is installed and started completely at the OS side of the server. ● Obtained from the Intel ME when the iSDMA is not installed at the OS side of the server or it is installed but not started completely. For a non-Intel model, the dynamic CPU usage cannot be displayed.
IOUsagePercent	Number	Dynamic I/O usage detected by CUPS. It is obtained from the from Intel ME in any case. For a non-Intel model, the dynamic I/O usage cannot be displayed.
MemoryUsagePercent	Number	Dynamic memory usage detected by CUPS. ● Obtained from the iSDMA when the iSDMA is installed and started completely at the OS side of the server. ● Obtained from Intel ME when the iSDMA is not installed at the OS side of the server or it is installed but not started completely. For a non-Intel model,

Field	Type	Description
		the dynamic memory usage cannot be displayed.
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 custom delay mode.
PowerButtonEnable	String	Whether the custom power button function is enabled: ● Enabled ● Disabled
PowerOnStrategy	String	Custom power-on policy: ● TurnOn: The server powers on. ● RestorePreviousState: same as before. ● StayOff: The server stays off.
BootSourceOverrideMode	String	System boot mode: ● Legacy ● UEFI
MaintenanceSerialNumber	String	Serial number of the mainboard.
ProductName	String	Custom product name.
ProductSpecificIdentity	String	Product ID, planned product name, mainboard name, and CPU manufacturer.
ProductVersion	String	Product version number.
DiskIndex	Number	Disk partition number.
PartitionName	String	Disk partition name.
TotalCapacityGB	Number	Total Capacity of a disk partition.
UsagePercent	Number	Usage of a disk partition in percentage.
SystemMemoryTotalGiB	Number	Total available memory size of the system, unit: GB (valid after the iSDMA 2.0 is installed on the OS side of the server and is completely started).
SystemMemoryUsageGiB	Number	Used memory size of the system, unit: GB (valid after the iSDMA 2.0 is installed on

Field	Type	Description
		the OS side of the server and is completely started).
SystemMemoryFreeGiB	Number	Remaining memory size of the system, unit: GB (valid after the iSDMA 2.0 is installed on the OS side of the server and is completely started).

5.3 Performing Remote Power-On, Remote Power-Off, and Remote Reset

Function

Remotely power on, power off, and reset a System resource.

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 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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json

Parameter	Description	Value
value	Operation type.	• On: power-on • 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:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1571459532\"",
    "@odata.id": "/redfish/v1/Systems/1/Actions/ComputerSystem.Reset",
    "error":
    {
        "@Message.ExtendedInfo":
        [{
            "@odata.type": "#Message.v1_0_5.Message",
            "Message": "Successfully Completed Request",
            "MessageId": "Base.1.0.Success",
            "Resolution": "None",
            "Severity": "OK"
        }],
        "code": "Base.1.0.Success",
        "message": "Successfully Completed Request"
```

```
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you perform remote operations, 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	Error message corresponding to the message 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.
Severity	String	Severity levels supported by Redfish, including: ● 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, hostname, and typical configuration model.

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,
    "Boot": {
        "BootSourceOverrideMode": bootsourceoverride_mode,
        "BootSourceOverrideEnabled":bootsourceoverride_enable
    },
    "Oem": {
        "Public": {
            "CmccVersion": "cmcc_version",
            "Version": "version",
            "ConfigurationModel":model,
            "PowerOnDelayEnabled":powerondealy_enable,
            "PowerOnDelayMode":powerondelay_mode,
            "PowerOnDelaySeconds":powerondealy_seconds,
            "PowerButtonEnable":value,
            "PowerOnStrategy": "RestorePreviousState"
        }
    }
}
```

Description

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
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 PATCH request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
tag	Customized asset tags.	• Length: 1–63 characters. • Consists of digits or letters, case-sensitive. • The allowed special characters include hyphens, underscores, spaces, "at" signs, and colons. • The tag cannot start or end with a hyphen, an underscore, or a space.

Parameter	Description	Value
name	Custom hostname.	● The length cannot exceed 63 characters. ● Only letters, digits, and hyphens are allowed. ● No blank characters including spaces, tabs, and line breaks, are allowed. The name is not case-sensitive. ● The first character must be a letter, and the last character cannot be a hyphen.
model	Custom 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
powerondelay_mode	Power-on delay mode.	● RandomDelay: random delay mode. ● CustomDelay: custom delay mode.
powerondealy_seconds	Power-on delay time.	Range: 1–120, unit: seconds.
powerButtonEnable	Whether the power button function is enabled:	● Enabled: The power button function is enabled. ● Disabled: The power button function is disabled.
PowerOnStrategy	Power-on policy.	● StayOff: The server stays off. ● RestorePreviousState: restores the state before power-off. ● TurnOn: The server powers on.
BootSourceOverrideMode	String	System boot mode, options: ● Legacy ● UEFI
bootsourceoverride_enable	String	Mode for applying the current boot settings of the System. Options: ● Once ● Continuous

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": "mytest",
    "HostName": "mytest",
    "Boot": {
        "BootSourceOverrideMode": "UEFI only",
        "BootSourceOverrideEnabled": "Once"
    }
    "Oem": {
        "Public": {
            "CmccVersion": "2022V1",
            "Version": "2022V1",
            "ConfigurationModel": "2019C1",
            "PowerOnDelayEnabled": true,
            "PowerOnDelayMode": "CustomDelay",
            "PowerOnDelaySeconds": 20,
            "PowerButtonEnable": "Disabled"
        }
    }
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#ComputerSystem.ComputerSystem",
    "@odata.etag": "W/\"1620798675\"",
    "@odata.id": "/redfish/v1/Systems/1",
    "@odata.type": "#ComputerSystem.v1_5_0.ComputerSystem",
    "Actions": {
        "#ComputerSystem.Reset": {
            "ResetType@Redfish.AllowableValues": [
                "On",
                "ForceOff",
                "GracefulShutdown",
                "ForceRestart",
```

```
            "PowerCycle",
            "ForcePowerCycle"
        ],
        "target": "/redfish/v1/Systems/1/Actions/ComputerSystem.Reset"
    }
},
"AssetTag": "CYMHsV3kDojd",
"Bios": {
    "@odata.id": "/redfish/v1/Systems/1/Bios"
},
"BiosVersion": "03.18.0100",
"Boot": {
    "BootSourceOverrideMode" "Legacy only",
        "BootSourceOverrideEnabled@Redfish.AllowableValues": [
        "Legacy only",
        "UEFI only"
    ],
    "BootSourceOverrideEnabled": "Once",
    "BootSourceOverrideEnabled@Redfish.AllowableValues": [
        "Once",
        "Continuous"
    ],
    "BootSourceOverrideTarget": "None",
    "BootSourceOverrideTarget@Redfish.AllowableValues": [
        "None",
        "Pxe",
        "Cd",
        "Floppy",
        "Hdd",
        "BiosSetup",
        "RemotelyHdd",
    ]
},
"Description": "System 1",
"HostName": "ZyzuOO-1dy-Xoy4-LDmoZFOiR43XYFqVX2tfwRYqdC9iJd9KDzRe",
"Id": "1",
"IndicatorLED": "Off",
"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"
    },
    "Model": "2230-RE",
    "Name": "System",
    "Oem": {
        "Public": {
            "BiosVersionDate": "Jan 1 2023",
            "CPUUsagePercent": 0,
            "CmccVersion": "2020V1",
            "Version": "2020V1",
            "ConfigurationModel": "202011031558",
            "IOUsagePercent": 0,
            "MaintenanceSerialNumber":"",
            "MemoryUsagePercent": 0,
            "PartitionLists": [
                {
                    "DiskIndex": 1,
                    "PartitionName": "/",
                    "TotalCapacityGB": 50,
                    "UsagePercent": 14
                },
                {
                    "DiskIndex": 2,
                    "PartitionName": "/boot",
                    "TotalCapacityGB": 1,
                    "UsagePercent": 17
                },
```

```
                {
                    "DiskIndex": 3,
                    "PartitionName": "/boot/efi",
                    "TotalCapacityGB": 0.2,
                    "UsagePercent": 5
                },
                {
                    "DiskIndex": 4,
                    "PartitionName": "/home",
                    "TotalCapacityGB": 212.6,
                    "UsagePercent": 1
                }
            ],
            "PowerOnDelayEnabled": false,
            "PowerOnDelayMode": "CustomDelay",
            "PowerOnDelaySeconds": 20,
            "PowerButtonEnable":"Disabled",
            "PowerOnStrategy": "TurnOn",
            "ProductName": "2230-RE",
            "ProductSpecificIdentity": "2230-RE,SPLMA,Intel",
            "ProductExtra": "SSC02-X17-25D-NA",
            "SystemMemoryFreeGiB": 41.40,
            "SystemMemoryUsageGiB": 4.60,
            "SystemMemoryTotalGiB": 46
        }
    },
    "PartNumber": "202011031446",
    "PowerState": "Off",
    "Processors": {
        "@odata.id": "/redfish/v1/Systems/1/Processors"
    },
    "SerialNumber": "202011031440",
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "Storages": {
        "@odata.id": "/redfish/v1/Systems/1/Storages"
    },
    "SystemType": "Physical",
    "UUID": "60816054-0000-1000-0000-202103221328",
    "ProductVersion": "Intel Whitley IceLake"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you modify properties of the specific System resource, refer to Table 5-9.

Table 5-9 Output Descriptions for Modifying Properties of the Specified System Resource

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Error message corresponding to the message in the message registry.
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Detailed information.
Severity	String	Severity levels supported by Redfish, including: ● OK ● Warning ● Critical
Resolution	String	Solution.

5.5 Setting the System Boot Mode

Function

Set the system boot mode.

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:

```
{
    "Boot": {
        "BootSourceOverrideEnabled": state,
        "BootSourceOverrideTarget": target
    }
```

```
}
```

Parameters

For a description of the parameters for boot mode, refer to Table 5-10.

Table 5-10 Parameter Descriptions for Boot Mode

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
system_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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
Boot	Parameters for boot mode.	-
state	Mode for applying the boot settings.	• "Once": effective only once • "Continuous": effective permanently
target	Type of boot mode.	Boot devices defined by the Redfish, including: • "None": no override • "Pxe": network • "Cd": CD-ROM drive • "Floppy": USB • "Hdd": hard disk • "BiosSetup": BIOS • "RemotelyHdd": volume

Usage Guidelines

When the setting is completed, the "Boot" field 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:

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

- Request Message Body:

```
{
```

```
    "Boot":
    {
        "BootSourceOverrideTarget": "Pxe",
        "BootSourceOverrideEnabled": "Once"
    }
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1587980565\"",
    "@odata.id": "/redfish/v1/Systems/1",
    "error":
    {
        "@Message.ExtendedInfo":
        [{
            "@odata.type": "#Message.v1_0_5.Message",
            "Message": "Successfully Completed Request",
            "MessageId": "Base.1.0.Success",
            "Resolution": "None",
            "Severity": "OK"
        }],
        "code": "Base.1.0.Success",
        "message": "Successfully Completed Request"
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you set system boot mode, refer to Table 5-11.

Table 5-11 Output Descriptions for Setting System Boot Mode

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Error message corresponding to the message 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.
Severity	String	Severity levels supported by Redfish, including:

Field	Type	Description
		• OK • Warning • Critical
Resolution	String	Solution.

5.6 Querying Information About the CPU Resource Collection

Function

Query information about the CPU resource collection of a server.

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 5-12.

Table 5-12 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.
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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1581184010\"",
    "@odata.id": "/redfish/v1/Systems/1/Processors",
    "@odata.type": "#ProcessorCollection.ProcessorCollection",
    "Description": "Collection of processors for this system",
    "Members":
    [{
        "@odata.id": "/redfish/v1/Systems/1/Processors/0"
    },
    {
        "@odata.id": "/redfish/v1/Systems/1/Processors/1"
    }],
    "Members@odata.count": 2,
    "Name": "Processors Collection"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the CPU resource collection, refer to Table 5-13.

Table 5-13 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.
Name	String	Name of the CPU resource collection.
Members@odata.count	Number	Number of CPU resource members.
Members	Object	CPU resource list.
@odata.id	String	Access path of a single CPU resource node.

5.7 Querying Information About a Specified CPU Resource

Function

Query information about a specified CPU resource of a server.

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

Description

For a description of the parameters for querying information about the specified CPU resource, refer to Table 5-14.

Table 5-14 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 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 */redfish/v1/SessionService/Sessions*.
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.etag": "W/\"1593355555\"",
    "@odata.id": "/redfish/v1/Systems/1/Processors/0",
    "@odata.type": "#Processor.v1_2_0.Processor",
    "Id": "0",
    "InstructionSet": "X86-64",
    "Manufacturer": "Intel(R) Corporation",
    "MaxSpeedMHz": 2000,
    "Model": "Intel(R) Xeon(R) Gold 5117M CPU @ 2.00GHz",
    "Name": "Intel Processor 0",
    "Oem": {
        "Public": {
            "FrequencyMHz": 2000,
            "L1CacheKiB": 896,
            "L2CacheKiB": 14336,
            "L3CacheKiB": 19712,
            "SerialNumber": "A64A681526E47C98"
        }
    },
    "ProcessorArchitecture": "x86",
    "ProcessorId": {
        "IdentificationRegisters":  "54-06-05-00-ff-fb-eb-bf"
    },
    "ProcessorType": "Central Processor",
    "Socket": 0,
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "TDPWatts": 270,
    "TotalCores": 14,
    "TotalThreads": 14
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified CPU resource, refer to Table 5-15.

Table 5-15 Output Descriptions for Querying Information About the Specified CPU Resource

Field	Type	Description
@odata.context	String	OData description of the specified CPU resource model.
@odata.id	String	Access path of the specified CPU resource node.
@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
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.
TDPWatts	Number	Nominal TDP of the specified CPU resource, unit: Watts.
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

Field	Type	Description
Oem.Public	Object	Manufacturer-customized properties.
L1CacheKiB	Number	Level I cache of the specified CPU resource, unit: KiB.
L2CacheKiB	Number	Level II cache of the specified CPU resource, unit: KiB.
L3CacheKiB	Number	Level III cache of the specified CPU resource, unit: KiB.
FrequencyMHz	Number	Frequency of the specified CPU resource, unit: MHz.
SerialNumber	String	Serial number of the specified CPU resource.

5.8 Querying Information About All CPU Resources

Function

Query information about all CPU resources of a server.

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

Description

For a description of the parameters for querying information about all CPU resources, refer to Table 5-16.

Table 5-16 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1593376255\"",
    "@odata.id": "/redfish/v1/Systems/1/Processors",
    "@odata.type": "#ProcessorCollection.ProcessorCollection",
    "Members": [{
        "@odata.id": "/redfish/v1/Systems/1/Processors/0",
        "@odata.type": "Processor.v1_2_0.Processor",
        "Id": "0",
        "InstructionSet": "X86_64",
        "Manufacturer": "Intel(R) Corporation",
        "MaxSpeedMHz": 2000,
        "Model": "Intel(R) Xeon(R) Gold 5117M CPU @ 2.00GHz",
        "Name": "Intel Processor 0",
        "Oem": {
            "Public": {
                "FrequencyMHz": 2000,
                "L1CacheKiB": 896,
                "L2CacheKiB": 14336,
                "L3CacheKiB": 19712,
                "SerialNumber": "A64A681526E47C98"
            }
        },
        "ProcessorArchitecture": "x86",
        "ProcessorId": {
            "IdentificationRegisters":  "54-06-05-00-ff-fb-eb-bf"
        },
        "ProcessorType": "Central Processor",
        "Socket": 0,
        "Status": {
```

```
            "Health": "OK",
            "State": "Enabled"
        },
        "TDPWatts": 270,
        "TotalCores": 14,
        "TotalThreads": 14
    }, {
        "@odata.id": "/redfish/v1/Systems/1/Processors/1",
        "@odata.type": "Processor.v1_2_0.Processor",
        "Id": "1",
        "InstructionSet": "X86_64",
        "Manufacturer": "Intel(R) Corporation",
        "MaxSpeedMHz": 2000,
        "Model": "Intel(R) Xeon(R) Gold 5117M CPU @ 2.00GHz",
        "Name": "Intel Processor 1",
        "Oem": {
            "Public": {
                "FrequencyMHz": 2000,
                "L1CacheKiB": 896,
                "L2CacheKiB": 14336,
                "L3CacheKiB": 19712,
                "SerialNumber": "A64A6612C85F06A0"
            }
        },
        "ProcessorArchitecture": "x86-64",
        "ProcessorId": {
            "IdentificationRegisters":  "54-06-05-00-ff-fb-eb-bf"
        },
        "ProcessorType": "Central Processor",
        "Socket": 1,
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        },
        "TDPWatts": 270,
        "TotalCores": 14,
        "TotalThreads": 14
    }],
    "Members@odata.count": 2,
    "Name": "Processors Collection"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about all CPU resources, refer to Table 5-17.

Table 5-17 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 node.
@odata.type	String	Type of 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. For the requirements for the parameters, refer to 5.7 Querying Information About a Specified CPU Resource.

5.9 Querying Information About the Memory Resource Collection

Function

Query information about the current memory resource collection of a server.

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 5-18.

Table 5-18 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.

Parameter	Description	Value
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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1593007779\"",
    "@odata.id": "/redfish/v1/Systems/1/Memory",
    "@odata.type": "#MemoryCollection.MemoryCollection",
    "Description": "Collection of Memories for this system",
    "Members":
    [{
        "@odata.id": "/redfish/v1/Systems/1/Memory/DIMM7"
    },
    {
        "@odata.id": "/redfish/v1/Systems/1/Memory/DIMM13"
    }],
    "Members@odata.count": 2,
    "Name": "Memory Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the memory resource collection, refer to Table 5-19.

Table 5-19 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.
Name	String	Name of the memory resource collection.
Members@odata.count	Number	Number of memory resource members.
Members	Object	Memory resource list.
@odata.id	String	Access path of a single memory resource node.

5.10 Querying Information About a Specified Memory Resource

Function

Query information about a specified memory resource of a server.

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

Description

For a description of the parameters for querying information about the specified memory resource, refer to Table 5-20.

Table 5-20 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 */redfish/v1/SessionService/Sessions*.

Parameter	Description	Value
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/DIMM7
```

- Request Header:

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

- Request Message Body: None
- Response Example:


```
{
    "@odata.context": "/redfish/v1/$metadata#Memory.Memory",
    "@odata.etag": "W/\"1593007796\"",
    "@odata.id": "/redfish/v1/Systems/1/Memory/DIMM7",
    "@odata.type": "#Memory.v1_4_0.Memory",
    "AllowedSpeedsMHz":2666,
    "BaseModuleType": "RDIMM",
    "CapacityMiB": 16384,
    "DataWidthBits": 64,
    "DeviceLocator": "DIMM7",
    "ECCType": "Multi-bit ECC",
    "Id": "DIMM7",
    "Manufacturer": "Samsung",
    "MemoryDeviceType": "DDR4",
    "MemoryLocation":
    {
        "Channel": 3,
        "Controller": 1,
        "Slot": 0,
        "Socket": 0
    },
    "Name": "DIMM7",
    "OperatingSpeedMhz": 2666,
    "PartNumber": "M393A2K43CB2-CTD",
    "RankCount": 2,
    "SerialNumber": "385cfb2e",
```

```
    "Status":
    {
        "Health": "OK",
        "State": "Enabled"
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified memory resource, refer to Table 5-21.

Table 5-21 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 node.
@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.
CapacityMiB	Number	Capacity of the specified memory resource, in MB.
Manufacturer	String	Manufacturer of the specified memory device.
AllowedSpeedsMHz	Number	Maximum speed of the specified memory resource.
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 or 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	Silk screen of the specified memory resource.
BaseModuleType	String	Basic module type of the specified memory resource, including: ● RDIMM ● UDIMM

Field	Type	Description
		• 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: enabling status of the specified memory resource

5.11 Querying Information About All Memory Resources

Function

Query information about the current memory resource collection of a server.

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 5-22.

Table 5-22 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/system_id/Memory?$expand=.
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#MemoryCollection.MemoryCollection",
    "@odata.etag": "W/\"1593007893\"",
    "@odata.id": "/redfish/v1/Systems/1/Memory",
    "@odata.type": "#MemoryCollection.MemoryCollection",
    "Description": "Collection of Memories for this system",
    "Members":
    [{
        "@odata.id": "/redfish/v1/Systems/1/Memory/DIMM7",
        "@odata.type": "Memory.v1_4_0.Memory",
        "BaseModuleType": "RDIMM",
        "CapacityMiB": 16384,
        "DataWidthBits": 64,
        "DeviceLocator": "DIMM7",
        "ECCType": "Multi-bit ECC",
        "Id": 7,
        "Manufacturer": "Samsung",
        "MemoryDeviceType": "DDR4",
        "MemoryLocation":
        {
```

```
            "Channel": 3,
            "Controller": 1,
            "Slot": 7,
            "Socket": 0
        },
        "Name": "DIMM7",
        "OperatingSpeedMhz": 2666,
        "PartNumber": "M393A2K43CB2-CTD",
        "RankCount": 2,
        "SerialNumber": "385cfb2e",
        "Status":
        {
            "Health": "OK",
            "State": "Enabled"
        }
    },
    {
        "@odata.id": "/redfish/v1/Systems/1/Memory/DIMM13",
        "@odata.type": "Memory.v1_4_0.Memory",
        "BaseModuleType": "RDIMM",
        "CapacityMiB": 16384,
        "DataWidthBits": 64,
        "DeviceLocator": "DIMM13",
        "ECCType": "Multi-bit ECC",
        "Id": 13,
        "Manufacturer": "Samsung",
        "MemoryDeviceType": "DDR4",
        "MemoryLocation":
        {
            "Channel": 0,
            "Controller": 0,
            "Slot": 13,
            "Socket": 1
        },
        "Name": "DIMM13",
        "OperatingSpeedMhz": 2666,
        "PartNumber": "M393A2K43CB2-CTD",
        "RankCount": 2,
        "SerialNumber": "385cf687",
        "Status":
        {
            "Health": "OK",
            "State": "Enabled"
        }
```

```
    }],
    "Members@odata.count": 2,
    "Name": "Memory Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all memory resource, refer to Table 5-23.

Table 5-23 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.
Name	String	Name of the memory resource collection.
Members@odata.count	Number	Number of memory resource members.
Members	Object	Information about all memory resources.

5.12 Querying Information About the Storage Resource Collection

Function

Query information about the current storage resource collection of a server.

Syntax

- Operation Type: GET
- URL: *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 5-24.

Table 5-24 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
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.etag": "W/\"1581184096\"",
    "@odata.id": "/redfish/v1/Systems/1/Storages",
    "@odata.type": "#StorageCollection.StorageCollection",
    "Members":
    [{
        "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage0008"
    }],
    "Members@odata.count": 1,
    "Name": "Storage Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the storage resource collection, refer to Table 5-25.

Table 5-25 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.
@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	Object	Storage resource list.
@odata.id	String	Access path of a single storage resource node.

5.13 Querying Information About a Specified Storage Resource

Function

Query information about the specified storage resource of a server.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Systems/system_id/Storages/storage_id*
- Request Header:

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

- Request Message Body: None

Description

For the parameter descriptions for querying information about the specified storage resource, refer to Table 5-26.

Table 5-26 Parameter Descriptions for Querying Information About the Specified Storage 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 */redfish/v1/SessionService/Sessions*.
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:

```
GET https://device_ip/redfish/v1/Systems/1/Storages/RAIDStorage0008
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#Storage.Storage",
    "@odata.etag": "W/\"1593008620\"",
    "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage0008",
    "@odata.type": "#Storage.v1_4_0.Storage",
    "Drives":
    [{
        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk00080011"
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk00080012"
    }],
    "Drives@odata.count": 2,
    "Name":"RAIDStorage0008",
    "StorageControllers":
    [{
        "CardManufacturer": "Broadcom",
        "CardModel": "AVAGO MegaRAID SAS 9361-8i",
        "Description": "RAID Controller",
        "FirmwareVersion": "4.680.00-8442",
        "Manufacturer": "Broadcom",
```

```
        "MemberId": "RAIDStorage0008",
        "Model": "RAID_SAS3108",
        "Name": "AVAGO MegaRAID SAS 9361-8i(RAIDStorage0008)",
        "Oem": {
            "Public": {
                "CapacitanceName": null,
                "CapacitanceStatus": {
                    "Health": null,
                    "State": "Absent"
                },
                "MemorySizeMiB": 2048,
                "OOBSupport": true,
                "PHYStatus": [
                    {
                        "InvalidDwordCount": 0,
                        "LossDwordSyncCount": 0,
                        "PHYId": 1,
                        "PhyResetProblemCount": 0,
                        "RunningDisparityErrorCount": 0
                    }
                ],
                "SASAddress": null,
                "SupportedRAIDLevels":
                ["RAID0", "RAID1", "RAID5", "RAID6", "RAID00", "RAID10", "RAID50",
                 "RAID60"]
            }
        },
        "SerialNumber": "SK82380527",
        "SpeedGbps": 12,
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        },
        "SupportedDeviceProtocols": ["SAS", "SATA"]
    }],
    "StorageControllers@odata.count": 1,
    "Volumes": {
        "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage0008/Volumes"
    }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified storage resource, refer to Table 5-27.

Table 5-27 Output Descriptions for Querying Information About the Specified Storage 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 node.
@odata.type	String	Type of the specified storage controller.
Name	String	Name of the specified storage controller.
StorageControllers@odata.count	Number	Number of storage controllers.
StorageControllers	Object	Information about the storage controller.
Name	String	Name of the specified storage controller.
MemberId	String	ID of the specified storage controller.
SpeedGbps	Number	Interface speed of the specified storage controller.
FirmwareVersion	String	Firmware version of the specified storage controller.
SupportedDeviceProtocols	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

Field	Type	Description
		• SFTP
Manufacturer	String	Manufacturer of the specified storage controller.
Model	String	Model of the specified storage controller.
CardManufacturer	Character string	Manufacturer of the specified storage controller.
CardModel	Character string	Model of the specified storage controller.
SerialNumber	String	Serial number of the specified storage controller.
Oem.Public	Object	Manufacturer-customized properties.
MemorySizeMiB	Number	Memory size of the specified storage controller.
CapacitanceStatus	Object	BBU status of the specified storage controller. • State: enabling status of storage controller, Options include: → absent: absent → present: present → null: not supported • Health: health status of the specified storage controller.
Drives@odata.count	Number	Number of drives managed by the storage controller.
Drives	Object	Drive list managed by the specified storage controller.
Status	Object	Status of the specified storage controller. • Health: BBU health status • State: BBU presence status
Description	String	Information about the specified storage controller.
PHYStatus	Object	Physical-layer bit error status of the specified controller.
InvalidDwordCount	Number	Number of invalid DWORDs.
LossDwordSyncCount	Number	Number of times that DWORD synchronization is lost.
PHYId	Number	PHY index
PhyResetProblemCount	Number	Number of PHY restart problems.
RunningDisparityErrorCount	Number	Number of running disparity errors.

5.14 Querying Information About All Storage Resources

Function

Query information about all current storage resources of a server.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Systems/system_id/Storages?$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 resources, refer to Table 5-28.

Table 5-28 Parameter Descriptions for Querying Information About All Storage 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/system_id/Storages?$expand=.
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#StorageCollection.StorageCollection",
    "@odata.etag": "W/\"1603390629\"",
    "@odata.id": "/redfish/v1/Systems/1/Storages",
    "@odata.type": "#StorageCollection.StorageCollection",
    "Members": [{
```

```
    "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage0008",
    "@odata.type": "#Storage.v1_4_0.Storage",
    "Drives": [{
        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk00080011"
    }, {
        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk00080012"
    }],
    "Drives@odata.count": 2,
    "StorageControllers": [{
        "CardManufacturer": "Broadcom",
        "CardModel": "AVAGO MegaRAID SAS 9361-8i",
        "Description": "RAID Controller",
        "FirmwareVersion": "4.680.00-8442",
        "Manufacturer": "Broadcom",
        "MemberId": "RAIDStorage0008",
        "Model": "RAID_SAS3108",
        "Name": "AVAGO MegaRAID SAS 9361-8i(RAIDStorage0008)",
        "Oem": {
            "Public": {
                "CapacitanceName": null,
                "CapacitanceStatus": {
                    "Health": null,
                    "State": "Absent"
                },
                "MemorySizeMiB": 2048,
                "OOBSupport": true,
                "SASAddress": null,
                "SupportedRAIDLevels":
                ["RAID0", "RAID1", "RAID5", "RAID6", "RAID00", "RAID10", "RAID50",
                 "RAID60"]
            }
        },
        "SerialNumber": "SK82380527",
        "SpeedGbps": 12,
        "Status": {
            "Health": "OK",
            "State": "Enabled"
         },
        "SupportedDeviceProtocols": ["SAS", "SATA"]
    }],
    "StorageControllers@odata.count": 1,
    "Volumes": {
        "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage0008/Volumes"
    }
```

```
    }],
    "Members@odata.count": 1,
    "Name": "Storage Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all storage resources, refer to Table 5-29.

Table 5-29 Output Descriptions for Querying Information About All Storage Resources

Field	Type	Description
@odata.context	String	OData description of the storage resource collection model.
@odata.id	String	Access path of the storage resource collection.
@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	Object	Storage resource list.

5.15 Querying Information About the Logical Volume Resource Collection

Function

Query information about the current logical volume resource collection of a server.

Syntax

- Operation Type: GET
- URL: *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 5-30.

Table 5-30 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.
manager_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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/1/Storages/storage_id/Volumes
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#VolumeCollection.VolumeCollection",
    "@odata.etag": "W/\"1581184202\"",
    "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage0008/Volumes",
    "@odata.type": "#VolumeCollection.VolumeCollection",
    "Members":
    [{
        "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage0008/Volumes/
                                LogicalDrive00080000"
    },
    {
        "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage0008/Volumes/
                                LogicalDrive00080001"
    }],
    "Members@odata.count": 2, "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 5-31.

Table 5-31 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	Object	Logical volume resource list.
@odata.id	String	Access path of a single logical volume resource node.

5.16 Querying Information About a Specified Logical Volume Resource

Function

Query information about a specified logical volume resource of a server.

Syntax

- Operation Type: GET
- URL: *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

Description

For a description of the parameters for querying information about the specified logical volume resource, refer to Table 5-32.

Table 5-32 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 */redfish/v1/SessionService/Sessions*.
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 Example:

```
GET https://device_ip/redfish/v1/Systems/1/Storages/RAIDStorage0008/Volumes/LogicalDrive00080000
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#Volume.Volume",
    "@odata.etag": "W/\"1593009062\"",
    "@odata.id":
    "/redfish/v1/Systems/1/Storages/RAIDStorage0008/Volumes/LogicalDrive00080000",
    "@odata.type": "#Volume.v1_0_3.Volume",
    "Id": "LogicalDrive00080000",
    "Links": {
        "Drives": [{
            "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk0006000a"
        }, {
            "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk0006000b"
        }],
        "Drives@odata.count": 2
    },
```

```
    "Name": "os",
    "Oem": {
        "Public": {
            "AccessPolicy": "ReadOnly",
            "BootEnable": true
            "IoPolicy": "CachedIO",
            "ReadPolicy": "NoReadAhead",
            "WritePolicy": "WriteThrough",
            "DriveCachePolicy": "Enabled",
            "NumDrive": 2,
            "RaidControllerID": 8,
            "State": "Degraded",
            "VolumeName": "os",
            "VolumeRaidLevel": "RAID1"
        }
    },
    "OptimumIOSizeBytes": 524288,
    "CapacityBytes": 21474836480,
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "VolumeType": "Mirrored",
    "NumDriveperspan": 1,
    "SpanNumber": 1
}
```


- 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 5-33.

Table 5-33 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.
@odata.id	String	Access path of the specified logical volume resource node.
@odata.type	String	Type of the specified logical volume.
Name	String	Name of the specified logic volume resource.

Field	Type	Description
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	Object	Drive list managed by the specified storage controller.
@odata.id	String	Access path of the specified drive node.
Drives@odata.count	Number	Number of member physical disks included in the RAID.
Status	Object	Status of the specified logical volume resource, in-cluding: ● State: enabling status of the logical volume. ● 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: ● RAID 0 ● RAID 1 ● RAID 5 ● RAID 6 ● RAID 00 ● RAID 10 ● RAID 50 ● RAID 60
DriveCachePolicy	String	Hard disk Cache policy: ● Unchanged ● Enabled ● Disabled
NumDrive	Number	Number of physical disk members.

Field	Type	Description
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
BootEnable	Boolean	Whether it is a boot disk. ● true: yes. ● false: no.
IoPolicy	String	I/O policy of the logical volume: ● DirectIO ● CachedIO
VolumeName	String	Name of the logical volume.
State	String	Status of the logical volume: ● Offline ● Partially degraded ● Degraded ● Optimal ● Initializing
NumDriveperspan	Number	Number of drive members in a span.
SpanNumber	Number	Number of spans of a volume.

5.17 Creating a Logical Volume

Function

Create a logical volume.

Syntax

- Operation Type: POST
- URL: *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 5-34.

Table 5-34 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.
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 */redfish/v1/SessionService/Sessions*.
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

Parameter	Description	Value
		• 1048576
name	String	Name of the logical volume, required, consisting of 1–15 characters, including letters, digits, hyphens, 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" 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	I/O policy of the logical volume, optional, including: • DirectIO • CachedIO
disk_cache_policy	String	Caching policy of the logical volume, optional, including: • Unchanged • Enabled

Parameter	Description	Value
		• 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.
drives	Array	Member volume list, required. It is obtained through the **Drives** field in 5.13 Querying Information About a Specified Storage Resource. The format of the drives field is: [HDDPlaneDiskid1,HDDPlaneDiskid2,...,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 Example:

```
POST https://device_ip/redfish/v1/Systems/1/Storages/RAIDStorage0006/Volumes
```

- Request Header:

```
Content-Type: application/json
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body:

```
{
    "OptimumIOSizeBytes": 262144,
    "Oem":
    {
        "Public":
        {
            "VolumeName": "testname",
            "VolumeRaidLevel": "RAID5",
```

```
            "ReadPolicy": "NoReadAhead",
            "WritePolicy": "WriteThrough",
            "AccessPolicy": "ReadWrite",
            "IoPolicy": "DirectIO",
            "DriveCachePolicy": "Disabled",
            "InitializationMode": "UnInit",
            "SpanNumber": 1,
            "Drives": ["HDDPlaneDisk00060001","HDDPlaneDisk00060002",
                        "HDDPlaneDisk00060003"]
        }
    }
}
```


- Response Example:


```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1571459532\"",
    "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage0006/Volumes",
    "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"
    }
}
```


- Status Code: 202

Output Description

For a description of the output returned when you create the logical volume, refer to Table 5-35.

Table 5-35 Output Descriptions for Creating the Logical Volume

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

Field	Type	Description
message	String	Error message corresponding to the message 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 levels supported by Redfish, including: ● OK ● Warning ● Critical
Resolution	String	Solution.

5.18 Deleting a Logical Volume

Function

Delete the logical volume.

Syntax

- Operation Type: DELETE
- URL: *https://device_ip/redfish/v1/Systems/system_id/Storages/storage_id/Volumes/volume_id*
- Request Header:

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

- Request Message Body: None

Parameters

For a description of the parameters for deleting the logical volume, refer to Table 5-36.

Table 5-36 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.

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json

Usage Guidelines

None

Example

- Request Example:

```
DELETE https://device_ip/redfish/v1/Systems/system_id/Storages/RAIDStorage0006/Volumes/LogicalDrive00060000
```

- Request Header:

```
Content-Type: application/json
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.id":
    "/redfish/v1/Systems/1/Storages/RAIDStorage0006/Volumes/LogicalDrive00060000",
    "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"
    }
}
```

- Status Code: 202

Output Description

For a description of the output returned when you delete the logical volume, refer to Table 5-37.

Table 5-37 Output Descriptions for Deleting the Logical Volume

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Error message corresponding to the message 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 levels supported by Redfish, including: ● OK ● Warning ● Critical
Resolution	String	Solution.

5.19 Querying Properties of the BIOS Resource

Function

Query information about the current BIOS resource of a server.

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

Description

For a description of the parameters for querying the information about the BIOS resource, refer to Table 5-38.

Table 5-38 Parameter Descriptions for Querying the Information About 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 */redfish/v1/SessionService/Sessions*.

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_1_0.Settings",
        "Oem": {
            "@odata.id": "/redfish/v1/Systems/1/Bios/SD"
        }
        "SettingsObject": {
            "@odata.id": "/redfish/v1/Systems/1/Bios/Settings"
        }
    },
    "@odata.context": "/redfish/v1/$metadata#Bios.Bios",
    "@odata.etag": "W/\"1636946324\"",
    "@odata.id": "/redfish/v1/Systems/1/Bios",
    "@odata.type": "#Bios.v1_0_3.Bios",
    "Actions": {
        "#Bios.ChangePassword": {
            "target": "/redfish/v1/Systems/1/Bios/Actions/Bios.ChangePassword"
        },
        "#Bios.ResetBios": {
            "ResetType@Redfish.AllowableValues": [
                "Reset"
```

```
        ],
        "target":  "/redfish/v1/Systems/1/Bios/Actions/Bios.ResetBios"
    }
},
"Attributes": {
    "BootMode": "UEFI Only",
    "BootType": "UEFIBoot",
    "BootTypeOrder0": "Others",
    "BootTypeOrder1": "None",
    "BootTypeOrder2": "None",
    "BootTypeOrder3": "None",
    "C1E": "Disabled",
    "C3report": "Enabled",
    "C6report": "Enabled",
    "CREnable": "Enabled",
    "CustomPowerPolicy": "Custom",
    "EIST": "Enabled",
    "EnergyPerformanceBIAS": "Balanced Power",
    "GlobalBaudRate": "Rate115200",
    "HardwarePStates": "Native Mode",
    "HyperThreading": : "Disabled",
    "IPv4PXESupport": : "Disabled",
    "IPv6PXESupport": "Disabled",
    "MonitorMWAIT": "Enabled",
    "MainBoardLOMPort1": "Enabled",
    "MainBoardLOMPort2": "Disabled",
    "MainBoardLOMPort3": "Enabled",
    "MainBoardLOMPort4": "Disabled",
    "NUMA":  "Disabled",
    "Numa": "Disabled",
    "OSACPICx": "ACPIC3",
    "PCIeSRIOVSupport": "Enabled",
    "PXEOnly": "Enabled",
    "PackageCState": "C2 state",
    "PowerPerformanceTuning": "OS controls EPB",
    "ProcessorHyperThreading": "Enabled",
    "Slot10PXE": "Enabled",
    "Slot11PXE": "Enabled",
    "Slot12PXE": "Enabled",
    "Slot1PXE": "Enabled",
    "Slot2PXE": "Enabled",
    "Slot3PXE": "Enabled",
    "Slot4PXE": "Enabled",
    "Slot5PXE": "Enabled",
```

```
        "Slot6PXE": "Enabled",
        "Slot7PXE": "Enabled",
        "Slot8PXE": "Enabled",
        "Slot9PXE": "Enabled",
        "TurboMode": "Enabled",
        "VTdSupport": "Enabled",
        "VTxSupport": "Enabled",
        "PCIeACSCTL": "Enabled",
        "OsNativeAERSupport": "Enabled",
        "EnforcePor": "Disabled",
        "PxeOnly": "Enabled",
        "OnboardLanBootPriority": "OnboardLanLast",
        "WindowsEMS": "Enabled",
        "X2APIC": "Enabled",
        "RestoreOnAcPowerLoss": "PowerOff",
        "BMCShareLink": "Enabled",
        "BmcSol": "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 5-39.

Table 5-39 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 node.
@odata.type	String	Type of BIOS resource.
@odata.etag	String	Whether the interface is changed.
Id	String	ID of the BIOS resource.
Name	String	Name of the BIOS resource.
Attributes	BIOS properties.	For details, refer to Table 5-40.
Actions	Object	Operations that can be performed on the BIOS resource.

Field	Type	Description
@Redfish.Settings	Object	Information about BIOS settings.

For a description of the attributes of the BIOS resource, refer to Table 5-40.

Table 5-40 Descriptions of BIOS Attributes

Field	Type	Description
BootType	String	Boot mode. ● UEFIBoot: UEFI boot mode ● LegacyBoot: Legacy boot mode
BootMode	String	Boot mode. ● UEFI Only: UEFI boot mode. ● Legacy Only: Legacy boot mode.
BootTypeOrder0	String	First boot device: ● HardDiskDrive: hard disk boot device (default) ● DVDROMDrive: CD boot device ● PXE: PXE boot device ● USB: USB boot device ● Others: other boot devices
BootTypeOrder1	String	Second boot device: ● HardDiskDrive: hard disk boot device (default) ● DVDROMDrive: CD boot device ● PXE: PXE boot device ● USB: USB boot device ● Others: other boot devices
BootTypeOrder2	String	Third boot device: ● HardDiskDrive: hard disk boot device (default) ● DVDROMDrive: CD boot device ● PXE: PXE boot device ● USB: USB boot device ● Others: other boot devices
BootTypeOrder3	String	Fourth boot device: ● HardDiskDrive: hard disk boot device (default) ● DVDROMDrive: CD boot device ● PXE: PXE boot device ● USB: USB boot device ● Others: other boot devices
BootTypeOrder4	String	Fifth boot device: ● HardDiskDrive: hard disk boot device (default) ● DVDROMDrive: CD boot device ● PXE: PXE boot device

Field	Type	Description
		● USB: USB boot device ● Others: other boot devices
CustomPowerPolicy	String	Energy efficiency mode: ● Efficiency: low power consumption ● Performance: high performance ● Custom: customization ● LoadBalance: load balancing ● IEMPower: IEM power saving mode. ● LatencyPerformance: low latency mode. ● Max Performance: maximum-performance mode. ● IEMBalancePerformance: IEM performance balancing mode.
ProcessorHyperThreading	String	Hyper-threading setting information (not available for some CPUs). ● Enabled ● Disabled
HyperThreading	String	Hyper-threading setting information (not available for some CPUs). ● Enabled ● Disabled
SMTControl	String	Hyper-threading setting information (not available for some CPUs). ● Enabled ● Disabled
TurboMode	String	Whether dynamic CPU acceleration is enabled: ● Enabled ● Disabled
CorePerformanceBoost	String	Whether dynamic CPU acceleration is enabled: ● Enabled ● Disabled
PCIeSRIOVSupport	String	Whether the SR-IOV technology is enabled for the PCIe card: ● Enabled ● Disabled
SRIOVSupport	String	Whether the SR-IOV technology is enabled: ● Enabled ● Disabled
VTdSupport	String	Whether the VT-D technology is enabled: ● Enabled

Field	Type	Description
		• Disabled • Auto: automatic
IOMMU	String	Whether the IOMMU technology is enabled: • Enabled • Disabled • Auto: automatic
CREnable	String	Whether serial port redirection control is enabled: • Enabled • Disabled
GlobalBaudRate	String	Serial port redirection rate: • Rate115200 (default) • Rate57600 • Rate38400 • Rate19200 • Rate9600
IPv4PXESupport	String	Whether NIC IPv4 PXE is enabled: • Enabled • Disabled
IPv6PXESupport	String	Whether NIC IPv6 PXE is enabled: • Enabled • Disabled
Numa	String	Whether NUMA is enabled: • Enabled • Disabled • NPS 0/NPS 1/NPS 2/NPS 4/Auto: NUMA mode
NUMA	String	Whether NUMA is enabled: • Enabled • Disabled
PXEOnly	String	Whether PXE is enabled for all NICs: • Enabled • Disabled

Field	Type	Description
MainBoardLOMPort1	String	PXE boot setting (the first network port of the onboard card): ● Enabled ● Disabled
MainBoardLOMPort2	String	PXE boot setting (the second network port of the on-board card): ● Enabled ● Disabled
MainBoardLOMPort3	String	PXE boot setting (the third network port of the on-board card): ● Enabled ● Disabled
MainBoardLOMPort4	String	PXE boot setting (the fourth network port of the on-board card): ● Enabled ● Disabled
VTxSupport	String	Whether the VT-X technology is enabled: ● Enabled ● Disabled
IntelVMDSupport	String	Whether the VMD function is enabled on the PCIe device: ● Enabled ● Disabled
SVMMode	String	Whether the VT-X technology is enabled: ● Enabled ● Disabled
Slot1PXE	String	Whether PXE is enabled on slot 1 of the standard card: ● Enabled ● Disabled
Slot2PXE	String	Whether PXE is enabled on slot 2 of the standard card: ● Enabled ● Disabled
Slot3PXE	String	Whether PXE is enabled on slot 3 of the standard card: ● Enabled ● Disabled

Field	Type	Description
Slot4PXE	String	Whether PXE is enabled on slot 4 of the standard card: ● Enabled ● Disabled
Slot5PXE	String	Whether PXE is enabled on slot 5 of the standard card: ● Enabled ● Disabled
Slot6PXE	String	Whether PXE is enabled on slot 6 of the standard card: ● Enabled ● Disabled
Slot7PXE	String	Whether PXE is enabled on slot 7 of the standard card: ● Enabled ● Disabled
Slot8PXE	String	Whether PXE is enabled on slot 8 of the standard card: ● Enabled ● Disabled
Slot9PXE	String	Whether PXE is enabled on slot 9 of the standard card: ● Enabled ● Disabled
Slot10PXE	String	Whether PXE is enabled on slot 10 of the standard card: ● Enabled ● Disabled
Slot11PXE	String	Whether PXE is enabled on slot 11 of the standard card: ● Enabled ● Disabled
Slot12PXE	String	Whether PXE is enabled on slot 12 of the standard card: ● Enabled ● Disabled
PState	String	P state. ● Enabled

Field	Type	Description
		• Disabled
EIST	String	P state. • Enabled • Disabled
CState	String	C state. • Enabled • Auto • Disabled
GlobalCstateControl	String	C state. • Enabled • Auto • Disabled The HG3-7390 model supports the following options: • Disabled • EnabledCC1 • EnabledCC6 • Auto
PackageCState	String	• C0/C1 state • C2 state • C6(non retention)state
C1E	String	• Enabled • Disabled
EnergyPerformanceBIA	String	• Performance • Balanced Performance • Balanced Power • Power
HardwarePStates	String	• Disabled • Native Mode • OutOfBandMode • WithNoLegacySupport
PowerPerformanceTuning	String	• OS controls EPB • BIOS controls EPB
VirtualNuma	String	Whether the virtual NUMA schema attribute of the system is enabled:

Field	Type	Description
		• Enabled • Disabled
SNC	String	Whether the SNC2 function is enabled: • Enabled • Disabled
PPRType	String	PPR type: • Hard: hardware PPR. • Soft: software PPR. • Disabled: PPR disabled.
ADDDCSparing	String	Whether ADDDC sparing is enabled: • Enabled • Disabled
MemoryFrequency	String	Memory frequency setting: Auto, 2666, 2933, or 3200
HaltOnMemoryFault	String	Whether halt on a memory fault is enabled: • Enabled • Disabled
PopulationPor	String	POR setting. After POR is enabled, memory modules must be installed in accordance with the POR. • Disable: POR disabled. • SupportedPopulation: POR supported. • ValidatedPopulation: POR validated.
MemTestOnColdFastBoot	String	Whether the memory test is enabled upon fast cold boot: • Enabled • Disabled
RmtOnColdFastBoot	String	Whether the RMT is enabled upon fast cold boot: • Enabled • Disabled
LegacyRmt	String	Whether the Rank Margin tool is enabled: • Enabled • Disabled
PagePolicy	String	Page management policy setting: • Closed: The page management policy is disabled. • Adaptive: Adaptive mode is used.

Field	Type	Description
MirrorTAD0	String	Whether mirroring of all memory for TAD0 is enabled: ● Enabled ● Disabled
PatrolScrub	String	Memory patrol scrubbing: ● Enabled ● Disabled ● EnableAtEndOfPOST
LeakBktTimeWinEn	String	Whether the interface based on the leaky bucket time window is enabled: ● Enabled ● Disabled
DMAControl	String	Whether DMA opt-in is enabled: ● Enabled ● Disabled
InterruptRemapping	String	VT_D interrupt remapping switch. After VT_D interrupt remapping is enabled, the management programs and operating systems that support this function can be used for the directed I/O device. Intel's virtualization technology provides the hardware function for interrupt remapping, so the InterruptRemapping option can be kept enabled for the management programs and operating systems where the option is not applied: ● Enabled: VT-D interrupt remapping is enabled. ● Disabled: VT-D interrupt remapping is disabled. ● Auto: automatic
X2APIC	String	X2APIC Opt Out: ● Enabled ● Disabled
Pre-bootDMAProtection	String	Whether pre-boot DMA protection is enabled: ● Enabled ● Disabled
RdcurforXPTPrefetch	String	Whether XPT prefetch is enabled: ● Enabled ● Disabled ● Auto
EVDFXFeatures	String	Whether EV DFX is enabled: ● Enabled

Field	Type	Description
		• Disabled
PerformanceTuningMode	String	IIO performance tuning mode: • SafeMode: safe mode. • PerformanceEnableMode: Recommended performance values are given.
MmcfgSize	String	MMCFG size: Auto, 64M, 128M, 256M, 512M, 1G, or 2G
PCIeARI	String	Whether ARI is enabled: • Enabled • Disabled
ARIForward	String	Whether the ARI forwarding function is enabled: • Enabled • Disabled
Use1GPageTable	String	Whether the 1 GB page table is used: • Enabled • Disabled
IOAPICMode	String	Whether the APIC-IO APIC mode is used: • Enabled • Disabled
TraceMessages	String	Whether Trace messages are enabled: • Enabled • Disabled Enabledforregistrywritesonly: indicates that the function is enabled only when data is written to the registry.
TrainingMessages	String	Whether Training messages are enabled: • Enabled • Disabled
MMIOHighBase	String	MMIOH start address: 56T, 40T, 32T, 24T, 16T, 4T, 2T, 1T, 512 G, or 3584T.
MMIOHighGranularitySize	String	MMIOH granularity size for each stack: 1 GB, 4 GB, 16 G, 64 G, 256 G, or 1024 G.
IsocEn	String	Whether isochronous transmission is enabled. After it is enabled, data transmission quality can be improved, but the memory performance may be reduced. • Enabled • Disabled

Field	Type	Description
		• Auto
Above4GDecoding	String	Whether the above-4G decoding function is enabled: • Enabled • Disabled
EnablePCI- ECompletionTime-out(Global)	String	Whether the completion timeout function is used: • Enabled • Disabled
PCI-EASPMSupport(Global)	String	PCIe ASPM support: • L1Only: Only L1 mode is entered. • Per-Port: The mode of each port is configured separately.
HardwarePrefetcher	String	Hardware prefetch means that the CPU prefetches instructions or data and stores it in the L2 cache before processing the instructions or data, thus reducing the time required for reading data from the memory, eliminating potential bottlenecks, and improving system efficiency. • Enabled: The hardware prefetch function is enabled. • Disabled: The hardware prefetch function is disabled.
AdjacentCachePrefetch	String	After the adjacent cache prefetch function is enabled, the server reads the adjacent data in advance when reading data, accelerating the read speed. • Enabled: The adjacent cache prefetch function is enabled. • Disabled: The adjacent cache prefetch function is disabled.
DCUStreamerPrefetcher	String	Whether the DCU stream prefetch function is enabled: • Enabled • Disabled
DCUIPPrefetcher	String	Whether the DCU IP prefetch function is enabled: • Enabled • Disabled
LinkFrequencySelect	String	Current UPI link frequency: 9.6GTs, 10.4GTs, 11.2GTs, or Auto UsePerLinkSetting.
Intel(R)TXT	String	Whether the Intel TXT security function is enabled: • Enabled

Field	Type	Description
		● Disabled Note: If it is set to Enabled, the VT-x item is greyed out.
ExtendedAPIC	String	Whether extended APIC is enabled: ● Enabled ● Disabled
CheckCPUBISTResult	String	Whether the CPU BIST result check is enabled: ● Enabled: The core of the fault is disabled based on the BIST result. ● Disabled: The BIST result is ignored.
LLCPrefetch	String	Whether the L3 cache prefetch function is enabled: ● Enabled ● Disabled
DCUMode	String	DCU mode: ● Normal ● Mirror-Mode
AES-NI	String	Whether the AES-NI function is enabled: ● Enabled ● Disabled
DirectoryMode	String	Whether the directory mode is enabled: ● Enabled ● Disabled ● Auto
L1StreamHwPrefetcher	String	Whether the processor allows the hardware prefetcher to speculatively fetch streams of data and instruction from memory into the L1 cache when necessary: ● Enabled ● Disabled
L2StreamHwPrefetcher	String	Whether the processor allows the hardware prefetcher to speculatively fetch streams of data and instruction from memory into the L2 cache when necessary:Enabled ● Disabled
APICPhysicalMode	String	Whether the APIC physical mode is enabled: ● Enabled ● Disabled
SmxEnable	String	Ehryhrt SMX is enabled: ● Enabled

Field	Type	Description
		• Disabled
LockChipset	String	Whether the chipset lock is enabled: • Enabled • Disabled • Auto
QpiLinkSpeedMode	String	UPI link speed mode: • Slow: slow mode. • Fast: fast mode.
XptRemotePrefetch	String	Whether the XPT remote prefetch function is enabled: • Enabled • Disabled • Auto
KtiPrefetch	String	Whether KTI prefetch is enabled: • Enabled • Disabled • Auto
IrqThreshold	String	Interrupt request threshold: • Disabled: Threshold configuration is disabled. • Auto: The threshold is set automatically. • Low: The threshold is set to low. • Medium: The threshold is set to medium. • High: The threshold is set to high.
IoDcMode	String	Whether IODC mode is enabled: • Enabled • Disabled • Auto
XptPrefetch	String	Whether XPT prefetch is enabled: • Enabled • Disabled • Auto
StaleAtoSOpt	String	Whether switchover between the SnoopAll (A) and Shared (S) states of memory is enabled: • Enabled • Disabled • Auto
LLCDeadLineAlloc	String	Whether LLC dead line allocation is enabled: • Enabled • Disabled • Auto

Field	Type	Description
PCIeHotPlug	String	Whether PCIe hot swapping is enabled: ● Enabled ● Disabled ● Auto
SataPort0	String	Whether control on the Sata port is enabled: ● Enabled ● Disabled
SataPort1	String	Whether control on the Sata port is enabled: ● Enabled ● Disabled
SataPort2	String	Whether control on the Sata port is enabled: ● Enabled ● Disabled
SataPort3	String	Whether control on the Sata port is enabled: ● Enabled ● Disabled
SataPort4	String	Whether control on the Sata port is enabled: ● Enabled ● Disabled
SataPort5	String	Whether control on the Sata port is enabled: ● Enabled ● Disabled
SataPort6	String	Whether control on the Sata port is enabled: ● Enabled ● Disabled
SataPor7	String	Whether control on the Sata port is enabled: ● Enabled ● Disabled
SataPort10	String	Whether control on the Sata port is enabled: ● Enabled ● Disabled
sSataPort1	String	Whether control on the sSata port is enabled: ● Enabled ● Disabled
sSataPort2	String	Whether control on the sSata port is enabled: ● Enabled ● Disabled

Field	Type	Description
sSataPort3	String	Whether control on the sSata port is enabled: ● Enabled ● Disabled
sSataPort4	String	Whether control on the sSata port is enabled: ● Enabled ● Disabled
sSataPort5	String	Whether control on the sSata port is enabled: ● Enabled ● Disabled
SATAController	String	Whether SATA controllers are enabled: ● Enabled ● Disabled ● Auto Note: If this function is disabled, the **Configure SATA as** option is hidden.
ConfigureSATAas	String	SATA controller mode: ● AHCI mode ● RAID mode
sSATAController	String	Whether sSATA controllers are enabled: ● Enabled ● Disabled Note: If this function is disabled, the **Configure sSATA as** option is hidden.
ConfiguresSATAas	String	SATA controller mode: ● AHCI mode ● RAID Mode
PcieSpreadSpectrum	String	Whether PCIe spread spectrum control is enabled: ● Enabled ● Disabled
ExternalSSCEnable-CK420	String	Whether external Spread Spectrum Clocking (SSC) is enabled: ● Enabled ● Disabled
USBXHCIMSIDisableWA	String	Whether the xHCI MSI function is enabled: ● Enabled ● Disabled
XHCIOverCurrentPins	String	Whether the XHCI OC function is enabled:

Field	Type	Description
		• Enabled • Disabled
XHCIWakeOnUsbEnable	String	Whether the XHCI Wake On USB function is enabled: • Enabled • Disabled
HostPartitionResetADREnable	String	Whether the address reset function is enabled: • Enabled • Disabled • Platform-POR
Onboardlan	String	Whether onboard NIC control is enabled: • Enabled • Disabled
C3report	String	Whether C3 state reporting to the OS is enabled: • Enabled • Disabled
C6report	String	Whether C6 state reporting to the OS is enabled: • Enabled • Disabled
CPUC1autodemotion	String	Whether CPU C1 auto-demotion is enabled: • Enabled • Disabled
CPUC1AutoUndemotion	String	• Enabled • Disabled
BootPerformanceMode	String	Boot Performance State mode: • MaxPerformance mode. • MaxEfficient mode.
PECI_PCS_EPB	String	EPB mode: • OSControlsEPB: EPB is used in OS mode. • PECIControlsEPB: In PECI mode, EPB is controlled through PCS.
UncoreCLRFreqOVRD	String	Configuration mode of maximum/minimum CPU uncore clock ratio: • Auto: The default maximum/minimum CPU uncore clock ratio is used. • Manual: The maximum/minimum CPU uncore clock ratio is configured manually.
ConfigTDPLock	String	Whether the TDP lock is enabled:

Field	Type	Description
		• Enabled • Disabled • Auto
ActivateSST-BF	String	Whether SST-BF activation is enabled: • Enabled • Disabled • Auto
ConfigureSST-BF	String	Whether SST-BF configuration is enabled: • Enabled • Disabled • Auto
EistPsd	String	EIST PSD function: HW_ALL SW_ALL
Energy_Efficient_Turbo	String	Whether the Energy Efficient Turbo function is enabled: • Enabled • Disabled
HardwarePMInterrupt	String	Whether the hardware PM interrupt control is enabled: • Enabled • Disabled
EPPEnable	String	Whether EPP is enabled: • Enabled • Disabled
APSrocketing	String	Whether APS is enabled: • Enabled • Disabled
Scalability	String	Whether scalability is enabled: • Enabled • Disabled
OSACPICx	String	OS ACPI state mapping mode: • ACPIC2 mode • ACPIC3 mode
EETMode	String	EET mode: • Coarse Grained • Fine Grained
DRAMRapl	String	Whether DRAM RAPL is enabled: • Enabled • Disabled

Field	Type	Description
ThrottlingMode	String	Heat energy throttling mode: ● CLTT: CLTT mode. ● OLTT: OLTT mode. ● CLTT_with_PECI ● Disabled
PKGC_SREF	String	Whether PKGC self-refresh is enabled: ● Enabled ● Disabled
SW_Control_T-States	String	Whether software-based T state control is enabled: ● Enabled ● Disabled
T-State_Throttle_Level	String	CPU duty cycle function: Disabled, 6.25%, 12.5%, 18.75%, 25.0%, 31.25%, 37.5%, 43.75%, 50.0%, 56.25%, 62.5%, 68.75%, 75.0%, 81.25%, 87.5%, 93.75%
WakeOnPME	String	Whether PME is enabled: ● Enabled ● Disabled
LinkL0p	String	Whether L0p is enabled: ● Enabled ● Disabled ● Auto
LinkL1	String	Whether L1 is enabled: ● Enabled ● Disabled ● Auto
ActivateSST-BF	String	Whether SST-BF activation is enabled: ● Enabled ● Disabled
RAPLPrioritizationate	String	Whether RAPL prioritization is enabled: ● Enabled ● Disabled
Hibernation	String	Whether OS hibernation status can be entered: ● Enabled: The OS can enter hibernation status. ● Disabled: The OS cannot enter hibernation status.
PowerOnPassword	String	Whether power-on password is enabled: ● Enabled ● Disabled

Field	Type	Description
SecurityFreezeLock	String	Whether Security_Freeze_Lock function execution is enabled: ● Enabled ● Disabled
Language	String	System language: ● en-US: English ● zh-CN: simplified Chinese
BootRetry	String	Whether reboot from all available bootable devices is enabled: ● Enabled ● Disabled
USBBoot	String	Whether boot from an external USB device is enabled: ● Enabled: Boot from an external USB device (such as the virtual CD-ROM drive, floppy drive, or physical USB CD-ROM drive) is enabled. ● Disabled: If this option is selected, the external USB device cannot be used to boot the system.
IPv4HTTPSupport	String	Whether the IPv4 HTTP Boot function is enabled: ● Enabled ● Disabled
IPv6HTTPSupport	String	Whether the IPv6 HTTP Boot function is enabled: ● Enabled ● Disabled
QuickBoot	String	Whether quick boot is enabled. If quick boot is enabled, the memory test is skipped so that the boot time is shortened. ● Enabled ● Disabled
QuietBoot	String	Whether quiet boot is enabled. ● Enabled: Quiet boot is enabled. In this case, the product logo instead of the POST information is displayed on the boot screen. ● Disabled: Quiet boot is disabled. In this case, POST information is displayed on the boot screen.
OCP1PXE	String	Whether OCP1 PXE is enabled: ● Enabled ● Disabled
BIOSLoadDefault	String	Whether default BIOS setting restoration is enabled:

Field	Type	Description
		● Enabled ● Disabled
EmbeddedShell	String	Whether embedded Shell is enabled: ● Enabled ● Disabled
MemTest86	String	Whether Memtest86 is enabled: ● Enabled ● Disabled
POSTTimer	String	Whether the POST timer is enabled. After the POST timer is enabled, the POST timer is started during the POST. ● Enabled ● Disabled When this function is disabled, the **POST Timer Timeout** and **POST Timer Policy** parameters are greyed out.
POSTTimerPolicy	String	Power policy applied after POST timer timeout: ● NoAction: No operation is performed. ● HardReset: Reset is performed. ● PowerDown: Power-off is performed. ● PowerCycle: The server is powered down and then on.
OSWatchdogTimer	String	Whether the OS watchdog timer is enabled. After the OS watchdog timer is enabled, the watchdog timer is started when the operating system is started. ● Enabled ● Disabled When the OS watchdog timer is enabled. the **OS Wtd TimerTimeout** and **OS Wtd Timer Policy** items are displayed, and their functions are similar to those of the POST Timer. Options supported by the HG model: Enabled and Disabled.
OSWtdTimerPolicy	String	OS watchdog timeout policy: ● NoAction: No operation is performed. ● HardReset: Reset is performed. ● PowerDown: Powerdown is performed. ● PowerCycle: The server is powered down and then on.

Field	Type	Description
SerialDebugMessageLevel	String	Level of the debugging messages output through the serial port: ● Disabled: No system debugging messages are output through the serial port. ● Minimum: Only key debugging messages are output. ● Normal: Key and general debugging messages are output. ● Maximum: All debugging messages are output.
WHEASupport	String	Whether WHEA support is enabled: ● Enabled ● Disabled
WheaLogMemoryError	String	Whether the support for WHEA in logging memory errors is enabled: ● Enabled ● Disabled
LMCESupport	String	Whether LMCE support is enabled: ● Enabled ● Disabled
IIOeDPCSupport	String	Whether IIO eDPC support is enabled: ● Disabled ● OnFatalError ● OnFatalandNonFatalErrors
SystemErrors	String	Whether system error collection is enabled: ● Enabled ● Disabled ● Auto
SystemMemoryPoison	String	Whether system memory poisoning mode is enabled. After this function is enabled, if an error is found, a Poison flag is marked on the error information but no interrupt is triggered immediately. An interrupt is triggered only when the error information is used. ● Enabled ● Disabled
EMCALoggingSupport	String	Whether eMCA logging support is enabled: ● Enabled. When the support is enabled, an area is allocated in memory to store mcbank register information and incorrect DIMM information for the

Field	Type	Description
		OS to access. In addition, an uncorrectable error can trigger SMI. ● Disabled.
VGASelect	String	VGA mode: ● Onboard: onboard VGA preferred ● Offboard: external VGA card preferred
TerminalType	String	Terminal type: ● VT100 ● VT100+ ● VT-UTF8 ● ANSI ● LOG-TERM
DataBits	String	Number of actual data bits in each byte: ● 7 ● 8
Parity	String	Parity bit configuration: ● None ● Even: even parity ● Odd: odd parity
StopBits	String	Stop bit (last bit of a single packet configuration): ● 1: The stop bit is 1. ● 2: The stop bit is 2.
FlowControl	String	Flow control type: ● None ● RTS-CTS ● XON-XOFF
InformationWaitTime	String	Wait time: ● 0 Second ● 2 Seconds ● 5 Seconds ● 10 Seconds ● 30 Seconds
CRAfterLegacyBoot	String	Whether to continue using serial port redirection after the POST process is completed. This option only affects the display of GRUB and DOS, and does not affect the OS. Serial port redirection of the OS such as Redhat is controlled by the OS. ● Yes. ● No.

Field	Type	Description
AutoRefresh	String	Whether automatic refresh is enabled: ● Enabled ● Disabled
OpportunisticSR	String	Whether memory Self-Refresh is enabled: ● Enabled ● Disabled
CPUFlexRatioOverride	String	Whether the maximum frequency configuration for non-Turbo is enabled: ● Enabled ● Disabled
UncoreFreqScaling	String	Whether uncore frequency scaling is enabled: ● Enabled ● Disabled
CoreDisable	Number	Number of disabled physical CPU cores. Range: 0–127.
PatrolScrubInterval	Number	Time interval for regular memory preventive maintenance. Range: 0–24.
CorrectableErrorThreshold	Number	Threshold for the number of correctable memory errors. Range: 1–32767.
LeakBktTimeWinHour	Number	Number of hours as the size of the leaky bucket time window. Range: 0–3744.
LeakBktTimeWinMin	Number	Number of minutes as the size of the leaky bucket time window. Range: 0–60.
LeakyBktLo	Number	Leaky bucket low bit, range: 0–63.
LeakyBktHi	Number	Leaky bucket high bit, range: 0–41.
UncoreMinFreq	Number	Minimum Uncore frequency, range: 0–127.
UncoreMaxFreq	Number	Maximum Uncore frequency, Range: 0–127. 127.
PL1PowerLimit	Number	Power limit 1. Range: 0–32767.
PL2PowerLimit	Number	Power limit 2. Range: 0–32767.

Field	Type	Description
PxeRetryCount	Number	Number of PXE startup retries. Range: 1–99.
POSTTimerTimeout	Number	Power timer timeout period. Range: 10–60. The value ranges from 10 to 60.
OSWtdTimerTimeout	Number	OS watchdog timeout period. Range: 5–20.
IPv4PXEBootTimout1	Number	The value ranges from 0 to 60.
IPv4PXEBootTimout2	Number	The value ranges from 0 to 60.
IPv4PXEBootTimout3	Number	The value ranges from 0 to 60.
IPv4PXEBootTimout4	Number	The value ranges from 0 to 60.
UMABasedClustering	String	When the processor is configured as a UMA node, this function allows you to choose a clustering mode: ● Hemisphere(2-clusters): Two clusters are configured. ● Disable(All2All): No cluster is configured.
UncoreFreqRAPL	String	Whether the Uncore RAPL is enabled: ● Enabled: default ● Disabled: You can manually enter the Uncore Frequency Limit value.
SelectTemperatureRefreshValue	String	Temperature thresholds for triggering memory data refresh: ● Auto: The thresholds for triggering 1/2 x refresh, 2x refresh, and 4x refresh are automatically selected. ● Manual: The thresholds for triggering 1/2 x refresh, 2x refresh, and 4x refresh are manually specified.
SetHalfxTemperatureRefresh	Number	Temperature threshold for triggering 1/2 x refresh. Range: 0–255.
SetTWOxTemperatureRefresh	Number	Temperature threshold for triggering 2x refresh. Range: 0–255.
SetFOURxTemperatureRefresh	Number	Temperature threshold for triggering 4x refresh. Range: 0–255.

Field	Type	Description
MemhotOutputPin	String	● Enabled: Memory overheating signals are sent to the BMC for query. ● Disabled: Memory overheating signals are not sent to the BMC for query.
MemHotThrottlingModeOptions	String	● Disabled: Alarms are disabled. ● EnableOnlyH: When the temperature exceeds the maximum threshold, a THR_CRIT alarm is reported. ● EnableOnlyHM: When the temperature exceeds the medium threshold, no alarm is raised. ● EnableOnlyHML: When the temperature exceeds the low threshold, the assetTHRT_MID alarm is reported.
CheckCPUBISTResult	String	● Enabled ● Disabled
NvmePcieMaxPayload	String	Maximum NVMe PCIE payload: ● 128B ● 256B ● 512B ● Auto
PxeOnly	String	Whether the PXE boot policy is enabled: ● Enabled ● Disabled
OnboardLanBootPriority	String	Control on the onboard card boot priority: ● OnboardLanFirst: The onboard card has the highest boot priority. ● OnboardLanLast: The onboard card has the lowest boot priority, which is lower than that of all 10G NICs.
WindowsEMS	String	Whether the WindowsEMS function is enabled: ● Enabled ● Disabled
X2APIC	String	Whether the X2APIC function is enabled: ● Enabled ● Disabled
DeterminismControl	String	CPU performance mode control: ● Manual ● Auto
DeterminismSlider	String	CPU Performance mode:

Field	Type	Description
		• Balance: balance mode. • Performance: high-performance mode. • Auto; automatic mode.
cTDPControl	String	CPU TDP control: • Manual • Auto
cTDP	Number	CPU TDP value. Range: 0–300.
EfficiencyOptimized	String	Whether CPU efficiency optimization is enabled: • Enabled • Disabled
PackagePowerLimitControl	String	CPU power capping control: • Manual • Auto
PackagePowerLimit	Number	CPU power limit: 0–300.
xGMILinkWidthControl	String	XGMI link bandwidth control: • Manual • Auto
xGMIForceLinkWidthControl	String	Whether the XGMI link bandwidth is forced to a value: • Unforce • Force
xGMIForceLinkWidth	Number	The XGMI link bandwidth is forced to a value. Options: 0, 1, and 2.
APBDIS	String	P state: 0/1/Auto
FixedSOCPstate	String	Fixed system chip in P state: P0/P1/P2/P3/Auto
DRAMScrubTime	String	DRAM refresh time: Disabled/1hour/4hours/8hours/16hours/24hours/48hours/Auto
MemOverclock	String	Memory overclocking: • Enabled • Auto
PowerDownEnable	String	Memory power-down setting: • Enabled • Disabled • Auto
SMEE	String	Whether SMEE is enabled: • Enabled • Disabled • Auto

Field	Type	Description
SATAInterfaceMode	String	SATA interface mode: AHCI/IDE/Auto
CpuOcMode	String	Overclocking mode: NormalOperation or Customized.
LocalAPICMode	String	Advanced program interrupt control mode: Compatibility/XAPIC/X2APIC/XAPIC/Auto
PCIeTenBitTagSupport	String	Whether PCIe10 bit tag support is enabled: ● Enabled ● Disabled ● Auto
ACPISRATL3Cache	String	Whether ACPI SRAT L3 cache as a NUMA domain: ● Enabled ● Disabled ● Auto
TSME	String	Whether TSME is enabled: ● Enabled ● Disabled ● Auto
DFCStates	String	DF C state: ● Enabled ● Disabled ● Auto
ACSEnable	String	Whether ACS is enabled: ● Enabled ● Disabled ● Auto
PFEH	String	Whether PFEH is enabled: ● Enabled ● Disabled ● Auto

Field	Type	Description
RearUSB1	String	Whether the rear USB control switch 1 is enabled: ● Enabled ● Disabled
RearUSB2	String	Whether the rear USB control switch 2 is enabled: ● Enabled ● Disabled
DEBUGUSB3	String	Whether the DEBUG USB control switch 3 is enabled: ● Enabled ● Disabled
DEBUGUSB4	String	Whether the DEBUG USB control switch 4 is enabled: ● Enabled ● Disabled
FrontUSBLower	String	Whether the upper front USB control switch is enabled: ● Enabled ● Disabled
FrontUSBUpper	String	Whether the lower front USB control switch is enabled: ● Enabled ● Disabled
RearUSB1_3.0	String	Whether the rear USB3.0 control switch 1 is enabled: ● Enabled ● Disabled
RearUSB2_3.0	String	Whether the rear USB3.0 control switch 2 is enabled: ● Enabled ● Disabled
DEBUGUSB3_3.0	String	Whether the DEBUG USB3.0 control switch 3 is enabled: ● Enabled ● Disabled

Field	Type	Description
DEBUGUSB4_3.0	String	Whether the DEBUG USB3.0 control switch 4 is enabled: ● Enabled ● Disabled
TotalMemoryEncryption(TME)	String	Whether TME is enabled: ● Enabled ● Disabled
MemoryCEAccumulation-Threshold	String	Memory correctable error accumulation threshold: Disabled/1/500/960/1000/1200/2400/4800/5000/9600/10000/12000/1
MemoryCEAccumulation-TimeWindow	Number	Time window for memory correctable error accumulation, range: 1–24.
MemoryCEStormThreshold	String	Correctable memory error storm threshold: Disabled/60/120/240/480/960/1200
MemoryCEStormTimeWindow	Number	Time window for memory correctable error storm, range: 1–60.
PPINControl	String	Whether PPIN control is enabled: ● Enabled ● Disabled
TurboPowerLimitLock	String	Whether Turbo power limit lock is enabled: ● Enabled ● Disabled
BoostFmax	String	Maximum CPU boost frequency. ● Manual ● Auto
BoostFmaxManual	Number	Manually configured maximum CPU boost frequency. Range: 0–65535.
PlatformEnergyPerformance-Mode	String	Platform performance mode: ● Balanced Perf ● Balanced Power ● Power
SubNUMAClustering	String	Whether the SNC function is enabled: ● Disabled ● Enabled
SATAController1	String	Whether SATA controllers are enabled:

Field	Type	Description
		● Enabled ● Disabled
SataControler1Mode	String	SATA controller mode: ● AHCI mode ● RAID Mode
SATAController2	String	Whether sSATA controllers are enabled: ● Enabled ● Disabled
SataControler2Mode	String	SATA controller mode: ● AHCI mode ● RAID Mode
MemoryRankSparing	String	Whether memory rank sparing control is enabled: ● Enabled ● Disabled
RearUSBPort1	String	Rear USB port switch: ● Enabled ● Disabled
FrontUSBPort	String	Front USB port switch: ● Enabled ● Disabled
DebugUSBPort3	String	Debugging USB port switch: ● Enabled ● Disabled
BMCUSBPort	String	BMC USB port switch: ● Enabled ● Disabled
RDSEEDandRDRANDControl	String	RDSEED and RDRAND control: ● Enabled ● Disabled ● Auto: automatic
DowncoreControl	String	Downlink control: ● 1+1 ● 2+0 ● 3+0 ● 2+2 ● 4+0 ● 3+3 ● Auto

Field	Type	Description
MemDataPoisoningDdr4	String	Data poisoning control: ● Enabled ● Disabled ● Auto: automatic
MemoryClockSpeed	String	Memory clock speed. Options: Auto, 1600, 1866, 2133, 2400, 2666, 2933, 3200.
MemoryInterleaving	String	NUMA status: ● None ● Channel ● Auto ● Die ● Socket
COM	Number	BMC USB port switch: ● 0 ● 1
WaitTimeForBF2Card	String	BF2 card wait time: 0/1/2/3/4/5
PCIECorrectedErrorThreshold	String	PCIE CE threshold. Options: Disable/2000/4000/8000
4-LinkxGMIMaxSpeed	String	Maximum 4-link xGMI speed: ● 6.4 Gbps ● 7.467 Gbps ● 8.533 Gbps ● 9.6 Gbps ● 10.667 Gbps ● 11 Gbps ● 12 Gbps ● 13 Gbps ● 14 Gbps ● 15 Gbps ● 16 Gbps ● 17 Gbps ● 18 Gbps ● 19 Gbps ● 20 Gbps ● 21 Gbp ● 22 Gbps ● 23 Gbps ● 24 Gbps ● 25 Gbps

Field	Type	Description
		• Auto
3-LinkxGMIMaxSpeed	String	Maximum 3-link xGMI speed: • 6.4 Gbps • 7.467 Gbps • 8.533 Gbps • 9.6 Gbps • 10.667 Gbps • 11 Gbps • 12 Gbps • 13 Gbps • 14 Gbps • 15 Gbps • 16 Gbps • 17 Gbps • 18 Gbps • 19 Gbps • 20 Gbps • 21 Gbp • 22 Gbps • 23 Gbps • 24 Gbps • 25 Gbps • Auto
PreferredIO	String	Preferred IO. • Manual • Auto
PreferredIOBus	String	Preferred IO bus: 0–255.
EnhancedPreferredIOMode	String	Enhanced preferred IO mode. • Enabled • Disabled • Auto: automatic
DLWMSupport	String	Whether support for DLWM is enabled: • Enabled • Disabled • Auto: automatic
EnableAERCap	String	Whether the AER function is enabled: • Enabled • Disabled • Auto: automatic
CorrectedErrorReportOS	String	Whether corrected errors are reported to the OS:

Field	Type	Description
		• Enabled • Disabled
PCIeACSCTL	String	PCIe ACS control: • Enabled • Disabled
OsNativeAERSupport	String	Whether the OS controls AER: • Enabled • Disabled
EnforcePor	String	Whether POR restrictions are enforced for DDR frequency. If this item is disabled, system memory can be run at frequencies higher than the memory supports. • PORP • Disabled
RestoreOnAcPowerLoss	String	Power-on policy upon power loss. • PowerOff: stays off. • PowerOn: automatic power-on. • Last State: restores the server to the state before power-off.
BMCShareLink	String	Whether link sharing is enabled for BMC. • Enabled • Disabled • Auto: network port self-adaptive mode
BmcSol	String	BMC SOL: • Enabled • Disabled

Note

Some field names or values vary with CPU platforms.

5.20 Querying BIOS Settings

Function

Query information about the current BIOS settings of a server.

Syntax

- Operation Type: GET
- URL1: *https://device_ip/redfish/v1/Systems/system_id/Bios/Settings*

- URL2: *https://device_ip/redfish/v1/Systems/system_id/Bios/SD*
- Request Header:

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the BIOS settings, refer to Table 5-41.

Table 5-41 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example 1:

```
GET https://device_ip/redfish/v1/Systems/1/Bios/Settings
```

- Request Example 2:

```
GET https://device_ip/redfish/v1/Systems/Self/Bios/SD
```

- Request Header:

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

- Request Message Body: None
- Response Example 1:


```
{
    "@odata.context": "/redfish/v1/$metadata#Bios.Bios",
    "@odata.etag": "W/\"1636946364\"",
    "@odata.id": "/redfish/v1/Systems/1/Bios/Settings",
    "@odata.type": "#Bios.v1_0_3.Bios",
    "Attributes": {
        "BootMode": "UEFI Only",
```

```
    "BootType": "UEFIBoot",
    "BootTypeOrder0": "Others",
    "BootTypeOrder1": "None",
    "BootTypeOrder2": "None",
    "BootTypeOrder3": "None",
    "C1E": "Disabled",
    "C3report": "Enabled",
    "C6report": "Enabled",
    "CREnable": "Enabled",
    "CustomPowerPolicy": "Custom",
    "EIST": "Enabled",
    "EnergyPerformanceBIAS": "Balanced Power",
    "GlobalBaudRate": "Rate115200",
    "HardwarePStates": "Native Mode",
    "HyperThreading": "Enabled",
    "IPv4PXESupport": "Disabled",
    "IPv6PXESupport": "Disabled",
    "MonitorMWAIT": "Enabled",
    "MainBoardLOMPort1": "Enabled",
    "MainBoardLOMPort2": "Disabled",
    "MainBoardLOMPort3": "Enabled",
    "MainBoardLOMPort4": "Disabled",
    "NUMA": "Disabled",
    "Numa": "Disabled",
    "OSACPICx": "ACPIC3",
    "PCIeSRIOVSupport": "Enabled",
    "PXEOnly": "UEFI",
    "PackageCState": "C2 state",
    "PowerPerformanceTuning": "OS controls EPB",
    "ProcessorHyperThreading": "Enabled",
    "Slot10PXE": "Enabled",
    "Slot11PXE": "Enabled",
    "Slot12PXE": "Enabled",
    "Slot1PXE": "Enabled",
    "Slot2PXE": "Enabled",
    "Slot3PXE": "Enabled",
    "Slot4PXE": "Enabled",
    "Slot5PXE": "Enabled",
    "Slot6PXE": "Enabled",
    "Slot7PXE": "Enabled",
    "Slot8PXE": "Enabled",
    "Slot9PXE": "Enabled",
    "TurboMode": "Enabled",
    "VTdSupport": "Enabled",
```

```
        "VTxSupport": "Enabled",
        "PCIeACSCTL": "Enabled",
        "OsNativeAERSupport": "Enabled",
        "EnforcePor": "Disabled",
        "PxeOnly": "Enabled",
        "OnboardLanBootPriority": "OnboardLanLast",
        "WindowsEMS": "Enabled",
        "X2APIC": "Enabled",
        "RestoreOnAcPowerLoss": "PowerOff",
        "BMCShareLink": "Enabled",
        "BmcSol": "Enabled
    },
    "Description": "Future BIOS Settings",
    "Id": "Settings",
    "Name": "Future BIOS Settings"
}
```


- Response Example 2:


```
{
    "@odata.context": "/redfish/v1/$metadata#Bios.Bios",
    "@odata.etag": "W/\"1636946381\"",
    "@odata.id": "/redfish/v1/Systems/1/Bios/SD",
    "@odata.type": "#Bios.v1_0_3.Bios",
    "AttributeRegistry": "",
    "Description": "Future BIOS Settings",
    "Id": "SD",
    "Name": "Future BIOS Settings""Attributes": {
        "BootMode": "UEFI Only",
        "BootType": "UEFIBoot",
        "BootTypeOrder0": "Others",
        "BootTypeOrder1": "None",
        "BootTypeOrder2": "None",
        "BootTypeOrder3": "None",
        "C1E": "Disabled",
        "C3report": "Enabled",
        "C6report": "Enabled",
        "CREnable": "Enabled",
        "CustomPowerPolicy": "Custom",
        "EIST": "Enabled",
        "EnergyPerformanceBIAS": "Balanced Power",
        "GlobalBaudRate": "Rate115200",
        "HardwarePStates": "Native Mode",
        "HyperThreading": "Enabled",
        "IPv4PXESupport": "Disabled",
```

```
        "IPv6PXESupport": "Disabled",
        "MonitorMWAIT": "Enabled",
        "MainBoardLOMPort1": "Enabled",
        "MainBoardLOMPort2": "Disabled",
        "MainBoardLOMPort3": "Enabled",
        "MainBoardLOMPort4": "Disabled",
        "NUMA": "Disabled",
        "Numa": "Disabled",
        "OSACPICx": "ACPIC3",
        "PCIeSRIOVSupport": "Enabled",
        "PXEOnly": "UEFI",
        "PackageCState": "C2 state",
        "PowerPerformanceTuning": "OS controls EPB",
        "ProcessorHyperThreading": "Enabled",
        "Slot10PXE": "Enabled",
        "Slot11PXE": "Enabled",
        "Slot12PXE": "Enabled",
        "Slot1PXE": "Enabled",
        "Slot2PXE": "Enabled",
        "Slot3PXE": "Enabled",
        "Slot4PXE": "Enabled",
        "Slot5PXE": "Enabled",
        "Slot6PXE": "Enabled",
        "Slot7PXE": "Enabled",
        "Slot8PXE": "Enabled",
        "Slot9PXE": "Enabled",
        "TurboMode": "Enabled",
        "VTdSupport": "Enabled",
        "VTxSupport": "Enabled",
        "PxeOnly": "Enabled",
        "OnboardLanBootPriority": "OnboardLanLast",
        "WindowsEMS": "Enabled",
        "X2APIC": "Enabled"
    },
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the BIOS settings, refer to Table 5-42.

Table 5-42 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 node.
@odata.type	String	Type of BIOS setting resource.
@odata.etag	String	Whether the interface is changed.
Id	String	ID of the BIOS setting resource.
Name	String	Name of the BIOS setting resource.
Attributes	BIOS properties	For details, refer to Table 5-40.
Actions	Object	Operations that can be performed on the BIOS resource.
@Redfish.Settings	Object	Information about BIOS settings.

5.21 Modifying the BIOS Settings

Function

Modify the current BIOS settings of a server.

Syntax

- Operation Type: PATCH
- URL1: *https://device_ip/redfish/v1/Systems/system_id/Bios/Settings*
- URL2: *https://device_ip/redfish/v1/Systems/system_id/Bios/SD*
- Request Header:

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

- Request Message Body:

```
{
    "Attributes":
        {
        "BootType": boottype_value,
        "BootMode": BootMode_value,
        "PXEOnly": pxeonly_value,
        "ProcessorHyperThreading":  processorHyperThreading_value,
        "HyperThreading": HyperThreading_value,
        "BootTypeOrder0": boottypeorder0_value,
```

```
"BootTypeOrder1": boottypeorder1_value,
"BootTypeOrder2": boottypeorder2_value,
"BootTypeOrder3": boottypeorder3_value,
"BootTypeOrder4": boottypeorder4_value,
"CustomPowerPolicy": custompowerpolicy_value,
"TurboMode": TurboMode_value ,
"PCIeSRIOVSupport": pciesriovsupport_value,
"VTdSupport": vtdsupport_value,
"CREnable": crenable_value,
"GlobalBaudRate": globalbaudrate_value,
"IPv4PXESupport": iPv4PXESupport_value,
"IPv6PXESupport": iPv6PXESupport_value,
"Numa": numa_value,
"VTxSupport": vTxSupport_value,
"MainBoardLOMPort1":MainBoardLOMPort1_value,
"MainBoardLOMPort2":MainBoardLOMPort2_value,
"MainBoardLOMPort3":MainBoardLOMPort3_value,
"MainBoardLOMPort4":MainBoardLOMPort4_value,
"Slot1PXE": Slot1PXE_value,
"Slot2PXE": Slot2PXE_value,
"Slot3PXE": Slot3PXE_value,
"Slot4PXE": Slot4PXE_value,
"Slot5PXE": Slot5PXE_value,
"Slot6PXE": Slot6PXE_value,
"Slot7PXE": Slot7PXE_value,
"Slot8PXE": Slot8PXE_value,
"Slot9PXE": Slot9PXE_value,
"Slot10PXE": Slot10PXE_value,
"Slot11PXE": Slot11PXE_value,
"Slot12PXE": Slot12PXE_value,
"PState": PState_value,
"EIST": EIST_value,
"CState": CState_value,
"PackageCState": PackageCState_value,
"C1E": C1E_value,
"EnergyPerformanceBIAS": EnergyPerformanceBIAS_value,
"MonitorMWAIT": MonitorMWAIT_value,
"HardwarePStates": HardwarePStates_value,
"PowerPerformanceTuning": PowerPerformanceTuning_value,
"C3report": C3report_value,
"C6report": C6report_value,
"OSACPICx": OSACPICx_value,
"PxeOnly": PxeOnly_value,
"OnboardLanBootPriority": OnboardLanBootPriority_value,
```

```
        "WindowsEMS": WindowsEMS_value,
        "X2APIC": X2APIC_value,
        "RestoreOnAcPowerLoss": RestoreOnAcPowerLoss_value,
        "BMCShareLink": BMCShareLink_value,
        "BmcSol": BmcSol_value
    }
}
```

Description

For a description of the parameters for modifying of the BIOS settings, refer to Table 5-40.

Usage Guidelines

None

Example

- Request Example 1:

```
PATCH https://device_ip/redfish/v1/Systems/1/Bios/Settings
```

- Request Example 2:

```
PATCH https://device_ip/redfish/v1/Systems/Self/Bios/SD
```

- Request Header:

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

- Request Message Body:

```
{
    "BootType": "UEFIBoot",
    "BootTypeOrder0": "DVDROMDrive",
    "BootTypeOrder1": "PXE",
    "BootTypeOrder2": "DVDROMDrive",
    "BootTypeOrder3": "DVDROMDrive",
    "CREnable": "Disabled",
    "CustomPowerPolicy": "Efficiency",
    "GlobalBaudRate": "Rate19200",
    "PCIeSRIOVSupport": "Enabled",
    "PXEOnly": "Enabled",
    "ProcessorHyperThreading": "Disabled",
    "TurboMode": "Enabled",
    "VTdSupport": "Disabled",
    "Numa": "Disabled",
    "VTxSupport": "Disabled",
    "IPv4PXESupport": "Enabled",
```

```
    "IPv6PXESupport": "Disabled",
    "Slot1PXE": "Enabled",
    "Slot2PXE": "Enabled",
    "Slot3PXE": "Enabled",
    "Slot4PXE": "Enabled",
    "Slot5PXE": "Enabled",
    "Slot6PXE": "Enabled",
    "Slot7PXE": "Enabled",
    "Slot8PXE": "Enabled",
    "Slot9PXE": "Enabled",
    "Slot10PXE": "Enabled",
    "Slot11PXE": "Enabled",
    "Slot12PXE": "Enabled",
    "PState": "Enabled",
    "CState": "Enabled"
}
```


- Response Example: None
- Status Code: 204

Output Description

For a description of the output returned when you modify the BIOS settings, refer to Table 5-43.

Table 5-43 Output Descriptions for Modifying 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 node.
@odata.type	String	Type of BIOS setting resource.
@odata.etag	String	Whether the interface is changed.
Id	String	ID of the BIOS setting resource.
Name	String	Name of the BIOS setting resource.
Attributes	BIOS properties	For details, refer to Table 5-40.
Actions	Object	Operations that can be performed on the BIOS resource.
@Redfish.Settings	Object	Information about BIOS settings.

5.22 Setting the BIOS Password

Function

Set the current BIOS password of a server.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/Systems/system_id/Bios/Actions/Bios.ChangePassword*
- Request Header:

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

- Request Message Body:

```
{
    "NewPassword":NewPassword_value,
    "OldPassword":OldPasswordvalue
}
```

Description

For a description of the parameters for setting the BIOS password, refer to Table 5-44.

Table 5-44 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**.
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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
OldPassword_value	Original BIOS password.	Password length: 8–32 characters. The password must contain lowercase letters, uppercase letters, digits, and special characters.
NewPassword_value	New BIOS password.	Password length: 8–32 characters.

Parameter	Description	Value
		The password must contain lowercase letters, uppercase letters, digits, and special characters.

Usage Guidelines

- If no password is set at the BIOS side, OldPassword can be left blank or set to "".
- If there is a password at the BIOS side and the value of NewPassword is "", the password is cleared.

Example

- Request Example:

```
POST https://deviceip/redfish/v1/Systems/1/Bios/Actions/Bios.ChangePassword
```

- Request Header:

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

- Request Message Body:

```
{
    NewPassword":"Superuser7!",
    "OldPassword":"Superuser6!"
}
```

- Response Example:

```
{
   "@odata.context": "/redfish/v1/$metadata",
   "@odata.etag": "W/\"1584545912\"",
    "@odata.id": "/redfish/v1/Systems/1/Bios/Actions/Bios.ChangePassword",
    "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"
```

```
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you set the BIOS password, refer to Table 5-45.

Table 5-45 Output Descriptions for Setting the BIOS Password

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Error message corresponding to the message in the message registry.
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Detailed information.
Severity	String	Severity levels supported by Redfish, including: ● OK ● Warning ● Critical
Resolution	String	Solution.

5.23 Restoring Manufacturer-Specified BIOS Configurations

Function

Restore manufacturer-specified BIOS configurations.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/Systems/system_id/Bios/Actions/Bios.ResetBios*
- Request Header:

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

- Request Message Body:

```
{
    "ResetType":ResetType_value
```

```
}
```

Description

For a description of the parameters for restoring manufacturer-specified BIOS configurations, refer to Table 5-46.

Table 5-46 parameter Descriptions for Restoring Manufacturer-Specified BIOS Configurations

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
ResetType_value	Restoration type.	ResetBios: restores manufacturer-specified BIOS configurations.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Systems/1/Bios/Actions/Bios.ResetBios
```

- Request Header:

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

- Request Message Body:

```
{
    "ResetType":"ResetBios"
}
```

- Response Example: None
- Status Code: 204

Output Description

For a description of the output returned when you restore manufacturer-specified BIOS configurations, refer to Table 5-47.

Table 5-47 Ouptut Descriptions for Restoring Manufacturer-Specified BIOS Configurations

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Error message corresponding to the message in the message registry.
@odata.type	String	OData description of the message resource model.
MessageId	String	Message ID.
RelatedProperties	Array	Message-related properties.
Message	String	Detailed information.
Severity	String	Severity levels supported by Redfish, including: ● OK ● Warning ● Critical
Resolution	String	Solution.

5.24 Deleting All Logical Volumes

Function

Delete all logical volumes.

Syntax

- Operation Type: DELETE
- URL: *https://device_ip/redfish/v1/Systems/system_id/Storages/storage_id*
- Request Header:

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

- Request Message Body: None

Description

For a description of the parameters for deleting all logical volumes, refer to Table 5-48.

Table 5-48 Parameter Descriptions for Deleting All Logical Volumes

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 DELETE request for authentication.	It can be obtained by creating a session via */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json

Usage Guidelines

None

Example

- Request Example:

```
DELETE https://device_ip/redfish/v1/Systems/system_id/Storages/RAIDStorage0006
```

- Request Header:

```
Content-Type: application/json
X-Auth-Token: 8574621d21b84756218c7456821c234
```

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

Output Description

None

5.25 Setting Whether a Logical Disk Is a Boot Disk

Function

Set whether a logical disk is a boot disk.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/Systems/system_id/Storages/storage_id/Volumes/volumes_id*

- Request Header:

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

- Request Message Body:

```
{
    "Oem": {
        "Public": {
            "BootEnable": enabled_value
        }
    }
}
```

Description

For a description of the parameters for setting whether a logical disk is a logic volume, refer to Table 5-49.

Table 5-49 Parameter Descriptions for Setting Whether a Logical Disk Is a Boot Disk

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
enabled_value	Boolean	Whether to set the logical disk as a boot disk. Options: • true • false

Usage Guidelines

Set whether a logical disk is a boot disk.

Example

- Request Example:

PATCH https://device_ip/redfish/v1/Systems/1/Storages/RAIDStorage0006/Volumes/LogicalDrive000400ee

- Request Header:

```
Content-Type: application/json
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body:

```
{
    "Oem": {
        "Public": {
            "BootEnable": true
        }
    }
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#Volume.Volume",
    "@odata.etag": "W/\"1616218658\"",
    "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage0004/Volumes/
      LogicalDrive000400ee",
    "@odata.type": "#Volume.v1_0_3.Volume",
    "CapacityBytes": 6000069312512,
    "Id": "LogicalDrive000400ee",
    "Links": {
        "Drives": [
            {
                "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk0004000c"
            },
            {
                "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk0004000f"
            }
        ],
        "Drives@odata.count": 2
    },
    "Name": "aaa",
    "NumDriveperspan": 2,
    "Oem": {
        "Public": {
            "AccessPolicy": "ReadWrite",
            "BootEnable": true,
            "DriveCachePolicy": "Disabled",
            "IOPolicy": "DirectIO",
```

```
            "NumDrive": 2,
            "RaidControllerID": 4,
            "ReadPolicy": "NoReadAhead",
            "State": "Optimal",
            "VolumeName": "aaa",
            "VolumeRaidLevel": "RAID1",
            "WritePolicy": "WriteThrough"
        }
    },
    "OptimumIOSizeBytes": 262144,
    "SpanNumber": 1,
    "Status": {
            "Health": "OK",
            "State": "Enabled"
    },
    "VolumeType": "Mirrored"
}
```


- Status Code: 202

Output Description

For a description of the output returned when you set whether the logic volume is a boot disk, refer to Table 5-50.

Table 5-50 Output Descriptions for Setting Whether a Logical Disk Is a Boot Disk

Field	Type	Description
@odata.context	Character string	OData description of the specified logical volume resource model.
@odata.id	Character string	Access path of the specified logical volume resource.
@odata.type	Character string	Type of the specified logical volume.
Name	Character string	Name of the specified logic volume resource.
Id	Array	ID of the specified logical volume ID.
VolumeType	Character string	Redundancy type of the specified logical volume: ● RawDevice ● NonRedundant ● Mirrored ● StripedWithParity ● SpannedMirrors ● SpannedStripesWith ● Parity
CapacityBytes	Number	Capacity of the logical volume.

Field	Type	Description
OptimumIOSizeBytes	Number	Stripe size of the logical volume.
Links	Object	Member logical volume list.
Drives	Object	Drive list managed by the specified storage controller.
@odata.id	Character 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: enabling status of the logical volume. ● Health: health status of the logical volume.
Oem.Public	Object	Customized logical volume information.
RaidControllerID	Number	Controller ID of the logical volume.
VolumeRaidLevel	Character string	RAID level of the logical volume. The value must be in dictionary format. Options: ● RAID0 ● RAID1 ● RAID5 ● RAID6 ● RAID00 ● RAID10 ● RAID50 ● RAID60
DriveCachePolicy	Character string	Hard disk Cache policy: ● Unchanged ● Enabled ● Disabled
NumDrive	Number	Number of physical disk members.
ReadPolicy	Character string	Read policy of the logical volume: ● NoReadAhead ● ReadAhead
WritePolicy	Character string	Write policy of the logical volume: ● WriteThrough ● WriteBack ● AlwaysWriteBack
AccessPolicy	Character string	Access policy of the logical volume: ● ReadWrite ● ReadOnly

Field	Type	Description
		• Blocked
BootEnable	Boolean	Whether it is a boot disk. • true • false
IoPolicy	Character string	I/O policy of the logical volume: • DirectIO • CachedIO
VolumeName	Character string	Name of the logical volume.
State	Character string	Status of the logical volume: • Offline • Partially degraded • Degraded • Optimal • Initializing
NumDriveperspan	Number	Number of drive members in a span.
SpanNumber	Number	Number of spans of a volume.

Chapter 6
Operations on Chassis Resources

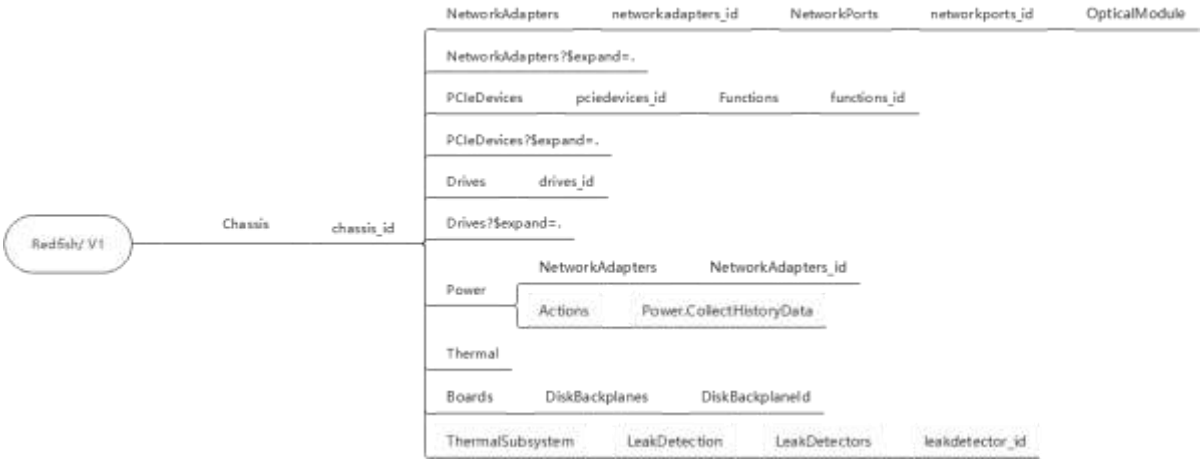
Table of Contents

Querying Information About the Chassis Resource Collection 381
Querying Information About the Specified Chassis Resource 382
Modifying the Position Indicator Status of a Chassis 387
Querying Information About the Network Adapter Resource Collection 389
Querying Information About a Specified Network Adapter Resource 391
Querying Information About All Network Adapter Resources 401
Querying Information About the Network Port Resource Collection 408
Querying Information About a Specified Network Port Resource 410
Modifying the LLDP Switch of a Network Port 414
Querying Information About the PCIe Device Resource Collection 418
Querying Information About a Specified PCIe Device Resource 420
Querying Information About a Specified PCIe Function Resource 425
Querying Information About All PCIe Device Resources 428
Querying Information About the Drive Resource Collection 433
Querying Information About a Specified Drive Resource 435
Querying Information About All Drive Resources 440
Querying Information About a Specified Chassis Power Supply 445
Modifying Properties of a Specified Power Supply 454
Querying the Cooling Resource Information About a Specified Chassis 463
Modifying the Cooling Resource Information About a Specified Chassis 471
Modifying the Status of a Specified Drive 481
Querying the Information About the Optical Module Resources Connected to a Specified Network Port 486
Querying Information About Extended Boards 490
Querying Information About the Disk Backplane Resource Collection 492
Querying Information About a Specified Disk Backplane Resource 494
Modifying Information About a Specified NEO Card 497

Querying Power Statistics.....503
Querying Information About the Leak Detection System.....504
Querying Information About the Leak Detector Resource Collection.....506
Querying Information About a Specified Leak Detector Resource.....508

Figure 6-1 shows the path requirements for the Redfish 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	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
	Manufacturer	Manufacturer information about the chassis.	GET
	PartNumber	Part number of the chassis.	GET

URL	Property	Description	Operation
	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 status range of the specified chassis resource.	GET
	Status	Status of the specified chassis resource.	GET
	PowerState	Power-on status of the specified chassis resource.	GET
	Oem. Public	OEM field.	GET
	Thermal	Access path of the cooling resource node of the specified chassis.	GET
	DeviceMaxNum	Maximum number of board components.	GET
	CPUNum	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
	BoardExtra	Additional mainboard information.	GET
	BoardName	Mainboard name.	GET
	SerialNumber	Serial number of the mainboard.	GET
	Links	Links related to the chassis resource.	GET
	ComputerSystems	Link to System resources.	GET
	ManagedBy	Link to Manager resources.	GET
	PCIeDevices	Navigation of the PCIe device resources.	GET
	Drives	Navigation of the drive resources.	GET

URL	Property	Description	Operation
	NetworkAdapters	Information about the related network adapters.	GET
	Power	Information about the related power supplies.	GET
	Mainboard	Mainboard information about the server.	GET
	Power	Access path of the power resource node of the specified chassis.	GET
	ThermalSubsystem	Thermal sub-system resource information.	GET
	ChassisHeight	Chassis height.	GET
	ProductName	Customized product name.	GET
	ProductLocation	Product location.	GET
	ProductSpecificIdentity	Product ID, including product name, mainboard name, and CPU manufacturer.	GET
	Productdate	Extended card production date.	GET
	ChassisType	Chassis type.	GET
	BoardPartNum	Extended card material number.	GET
	ChassisSerialNum	Chassis serial number, which is null if it cannot be obtained.	GET
	boardProductVer	Extended card product version.	GET
	Members@odata.count	Number of current network adapter resources.	PATCH
	Members	List of network adapter resources.	PATCH
/redfish/v1/Chassis/chassis_id/NetworkAdapters?$expand=.	Name	Name of the network adapter resource collection.	GET
	Members@odata.count	Number of current network adapter resources.	GET
	Members	List of network adapter resources.	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/net-	Name	Name of the network port resource collection.	GET
	Members@odata.count	Number of network port resources.	GET

URL	Property	Description	Operation
workadapter-s_id/NetworkPorts	Members	List of network port resources.	GET
/redfish/v1/Chas-sis/chassis_id/Net-workAdapters/net-workadapteras_id/NetworkPorts/net-workports_id	Name	Name of the specified network port resource.	GET/PATCH
	Id	UID of the specified network port re-source in the iBMC system.	GET/PATCH
	PhysicalPortNumber	Physical silk screen of the specified network port.	GET/PATCH
	LinkStatus	Status of the specified network port.	GET/PATCH
	AssociatedNetworkAddresses	Network address of the specified net-work port.	GET/PATCH
	Oem.Public	Customized properties.	GET/PATCH
	PortMaxSpeed	Speed 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 net-work port.	GET/PATCH
	FirmwarePackageVersion	Firmware version of the specified network port.	GET/PATCH
	DriverVersion	Driver version of the specified net-work port.	GET/PATCH
	LldpService	LLDP-related properties.	GET/PATCH
	LldpEnable	Whether LLDP is enabled for the specified network port.	GET/PATCH
	OpticalModule	Optical module resource connected to the specified network port.	GET
	WorkMode	LLDP operation mode.	GET/PATCH
	SupportSpeed	Supported speed of the specified network port.	GET/PATCH
/redfish/v1/Chas-sis/chassis_id/Ther-mal	Oem.Public	Customized information about the cooling resource.	GET/PATCH
	FanSpeedAdjustmentMode	Fan speed adjustment mode, includ-ing: ● Automatic mode	GET/PATCH

URL	Property	Description	Operation
		• Manual mode	
	FanSmartCoolingMode	Fan speed smart-adjustment mode, including: • NormalMode: balance mode • LowNoiseMode: low noise mode • HighPerformanceMode: high-performance mode	GET/PATCH
	SpeedRatio	Fan rotation speed ratio.	GET/PATCH
	FanSummary	Information about the specified fan sensors.	GET
	Count	Number of fan sensors.	GET
	Fans	Fan sensor list.	GET
	Name	Name of the specified fan sensor.	GET
	Status	Status of the specified fan sensor.	GET
	LowerThresholdCritical	Critical warning threshold for low rotational speed of the specified fan sensor.	GET
	LowerThresholdFatal	Fatal warning threshold for low rotational speed of the specified fan sensor.	GET
	LowerThresholdNonCritical	Non-critical warning threshold for low rotational speed of the specified fan sensor.	GET
	UpperThresholdCritical	Critical warning threshold for high rotational speed of the specified fan sensor.	GET
	UpperThresholdFatal	Fatal warning threshold for high rotational speed of the specified fan sensor.	GET
	UpperThresholdNonCritical	Non-critical warning threshold for high rotational speed of the specified fan sensor.	GET
	MaxReadingRange	Maximum rotation speed that can be read by the specified fan sensor.	GET
	MemberId	ID of the specified fan sensor.	GET

URL	Property	Description	Operation
	MinReadingRange	Minimum rotation speed that can be read by the specified fan sensor.	GET
	Reading	Current reading of the specified fan sensor.	GET
	ReadingUnits	Unit of the fan rotation speed read by the fan sensor, including: RPM and Percent.	GET
	SlotNumber	Slot number of the specified fan sensor.	GET
	SpeedRatio	Current reading of the specified fan sensor, in percentage.	GET
	Temperatures	Temperature sensor list.	GET
	LowerThresholdCritical	Critical warning threshold for low temperature of the specified temperature sensor.	GET
	LowerThresholdFatal	Fatal warning threshold for low temperature of the specified temperature sensor.	GET
	LowerThresholdNonCritical	Non-critical warning threshold for low temperature of the specified temperature sensor.	GET
	UpperThresholdCritical	Critical warning threshold for high temperature of the specified temperature sensor.	GET
	UpperThresholdFatal	Fatal warning threshold for high temperature of the specified temperature sensor.	GET
	UpperThresholdNonCritical	Non-critical warning threshold for high temperature of the specified temperature sensor.	GET
	MaxReadingRangeTemp	Maximum temperature that can be read by the specified temperature sensor.	GET
	MinReadingRangeTemp	Minimum temperature that can be read by the specified temperature sensor.	GET

URL	Property	Description	Operation
	Name	Name of the specified temperature sensor.	GET
	PhysicalContext	Area or device used for temperature measurement.	GET
	ReadingCelsius	Current reading of the specified temperature sensor.	GET
	SensorNumber	Serial number of the specified temperature sensor.	GET
	Status	Status of the specified fan sensor, including: ● State: enabling status of the fan sensor ● Health: health status of the fan sensor	GET
/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.	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, unit: V.	GET
	LowerThresholdCritical	Critical alarm threshold for undervoltage, unit: V.	GET
	UpperThresholdCritical	Critical alarm threshold for overvoltage, unit: V.	GET

URL	Property	Description	Operation
	RXPower	Receive power of the optical module.	GET
	ReadingDBM	Current receive power reading of the optical module, unit: dBm.	GET
	LowerThresholdCritical	Critical alarm threshold for too low receive power, unit: dBm.	GET
	UpperThresholdCritical	Critical alarm threshold for too high receive power, unit: dBm.	GET
	OutputPower	Transmit power information about the optical module.	GET
	ReadingDBM	Current transmit power reading of the optical module, unit: dBm.	GET
	LowerThresholdCritical	Critical alarm threshold for too low transmit power, unit: dBm.	GET
	UpperThresholdCritical	Critical alarm threshold for too high transmit power, unit: dBm.	GET
	Temperature	Temperature information about the optical module.	GET
	ReadingCelsius	Current temperature reading of the optical module, unit: °C.	GET
	LowerThresholdCritical	Critical alarm threshold for too low temperature, unit: °C.	GET
	UpperThresholdCritical	Critical alarm threshold for overtemperature, unit: °C.	GET
	BiasCurrent	Transmit bias current of the optical module.	GET
	ReadingMilliAmperes	Current bias current reading of the optical module, unit: mA.	GET
	LowerThresholdCritical	Critical alarm threshold for too low bias current, unit: mA.	GET
	UpperThresholdCritical	Critical alarm threshold for too high bias current, unit: mA.	GET
/redfish/v1/Chassis/chassis_id/Boards	Id	ID of the extended card resource collection.	GET
	Name	Extended card resource name.	GET

URL	Property	Description	Operation
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
	Members	List of hard disk backplane resources.	GET
/redfish/v1/Chassis/chassis_id/Boards/DiskBackplanes/DiskBackplaneId	ID	Serial number of the specified hard disk backplane resource.	GET
	BoardName	Name of the specified hard disk backplane resource.	GET
	SerialNumber	Serial number of the specified hard disk backplane resource.	GET
	MaxDiskCountSupported	Maximum number of hard disks supported by the specified hard disk backplane resource.	GET
	Manufacturer	Manufacturer of the specified hard disk backplane resource.	GET
	Type	Type of the specified hard disk backplane resource.	GET
	EpldVersion	EPLD version of the specified hard disk backplane resource.	GET
	Location	Location of the specified hard disk backplane.	GET
	PcbID	PCB ID of the specified hard disk backplane resource.	GET
	PortCount	Maximum number of ports supported by the specified hard disk backplane resource.	GET
	OnlineDiskCount	Number of present hard disks supported by the specified hard disk backplane resource.	GET
	DiskSpec(inch)	Specifications of hard disks supported by the specified hard disk backplane resource.	GET

URL	Property	Description	Operation
/redfish/v1/Chassis/chassis_id/Power	Id	ID of the power resource.	GET
	Name	Name of the power resource.	GET
	Maximum	Maximum number of power supplies.	GET
	OverallHealth	Health status of all power supplies.	GET
	PowerControl	Power control list.	GET
	MemberId	ID of the power control. The ID is the unique identifier of the power control in the power control list.	GET
	Name	Name of the specified power control.	GET
	Oem.Public	Customized properties.	GET
	PowerConsumedWatts	Current power of the device.	GET
	PowerLimit	Power capping setting.	GET
	LimitInWatts	Server power limit.	GET/PATCH
	LimitException	Action to be taken when the power capping becomes invalid.	GET
	PowerSupplies@odata.count	Number of power supplies.	GET
	PowerSupplies	Power supply list.	GET
	Oem.Public	Customized properties.	GET/PATCH
	ActiveStandby	Active or standby power supply mode.	GET
	SlotNumber	Slot number of the specified power supply.	GET
	InletTemperatureCelsius	Air inlet temperature of the specified power supply.	GET
	Location	Location of the power supply, which is fixed to *Chassis*.	GET
	PartNumber	Part number of the power supply, which is fixed to *null*.	GET
	Protocol	Protocol, which is fixed to *PMBus*.	GET
	InputAmperage	Input current of the specified power supply.	GET

URL	Property	Description	Operation
	OutputVoltage	Output voltage of the specified power supply.	GET
	OutputAmperage	Output current of the specified power supply.	GET
	MemberId	ID of the specified power supply. The ID is the unique identifier of the power supply in the power supply list.	GET
	Name	Name of the specified power supply.	GET
	PowerSupplyType	Type of the specified power supply.	GET
	LineInputVoltage	Input voltage of the specified power supply.	GET
	PowerCapacityWatts	Rated power of the specified power supply.	GET
	PowerInputWatts	Input power of the specified power supply.	GET
	PowerOutputWatts	Output power of the specified power supply.	GET
	Manufacturer	Manufacturer of the specified power supply.	GET
	Model	Model of the specified power supply.	GET
	FirmwareVersion	Firmware version of the specified power supply.	GET
	SerialNumber	Serial number of the specified power supply.	GET
	Status	Power supply status.	GET
	Redundancy	Power redundancy group list.	GET
	Name	Name of the specified power redundancy group.	GET
	Mode	Redundancy mode of the specified power redundancy group.	GET
	Voltages	Voltage sensor list.	GET
	Name	Name of the specified voltage sensor.	GET

URL	Property	Description	Operation
	SensorNumber	Serial number of the specified voltage sensor.	GET
	Status	Status of the specified voltage sensor.	GET
	ReadingVolts	Current reading of the specified voltage sensor.	GET
	UpperThresholdNonCritical	Non-critical warning threshold for high voltage of the specified voltage sensor.	GET
	UpperThresholdCritical	Critical warning threshold for high voltage of the specified voltage sensor.	GET
	UpperThresholdFatal	Fatal warning threshold for high voltage of the specified voltage sensor.	GET
	LowerThresholdNonCritical	Non-critical warning threshold for low voltage of the specified voltage sensor.	GET
	LowerThresholdCritical	Critical warning threshold for low voltage of the specified voltage sensor.	GET
	LowerThresholdFatal	Fatal warning threshold for low voltage of the specified voltage sensor.	GET
	MinReadingRange	Minimum voltage that can be read by the specified voltage sensor.	GET
	MaxReadingRange	Maximum voltage that can be read by the specified voltage sensor.	GET
	PowerLimitEnable	Whether power capping is enabled.	GET/PATCH
/redfish/v1/Chassis/chassis_id/NetworkAdapters	Name	Name of the network adapter resource.	GET
	Members@odata.count	Number of network adapter resource members.	GET
	Members	Access path of a single network adapter resource node.	GET
/redfish/v1/Chassis/chassis_id/Net-	Controllers	Information about adapter controllers.	GET

URL	Property	Description	Operation
workAdapters/NetworkAdapters_id	FirmwarePackageVersion	Firmware version of the specified network adapter.	GET
	Links	Link to the related resources.	GET
	NetworkPorts@odata.count	Number of network port resources.	GET
	Id	ID of the specified network adapter resource.	GET
	Name	Name of the specified network adapter resource.	GET
	Manufacturer	Manufacturer of the specified network adapter.	GET
	Model	Model the specified network adapter.	GET
	Controllers	Controllers of the specified network adapter.	GET
	DriverVersion	Driver version of the specified network adapter.	GET
	NetworkPorts	Relevant network port object collection of the specified network adapter.	GET
	Status	Status of the specified network adapter resource.	GET
	Oem.Public	Field customized by the manufacturer of the network adapter resource.	GET
	CardManufacturer	Manufacturer of the specified network adapter.	GET
	CardModel	Interface mode of the specified network adapter.	GET
	CardType	Type of the specified network adapter.	GET
	ConfigFpgaTmp	Alarm temperature of the specified network adapter.	GET
	CurrentFpgaTmp	Main chip temperature of the specified network adapter.	GET

URL	Property	Description	Operation
	DeviceLocator	Silk screen of the specified network adapter.	GET
	DriverVersion	Driver version of the specified network adapter.	GET
	FpgaStatus	FPGA status of the specified network adapter.	GET
	HistoryMaxTmp	Maximum historical temperature of the specified network adapter.	GET
	NetworkTechnology	Network protocol of the specified network adapter.	GET
	NicMemory	Memory information about the specified network adapter.	GET
	CapacityGb	Memory capacity of the specified network adapter.	GET
	Model	Memory model of the specified network adapter.	GET
	Status	Memory status of the specified network adapter.	GET
	nicNeoCpuArch	NEO CPU architecture.	GET
	nicNeoCpuCore	Number of NEO CPU cores.	GET
	nicNeoDiskSize	NEO hard disk capacity.	GET
	nicNeoMemSize	NEO memory capacity.	GET
	RootBDF	Root port BDF of the specified network adapter.	GET
	SlotNumber	Slot number of the specified network adapter.	GET
	BoardId	Board ID of the specified network adapter.	GET
	BootOption	Boot mode of the specified network adapter.	GET
	TmpStatus	FPGA temperature of the specified network adapter.	GET
	Status	Network adapter status.	GET

URL	Property	Description	Operation
	SerialNumber	Serial number of the specified network adapter.	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/NetworkAdapters_id/NetworkPorts/NetworkPorts_id	Id	ID of the network port resource.	GET
	Name	Name of the network port resource.	GET
	PhysicalPortNumber	Physical silk screen of the specified network port.	GET
	LinkStatus	Status of the specified network port.	GET
	AssociatedNetworkAddresses	Network address of the specified network port. The FC cards are classified into WWPN and WWNN. By order, the first one is WWPN, and the other is WWNN.	GET
	Oem	Status of the specified network port.	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
	CapableSpeedGbs	Maximum interface speed of the specified drive.	GET/PATCH
	DiskTemperatureCelsius	Drive temperature (°C).	GET
	NegotiatedSpeedGbs	Negotiated interface speed of the specified drive.	GET
	CapacityBytes	Capacity of the specified drive, in bytes.	GET/PATCH
	FailurePredicted	Whether a failure is predicted by the specified drive.	GET/PATCH
	HotspareType	Hotspare status of the specified drive.	GET/PATCH
	Manufacturer	Manufacturer of the specified drive.	GET

URL	Property	Description	Operation
	Status	Status of the specified drive.	GET
	CapacityBytes	Capacity of the specified drive, in bytes.	GET
	MediaType	Media type of the specified drive.	GET
	Protocol	Compliant protocol of the specified drive.	GET
	PredictedMediaLifeLeftPercent	Percentage of the remaining service life 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
	SerialNumber	Serial number of the specified drive.	GET
	PartNumber	Part number of the specified drive.	GET/PATCH
	SlotNumber	Slot number of the specified drive.	GET/PATCH
	Location	Silk screen of the specified drive.	GET/PATCH
	Info	Silk screen information about the specified drive.	GET/PATCH
	InfoFormat	Silk screen format of the specified drive.	GET/PATCH
	BackpanelId	FRU ID of the U.2 NVMe hard disk backplane.	GET
	RotationSpeedRPM	Rotation speed of the specified drive, unit: RPM.	GET
	Oem.Public	Customized field.	GET
	BelongCPU	CPU that the controller belongs to.	GET
	ControllerBDF	Controller BDF.	GET
	ControllerPortNum	Controller port number.	GET
	DiskLocater	Locator ID of the specified disk drive: For the PMC, the format is as follows: controller slot:controller port:cabinet ID:hard disk slot reported by the controller.	GET

URL	Property	Description	Operation
		For the LSI, the format is as follows: controller slot:cabinet ID:hard disk slot reported by the controller.	
	mediaErrCount	Number of media errors of the specified disk drive.	GET
	otherErrCount	Number of other errors of the specified disk drive.	GET
	prefailErrCount	Number of predicted failure errors of the specified disk drive.	GET
	DriveState	Logical disk status.	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	List of drive resources.	GET
/redfish/v1/Chassis/chassis_id/PCIeDevices	Name	Name of the PCIe 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/PCIeDevices/PCIeDevices_id	Id	ID of the specified PCIe device resource.	GET
	Name	Name 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

URL	Property	Description	Operation
	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 speed supported by the specified PCIe device, unit: GT/s.	GET
	DeviceLocator	Silk screen of the specified PCIe device.	GET
	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
	PCIeCardType	Type of the specified PCIe device.	GET
	PowerCapacityWatts	Rated power of the specified PCIe device.	GET
	PowerWatts	Power of the specified PCIe device.	GET
	SlotNumber	Slot number of the specified PCIe device.	GET

URL	Property	Description	Operation
	Oem.Public.GpuCore	-	GET
	BuildTime	Production date of memory of the specified PCIe device.	GET
	CapacityGB	Capacity of memory 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
/redfish/v1/Chassis/chassis_id/PCIeDevices?$expand=	Name	Name of the PCIe device resource collection.	GET
	Members@odata.count	Number of PCIe device resources.	GET
	Members	List of PCIe device resources.	GET
/redfish/v1/Chassis/Chassis_id/Power/NetworkAdapters/NetworkAdapters_id	Controllers	Information about adapter controllers.	PATCH
	FirmwarePackageVersion	Firmware version of the specified network adapter.	PATCH
	Links	Link to the related resources.	PATCH
	NetworkPorts@odata.count	Number of network port resources.	PATCH
	Id	Unique ID of the network adapter resource in the iBMC system.	PATCH
	Manufacturer	Chip manufacturer of the specified network adapter.	PATCH
	Model	Model of the specified network adapter.	PATCH
	Name	Name of the specified network adapter resource.	PATCH
	NetworkPorts	Network port resource description.	PATCH

URL	Property	Description	Operation
	@odata.id	Access path of the network port resource collection.	PATCH
	Oem.Public	Customized properties.	PATCH
	Name	Name of the specified network adapter.	PATCH
	CardManufacturer	Manufacturer of the specified network adapter.	PATCH
	CardModel	Interface mode of the specified network adapter.	PATCH
	CardType	Type of the specified network adapter.	PATCH
	ConfigFpgaTmp	Alarm temperature of the specified network adapter.	PATCH
	CurrentFpgaTmp	Main chip temperature of the specified network adapter.	PATCH
	DeviceLocator	Silk screen of the specified network adapter.	PATCH
	DriverVersion	Driver version of the specified network adapter.	PATCH
	FpgaStatus	FPGA status of the specified network adapter.	PATCH
	HistoryMaxTmp	Maximum historical temperature of the specified network adapter.	PATCH
	NetworkTechnology	Network protocol of the specified network adapter.	PATCH
	NicMemory	Memory information about the specified network adapter.	PATCH
	CapacityGb	Memory capacity of the specified network adapter.	PATCH
	Model	Memory model of the specified network adapter.	PATCH
	Status	Memory status of the specified network adapter.	PATCH
	nicNeoCpuArch	NEO CPU architecture.	PATCH

URL	Property	Description	Operation
	nicNeoCpuCore	Number of NEO CPU cores.	PATCH
	nicNeoMemSize	NEO memory capacity.	PATCH
	nicNeoDiskSize	NEO hard disk capacity.	PATCH
	RootBDF	Root port BDF of the specified network adapter.	PATCH
	SlotNumber	Slot number of the specified network adapter.	PATCH
	BoardId	Board ID of the specified network adapter.	PATCH
	BootOption	Boot mode of the specified network adapter.	PATCH
	TmpStatus	FPGA temperature status of the specified network adapter.	PATCH
	Status	Network adapter status.	PATCH
	SerialNumber	Serial number of the specified network adapter.	PATCH
/redfish/v1/Chassis/chassis_id/ThermalSubsystem/LeakDetection	Id	ID of the leakage detection system.	GET
	Name	Name of the leakage detector system.	GET
	LeakDetectors	List of leakage detector resources.	GET
/redfish/v1/Chassis/chassis_id/ThermalSubsystem/LeakDetection/LeakDetectors	Id	ID of the leakage detector resource collection.	GET
	Name	Name of the leakage detector resource collection.	GET
	Members@odata.count	Number of leakage detector resources.	GET
	Members	List of leakage detector resources.	GET
/redfish/v1/Chassis/chassis_id/ThermalSubsystem/LeakDetection/Lea kDetectors/leakdetector_id	Id	ID of the specified leakage detector resource.	GET
	Name	Name of the specified leakage detector resource.	GET
	DetectorState	Leakage status of the specified leakage detector resource.	GET

URL	Property	Description	Operation
	Status	Status of the specified leakage detector resource.	GET

6.1 Querying Information About the Chassis Resource Collection

Function

Query information about the current chassis resource collection of a server.

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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1579064918\"",
    "@odata.id": "/redfish/v1/Chassis",
    "@odata.type": "#ChassisCollection.ChassisCollection",
    "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.etag	String	Whether the interface is changed.
@odata.id	String	Access path of the chassis resource collection.
@odata.type	String	Type of chassis resource collection.
Name	String	Name of the chassis resource collection.
Members@odata.count	Number	Number of chassis resource members.
Members	Object array	Chassis resource list.
@odata.id	String	Access path of a single chassis resource node.

6.2 Querying Information About the Specified Chassis Resource

Function

Query information about the specified chassis resource of a server.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Chassis/chassis_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 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 */redfish/v1/SessionService/Sessions*.
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 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.etag": "W/\"1593359038\"",
    "@odata.id": "/redfish/v1/Chassis/1",
    "@odata.type": "#Chassis.v1_6_0.Chassis",
    "AssetTag": "@mbX9ZY@AaYeS",
    "ChassisType": "RackMount",
    "Description": "",
    "Drives": {
        "@odata.id": "/redfish/v1/Chassis/1/Drives"
    },
    "Id": "1",
    "IndicatorLED": "Off",
    "IndicatorLED@Redfish.AllowableValues": ["Lit","Blinking","Off"],
    "Links": {
        "ComputerSystems": [{
            "@odata.id": "/redfish/v1/Systems/1"
        }],
        "ManagedBy": [{
            "@odata.id": "/redfish/v1/Managers/1"
        }]
    },
    "Manufacturer": "Vantageo",
    "Model": "SPLMA",
    "Name": "Computer System Chassis",
    "BoardPartNum": "19010100",
    "boardProductVer": "00",
    "Productdate": "2023-02-20 19:36:00",
    "ChassisType": "Rack Mount Chassis",
    "PartNumber": "127038731145",
    "ChassisSerialNum": "null"
    "NetworkAdapters": {
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters"
    },
    "Oem": {
        "Public": {
            "Boards": {
                "@odata.id": "/redfish/v1/Chassis/1/Boards"
            },
            "ChassisHeight": "2U",
            "DeviceMaxNum": {
```

```
                "CPUNum": 2,
                "DiskNum": 10,
                "FanNum": 6,
                "MemoryNum": 24,
                "PCIeNum": 8,
                "PowerSupplyNum": 2
            },
            "Mainboard": {
                "BoardExtra":"Logic Board Name R53G4XP"
                "BoardName": "SPLMA",
                "Manufacturer": "Vantageo",
                "SerialNumber": "211111111111"
            },
            "ProductLocation": "123",
            "ProductName": "2230-RE",
            "ProductSpecificIdentity": "2230-RE,SPLMA,Intel"
        }
    },
    "PCIeDevices": {
        "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices"
    },
    "PartNumber": "16030200",
    "Power": {
        "@odata.id": "/redfish/v1/Chassis/1/Power"
    },
    "PowerState": "On",
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "Thermal": {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal"
    },
    "ThermalSubsystem": {
        "@odata.id": "/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection"
    }
}
```


- 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 node.
@odata.type	String	Type of the specified chassis resource.
@odata.etag	String	Whether the interface is changed.
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.
IndicatorLED	String	Positioning indicator status of the specified chassis resource, options: ● Lit ● Blinking ● Off
IndicatorLED@Redfish.AllowableValues	Array	Position indicator status range of the specified chassis resource.
Status	Object	Status of the specified chassis resource, including: ● State: enabling status of the chassis ● 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.
DeviceMaxNum	Object	Maximum number of board parts.
CPUNum	Number	Maximum number of CPUs.
DiskNum	Number	Maximum number of hard disks.
FanNum	Number	Maximum number of fans.
MemoryNum	Number	Maximum number of memory modules.

Field	Type	Description
PCIeNum	Number	Maximum number of PCIe cards.
PowerSupplyNum	Number	Maximum number of power supplies.
Mainboard	Object	Mainboard information.
BoardExtra	Character string	Additional mainboard information.
BoardName	String	Mainboard name.
SerialNumber	String	Serial number of the mainboard.
Links	Object	Links related to the chassis resource.
ComputerSystems	Array	Link to System resources.
ManagedBy	Array	Link to Manager resources.
PCIeDevices	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.
ThermalSubsystem	Object	Thermal sub-system resource information.
ChassisHeight	String	Chassis height.
ProductName	String	Custom product name.
ProductLocation	Character string	Product location.
ProductSpecificIdentity	String	Product ID: planned product name, mainboard name, and CPU manufacturer.
Productdate	String	Extended card production date.
ChassisType	String	Chassis type.
BoardPartNum	String	Extended card material number.
ChassisSerialNum	String	Chassis serial number, which is null if it cannot be obtained.
boardProductVer	String	Extended card product version.

6.3 Modifying the Position Indicator Status of a Chassis

Function

Turn on or off the position indicator of a chassis.

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,
    "Oem": {
        "Public": {
            "ProductLocation": productlocation
        }
    }
}
```

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 GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
state	Position indicator status of the chassis resource.	Including: ● Lit ● Off
productlocation	Product location.	String of 0 to 64 characters. This parameter consists of digits, letters, and special characters.

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.

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 Informations 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1581377860\"",
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters",
    "@odata.type": "#NetworkAdapterCollection.NetworkAdapterCollection",
    "Description": "Collection of Network Adapters for this Manager",
    "Members":
    [{
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1"
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard5"
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard8"
    }],
    "Members@odata.count": 3,
    "Name": "Network Adapters Collection"
```

```
}
```

- 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.
Members@odata.count	Number	Number of network adapter resource members.
Members	Object 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.

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

Description

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 */redfish/v1/SessionService/Sessions*.
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/mainboardLOM1
```

- Request Header:

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

- Request Message Body: None
- Response Example 1:


```
{
    "@odata.context": "/redfish/v1/$metadata#NetworkAdapter.NetworkAdapter",
    "@odata.etag": "W/\"1597744869\"",
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1",
    "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
    "Controllers":
    [{
        "FirmwarePackageVersion": null,
        "Links":
        {
            "NetworkPorts":
            [{
```

```
                "@odata.id":
                "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts/0"
            },
            {
                "@odata.id":
                "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts/1"
            },
            {
                "@odata.id":
                "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts/2"
            },
            {
                "@odata.id":
                "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts/3"
            }],
            "NetworkPorts@odata.count": 4
        }
    }],
    "Id": "mainboardLOM1",
    "Manufacturer": "Intel",
    "Model": "X722",
    "Name": : "mainboardLOM1",
    "NetworkPorts":
    {
        "@odata.id":
        "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts"
    },
    "Oem":
    {
        "Public":
        {
            "CardManufacturer": "",
            "CardModel": "2*10GE+2*GE",
            "CardType": "copperfiber",
            "DriverVersion": null,
            "NetworkTechnology": ["Ethernet"],
            "DeviceLocator":"mainboardLOM1",
            "SlotNumber": 1,
            "RootBDF": "0000:1a:00.0"
        }
    },
    "Status": { "Health": "OK", "State": "Enabled"},
    "SerialNumber": null
}
```

- Response Example 2 (H2PCX):


```
{
    "@odata.context": "/redfish/v1/$metadata#NetworkAdapter.NetworkAdapter",
    "@odata.etag": "W/\"1602293267\"",
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard5",
    "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
    "Controllers": [
     {
         "FirmwarePackageVersion": "0002",
         "Links": {
         "NetworkPorts": [
         {
         "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard5
                       /NetworkPorts/0"
         },
         {
         "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard5
                       /NetworkPorts/1"
         }
             ],
             "NetworkPorts@odata.count": 2
         }
     }
    ],
    "Id": "mainboardPCIeCard5",
    "Manufacturer": "Xilinx",
    "Model": "FPGA-Xi7p",
    "Name": "mainboardPCIeCard5",
    "NetworkPorts": {
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard5/NetworkPorts"
    },
    "Oem": {
        "Public": {
            "CardManufacturer": "",
            "Name": "H2PCX",
            "CardModel": "2*100GE",
            "CardType": "fiber",
            "ConfigFpgaTmp": 100,
            "CurrentFpgaTmp": 56,
            "DeviceLocator": "mainboardPCIeCard5",
            "DriverVersion": null,
            "FpgaStatus": 0,
            "HistoryMaxTmp": 60,
```

```
            "NetworkTechnology": [
                "Ethernet"
            ],
            "NicMemory": [
                {
                    "CapacityGb": 128,
                    "Model": "QDR4_2000MHz",
                    "Status": 0
                },
                {
                    "CapacityGb": 81920,
                    "Model": "DDR4_2400MHz",
                    "Status": 0
                },
                {
                    "CapacityGb": 32768,
                    "Model": "DDR4_2400MHz",
                    "Status": 0
                },
                {
                    "CapacityGb": 16384,
                    "Model": "DDR4_2400MHz",
                    "Status": 0
                },
                {
                    "CapacityGb": 32768,
                    "Model": "DDR4_2400MHz",
                    "Status": 0
                }
            ],
            "RootBDF": "0000:af:00.0",
            "SlotNumber": 5,
            "TmpStatus": 0
        }
    },
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "SerialNumber": "730603300009"
}
```


- Response Example 3 (NEO card):


```
{
```

```
"@odata.context": "/redfish/v1/$metadata#NetworkAdapter.NetworkAdapter",
"@odata.etag": "W/\"1656560446\"",
"@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard4",
"@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
"Controllers": [
{
  "FirmwarePackageVersion": null,
  "Links": {
  "NetworkPorts": [
{
"@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard4
              /NetworkPorts/1"
 },
 {
"@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard4
              /NetworkPorts/2"
 },
 {
"@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard4
              /NetworkPorts/3"
 },
 {
"@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard4
              /NetworkPorts/4"
  }
      ],
       "NetworkPorts@odata.count": 4
        }
    }
],
"Id": "mainboardPCIeCard4",
"Manufacturer": "NXP",
"Model": "CPU-LX2160",
"Name": "mainboardPCIeCard4",
"NetworkPorts": {
"@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard4/NetworkPorts"
},
"Oem": {
    "Public": {
        "CardManufacturer": "",
        "CardModel": "2*10GE+2*25GE",
        "CardType": "fiber",
        "DeviceLocator": "mainboardPCIeCard4",
        "DriverVersion": null,
```

```
            "Name": null,
            "NeoCpuArch": "aarch64",
            "NeoCpuCore": 16,
            "NeoDiskSize": 32,
            "NeoMemSize": 32,
            "NetworkTechnology": [
                "Ethernet"
            ],
            "RootBDF": "0000:31:00.0",
            "SlotNumber": 4
        }
    },
    "SerialNumber": null,
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    }
}
```


- Response Example 4 (NEO acceleration card):


```
{
    "@odata.context": "/redfish/v1/$metadata#NetworkAdapter.NetworkAdapter",
    "@odata.etag": "W/\"946685110\"",
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard7",
    "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
    "Controllers": [
        {
            "FirmwarePackageVersion": "0103",
            "Links": {
                "NetworkPorts": [
                    {
                        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/
                          mainboardPCIeCard7/NetworkPorts/1"
                    },
                    {
                        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/
                          mainboardPCIeCard7/NetworkPorts/2"
                    },
                    {
                        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/
                         mainboardPCIeCard7/NetworkPorts/3"
                    },
                    {
                        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/
```

```
                    mainboardPCIeCard7/NetworkPorts/4"
                }
            ],
                "NetworkPorts@odata.count": 4
        }
    }
],
"Id": "mainboardPCIeCard7",
"Manufacturer": "Xilinx",
"Model": "FPGA-Xi9p",
"Name": "mainboardPCIeCard7",
"NetworkPorts": {
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard7/
     NetworkPorts"
},
"Oem": {
     "Public": {
        "BoardId": "0x3168",
        "CardManufacturer": "",
        "CardModel": "2*100GE+2*25GE",
        "CardType": "fiber",
        "ConfigFpgaTmp": 100,
        "CurrentFpgaTmp": 49,
        "DeviceLocator": "mainboardPCIeCard7",
        "DriverVersion": null,
        "FpgaStatus": 0,
        "HistoryMaxTmp": 49,
        "Name": "NEO XE310",
        "NetworkTechnology": [
            "Ethernet"
        ],
        "NicMemory": [
            {
                "CapacityGb": 64, "Model": "DDR4_2000MHz",
                "Status": 0
            },
            {
                "CapacityGb": 32,
                "Model": "DDR4_2000MHz",
                "Status": 0
            },
            {
                "CapacityGb": 16,
                "Model": "DDR4_2000MHz",
```

```
                    "Status": 0
                }
            ],
            "RootBDF": "0000:c3:00.0",
            "SlotNumber": 7,
            "TmpStatus": 0
        }
    },
    "SerialNumber": "727943600035",
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    }
}
```


- 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.
@odata.id	String	Access path of the specified network adapter resource node.
@odata.type	String	Type of the specified network adapter resource.
Controllers	Array	Information about adapter controllers.
FirmwarePackageVersion	String	Firmware version of the specified network adapter.
Links	Object	Links to the related resources.
@odata.id	String	Access path of a network port resource node.
NetworkPorts@odata.count	Number	Number of network port resources.
Id	String	Unique ID of the network adapter resource in the i BMC system.

Field	Type	Description
Manufacturer	String	Manufacturer of the specified network adapter.
Model	String	Model of the specified network adapter.
Name	String	Name of the specified network adapter resource.
NetworkPorts	Object	Network port resource information.
@odata.id	String	Access path of the network port resource collection node.
Oem.Public	Object	Manufacturer-customized properties.
CardManufacturer	String	Manufacturer of the specified network adapter.
CardModel	String	Interface mode of the specified network adapter.
CardType	String	Type of the specified network adapter.
ConfigFpgaTmp	Number	Warning temperature of the specified network adapter.
CurrentFpgaTmp	Number	Main chip temperature of the specified network adapter.
DeviceLocator	String	Silk screen of the specified network adapter.
DriverVersion	String	Driver version of the specified network adapter.
FpgaStatus	Number	FPGA status of the specified network adapter, including: ● 0: normal FPGA status of the network adapter ● 1: abnormal FPGA status of the network adapter
HistoryMaxTmp	Number	Maximum Historical temperature of the specified network adapter.
NetworkTechnology	Array	Network protocol of the specified network adapter: ● Ethernet ● FC ● iSCSI ● FCoE ● OPA ● IB
NicMemory	Array	Memory information about the specified network adapter.
CapacityGb	Number	Memory capacity of the specified network adapter.
Model	String	Memory model of the specified network adapter.

Field	Type	Description
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
nicNeoCpuArch	String	NEO CPU architecture.
nicNeoCpuCore	Number	Number of NEO CPU cores.
nicNeoMemSize	Number	NEO memory capacity.
nicNeoDiskSize	Number	NEO disk capacity.
RootBDF	String	Root, port, and BDF of the specified network adapter.
SlotNumber	Number	Slot number of the specified network adapter.
BoardId	String	Board ID of the specified network adapter.
BootOption	String	Boot mode of the specified network adapter.
TmpStatus	Number	FPGA temperature of the specified network adapter, including: ● 0: normal FPGA temperature status of the network adapter ● 1: abnormal FPGA temperature 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.

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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1602295423\"",
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters",
    "@odata.type": "#NetworkAdapterCollection.NetworkAdapterCollection",
    "Description": "Collection of Network Adapters for this Manager",
    "Members":
    [{
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1",
        "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
        "Controllers":
        [{
            "FirmwarePackageVersion": "N/A",
            "Links":
```

```
            {
                "NetworkPorts":
                [{
                    "@odata.id":
                    "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts/0"
                },
                {
                    "@odata.id":
                    "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts/1"
                },
                {
                    "@odata.id":
                    "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts/2"
                },
                {
                    "@odata.id":
                    "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts/3"
                }],
                "NetworkPorts@odata.count": 4
            }
        }],
        "Id": "mainboardLOM1",
        "Manufacturer": "Intel",
        "Model": "X722",
        "Name": "SXGFA",
        "NetworkPorts":
        {
            "@odata.id":
            "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts"
        },
        "Oem":
        {
            "Public":
            {
                "CardManufacturer": "",
                "CardModel": "2*10GE+2*GE",
                "CardType": "copperfiber",
                "DeviceLocator": "mainboardLOM1",
                "DriverVersion": "N/A",
                "NetworkTechnology": ["Ethernet"],
                "RootBDF": "0000:1a:00.0",
                "SlotNumber": 0
            }
        },
```

```
    "Status": { "Health": "OK", "State": "Enabled"},
    "SerialNumber": "N/A"
  },
  {
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard2",
    "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
    "Controllers":
    [{
        "FirmwarePackageVersion": "N/A",
        "Links":
        {
            "NetworkPorts":
            [{
                "@odata.id":
                "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard2/
                  NetworkPorts/0"
            },
            {
                "@odata.id":
                "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard2/
                  NetworkPorts/1"
            }],
            "NetworkPorts@odata.count": 2
        }
    }],
    "Id": "mainboardPCIeCard2",
    "Manufacturer": "Intel",
    "Model": "X710",
    "Name": "EX710DA2",
    "NetworkPorts":
    {
        "@odata.id":
        "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard2/NetworkPorts"
    },
    "Oem":
    {
        "Public":
        {
            "CardManufacturer": "Intel",
            "CardModel": "2*10GE",
            "CardType": "fiber",
            "DeviceLocator": "mainboardPCIeCard2",
            "DriverVersion": "N/A",
            "NetworkTechnology": ["Ethernet"],
```

```
                "RootBDF": "0000:5e:00.0",
                "SlotNumber": 2
            }
        },
        "Status": { "Health": "OK", "State": "Enabled"},
        "SerialNumber": "N/A"
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard3",
        "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
        "Controllers":
        [{
            "FirmwarePackageVersion": "N/A",
            "Links":
            {
                "NetworkPorts":
                [{
                    "@odata.id":
                    "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard3/
                      NetworkPorts/0"
                },
                {
                    "@odata.id":
                    "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard3/
                      NetworkPorts/1"
                }],
                "NetworkPorts@odata.count": 2
            }
        }],
        "Id": "mainboardPCIeCard3",
        "Manufacturer": "Intel",
        "Model": "X710",
        "Name": "NS214",
        "NetworkPorts":
        {
            "@odata.id":
            "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard3/NetworkPorts"
        },
        "Oem":
        {
            "Public":
            {
                "CardManufacturer": "",
                "CardModel": "2*10GE",
```

```
            "CardType": "fiber",
            "DeviceLocator": "mainboardPCIeCard3",
            "DriverVersion": "N/A",
            "NetworkTechnology": ["Ethernet"],
            "RootBDF": "0000:60:00.0",
            "SlotNumber": 3
        }
    },
    "Status": { "Health": "OK", "State": "Enabled"},
    "SerialNumber": "014613ffff132000"
},
{
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard5",
    "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
    "Controllers":
    [{
        "FirmwarePackageVersion": "0002",
        "Links":
        {
            "NetworkPorts":
            [{
                "@odata.id":
                "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard5/
                  NetworkPorts/0"
            },
            {
                "@odata.id":
                "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard5/
                  NetworkPorts/1"
            }],
            "NetworkPorts@odata.count": 2
        }
    }],
    "Id": "mainboardPCIeCard5",
    "Manufacturer": "Xilinx",
    "Model": "Xi7p",
    "Name": "H2PCX",
    "NetworkPorts":
    {
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard5/
                                NetworkPorts"
    },
    "Oem":
    {
```

```
            "Public":
            {
                "CardManufacturer": "",
                "CardModel": "2*100GE",
                "CardType": "fiber",
                "ConfigFpgaTmp": 100,
                "CurrentFpgaTmp": 56,
                "DeviceLocator": "mainboardPCIeCard5",
                "DriverVersion": "N/A",
                "FpgaStatus": 0,
                "HistoryMaxTmp": 60,
                "NetworkTechnology": ["Ethernet"],
                "NicMemory":
                [{
                    "CapacityGb": 128,
                    "Model": "QDR4_2000MHz",
                    "Status": 0
                },
                {
                    "CapacityGb": 81920,
                    "Model": "DDR4_2400MHz",
                    "Status": 0
                },
                {
                    "CapacityGb": 32768,
                    "Model": "DDR4_2400MHz",
                    "Status": 0
                },
                {
                    "CapacityGb": 16384,
                    "Model": "DDR4_2400MHz",
                    "Status": 0
                },
                {
                    "CapacityGb": 32768,
                    "Model": "DDR4_2400MHz",
                    "Status": 0
                }],
                "RootBDF": "0000:af:00.0",
                "SlotNumber": 5,
                "TmpStatus": 0
            }
        },
        "Status": { "Health": "OK", "State": "Enabled"},
```

```
        "SerialNumber": "730603300009"
    }],
    "Members@odata.count": 4,
    "Name": "Network Adapters Collection"
}
```

- 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	Object array	Network adapter resource information.

6.7 Querying Information About the Network Port Resource Collection

Function

Query information about the network port resource collection of a server.

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, refer to Table 6-13.

Table 6-13 Parameter Descriptions for Querying Information About the Network Port 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 */redfish/v1/SessionService/Sessions*.
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/mainboardLOM1/NetworkPorts
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#NetworkAdapter.NetworkAdapter",
    "@odata.etag": "W/\"1599580835\"",
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts",
    "@odata.type": "#NetworkPortCollection.NetworkPortCollection",
    "Description": "Collection of Ethernet Interfaces for this Manager",
    "Members":
    [{
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts/0"
    },
    {
```

```
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts/1"
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts/2"
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1/NetworkPorts/3"
    }],
    "Members@odata.count": 4,
    "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, refer to Table 6-14.

Table 6-14 Output Descriptions for Querying Information About the Network Port Resource Collection

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

6.8 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.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapteras_id/NetworkPorts/networkports_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 network port resource, refer to Table 6-15.

Table 6-15 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 */redfish/v1/SessionService/Sessions*.
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/mainboardPCIeCard8/NetworkPorts/2
```

- Request Header:

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

- Request Message Body: None

- Response Example:


```
{
    "@odata.context": "/redfish/v1/$metadata#EthernetInterface.EthernetInterface",
    "@odata.etag": "W/\"1593389371\"",
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard8
                  /NetworkPorts/0",
    "@odata.type": "#NetworkPort.v1_4_0.NetworkPort",
    "AssociatedNetworkAddresses": [
        null,
        null
    ],
    "AutoNeg": null,
    "Id": "0",
    "LinkStatus": null,
    "Name": "0",
    "Oem": {
        "Public": {
            "BDF": "0000:d8:00.0",
            "CurrentSpeed": null,
            "DriverVersion": null,
            "FirmwarePackageVersion": null,
            "PortMaxSpeed": "1000Mb/s",
            "PortType": "OpticalPort",
            "LldpService": {
                "LldpEnabled": false,
                "WorkMode": null
            },
            "SupportSpeed": [
                "4000Mb/s",
                "8000Mb/s",
                "16000Mb/s"
            ]
        }
    },
    "OpticalModule": {
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard8/
                      NetworkPorts/0/OpticalModule"
    },
    "PhysicalPortNumber": "0"
}
```


- 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 6-16.

Table 6-16 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 node.
@odata.type	String	Type of the specified network port resource.
Name	String	Name of the specified network port resource.
Id	String	UID of the specified network port resource in the iBMC system.
PhysicalPortNumber	String	Physical silk screen of the specified network port.
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	Speed of the specified network port, unit: Mb/s.
PortType	String	Type of the specified network port, including: ● Optical port: OpticalPort ● Electrical port: ElectricalPort ● Unknown: null
BDF	String	BDF of the specified network port.
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
OpticalModule	Object	Optical module resource of the specified network port.
WorkMode	String	Operational mode of the LLDP resource: ● Tx: transmitting mode ● Rx: receiving mode ● TxRx: transmitting & receiving mode ● Disabled: neither transmitting nor receiving.
SupportSpeed	Array	Supported speed of the specified network port.

6.9 Modifying the LLDP Switch of a Network Port

Function

Modify the LLDP switch of a network port.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapteras_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
```

```
            }
        }
    }
}
```

Description

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.
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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
enable_value	Whether LLDP is enabled.	• true: enabled • false: disabled
workmode_valueLLDP	Operational mode.	• TxRx: transmitting & receiving mode • Rx: receiving mode • Tx: transmitting mode TxRx mode is the default mode used when LLDP is enabled. If LLDP is disabled, **workmode_valueLLDP** is unavailable.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard3/NetworkPorts/0
```

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type:application/json
```

- Request Message Body:

```
{
```

```
    "Oem":
    {
        "Public":
        {
            "LldpService":
            {
                "LldpEnabled": true
            }
        }
    }
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#EthernetInterface.EthernetInterface",
    "@odata.etag": "W/\"1603077474\"",
    "@odata.id":
    "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard3/NetworkPorts/0",
    "@odata.type": "#EthernetInterface.v1_4_0.EthernetInterface",
    "AssociatedNetworkAddresses": ["84:13:9F:32:23:26"],
    "AutoNeg": "Auto",
    "Id": "0",
    "LinkStatus": "Down",
    "Name": "0",
    "Oem":
    {
        "":
        {
            "BDF": "0000:60:00.0",
            "CurrentSpeed": null,
           "DriverVersion": null,
           "FirmwarePackageVersion": null,
           "LldpService":
           {
               "LldpEnable": false,
               "WorkMode": null
           },
           "PortMaxSpeed": "10000Mb/s",
           "PortSpeed": "10000Mb/s",
           "PortType": "OpticalPort",
           "SupportSpeed": null
        }
    },
    "PhysicalPortNumber": "0"
```

```
}
```

- 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 node.
@odata.type	String	Type of the specified network port resource.
Name	String	Name of the specified network port resource.
Id	String	UID of the specified network port resource in the iBMC system.
PhysicalPortNumber	String	Physical silk screen of the specified network port.
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	Speed of the specified network port, unit: Mb/s.
PortType	String	Type of the specified network port, including: ● Optical port: OpticalPort ● Electrical port: ElectricalPort ● Unknown: null
BDF	String	BDF of the specified network port.

Field	Type	Description
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
WorkMode	String	LLDP operation mode.
SupportSpeed	Array	Supported speed 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.

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.

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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/PCIeDevices
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/
         $metadata#PCIeDevicesCollection.PCIeDevicesCollection",
    "@odata.etag": "W/\"1593003194\"",
    "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices",
    "@odata.type": "#PCIeDeviceCollection.PCIeDeviceCollection",
    "Description": "PCIe Device Collection",
    "Members":
    [{
        "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard7"
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard8"
    }],
    "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 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.
Name	String	Name of the PCIe device resource collection.
Members@odata.count	Number	Number of PCIe device resource members.
Members	Object array	PCIe device resource list.
@odata.id	String	Access path of the PCIe device resource node.

6.11 Querying Information About a Specified PCIe Device Resource

Function

Query information about a specified PCIe device resource of a server.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Chassis/chassis_id/PCIeDevices/pciedevices_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 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**.

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 */redfish/v1/SessionService/Sessions*.
pciedevices_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/PCIeCard6
```

- Request Header:

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

- Request Message Body: None
- Response Example 1:


```
{
    "@odata.context": "/redfish/v1/$metadata#PCIeDevices.PCIeDevices",
    "@odata.etag": "W/\"1603393787\"",
    "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard8",
    "@odata.type": "#PCIeDevice.v1_2_0.PCIeDevice",
    "Description": "Raid Controller",
    "FirmwareVersion": null,
    "Id": "mainboardPCIeCard8",
    "Links": {
        "PCIeFunctions": [
            {
                "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard8/Functions/1"
            }
        ]
    },
    "Manufacturer": "Broadcom",
    "Model": "RAID_SAS3108",
    "Name": "RAID8",
    "Oem": {
        "Public": {
            "LinkSpeed": 3GT/s,
```

```
            "MaxLinkSpeed": 3GT/s,
            "DeviceLocator": "PCIeCard8",
            "MemorySizeMiB": null,
            "PCIeCardType": "RAID",
            "PowerCapacityWatts": null,
            "PowerWatts": null,
            "SlotNumber": 8
        }
    },
    "PCIeInterface": {
        "LanesInUse": 3,
        "MaxLanes": 8
    },
    "SerialNumber": null,
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    }
}
```


- Response Example 2 (GPU card):


```
{
    "@odata.context": "/redfish/v1/$metadata#PCIeDevices.PCIeDevices",
    "@odata.etag": "W/\"1658955027\"",
    "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard1",
    "@odata.type": "#PCIeDevice.v1_2_0.PCIeDevice",
    "Description": "MLU270-S4",
    "FirmwareVersion": "V1.1.3",
    "Id": "mainboardPCIeCard1",
    "Links": {
        "PCIeFunctions": [
            {
                "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard1/Functions/1"
            }
        ]
    },
    "Manufacturer": "Cambricon",
    "Model": "MLU270-S4",
    "Name": "GPU1",
    "Oem": {
        "Public": {
            "DeviceLocator": "PCIeCard1",
            "GpuCore": [
                {
```

```
                    "BuildTime": "2020/11",
                    "CapacityGB": 16,
                    "MemberId": 0,
                    "PartNum": "0270-0012",
                    "Power": 18,
                    "Temperature": 44
                }
            ],
            "MemoryBandWidth": "102.4GB/s",
            "MemorySizeMiB": 16384,
            "PCIeCardType": "GPU",
            "PowerCapacityWatts": 70,
            "PowerConsumedWatts": 18,
            "PowerWatts": 18,
            "ReadingCelsius": 44,
            "SlotNumber": 1
        }
    },
    "PCIeInterface": {
        "LanesInUse": 16,
        "MaxLanes": 16
    },
    "SerialNumber": "122011101424",
    "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 node.
@odata.type	String	Type of the specified PCIe device resource.

Field	Type	Description
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	Object	Links to the related resources.
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: enabling status of the specified PCIe device
PCIeInterface	Object	Interface of 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.
DeviceLocator	String	Silk screen of the specified PCIe device.
MemorySizeMiB	String	Total memory capacity of the specified PCIe device.
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.
PowerConsumedWatts	Number	Actual power consumed by the specified GPU.
ReadingCelsius	Number	Actual temperature of the specified GPU.
PCIeCardType	String	Type of the specified PCIe device.

Field	Type	Description
PowerCapacityWatts	Number	Rated power of the specified PCIe device.
PowerWatts	Number	Power of the specified PCIe device.
SlotNumber	Number	Slot number of the specified PCIe device.
Oem.Public.GpuCore	Memory resource list of the specified PCIe device.	-
BuildTime	String	Production date of memory of the specified PCIe device.
CapacityGB	Number	Memory capacity of the specified PCIe device.
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.
Temperature	Number	Temperature of the specified PCIe device.

6.12 Querying Information About a Specified PCIe Function Resource

Function

Query information about a specified PCIe 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 information about the specified PCIe function resource, refer to Table 6-23.

Table 6-23 Parameter Descriptions for Querying Information About the Specified PCIe 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	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
pciedevices_id	ID of specified PCIe device resource.	It can be obtained by querying the information about the PCIe resource collection.
functions_id	ID of the specified PCIe function resource.	It can be obtained by querying the information about the specified PCIe resource.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/PCIeDevices/PCIeCard7/Functions/1
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1597747030\"",
    "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard7/Functions/1",
    "@odata.type": "#PCIeFunction.v1_1_1.PCIeFunction",
    "DeviceClass": "MassStorageController",
    "DeviceId": "0x0023",
    "Id": "1",
    "Links":
    {
        "PCIeDevice":
        [{
            "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard7"
        }]
```

```
    },
    "Name": "Function1",
    "Oem":
    {
        "Public":
        {
            "AssociatedResource": "CPU1",
            "BusNumber": "0x86",
            "DeviceNumber": "0x00",
            "FunctionNumber": "0x00"
        }
    },
    "SubsystemId": "0x0023",
    "SubsystemVendorId": "0x1c58",
    "VendorId": "0x1c58"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified PCIe function resource, refer to Table 6-24.

Table 6-24 Output Descriptions for Querying Information About the Specified PCIe Function Resource

Field	Type	Description
@odata.context	String	OData description of the specified PCIe function resource model.
@odata.id	String	Access path of the specified PCIe function resource.
@odata.type	String	Type of the specified PCIe function resource.
Name	String	Name of the specified PCIe function resource.
Id	String	UID of the specified PCIe function resource in the iBMC system.
DeviceClass	String	Classifications of the specified PCIe devices, including: ● UnclassifiedDevice ● MassStorageController ● NetworkController ● DisplayController ● MultimediaController ● MemoryController ● Bridge

Field	Type	Description
		• CommunicationController • GenericSystemPeripheral • InputDeviceController • IntelligentController • SatelliteCommunicationsController • EncryptionController • SignalProcessingController • ProcessingAccelerators • NonEssentialInstrumentation • Coprocessor • UnassignedClass • Other
DeviceId	String	Device ID of the specified PCIe device.
SubsystemId	String	Sub-system ID of the specified PCIe device.
SubsystemVendorId	String	Sub-system manufacturer ID of the specified PCIe device.
VendorId	String	Manufacturer ID of the specified PCIe device.
Links	Object	Links to the related resources.
PCIeDevice	Object array	PCIe device resource list.
@odata.id	String	Access path of the specified PCIe device resource.
Oem.Public	Object	Customized properties.
AssociatedResource	String	Associated resource of the specified PCIe device.
BusNumber	String	Bus number of the root port of the specified PCIe device.
DeviceNumber	String	Device number of the root port of the specified PCIe device.
FunctionNumber	String	Function number of the root port of the specified PCIe device.

6.13 Querying Information About All PCIe Device Resources

Function

Query information about all PCIe device resources of a server.

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

Description

For the parameter descriptions for querying information about all PCIe device resources, refer to Table 6-25.

Table 6-25 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1603390638\"",
    "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices",
    "@odata.type": "#PCIeDeviceCollection.PCIeDeviceCollection",
    "Members": [
        {
```

```
"@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard5",
"@odata.type": "#PCIeDevice.v1_2_0.PCIeDevice",
"Description": "Tesla V100-PCIE-32GB",
"FirmwareVersion": "88.00.7E.00.03",
"Id": "mainboardPCIeCard5",
"Links": {
    "PCIeFunctions": [
    {
    "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard5/Functions/1"
     }
    ]
},
"Manufacturer": "Nvidia",
"Model": "Tesla V100-PCIE-32GB",
"Name": "GPU5",
"Oem": {
    "Public": {
        "DeviceLocator": "PCIeCard5",
        "GpuCore": [
            {
                "BuildTime": "2019/02/26",
                "CapacityGB": 32,
                "MemberId": 0,
                "PartNum": "1DB6-897-A1",
                "Power": 27.705,
                "Temperature": 45
            }
        ],
        "LinkSpeed": "8GT/s",
        "MaxLinkSpeed": "8GT/s",
        "MemoryBandWidth": 1134GB/s,
        "MemorySizeMiB": 32768,
        "PCIeCardType": "GPU",
        "PowerCapacityWatts": 250,
        "PowerConsumedWatts": 27.705,
        "PowerWatts": 27.705,
        "ReadingCelsius": 45,
        "SlotNumber": 5
    }
},
"PCIeInterface": {
    "LanesInUse": 16,
    "MaxLanes": 16
},
```

```
            "SerialNumber": "0420919001247",
            "Status": {
                "Health": "OK",
                "State": "Enabled"
            }
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard7",
            "@odata.type": "#PCIeDevice.v1_2_0.PCIeDevice",
            "Description": "NVME SSd",
            "FirmwareVersion": null,
            "Id": "mainboardPCIeCard7",
            "Links": {
                "PCIeFunctions": [
                {
                "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard7/Functions/1"
                 }
                ]
            },
            "Manufacturer": "HGST, Inc.",
            "Model": "NVME",
            "Name": "RAID7",
            "Oem": {
                "Public": {
                    "LinkSpeed": 3GT/s,
                    "MaxLinkSpeed": 3GT/s,
                    "DeviceLocator": "PCIeCard7",
                    "MemorySizeMiB": null,
                    "PCIeCardType": "RAID"
                }
            },
            "PCIeInterface": {
                "LanesInUse": 3,
                "MaxLanes": 8
            },
            "SerialNumber": null,
            "Status": {
                "Health": "OK",
                "State": "Enabled"
            }
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard8",
            "@odata.type": "#PCIeDevice.v1_2_0.PCIeDevice",
```

```
            "Description": "Raid Controller",
            "FirmwareVersion": null,
            "Id": "mainboardPCIeCard8",
            "Links": {
                "PCIeFunctions": [
                {
                "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard8/Functions/1"
                }
                ]
            },
            "Manufacturer": "Broadcom",
            "Model": "RAID_SAS3108",
            "Name": "RAID8",
            "Oem": {
                "Public": {
                    "LinkSpeed": 3GT/s,
                    "MaxLinkSpeed": 3GT/s,
                    "DeviceLocator": "PCIeCard8",
                    "MemorySizeMiB": null,
                    "PCIeCardType": "RAID"
                }
            },
            "PCIeInterface": {
                "LanesInUse": 3,
                "MaxLanes": 8
            },
            "SerialNumber": null,
            "Status": {
                "Health": "OK",
                "State": "Enabled"
            }
        }
    ],
    "Members@odata.count": 3,
    "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 6-26.

Table 6-26 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 noe.
@odata.type	String	Type of 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. For the requirements for the parameters, refer to 6.11 Querying Information About a Specified PCIe Device Resource.

6.14 Querying Information About the Drive Resource Collection

Function

Query information about the drive resource collection of a server.

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 6-27.

Table 6-27 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.

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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1592997919\"",
    "@odata.id": "/redfish/v1/Chassis/1/Drives",
    "@odata.type": "#DriverCollection.DriverCollection",
    "Description": "Drivers Collection",
    "Members":
    [{
        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk00080011"
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk00080012"
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk03010007"
    }],
    "Members@odata.count": 3, "Name": "Drivers Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the drive resource collection, refer to Table 6-28.

Table 6-28 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.
Name	String	Name of the drive resource collection.
Members@odata.count	Number	Number of drive resource members.
Members	Object array	Drive resource list.
@odata.id	String	Access path of the drive resource node.

6.15 Querying Information About a Specified Drive Resource

Function

Query the information about a specified drive resource on a server. Note that before querying this information, you need to query the drive resource collection information.

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

Description

For a description of the parameters for querying information about the specified drive resource, refer to Table 6-29.

Table 6-29 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**.

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 */redfish/v1/SessionService/Sessions*.
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/HDDPlaneDisk00080011
```

- Request Header:

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

- Request Message Body: None
- Response Example:


```
{
    "@odata.context": "/redfish/v1/$metadata#Drives.Drives",
    "@odata.etag": "W/\"1592997794\"",
    "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk00080011",
    "@odata.type": "#Drive.v1_1_0.Drive",
    "CapableSpeedGbs": 12,
    "CapacityBytes": 1288490188800,
    "DiskTemperatureCelsius": 27,
    "FailurePredicted": false,
    "HotspareType": null,
    "Id": "HDDPlaneDisk00080011",
    "Location": [
        {
            "Info": "Disk1",
            "InfoFormat": "DeviceName"
        }
    ],
    "Manufacturer": "SEAGATE",
    "MediaType": "HDD",
    "Model": "ST1200MM0129",
    "Name": "Disk00080011",
    "NegotiatedSpeedGbs": 12,
```

```
    "Oem": {
        "Public": {
            "DiskLocater": "Pcie Slot4 : EID14 : Slot0",
            "DriveState": "Online",
            "SATAPort": null,
            "mediaErrCount": 0,
            "otherErrCount": 0,
            "prefailErrCount": 0,
        }
    },
    "PartNumber": null,
    "PredictedMediaLifeLeftPercent": null,
    "Protocol": "SAS",
    "Revision": "C003",
    "RotationSpeedRPM": null,
    "SerialNumber": "WFK05GR9",
    "SlotNumber": 0,
    "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 6-30.

Table 6-30 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 node.
@odata.type	String	Type of the specified drive resource.
Id	String	ID of the specified drive resource.
Name	String	Name of the specified drive resource.
Model	String	Model of the specified drive.
Revision	String	Version information about the specified drive.

Field	Type	Description
Status	Object	Status of the specified drive, including: ● State: enabling status of drives ● Health: health status of the drives
CapableSpeedGbs	Number	Maximum interface speed of the specified drive.
DiskTemperatureCelsius	Number	Drive temperature (°C).
NegotiatedSpeedGbs	Number	Negotiated speed of the interface of the specified drive.
CapacityBytes	Number	Capacity of the specified drive, in bytes.
FailurePredicted	Boolean	Pre-failure status of the specified drive, including: ● true ● false
HotspareType	String	Hot-spare status of the specified drive, including: ● None: none ● Global:global hot-spare mode ● Dedicated: partial hot-spare mode
Protocol	Array	Compliant protocol of the specified drive: ● SPI ● PCIe ● AHCI ● UHCI ● SAS ● SATA ● USB ● NVMe ● FC ● iSCSI ● FCoE ● NVMeOverFabrics ● SMB ● NFSv3 ● NFSv4 ● HTTP ● HTTPS ● FTP ● SFTP
MediaType	String	Media type of the specified drive:

Field	Type	Description
		● 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.
Location	Array	Silk screen of the specified drive.
Info	String	Silk screen information about the specified drive.
InfoFormat	String	Silk screen format of the specified drive.
BackpanelId	Number	FRU ID of the U.2 NVMe hard disk back-plane.
RotationSpeedRPM	Number	Rotational speed of the specified drive, unit: RPM.
Oem.Public	Object	Customized BMC properties.
BelongCPU	String	CPU of the controller.
ControllerBDF	String	Controller BDF.
ControllerPortNum	Number	Controller port number.
DiskLocater	String	Locator ID of the specified disk drive: ● For the PMC, the format is as follows: controller slot:controller port:cabinet ID:hard disk slot reported by the con-troller. ● For the LSI, the format is as follows: controller slot:cabinet ID:hard disk slot reported by the controller.
mediaErrCount	Number	Number of hard disk media errors.
otherErrCount	Number	Number of other hard disk errors.
prefailErrCount	Number	Number of predicted failure errors of the specified disk drive.
DriveState	String	Logical disk status.

6.16 Querying Information About All Drive Resources

Function

Query information about the drive resource collection of a server.

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

Description

For a description of the parameters for querying information about all drive resources, refer to Table 6-31.

Table 6-31 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/chassis_id/Drives?$expand=.
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
```

```
"@odata.context": "/redfish/v1/$metadata#DrivesCollection.DrivesCollection",
"@odata.etag": "W/\"1592999011\"",
"@odata.id": "/redfish/v1/Chassis/1/Drives",
"@odata.type": "#DriverCollection.DriverCollection",
"Members": [
    {
        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk00080011",
        "@odata.type": "Drive.v1_1_0.Drive",
        "CapableSpeedGbs": 12,
        "CapacityBytes": 1288490188800,
        "FailurePredicted": false,
        "HotspareType": null,
        "Id": "HDDPlaneDisk00080011",
        "Location": [
            {
                "Info": "Disk1",
                "InfoFormat": "DeviceName"
            }
        ],
        "Manufacturer": "SEAGATE",
        "MediaType": "HDD",
        "Model": "ST1200MM0129",
        "Name": "Disk00080011",
        "NegotiatedSpeedGbs": 12,
        "Oem": {
            "Public": {
                "DiskLocater": "Pcie Slot4 : EID14 : Slot0",
                "SATAPort": null,
                "mediaErrCount": 0,
                "otherErrCount": 0,
                "prefailErrCount": 0,
            }
        },
        "PredictedMediaLifeLeftPercent": null,
        "Protocol": "SAS",
        "Revision": "C003",
        "RotationSpeedRPM": null,
        "SerialNumber": "WFK05GR9",
        "PartNumber": null,
        "SlotNumber": 0,
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        }
```

```
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk00080012",
        "@odata.type": "Drive.v1_1_0.Drive",
        "CapableSpeedGbs": 6,
        "CapacityBytes": 966367641600,
        "FailurePredicted": false,
        "HotspareType": null,
        "Id": "HDDPlaneDisk00080012",
        "Location": [
            {
                "Info": "Disk5",
                "InfoFormat": "DeviceName"
            }
        ],
        "Manufacturer": "SEAGATE",
        "MediaType": "HDD",
        "Model": "ST900MM0006",
        "Name": "Disk00080012",
        "NegotiatedSpeedGbs": 6,
        "Oem": {
            "Public": {
                "DiskLocater": "Pcie Slot4 : EID14 : Slot1",
                "SATAPort": null,
                "mediaErrCount": 0,
                "otherErrCount": 0,
                "prefailErrCount": 0,
            }
        },
        "PredictedMediaLifeLeftPercent": null,
        "Protocol": "SAS",
        "Revision": "0003",
        "RotationSpeedRPM": null,
        "SerialNumber": "S0N48CEZ",
        "PartNumber": null,
        "SlotNumber": 1,
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        }
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk03010007",
        "@odata.type": "Drive.v1_1_0.Drive",
```

```
            "CapableSpeedGbs": 8,
            "CapacityBytes": 1717986918400,
            "FailurePredicted": true,
            "HotspareType": null,
            "Id": "HDDPlaneDisk03010007",
            "Location": [
                {
                    "Info": " Disk7",
                    "InfoFormat": "DeviceName"
                }
            ],
            "Manufacturer": "HGST",
            "MediaType": "SSD",
            "Model": "HUSMR7616BHP301",
            "Name": "Disk03010007",
            "NegotiatedSpeedGbs": 8,
            "Oem": {
                "Public": {
                    "DiskLocater": "Pcie Slot4 : EID14 : Slot2",
                    "SATAPort": null,
                    "mediaErrCount": 0,
                    "otherErrCount": 0,
                    "prefailErrCount": 0,
                }
            },
            "PredictedMediaLifeLeftPercent": 94,
            "Protocol": "PCIE",
            "Revision": null,
            "RotationSpeedRPM": null,
            "SerialNumber": "SDM000004528B",
            "PartNumber": null,
            "SlotNumber": 2,
            "Status": {
                "Health": null,
                "State": "Enabled"
            }
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk05008d00",
            "@odata.type": "Drive.v1_1_0.Drive",
            "CapableSpeedGbs": 6,
            "CapacityBytes": 4000000000000,
            "FailurePredicted": false,
            "HotspareType": null,
```

```
            "Id": "HDDPlaneDisk05008d00",
            "Location": [
                {
                    "Info": "Disk60",
                    "InfoFormat": "DeviceName"
                }
            ],
            "Manufacturer": null,
            "MediaType": "HDD",
            "Model": "ST4000NM0035-1V4107",
            "Name": "Disk05008d00",
            "NegotiatedSpeedGbs": 6,
            "Oem": {
                "Public": {
                    "SATAPort": {
                        "BelongCPU": "CPU1",
                        "ControllerBDF": "0000:00:11.5",
                        "ControllerPortNum": 0
                    }
                }
            },
            "PartNumber": null,
            "PredictedMediaLifeLeftPercent": null,
            "Protocol": "SATA",
            "Revision": "TN04",
            "RotationSpeedRPM": 7200,
            "SerialNumber": "ZC197F2W",
            "SlotNumber": 60,
            "Status": {
                "Health": null,
                "State": null
            }
        }
    ],
    "Members@odata.count": 4,
    "Name": "Drivers Collection"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about all drive resources, refer to Table 6-32.

Table 6-32 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 node.
@odata.type	String	Type of 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. For the requirements for the parameters, refer to 6.5 Querying Information About a Specified Network Adapter Resource.

6.17 Querying Information About a Specified Chassis Power Supply

Function

Query information about a specified Chassis power supply.

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

Description

For a description of the parameters for querying information about the specified chassis power supply, refer to Table 6-33.

Table 6-33 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**.

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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Power
```

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#Power.Power",
    "@odata.etag": "W/\"1274418368\"",
    "@odata.id": "/redfish/v1/Chassis/1/Power",
    "@odata.type": "#Power.v1_5_0.Power",
    "Actions": {
        "Oem": {
            "Public": {
                "#Power.CollectHistoryData": {
                    "target": "/redfish/v1/Chassis/1/Power/Actions/
                    Power.CollectHistoryData"
                }
            }
       }
    },
    "Id": "Power",
    "Name": "Power",
    "Oem": {
        "Public": {
            "Maximum": 1,
            "OverallHealth": "OK"
        }
    },
    "PowerControl": [
        {
```

```
        "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerControl/1",
        "MemberId": "1",
        "Name": "Chassis Power Control",
        "Oem": {
            "Public": {
                "ExpectedActivePSU": [
                    {
                        "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/1"
                    }
                ]
            }
        },
        "PowerConsumedWatts": 175,
        "PowerLimit": {
            "LimitException": "NoAction",
            "LimitInWatts": 2000,
            "PowerLimitEnable": true
        }
    }
],
"PowerSupplies": [
    {
        "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/1",
        "FirmwareVersion": "00",
        "LineInputVoltage": 223,
        "Manufacturer": "Great Wall",
        "MemberId": "2",
        "Model": "CRPS1200D ",
        "Name": "Power Supply Bay2",
        "Oem": {
            "Public": {
                "ActiveStandby": "Active",
                "InletTemperatureCelsius": 28,
                "InputAmperage": 0,
                "LineInputCurrent": 0,
                "Location": "Chassis",
                "OutputAmperage": 0,
                "OutputVoltage": 0,
                "PartNumber": null,
                "Protocol": "PMBus",
                "SlotNumber": 1
            }
        },
        "PowerCapacityWatts": 1200,
```

```
            "PowerInputWatts": 127,
            "PowerOutputWatts": 131,
            "PowerSupplyType": "AC",
            "ProductionDate": "191209",
            "SerialNumber": "22I120011920",
            "Status": {
                "Health": "OK",
                "State": "Enabled"
            }
        },{
            "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/2",
            "FirmwareVersion": null,
            "LineInputVoltage": null,
            "Manufacturer": null,
            "MemberId": "2",
            "Model": null,
            "Name": "Power Supply Bay2",
            "Oem": {
                "Public": {
                    "ActiveStandby": null,
                    "InletTemperatureCelsius": null,
                    "InputAmperage": null,
                    "LineInputCurrent": null,
                    "Location": "Chassis",
                    "OutputAmperage": null,
                    "OutputVoltage": null,
                    "PartNumber": null,
                    "Protocol": null,
                    "SlotNumber": 2
                }
            },
            "PowerCapacityWatts": null,
            "PowerInputWatts": null,
            "PowerOutputWatts": null,
            "PowerSupplyType": null,
            "ProductionDate": null,
            "SerialNumber": null,
            "Status": {
                "Health": null,
                "State": "Absent"
            }
        }
    ],
    "PowerSupplies@odata.count": 2,
```

```
"Redundancy": [
    {
        "@odata.id": "/redfish/v1/Chassis/1/Power#/Redundancy/1",
        "Mode": "String",
        "Name": "PowerSupply Redundancy Group 1"
    }
],
"Voltages": [
    {
        "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/5",
        "LowerThresholdCritical": 1.359,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 2.423,
        "MinReadingRange": 0,
        "Name": "CPU1 VCore",
        "ReadingVolts": 1.815,
        "SensorNumber": 5,
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        },
        "UpperThresholdCritical": 2.157,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/11",
        "LowerThresholdCritical": 1.359,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 2.423,
        "MinReadingRange": 0,
        "Name": "CPU2 VCore",
        "ReadingVolts": 1.729,
        "SensorNumber": 11,
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        },
        "UpperThresholdCritical": 2.157,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    },
```

```
        {
            "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/66",
            "LowerThresholdCritical": 0,
            "LowerThresholdFatal": 0,
            "LowerThresholdNonCritical": 0,
            "MaxReadingRange": 255,
            "MinReadingRange": 0,
            "Name": "SYS 12V_1",
            "ReadingVolts": 12,
            "SensorNumber": 66,
            "Status": {
                "Health": "OK",
                "State": "Enabled"
            },
            "UpperThresholdCritical": 0,
            "UpperThresholdFatal": 0,
            "UpperThresholdNonCritical": 0
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/67",
            "LowerThresholdCritical": 0,
            "LowerThresholdFatal": 0,
            "LowerThresholdNonCritical": 0,
            "MaxReadingRange": 255,
            "MinReadingRange": 0,
            "Name": "SYS 12V_2",
            "ReadingVolts": 12,
            "SensorNumber": 67,
            "Status": {
                "Health": "OK",
                "State": "Enabled"
            },
            "UpperThresholdCritical": 0,
            "UpperThresholdFatal": 0,
            "UpperThresholdNonCritical": 0
        }
    ]
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified chassis power supply, refer to Table 6-34.

Table 6-34 Output Descriptions for Querying Information About the Specified Chassis 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 node.
@odata.type	String	Type of power supply resource.
Id	String	ID of the power supply resource.
Name	String	Name of the power supply resource.
Maximum	Number	Maximum number of power supplies.
OverallHealth	Character string	Health status of all power supplies.
PowerControl	Array	Power control list.
@odata.id	String	Access path of the specified power control node.
MemberId	String	ID of the specified power control. The ID is the unique identifier of the power control in the power control list.
Name	String	Name of the specified power control.
Oem.Public	Object	Customized properties.
ExpectedActivePSU	Object	Active power supply list.
PowerConsumedWatts	Number	Current power of the device.
PowerLimit	Object	Power capping information.
LimitInWatts	● Number ● null	Server power limit: ● Value: Power capping is enabled. The value indicates the currently valid configuration value. ● null: Power capping is disabled.
LimitException	String	Action to be taken when power capping becomes invalid. Value: NoAction (no action).
PowerSupplies@odata.count	Number	Number of power supplies.
PowerSupplies	Array	Power module list.
Oem.Public	Object	Customized properties.
ActiveStandby	String	Active or standby power supply mode. ● Active: active mode. ● Standby: standby mode.

Field	Type	Description
SlotNumber	Number	Slot number of the specified power supply.
InletTemperatureCelsius	Number	Inlet temperature of the power supply.
Location	Character string	Location of the power supply, which is fixed to *Chassis*.
PartNumber	Character string	Part number of the power supply, which is fixed to *null*.
Protocol	Character string	Protocol, which is fixed to *PMBus*.
InputAmperage	Number	Input current of the specified power supply.
OutputVoltage	Number	Output voltage of the specified power supply.
OutputAmperage	Number	Output current of the specified power supply.
@odata.id	String	Access path of a specified power supply node.
MemberId	String	ID of the specified power supply. The ID is the unique identifier of the power supply in the power supply list.
Name	String	Name of the specified power supply.
PowerSupplyType	String	Type of the specified power supply.
LineInputVoltage	Number	Input voltage of the specified power supply.
PowerCapacityWatts	Number	Rated power of the specified power supply.
PowerInputWatts	Number	Input power of the specified power supply.
PowerOutputWatts	Number	Output power of the specified power supply.
Manufacturer	String	Manufacturer of the specified power supply.
Model	String	Model of the specified power supply.
FirmwareVersion	String	Firmware version of the specified power supply.
ProductionDate	Number	Power supply manufacture date
SerialNumber	String	Serial number of the specified power supply.
Status	Object	PowerSupplies status. Options: ● State: enabling status of the power supply. ● Health: health status of the power supply.
Redundancy	Array	Power redundancy group list.
@odata.id	String	Access path of a specified power redundancy group node.
Name	String	Name of the specified power redundancy group.

Field	Type	Description
Mode	String	Redundancy mode of the specified power redundancy group. ● Sharing: load balancing mode. ● Failover: active-standby mode.
Voltages	Array	Voltage sensor list.
@odata.id	String	Access path of the specified voltage sensor node.
Name	String	Name of the specified voltage sensor.
SensorNumber	Number	Serial number of the specified voltage sensor.
Status	Object	Status of the specified voltage sensor, including: ● State: enabling status of the voltage sensor. ● Health: health status of the voltage sensor.
ReadingVolts	Number	Current reading of the specified voltage sensor.
UpperThresholdNonCritical	Number	Non-critical warning threshold for high voltage of the specified voltage sensor.
UpperThresholdCritical	Number	Critical warning threshold for high voltage of the specified voltage sensor.
UpperThresholdFatal	Number	Fatal warning threshold for high voltage of the specified voltage sensor.
LowerThresholdNonCritical	Number	Non-critical warning threshold for low voltage of the specified voltage sensor.
LowerThresholdCritical	Number	Critical warning threshold for low voltage of the specified voltage sensor.
LowerThresholdFatal	Number	Fatal warning threshold for low voltage of the specified voltage sensor.
MinReadingRange	Number	Minimum voltage reading for the specified voltage sensor.
MaxReadingRange	Number	Maximum voltage reading for the specified voltage sensor.
PowerLimitEnable	Boolean	Whether power capping is enabled: ● true: power capping enabled ● False: power capping disabled

6.18 Modifying Properties of a Specified Power Supply

Function

Modify properties of a specified power supply of a server.

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": [
        {
            "Oem": {
                "Public": {
                    "ExpectedActivePSU": [
                 {
                  "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/power_id"
                  }
                 ]
                }
            }
```

```
        }
    ]
}
```

Description

For a description of the parameters for modifying properties of the specified power supply, refer to Table 6-35.

Table 6-35 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 */redfish/v1/SessionService/Sessions*.
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	Power supply slot ID.	Range: 1–4. Set it based on the number of power supplies of a specified model.
redundancy_type	Power redundancy type.	• 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:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
Content-Type: application/json
```

- Request Message Body 1:

```
{
    "PowerControl":
    [{
        "PowerLimit":
        {
            "LimitInWatts": 700
        }
    }]
}
```

- Request Message Body 2:

```
{"Redundancy": [{"Mode": "Failover"}],
 "PowerControl": [{
  "Oem": {
    "Public": {
     "ExpectedActivePSU": [
      {"@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/1"}
      ]
     }
   }
 }]
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#Power.Power",
    "@odata.etag": "W/\"1604736687\"",
    "@odata.id": "/redfish/v1/Chassis/1/Power",
    "@odata.type": "#Power.v1_5_0.Power",
    "Id": "Power",
    "Name": "Power",
    "PowerControl": [
        {
            "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerControl/1",
            "MemberId": "1",
            "Name": "Chassis Power Control",
            "Oem": {
                "Public": {
                    "ExpectedActivePSU": [
                        {
                            "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/1"
                        }
                    ]
                }
```

```
        },
        "PowerConsumedWatts": 335,
        "PowerLimit": {
            "LimitException": "NoAction",
            "LimitInWatts": 700,
            "PowerLimitEnable": true
        }
    }
],
"PowerSupplies": [
    {
        "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/2",
        "FirmwareVersion": "00",
        "LineInputVoltage": 225,
        "Manufacturer": "Great Wall",
        "MemberId": "2",
        "Model": "CRPS1200D ",
        "Name": "Power Supply Bay2",
        "Oem": {
            "Public": {
                "ActiveStandby": "Active",
                "InletTemperatureCelsius": 34,
                "SlotNumber": 2
            }
        },
        "PowerCapacityWatts": 1200,
        "PowerSupplyType": "AC",
        "SerialNumber": "22I120011920",
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        }
    }
],
"PowerSupplies@odata.count": 1,
"Redundancy": [
    {
        "@odata.id": "/redfish/v1/Chassis/1/Power#/Redundancy/1",
        "Mode": "Failover",
        "Name": "PowerSupply Redundancy Group 1"
    }
],
"Voltages": [
    {
```

```
            "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/15",
            "LowerThresholdCritical": 1.889,
            "LowerThresholdFatal": 0,
            "LowerThresholdNonCritical": 0,
            "MaxReadingRange": 3.621,
            "MinReadingRange": 0,
            "Name": "CPU1 VCore",
            "ReadingVolts": 1.789,
            "SensorNumber": 15,
            "Status": {
                "Health": "Warning",
                "State": "Enabled"
            },
            "UpperThresholdCritical": 2.158,
            "UpperThresholdFatal": 0,
            "UpperThresholdNonCritical": 0
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/16",
            "LowerThresholdCritical": 1.363,
            "LowerThresholdFatal": 0,
            "LowerThresholdNonCritical": 0,
            "MaxReadingRange": 3.621,
            "MinReadingRange": 0,
            "Name": "CPU2 VCore",
            "ReadingVolts": 1.775,
            "SensorNumber": 16,
            "Status": {
                "Health": "OK",
                "State": "Enabled"
            },
            "UpperThresholdCritical": 2.158,
            "UpperThresholdFatal": 0,
            "UpperThresholdNonCritical": 0
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/57",
            "LowerThresholdCritical": 0,
            "LowerThresholdFatal": 0,
            "LowerThresholdNonCritical": 0,
            "MaxReadingRange": 255,
            "MinReadingRange": 0,
            "Name": "SYS 12V_1",
            "ReadingVolts": 0,
```

```
            "SensorNumber": 57,
            "Status": {
                "Health": null,
                "State": "Disabled"
            },
            "UpperThresholdCritical": 0,
            "UpperThresholdFatal": 0,
            "UpperThresholdNonCritical": 0
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/58",
            "LowerThresholdCritical": 0,
            "LowerThresholdFatal": 0,
            "LowerThresholdNonCritical": 0,
            "MaxReadingRange": 255,
            "MinReadingRange": 0,
            "Name": "SYS 12V_2",
            "ReadingVolts": 12,
            "SensorNumber": 58,
            "Status": {
                "Health": "OK",
                "State": "Enabled"
            },
            "UpperThresholdCritical": 0,
            "UpperThresholdFatal": 0,
            "UpperThresholdNonCritical": 0
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/59",
            "LowerThresholdCritical": 1.404,
            "LowerThresholdFatal": 0,
            "LowerThresholdNonCritical": 0,
            "MaxReadingRange": 3.06,
            "MinReadingRange": 0,
            "Name": "CPU1 VCore",
            "ReadingVolts": 1.764,
            "SensorNumber": 59,
            "Status": {
                "Health": "OK",
                "State": "Enabled"
            },
            "UpperThresholdCritical": 2.004,
            "UpperThresholdFatal": 0,
            "UpperThresholdNonCritical": 0
```

```
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/60",
            "LowerThresholdCritical": 1.404,
            "LowerThresholdFatal": 0,
            "LowerThresholdNonCritical": 0,
            "MaxReadingRange": 3.06,
            "MinReadingRange": 0,
            "Name": "CPU2 VCore",
            "ReadingVolts": 1.764,
            "SensorNumber": 60,
            "Status": {
                "Health": "OK",
                "State": "Enabled"
            },
            "UpperThresholdCritical": 2.004,
            "UpperThresholdFatal": 0,
            "UpperThresholdNonCritical": 0
        }
    ]
}
```


- Status Code: 200

Output Description

For a description of the output returned when you modify properties of the specified power supply, refer to Table 6-36.

Table 6-36 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 node.
@odata.type	String	Type of power supply resource.
Id	String	ID of the power supply resource.
Name	String	Name of the power supply resource.
Maximum	Number	Maximum number of power supplies.
OverallHealth	Character string	Health status of all power supplies.
PowerControl	Array	Power control list.
@odata.id	String	Access path of the specified power control node.

Field	Type	Description
MemberId	String	ID of the specified power control. The ID is the unique identifier of the power control in the power control list.
Name	String	Name of the specified power control.
PowerConsumedWatts	Number	Current power of the device.
PowerLimit	Object	Power capping information.
LimitInWatts	Number	Server power limit: ● Value: Power capping is enabled. The value indicates the currently valid configuration value. ● null: Power capping is disabled.
LimitException	String	Action to be taken when power capping becomes invalid. Value: NoAction (no action).
PowerSupplies@odata.count	Number	Number of power supplies.
PowerSupplies	Array	Power module list.
Oem.Public	Object	Customized properties.
ActiveStandby	Character string	Active or standby power supply mode. ● Active: active mode. ● Standby: standby mode.
SlotNumber	Number	Slot number of the specified power supply.
InletTemperatureCelsius	Number	Air inlet temperature of the specified power supply.
Location	Character string	Location of the power supply, which is fixed to *Chassis*.
PartNumber	Character string	Part number of the power supply, which is fixed to *null*.
Protocol	Character string	Protocol, which is fixed to *PMBus*.
InputAmperage	Number	Input current of the specified power supply.
OutputVoltage	Number	Output voltage of the specified power supply.
OutputAmperage	Number	Output current of the specified power supply.
@odata.id	String	Access path of a specified power supply node.
MemberId	String	ID of the specified power supply. The ID is the unique identifier of the power supply in the power supply list.
Name	String	Name of the specified power supply.
PowerSupplyType	String	Type of the specified power supply:

Field	Type	Description
		● AC ● HVDC ● LVDC ● null: input error
LineInputVoltage	Number	Input voltage of the specified power supply.
PowerCapacityWatts	Number	Rated power of the specified power supply.
Manufacturer	String	Manufacturer of the specified power supply.
Model	String	Model of the specified power supply.
FirmwareVersion	String	Firmware version of the specified power supply.
SerialNumber	String	Serial number of the specified power supply.
Status	Object	Power supply status.
Redundancy	List	Power redundancy group list.
@odata.id	String	Access path of a specified power redundancy group node.
Name	String	Name of the specified power redundancy group.
Mode	String	Redundancy mode of the specified power redundancy group: ● Sharing: load balancing mode. ● Failover: active-standby mode.
Voltages	List	Voltage sensor list.
@odata.id	String	Access path of the specified voltage sensor node.
Name	String	Name of the specified voltage sensor.
SensorNumber	Number	Serial number of the specified voltage sensor.
Status	Object	Status of the specified voltage sensor.
ReadingVolts	Number	Current reading of the specified voltage sensor.
UpperThresholdNonCritical	Number	Non-critical warning threshold for high voltage of the specified voltage sensor.
UpperThresholdCritical	Number	Critical warning threshold for high voltage of the specified voltage sensor.
UpperThresholdFatal	Number	Fatal warning threshold for high voltage of the specified voltage sensor.
LowerThresholdNonCritical	Number	Non-critical warning threshold for low voltage of the specified voltage sensor.

Field	Type	Description
LowerThresholdCritical	Number	Critical warning threshold for low voltage of the specified voltage sensor.
LowerThresholdFatal	Number	Fatal warning threshold for low voltage of the specified voltage sensor.
MinReadingRange	Number	Minimum voltage reading for the specified voltage sensor.
MaxReadingRange	Number	Maximum voltage reading for the specified voltage sensor.
PowerLimitEnable	Boolean	Whether power capping is enabled: ● true: power capping enabled ● False: power capping disabled

6.19 Querying the Cooling Resource Information About a Specified Chassis

Function

Query the temperature and fan sensor information about a specified Chassis.

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 6-37.

Table 6-37 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.

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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Thermal
```

- Request Header:

```
x-auth-token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:


```
{
    "@odata.context": "/redfish/v1/$metadata#Thermal.Thermal",
    "@odata.etag": "W/\"1600242810\"",
    "@odata.id": "/redfish/v1/Chassis/1/Thermal",
    "@odata.type": "#Thermal.v1_4_0.Thermal",
    "FanSummary": {"count": 8},
    "Fans":
    [{
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/46",
        "FanName": "FAN_SPEED_01",
        "LowerThresholdCritical": 800,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 8360,
        "MemberId": "1",
        "MinReadingRange": 800,
        "Oem":
        {
            "Public": { "SlotNumber": 1,"SpeedRatio": 59}
        },
        "Reading": 4966,
        "ReadingUnits": "RPM",
        "SerialNumber": "20150305",
        "Status": {"Health": "OK", "State": "Enabled"},
        "UpperThresholdCritical": 0,
```

```
    "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
},
{
    "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/47",
    "FanName": "FAN_SPEED_02",
    "LowerThresholdCritical": 800,
    "LowerThresholdFatal": 0,
    "LowerThresholdNonCritical": 0,
    "MaxReadingRange": 8360,
    "MemberId": "2",
    "MinReadingRange": 800,
    "Oem":
    {
        "Public": { "SlotNumber": 2,"SpeedRatio": 59}
    },
    "Reading": 5335,
    "ReadingUnits": "RPM",
    "SerialNumber": "20150305",
    "Status": {"Health": "OK", "State": "Enabled"},
    "UpperThresholdCritical": 0,
    "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
},
{
    "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/48",
    "FanName": "FAN_SPEED_03",
    "LowerThresholdCritical": 800,
    "LowerThresholdFatal": 0,
    "LowerThresholdNonCritical": 0,
    "MaxReadingRange": 8360,
    "MemberId": "3",
    "MinReadingRange": 800,
    "Oem":
    {
        "Public": { "SlotNumber": 3,"SpeedRatio": 59}
    },
    "Reading": 5429,
    "ReadingUnits": "RPM",
    "SerialNumber": "20150305",
    "Status": {"Health": "OK", "State": "Enabled"},
    "UpperThresholdCritical": 0,
    "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
```

```
},
{
    "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/49",
    "FanName": "FAN_SPEED_04",
    "LowerThresholdCritical": 800,
    "LowerThresholdFatal": 0,
    "LowerThresholdNonCritical": 0,
    "MaxReadingRange": 8360,
    "MemberId": "4",
    "MinReadingRange": 800,
    "Oem":
    {
        "Public": { "SlotNumber": 4,"SpeedRatio": 59}
    },
    "Reading": 5000,
    "ReadingUnits": "RPM",
    "SerialNumber": "20150305",
    "Status": {"Health": "OK", "State": "Enabled"},
    "UpperThresholdCritical": 0,
    "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
},
{
    "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/50",
    "FanName": "FAN_SPEED_05",
    "LowerThresholdCritical": 800,
    "LowerThresholdFatal": 0,
    "LowerThresholdNonCritical": 0,
    "MaxReadingRange": 8360,
    "MemberId": "5",
    "MinReadingRange": 800,
    "Oem":
    {
        "Public": { "SlotNumber": 5,"SpeedRatio": 59}
    },
    "Reading": 5326,
    "ReadingUnits": "RPM",
    "SerialNumber": "20150305",
    "Status": {"Health": "OK", "State": "Enabled"},
    "UpperThresholdCritical": 0,
    "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
},
{
```

```
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/51",
        "FanName": "FAN_SPEED_06",
        "LowerThresholdCritical": 800,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 8360,
        "MemberId": "6",
        "MinReadingRange": 800,
        "Oem":
        {
            "Public": { "SlotNumber": 6,"SpeedRatio": 59}
        },
        "Reading": 4707,
        "ReadingUnits": "RPM",
        "SerialNumber": "20150305",
        "Status": {"Health": "OK", "State": "Enabled"},
        "UpperThresholdCritical": 0,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/52",
        "FanName": "FAN_SPEED_07",
        "LowerThresholdCritical": 800,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 8360,
        "MemberId": "7",
        "MinReadingRange": 800,
        "Oem":
        {
            "Public": { "SlotNumber": 7,"SpeedRatio": 59}
        },
        "Reading": 5218,
        "ReadingUnits": "RPM",
        "SerialNumber": "20150305",
        "Status": {"Health": "OK", "State": "Enabled"},
        "UpperThresholdCritical": 0,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/53",
        "FanName": "FAN_SPEED_08",
```

```
        "LowerThresholdCritical": 800,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 8360,
        "MemberId": "8",
        "MinReadingRange": 800,
        "Oem":
        {
            "Public": { "SlotNumber": 8,"SpeedRatio": 59}
        },
        "Reading": 4785,
        "ReadingUnits": "RPM",
        "SerialNumber": "20150305",
        "Status": {"Health": "OK", "State": "Enabled"},
        "UpperThresholdCritical": 0,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    }],
    "Id": "Thermal",
    "Name": "Thermal",
    "Oem":
    {
        "Public":
        {
            "FanSmartCoolingMode": "NormalMode",
            "FanSpeedAdjustmentMode": "Automatic",
            "SpeedRatio": 59
        }
    },
    "Temperatures":
    [{
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/17",
        "LowerThresholdCritical": 0,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRangeTemp": 117,
        "MinReadingRangeTemp": -138,
        "Name": "INPUT_TEMP",
        "PhysicalContext": "Room",
        "ReadingCelsius": 23,
        "SensorNumber": 17,
        "Status": {"Health": "OK", "State": "Enabled"},
        "UpperThresholdCritical": 45,
        "UpperThresholdFatal": 50,
```

```
        "UpperThresholdNonCritical": 38
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/24",
        "LowerThresholdCritical": 0,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRangeTemp": 127,
        "MinReadingRangeTemp": -128,
        "Name": "CPU1_TEMP",
        "PhysicalContext": "Room",
        "ReadingCelsius": 61,
        "SensorNumber": 24,
        "Status": {"Health": "OK", "State": "Enabled"},
        "UpperThresholdCritical": 100,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    }]
}
```


- 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 6-38.

Table 6-38 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 model.
@odata.id	String	Access path of the cooling resource.
@odata.type	String	Type of cooling resource.
Oem.Public	Object	Customized information about the cooling resource.
FanSpeedAdjustmentMode	String	Fan speed adjustment mode, including: ● Automatic mode: automatic ● Manual mode: manual
FanSmartCoolingMode	String	Fan speed smart adjustment mode, including: ● NormalMode: balance mode ● LowNoiseMode: low noise mode ● HighPerformanceMode: high-performance mode
SpeedRatio	Number	Fan rotation speed ratio in percentage.

Field	Type	Description
Count	Number	Number of fan sensors.
FanSummary	Object	Information about the specified fan sensors.
Count	Number	Number of fan sensors.
Fans	Object array	Fan sensor list.
@odata.id	String	Access path of the specified fan sensor.
FanName	String	Name of the specified fan sensor.
Status	Object	Status of the specified fan sensor, including: ● State: enabling status of the fan sensors ● Health: health status of the fan sensors
SerialNumber	String	Fan serial number.
LowerThresholdCritical	Number	Critical warning threshold for low rotational speed of the specified fan sensor.
LowerThresholdFatal	Number	Fatal warning threshold for low rotational speed of the specified fan sensor.
LowerThresholdNonCritical	Number	Non-critical warning threshold for low rotational speed of the specified fan sensor.
UpperThresholdCritical	Number	Critical warning threshold for high rotational speed of the specified fan sensor.
UpperThresholdFatal	Number	Fatal warning threshold for high rotational speed of the specified fan sensor.
UpperThresholdNonCritical	Number	Non-critical warning threshold for high rotational speed of the specified fan sensor.
MaxReadingRange	Number	Maximum rotation speed that can be read by the specified fan sensor.
MemberId	String	ID of the specified fan sensor.
MinReadingRange	Number	Minimum rotation speed that can be read by the specified fan sensor.
Reading	Number	Current reading of the specified fan sensor.
ReadingUnits	String	Unit of the fan rotation speed read by the fan sensor, including: ● RPM ● Percent
Oem.Public	Object	-

Field	Type	Description
-SlotNumber	Number	Slot number of the specified fan sensor.
SpeedRatio	Number	Current reading of the specified fan sensor, in percentage.
Temperatures	Object array	Temperature sensor list.
@odata.id	String	Access path of a specified temperature sensor.
LowerThresholdCritical	Number	Critical warning threshold for low temperature of the specified temperature sensor.
LowerThresholdFatal	Number	Fatal warning threshold for low temperature of the specified temperature sensor.
LowerThresholdNonCritical	Number	Non-critical warning threshold for low temperature of the specified temperature sensor.
UpperThresholdCritical	Number	Critical warning threshold for high temperature of the specified temperature sensor.
UpperThresholdFatal	Number	Fatal warning threshold for high temperature of the specified temperature sensor.
UpperThresholdNonCritical	Number	Non-critical warning threshold for high temperature of the specified temperature sensor.
MaxReadingRangeTemp	Number	Maximum temperature that can be read by the specified temperature sensor.
MinReadingRangeTemp	Number	Minimum temperature that can be read by the specified temperature sensor.
Name	String	Name of the specified temperature sensor.
PhysicalContext	String	Area or device used for temperature measurement.
ReadingCelsius	Number	Current reading of the specified temperature sensor.
SensorNumber	Number	Serial number of the specified temperature sensor.
Status	Object	Status of the specified fan sensor, including: ● State: enabling status of the fan sensor ● Health: health status of the fan sensor

6.20 Modifying the Cooling Resource Information About a Specified Chassis

Function

Modify the cooling resource information about a specified Chassis of a server.

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": model_value,
            "FanSmartCoolingMode": smart_cool_mode_value,
            "SpeedRatio": speed_ratio_value
        }
    }
}
```

Parameters

For a description of the parameters for modifying cooling resource information about a specified Chassis, refer to Table 6-39.

Table 6-39 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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
model_value	Fan speed adjustment mode. This field is required.	• Automatic mode: automatic • Manual mode: manual
smart_cool_mode_value	Fan speed smart adjustment mode. If **model_value** is set to **Automatic**, this field is required.	• NormalMode: balance mode • LowNoiseMode: low noise mode • HighPerformanceMode: High-performance mode.

Parameter	Description	Value
speed_ratio_value	Fan rotation speed ratio in percentage. If **model_value** is set to **Manual**, this field is required.	10–100

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Chassis/1/Thermal
```

- Request Header:

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

- Request Message Body:

```
{
    "Oem":
    {
        "Public":
        {
            "FanSpeedAdjustmentMode": "Automatic",
            "FanSmartCoolingMode": "LowNoiseMode",
            "SpeedRatio": 50
        }
    }
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#Thermal.Thermal",
    "@odata.etag": "W/\"1593018925\"",
    "@odata.id": "/redfish/v1/Chassis/1/Thermal",
    "@odata.type": "#Thermal.v1_4_0.Thermal",
    "Oem":
    {
        "Public":
        {
            "FanSpeedAdjustmentMode": "Automatic",
            "FanSmartCoolingMode": "LowNoise",
            "SpeedRatio": 50
```

```
        }
    },
    "FanSummary": {
        "count": 6
    },
    "Fans":
    [{
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/51",
        "Name": "FAN_SPEED_01",
        "LowerThresholdCritical": 500,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 11000,
        "MemberId": "1",
        "MinReadingRange": 500,
        "Oem":
        {
            "Public": {
                "SlotNumber": 1,
                "SpeedRatio": 50
            }
        },
        "Reading": 0,
        "ReadingUnits": "RPM",
        "SerialNumber": "20150305",
        "Status": {"Health": null, "State": "Disabled"},
        "UpperThresholdCritical": 0,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/52",
        "Name": "FAN_SPEED_02",
        "LowerThresholdCritical": 500,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 11000,
        "MemberId": "2",
        "MinReadingRange": 500,
        "Oem": {
            "Public": {
                "SlotNumber": 2,
                "SpeedRatio": 50
            }
```

```
        },
        "Reading": 0,
        "ReadingUnits": "RPM",
        "SerialNumber": "20150305",
        "Status": {"Health": null, "State": "Disabled"},
        "UpperThresholdCritical": 0,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/53",
        "Name": "FAN_SPEED_03",
        "LowerThresholdCritical": 500,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 11000,
        "MemberId": "3",
        "MinReadingRange": 500,
        "Oem": {
            "Public": {
                 "SlotNumber": 3,
                "SpeedRatio": 50
            }
        },
        "Reading": 0,
        "ReadingUnits": "RPM",
        "SerialNumber": "20150305",
        "Status": {"Health": null, "State": "Disabled"},
        "UpperThresholdCritical": 0,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/54",
        "Name": "FAN_SPEED_04",
        "LowerThresholdCritical": 500,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 11000,
        "MemberId": "4",
        "MinReadingRange": 500,
        "Oem": {
            "Public": {
                "SlotNumber": 4,
```

```
            "SpeedRatio": 50
        }
    },
    "Reading": 0,
    "ReadingUnits": "RPM",
    "SerialNumber": "20150305",
    "Status": {"Health": null, "State": "Disabled"},
    "UpperThresholdCritical": 0,
    "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
},
{
    "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/55",
    "Name": "FAN_SPEED_05",
    "LowerThresholdCritical": 500,
    "LowerThresholdFatal": 0,
    "LowerThresholdNonCritical": 0,
    "MaxReadingRange": 11000,
    "MemberId": "5",
    "MinReadingRange": 500,
    "Oem": {
        "Public": {
            "SlotNumber": 5,
            "SpeedRatio": 50
        }
    },
    "Reading": 0,
    "ReadingUnits": "RPM",
    "SerialNumber": "20150305",
    "Status": {
        "Health": null,
        "State": "Disabled"
    },
    "UpperThresholdCritical": 0,
    "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
},
{
    "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/56",
    "FanName": "FAN_SPEED_06",
    "LowerThresholdCritical": 500,
    "LowerThresholdFatal": 0,
    "LowerThresholdNonCritical": 0,
    "MaxReadingRange": 11000,
```

```
        "MemberId": "6",
        "MinReadingRange": 500,
        "Oem": {
            "Public": {
                "SlotNumber": 6,
                "SpeedRatio": 50
            }
        },
        "Reading": 0,
        "ReadingUnits": "RPM",
        "SerialNumber": "20150305",
        "Status": {
            "Health": null,
            "State": "Disabled"
        },
        "UpperThresholdCritical": 0,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    }],
    "Id": "Thermal",
    "Name": "Thermal",
    "Temperatures":
    [{
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/17",
        "LowerThresholdCritical": 0,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRangeTemp": 126,
        "MinReadingRangeTemp": -129,
        "Name": "INPUT_TEMP",
        "PhysicalContext": "Room",
        "ReadingCelsius": 27,
        "SensorNumber": 17,
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        },
        "UpperThresholdCritical": 42,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/21",
        "LowerThresholdCritical": 0,
```

```
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRangeTemp": 127,
        "MinReadingRangeTemp": -128,
        "Name": "CPU1_TEMP",
        "ReadingCelsius": 0,
        "SensorNumber": 21,
        "Status": {
            "Health": null,
            "State": "Disabled"
        },
        "UpperThresholdCritical": 88,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    },
    {
        "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Temperatures/22",
        "LowerThresholdCritical": 0,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRangeTemp": 127,
        "MinReadingRangeTemp": -128,
        "Name": "CPU2_TEMP",
        "PhysicalContext": "Room",
        "ReadingCelsius": 0,
        "SensorNumber": 22,
        "Status": {
            "Health": null,
            "State": "Disabled"
        },
        "UpperThresholdCritical": 88,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    }]
}
```


- Status Code: 200

Output Description

For a description of the output returned when you modify the cooling resource information about the specified chassis, refer to Table 6-40.

Table 6-40 Output Descriptions for Modifying the Cooling Resource Information About a Specified Chassis

Field	Type	Description
@odata.context	String	OData description of the cooling resource model.
@odata.id	String	Access path of the cooling resource.
@odata.type	String	Type of cooling resource.
Oem.Public	Object	Customized information about the cooling resource.
FanSpeedAdjustmentMode	String	Fan speed adjustment mode, including: ● Automatic mode: automatic ● Manual mode: manual
FanSmartCoolingMode	String	Fan speed smart adjustment mode, including: ● Normal: balance mode ● LowNoise: low noise mode ● HighPerformance: high-performance mode
SpeedRatio	Number	Fan rotation speed ratio in percentage.
Count	Number	Number of fan sensors.
FanSummary	Object	Information about the specified fan sensor.
Fans	Object array	Fan sensor list.
@odata.id	String	Access path of the specified fan sensor.
FanName	String	Name of the specified fan sensor.
Status	Object	Status of the specified fan sensor, including: ● State: enabling status of the fan sensor ● Health: health status of the fan sensor
SerialNumber	String	Fan serial number.
LowerThresholdCritical	Number	Critical warning threshold for low rotational speed of the specified fan sensor.
LowerThresholdFatal	Number	Fatal warning threshold for low rotational speed of the specified fan sensor.
LowerThresholdNonCritical	Number	Non-critical warning threshold for low rotational speed of the specified fan sensor.
UpperThresholdCritical	Number	Critical warning threshold for high rotational speed of the specified fan sensor.
UpperThresholdFatal	Number	Fatal warning threshold for high rotational speed of the specified fan sensor.

Field	Type	Description
UpperThresholdNonCritical	Number	Non-critical warning threshold for high rotational speed of the specified fan sensor.
MaxReadingRange	Number	Maximum rotation speed that can be read by the specified fan sensor.
MemberId	String	ID of the specified fan sensor.
MinReadingRange	Number	Minimum rotation speed that can be read by the specified fan sensor.
Reading	Number	Current reading of the specified fan sensor.
ReadingUnits	String	Unit of the fan rotation speed read by the fan sensor, including: ● RPM ● Percent
Temperatures	Object array	Temperature sensor list.
@odata.id	String	Access path of a specified temperature sensor.
LowerThresholdCritical	Number	Critical warning threshold for low temperature of the specified temperature sensor.
LowerThresholdFatal	Number	Fatal warning threshold for low temperature of the specified temperature sensor.
LowerThresholdNonCritical	Number	Non-critical warning threshold for low temperature of the specified temperature sensor.
UpperThresholdCritical	Number	Critical warning threshold for high temperature of the specified temperature sensor.
UpperThresholdFatal	Number	Fatal warning threshold for high temperature of the specified temperature sensor.
UpperThresholdNonCritical	Number	Non-critical warning threshold for high temperature of the specified temperature sensor.
MaxReadingRangeTemp	Number	Maximum temperature that can be read by the specified temperature sensor.
MinReadingRangeTemp	Number	Minimum temperature that can be read by the specified temperature sensor.
Name	String	Name of the specified temperature sensor.
PhysicalContext	String	Area or device used for temperature measurement.
ReadingCelsius	Number	Current reading of the specified temperature sensor.
SensorNumber	Number	Serial number of the specified temperature sensor.

Field	Type	Description
Status	Object	Status of the specified fan sensor, including: ● State: enabling status of the fan sensor ● Health: health status of the fan sensor

6.21 Modifying the Status of a Specified Drive

Function

Modify the status of a specified drive.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/Chassis/chassis_id/Drives/drives_id*
- Request Header:

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

- Request Message Body:

→ Set health status.

```
{
    "Oem": {
        "Public": {
            "DriveState": State
        }
    }
}
```

→ Set the global hot spare drive

```
{
    "HotspareType":hotsparetype
}
```

→ Set the partial hot spare drive

```
{
    "HotspareType":hotsparetype,
    "Oem": {
        "Public": {
            "SpareforLogicalDrives": [
                {
                    "@odata.id": "/redfish/v1/Systems/1/Storages/RAIDStorage0004/
```

```
                    Volumes/Volume_id"
                }
            ]
        }
    }
}
```

Description

For a description of the parameters for modifying the status of a specified drive, refer to Table 6-41.

Table 6-41 Parameter Descriptions for Modifying the Status of a Specified Drive

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 */redfish/v1/SessionService/Sessions*.
drives_id	ID of the specified disk.	It can be obtained from the drive list managed by the current specified controllers
State	State	• Unconfigured Good: The physical disk is proper and can be used for RAID or hot spare disk configuration. • Unconfigured Bad: The physical disk is damaged or there is residual RAID information.
hotsparetype	Hot spare status of the drive.	• None: cancels hot spare status • Global: global hot spare configuration • Dedicated: partial hot spare configuration.
volume_id	Volume ID.	ID of the specified logical volume.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Chassis/chassis_id/Drives/drives_id
```

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0= Content-Type:application/json
```

- Request Message Body:

  → Set health status.

```
{
    Oem": {
        "Public": {
            "DriveState": "Unconfigured Good"
        }
    }
}
```

  → Set the global hot spare drive

```
{
    HotspareType":"Global"
}
```

  → Set the partial hot spare drive

```
{
    "HotspareType": "Dedicated",
    "Status": {
        "State": "Unconfigured Good"
    }
}
```

  → Cancel the global or partial hot spare configuration.

```
{
    "HotspareType":"None"
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#Drives.Drives",
    "@odata.etag": "W/\"1592997794\"",
    "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk00080011",
    "@odata.type": "#Drive.v1_1_0.Drive",
    "CapableSpeedGbs": 12,
    "CapacityBytes": 1288490188800,
    "FailurePredicted": false,
    "HotspareType": null,
    "Id": "HDDPlaneDisk00080011",
    "Location": [
        {
```

```
            "Info": "Disk1",
            "InfoFormat": "DeviceName"
        }
    ],
    "Manufacturer": "SEAGATE",
    "MediaType": "HDD",
    "Model": "ST1200MM0129",
    "Name": "Disk00080011",
    "NegotiatedSpeedGbs": 12,
    "PartNumber": null,
    "PredictedMediaLifeLeftPercent": null,
    "Protocol": "SAS",
    "Revision": "C003",
    "SerialNumber": "WFK05GR9",
    "SlotNumber": 0,
    "Status": {
        "Health": "OK",
        "State": "Unconfigured Good"
    }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you modify the status of a specified drive, refer to Table 6-42.

Table 6-42 Output Description for Modifying the Status of a Specified Drive

Field	Type	Description
@odata.context	String	OData description of the specified drive resource model.
@odata.id	String	Access path of the specified drive resource node.
@odata.type	String	Type of the specified drive resource.
Id	String	ID of the specified drive resource.
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:

Field	Type	Description
		● State: whether the drive is enabled. Options: Unconfigured Good and Unconfigured Bad. ● Health: health status of the drive
CapableSpeedGbs	Number	Maximum interface speed of the specified drive.
CapacityBytes	Number	Capacity of the specified drive, in bytes.
FailurePredicted	Boolean	Pre-failure status of the specified drive, including: ● true ● false
HotspareType	String	Hot-spare status of the specified drive, including: ● None: none ● Global:global hot-spare mode ● Dedicated: partial hot-spare mode
Protocol	Array	Compliant protocol of the specified drive: ● SPI ● PCIe ● AHCI ● UHCI ● SAS ● SATA ● USB ● NVMe ● FC ● iSCSI ● FCoE ● NVMeOverFabrics ● SMB ● NFSv3 ● NFSv4 ● HTTP ● HTTPS ● FTP ● SFTP
MediaType	String	Media type of the specified drive: ● HDD ● SSD ● SMR

Field	Type	Description
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.
Location	Array	Silk screen of the specified drive.
Info	String	Silk screen information about the specified drive.
InfoFormat	String	Silk screen format of the specified drive.

6.22 Querying the Information About the Optical Module Resources Connected to a Specified Network Port

Function

Query the information about the Optical module resources connected to the specified network port of a specified chassis of a server.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Chassis/Chassis_id/NetworkAdapters/networkadapteras_id/NetworkPorts/networkports_id/OpticalModule*
- Request Header:

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

- Request Message Body: None

Description

For a description of the parameters for querying the information about the optical module resources connected to the specified network port, refer to Table 6-43.

Table 6-43 Parameter Descriptions for Querying the Information About the Optical Module Resources Connected to the Specified 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 GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard3/NetworkPorts/1/OpticalModule
```

- Request Header:

```
X-Auth-Token:LXIrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=
```

- Request Message Body: None
- Response Example:


```
{
    "@odata.context": "/redfish/v1/$metadata#OpticalModule.OpticalModule",
    "@odata.etag": "W/\"1670005515\"",
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard7/
      NetworkPorts/1/OpticalModule",
    "@odata.type": "#OpticalModule.v1_0_0.OpticalModule",
    "Id": "OpticalModule",
    "Manufacturer": "Eoptolink",
    "Name": "OpticalModule",
    "PartNumber": "EOLQ-1HG-PCT-10",
    "ProductionDate": "2018-12-14",
    "RXPower": [
        {
            "LowerThresholdCritical": -10.3,
            "ReadingDBM": [
                0.94,
                1.03,
                0.96,
                0.98
             ],
            "UpperThresholdCritical": 2.4
        }
```

```
    ],
    "SerialNumber": "QJBG310001",
    "Status": {
        "State": "Enabled"
    },
    "BR_Nominal": 25500,
    "BiasCurrent": [
        {
            "LowerThresholdCritical": 1,
            "ReadingMilliAmperes": [
                5.94,
                5.96,
                5.97,
                5.98
            ],
            "UpperThresholdCritical": 12
        }
    ],
    "OutputPower": [
        {
            "LowerThresholdCritical": -8.4,
            "ReadingDBM": [
                1.21,
                0.94,
                1.07,
                1.05
            ],
            "UpperThresholdCritical": 2.4
        }
    ],
    "Temperature": {
        "LowerThresholdCritical": 0,
        "ReadingCelsius": 33.53,
        "UpperThresholdCritical": 70
    },
    "Voltage": {
        "LowerThresholdCritical": 3.13,
        "ReadingVolts": 3.32,
        "UpperThresholdCritical": 3.46
    },
    "WaveLengthNanometer": 850
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query the information about the Optical module resources connected to the specified network port, refer to Table 6-44.

Table 6-44 Output Descriptions for Querying the Information About the Optical Module Resources Connected to the Specified Network Port

Field	Type	Description
@odata.context	String	OData description of the optical module resource model.
@odata.id	String	Access path of the optical module resource node.
@odata.type	String	Type of optical module resource.
Id	String	ID of the optical module resource.
Name	String	Name of the optical module resource.
Status	Object	Status of the optical module. Options: ● Enabled ● Disabled
Manufacturer	String	Manufacturer of the optical module.
PartNumber	String	Component number of the optical module.
SerialNumber	String	Serial number of the optical module.
ProductionDate	String	Production date of the optical module.
WaveLengthNanometer	Number	Wavelength of the optical module.
BR_Nominal	Number	Speed supported by the optical module.
Voltage	Object	Voltage information about the optical module. Unit: V.
ReadingVolts	Number	Current voltage reading of the optical module. Unit: V.
LowerThresholdCritical	Number	Critical alarm threshold for too low voltage. Unit: V.
UpperThresholdCritical	Number	Critical alarm threshold for too high voltage.
RXPower	Object	Receiving power information about the optical module.
ReadingMilliWatts	Array	Current power reading of the optical module. Unit: dBm.

Field	Type	Description
LowerThresholdCritical	Number	Critical alarm threshold for too low receive power. Unit: dBm.
UpperThresholdCritical	Number	Critical alarm threshold for too high receive power. Unit: dBm.
OutputPower	Object	Sending power information about the optical module.
ReadingDBM	Array	Current transmit power reading of the optical module. Unit: dBm.
LowerThresholdCritical	Number	Critical alarm threshold for too low transmit. Unit: dBm.
UpperThresholdCritical	Number	Critical alarm threshold for too high transmit power. Unit: dBm.
Temperature	Object	Temperature information about the optical module.
ReadingCelsius	Number	Current temperature reading of the optical module. Unit: °C.
LowerThresholdCritical	Number	Critical alarm threshold for too low temperature. Unit: °C.
UpperThresholdCritical	Number	Critical alarm threshold for too high temperature. Unit: °C.
BiasCurrent	Object	Transmission bias current information about the optical module.
ReadingMilliAmperes	Array	Current transmission bias current reading of the optical module. Unit: dBm.
LowerThresholdCritical	Number	Critical alarm threshold for too low transmission bias current. Unit: mA.
UpperThresholdCritical	Number	Critical alarm threshold for too highs transmission bias current. Unit: mA.

6.23 Querying Information About Extended Boards

Function

Query the information about extended board resources.

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

Description

For a description of the parameters for querying information about extended board resources, refer to Table 6-45.

Table 6-45 Parameters Descriptions for Querying Information About Extended Board 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1644232024\"",
    "@odata.id": "/redfish/v1/Chassis/1/Boards",
    "@odata.type": "#BoardInformation.BoardInformation",
    "Description": "Board Information",
    "DiskBackplanes": {
        "@odata.id": "/redfish/v1/Chassis/1/Boards/DiskBackplanes"
    },
```

```
    "Id": "Boards",
    "Name": "Board Information"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about extended board resources, refer to Table 6-46.

Table 6-46 Output Descriptions for Querying Information About Extended Board Resources

Field	Type	Description
@odata.context	String	OData description of the extended board resource model.
@odata.etag	String	Whether the interface is changed.
@odata.id	String	Access path of the extended board resources.
@odata.type	String	Extended board resource type.
Id	String	Extended board resource ID.
@odata.id	String	Access path of the disk backplanes of the extended board resources.
Name	String	Extended board resource name.

6.24 Querying Information About the Disk Backplane Resource Collection

Function

Query information about the disk backplane resource collection.

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

Description

For a description of the parameters for querying information about the disk backplane resource collection, refer to Table 6-47.

Table 6-47 Parameter Descriptions for Querying Information About the 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	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Boards/DiskBackplanes
```

- Request Header:

```
X-Auth-Token: 85746d1212b84756218c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/
                       $metadata#DiskBackplanesCollection.DiskBackplanesCollection",
    "@odata.etag": "W/\"1644232091\"",
    "@odata.id": "/redfish/v1/Chassis/1/Boards/DiskBackplanes",
    "@odata.type": "#DiskBackplanesCollection.DiskBackplanesCollection",
    "Description": "DiskBackplanes Collection",
    "Members": [
        {
            "@odata.id": "/redfish/v1/Chassis/1/Boards/DiskBackplanes/DiskBackplane8"
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/Boards/DiskBackplanes/DiskBackplane11"
        }
    ],
```

```
    "Members@odata.count": 2,
    "Name": "DiskBackplanes Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the disk backplane resource collection, refer to Table 6-48.

Table 6-48 Output Descriptions for Querying Information About the Disk Backplane Resource Collection

Field	Type	Description
@odata.context	String	OData description of the disk backplane resource collection model.
@odata.etag	String	Whether the interface is changed.
@odata.id	String	Access path of the disk backplane resource collection node.
@odata.type	String	Type of disk backplane resource collection.
Name	String	Name of the disk backplane resource collection.
Members@odata.count	Number	Number of members in the disk backplane resource collection.
Members	Array	List of members in the disk backplane resource collection.
@odata.id	String	Access path of a disk backplane resource node.

6.25 Querying Information About a Specified Disk Backplane Resource

Function

Query information about a specified disk backplane resource.

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

Description

For a description of the parameters for querying information about a specified disk backplane resource, refer to Table 6-49.

Table 6-49 Parameter Descriptions for Querying Information About the Specified 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	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
DiskBackplaneId	ID of the specified disk backplane resource.	It can be obtained through the information about the slot where the backplane of the current hard disk is located.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Boards/DiskBackplanes/DiskBackplane8
```

- Request Header:

```
X-Auth-Token: 8574621d21b12657488c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#DiskBackplane.DiskBackplane",
    "@odata.etag": "W/\"1644232100\"",
    "@odata.id": "/redfish/v1/Chassis/1/Boards/DiskBackplanes/DiskBackplane11",
    "@odata.type": "#DiskBackplane.v1_0_0.DiskBackplane",
    "BoardName": "SBF12M",
    "DiskSpec(inch)": "3.5",
```

```
    "EPLDVersion": "00.00.0101",
    "ID": 11,
    "Location": "Back",
    "OnlineDiskCount": 3,
    "MaxDiskCountSupported": 12,
    "Manufacturer": "",
    "PcbID": "0",
    "PortCount": "SLIMSAS*2 + SLIMLINE*4",
    "SerialNumber": "732020800114",
    "Type": "U.2*8, SAS/SATA*12, Expander"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about a specified disk backplane resource, refer to Table 6-50.

Table 6-50 Output Descriptions for Querying Information About the Specified Disk Backplane Resource

Field	Type	Description
@odata.context	String	OData description of the specified disk backplane resource model.
@odata.etag	String	Whether the interface is changed.
@odata.id	String	Access path of the specified disk backplane resource node.
@odata.type	String	Type of the specified disk backplane resource.
ID	Number	Serial number of the specified hard disk backplane resource.
BoardName	String	Name of the specified disk backplane resource.
SerialNumber	String	Serial number of the specified disk backplane resource.
MaxDiskCountSupported	Number	Maximum number of hard disks supported by the specified hard disk backplane resource.
Manufacturer	String	Manufacturer of the specified disk backplane resource.

Field	Type	Description
Type	String	Type of the specified disk backplane resource.
EpldVersion	String	EPLD version of the specified disk backplane resource.
Location	String	Position of the specified disk backplane resource.
PcbID	Number	PCB ID of the specified disk backplane resource.
PortCount	String	Number of ports supported by the specified disk backplane resource.
OnlineDiskCount	Number	Number of present hard disks supported by the specified hard disk backplane resource.
DiskSpec(inch)	Number	Specification of the disks supported by the specified disk backplane resource.

6.26 Modifying Information About a Specified NEO Card

Function

Modify information about a specified NEO card of a server.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/Chassis/Chassis_id/NetworkAdapters/NetworkAdapters_id*
- Request Header:

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

- Request Message Body:

  → Restart the NEO card.

```
{
    "Oem": {
        "Public": {
            "BspFlag": "bspflag_type"
         }
    }
```

```
}
```

→ Set the boot mode for the ARM.

```
{
    "Oem": {
        "Public": {
            "BootOption": bootoption_type
        }
    }
}
```

Description

For a description of the parameters for modifying information about a specified NEO card, refer to Table 6-51.

Table 6-51 Parameter Descriptions for Modifying Information About a Specified NEO Card

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
bspflag_type	Restarts the NEO card.	ResetNeo
bootoption_type	ARM boot mode.	• PXE: The ARM boots from the PXE. • LOCAL: The ARM boots from the local disk.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://192.168.11.74/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard5
```

- Request Header:

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

- Request Message Body:

→ Restart the NEO card.

```
{
    "Oem": {
        "Public": {
             "BspFlag": "ResetNeo"
         }
    }
}
```

→ Set the boot mode for the ARM.

```
{
    "Oem": {
        "Public": {
            "BootOption": "LOCAL"
        }
    }
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#NetworkAdapter.NetworkAdapter",
    "@odata.etag": "W/\"1656560446\"",
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard4",
    "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
    "Controllers": [{
        "FirmwarePackageVersion": null,
        "Links": {
            "NetworkPorts": [{
                "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard4/
                 NetworkPorts/1"
            },
            {
                "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard4/
                 NetworkPorts/2"
            },
            {
                "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard4/
                 NetworkPorts/3"
            },
            {
                "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard4/
                 NetworkPorts/4"
            }],
```

```
            "NetworkPorts@odata.count": 4
        }
    }],
    "Id": "mainboardPCIeCard4",
    "Manufacturer": "NXP",
    "Model": "CPU-LX2160",
    "Name": "mainboardPCIeCard4",
    "NetworkPorts": {
        "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIeCard4/
         NetworkPorts"
    },
    "Oem": {
        "Public": {
            "CardManufacturer": "",
            "CardModel": "2*10GE+2*25GE",
            "CardType": "fiber",
            "DeviceLocator": "mainboardPCIeCard4",
            "DriverVersion": null,
            "Name": null,
            "NeoCpuArch": "aarch64",
            "NeoCpuCore": 16,
            "NeoDiskSize": 32,
            "NeoMemSize": 32,
            "NetworkTechnology": ["Ethernet"],
            "RootBDF": "0000:31:00.0",
            "SlotNumber": 4,
            "BoardId": "0x5495",
            "BootOption": "PXE",
        }
    },
    "SerialNumber": null,
     "Status": {
        "Health": "OK",
        "State": "Enabled"
    }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you modify information about the specified NEO card, refer to Table 6-52.

Table 6-52 Output Descriptions for Modifying Information About the Specified NEO Card

Field	Type	Description
@odata.context	Character string	OData description of the specified network adapter resource model.
@odata.id	Character string	Access path of the specified network adapter resource.
@odata.type	Character string	Type of the specified network adapter resource.
Controllers	Array	Information about adapter controllers.
FirmwarePackageVersion	Character string	Firmware version of the specified network adapter.
Links	Object	Links to the related resources.
NetworkPorts	Object	Network port resource list. the start port number is 0. For others, the start port number is 1.
@odata.id	Character string	Access path of a single network port resource.
NetworkPorts@odata.count	Number	Number of network port resources.
Id	Character string	Unique ID of the network adapter resource in the iBMC system.
Manufacturer	Character string	Manufacturer of the specified network adapter.
Model	Character string	Model of the specified network adapter.
Name	Character string	Name of the specified network adapter resource.
NetworkPorts	Object	Network port resource information.
@odata.id	Character string	Access path of the network port resource collection.
Oem.Public	Object	Customized properties.
Name	Character string	Name of the specified network adapter.
CardManufacturer	Character string	Manufacturer of the specified network adapter.
CardModel	Character string	Interface mode of the specified network adapter.
CardType	Character string	Type of the specified network adapter.
ConfigFpgaTmp	Number	Warning temperature of the specified network adapter.
CurrentFpgaTmp	Number	Main chip temperature of the specified network adapter.
DeviceLocator	Character string	Silk screen of the specified network adapter.
DriverVersion	Character string	Driver version of the specified network adapter.
FpgaStatus	Number	FPGA status of the specified network adapter, including: ● 0: normal FPGA status of the network adapter ● 1: abnormal FPGA status of the network adapter

Field	Type	Description
HistoryMaxTmp	Number	Maximum historical temperature of the specified network adapter.
NetworkTechnology	Array	Network protocol of the specified network adapter. Options: ● Ethernet ● FC ● iSCSI ● FCoE ● OPA ● IB
NicMemory	Array	Memory information about the specified network adapter.
CapacityGb	Number	Memory capacity of the specified network adapter.
Model	Character string	Memory model of the specified network adapter.
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
nicNeoCpuArch	Character string	NEO CPU architecture.
nicNeoCpuCore	Number	Number of NEO CPU cores.
nicNeoMemSize	Number	NEO memory capacity.
nicNeoDiskSize	Number	NEO hard disk capacity.
RootBDF	Character string	Root port BDF of the specified network adapter.
SlotNumber	Number	Slot number of the specified network adapter.
BoardId	Character string	Board ID of the specified network adapter.
BootOption	Character string	Boot mode of the specified network adapter.
TmpStatus	Number	FPGA temperature status of the specified network adapter. Options: ● 0: normal FPGA temperature of the specified network adapter ● 1: abnormal FPGA temperature of the specified network adapter
Status	Object	Status of the specified network adapter, including: ● Health: health status of the specified network adapter ● State: enabling status of the network adapter
SerialNumber	Character string	Serial number of the specified network adapter.

6.27 Querying Power Statistics

Function

Query power statistics.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/Chassis/chassis_id/Power/Actions/Power.CollectHistoryData*
- Request Header:

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

- Request Message Body:

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

Description

For a description of the parameters, for querying power statistics, refer to Table 6-53.

Table 6-53 Parameter Descriptions for Querying 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.
header_type	Format of the request message.	application/json
type_value	Method for collecting power statistics files.	• URI (TFTP mode) • HTTPS (HTTPS mode)
content_value	Path of power statistics files.	Valid only when **header_type** is **URI**.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Chassis/chassis_id/Power/Actions/Power.CollectHistoryData
```

- Request Header:

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

- Request Message Body:

  → TFTP:

```
{
    "Type":"URI",
    "Content":"tftp://10.10.10.10/power.csv"
}
```

  → HTTPS:

```
{
    "Type":"HTTPS"
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"d751713988987e9331980363e24189ce\"",
    "@odata.id": "/redfish/v1/Chassis/1/Power/Actions/Power.CollectHistoryData"
}
```

- Status Code: 202

Output Description

For a description of the output returned when you collect power statistics, refer to Table 6-54.

Table 6-54 Output Descriptions for Collecting Power Statistics

Field	Type	Description
@odata.context	Character string	OData description of the power statistics collection model.
@odata.etag	Character string	Whether the interface is changed.
@odata.id	Character string	Access path for collecting power statistics.

6.28 Querying Information About the Leak Detection System

Function

Query information about the leak detection system.

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 leak detection system, refer to Table 6-55.

Table 6-55 Parameter Descriptions for Querying Information About the Leak Detection System

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	Chassis ID.	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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection
```

- Request Header:

```
X-Auth-Token: 8574621d21b12657488c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#LeakDetection.LeakDetection",
    "@odata.etag": "W/\"1684851393\"",
    "@odata.id": "/redfish/v1/Chassis/Self/ThermalSubsystem/LeakDetection",
    "@odata.type": "#LeakDetection.v1_0_0.LeakDetection",
    "Id": "LeakDetection",
    "LeakDetectors": {
        "@odata.id": "/redfish/v1/Chassis/Self/ThermalSubsystem/LeakDetection/
```

```
        LeakDetectors"
    },
    "Name": "LeakDetection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the leak detection system, refer to Table 6-56.

Table 6-56 Output Descriptions for Querying Information About the Leak Detection System

Field	Type	Description
@odata.context	Character string	OData description of the leak detection resource model.
@odata.etag	Character string	Whether the interface is changed.
@odata.id	Character string	Access path of the leak detection resource.
@odata.type	Character string	Type of leakage detection resource.
Id	Number	ID of the leak detection resource.
Name	Character string	Name of the leak detection resource.
LeakDetectors	Object	List of leak detector resources.

6.29 Querying Information About the Leak Detector Resource Collection

Function

Query information about the leak detector resource collection.

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 6-57.

Table 6-57 Parameter Descriptions for Querying Information About the Leak Detector Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	Chassis ID.	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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection/LeakDetectors
```

- Request Header:

```
X-Auth-Token: 8574621d21b12657488c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context":
    "/redfish/v1/$metadata#LeakDetectorCollection.LeakDetectorCollection",
    "@odata. "@odata.id":
    "/redfish/v1/Chassis/Self/ThermalSubsystem/LeakDetection/ etag":
    "W/\"1684851393\"",
    "@odata.id": "/redfish/v1/Chassis/Self/ThermalSubsystem/LeakDetection/LeakDetectors",
    "@odata.type": "#LeakDetectorCollection.LeakDetectorCollection",
    "Members": [
        {
            "@odata.id": "/redfish/v1/Chassis/Self/ThermalSubsystem/LeakDetection/
            LeakDetectors/1"
        }
    ],
    "Members@odata.count": 1,
    "Name": "Leak Detector Collection"
}
```

- 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 6-58.

Table 6-58 Output Descriptions for Querying Information About the Leak Detector Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the leak detector resource collection model.
@odata.etag	Character string	Whether the interface is changed.
@odata.id	Character string	Access path of the leak detector resource collection.
@odata.type	Character string	Type of leak detector resource collection.
Id	Number	ID of the leak detector resource collection.
Name	Character 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.id	Character string	Access path of the specified leak detector resource node.

6.30 Querying Information About a Specified Leak Detector Resource

Function

Query information about a specified leak detector resource.

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 leak detector resource, refer to Table 6-59.

Table 6-59 Parameter Descriptions for Querying Information About a Specified Leak Detector Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	Chassis ID.	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 */redfish/v1/SessionService/Sessions*.
leakdetector_id	ID of the leak detector.	ID of the leak detector.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/ThermalSubsystem/LeakDetection/LeakDetectors/1
```

- Request Header:

```
X-Auth-Token: 8574621d21b12657488c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context":
    "/redfish/v1/$metadata#LeakDetector.LeakDetector",
    "@odata.etag": "W/\"1684851033\"",
    "@odata.id": "/redfish/v1/Chassis/Self/ThermalSubsystem/LeakDetection/
    LeakDetectors/1",
    "@odata.type": "#LeakDetector.v1_0_0.LeakDetector",
    "DetectorState": "OK",
    "Id": "1",
    "Name": "Moisture-type Leak Detector",
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    }
```

```
}
```

- Status Code: 200

Output Description

For the output descriptions for querying information about the specified leak detector resource, refer to Table 6-60.

Table 6-60 Output Descriptions for Querying Information About the Specified Leak Detector Resource

Field	Type	Description
@odata.context	Character string	OData description of the specified leak detector model.
@odata.etag	Character string	Whether the interface is changed.
@odata.id	Character string	Access path of the specified leak detector resource.
@odata.type	Character string	Type of the specified leak detector resource.
Id	Number	ID of the specified leak detector resource.
Name	Character string	Name of the specified leak detector resource.
DetectorState	Number	Status of leakage related to the specified leak detector resource. Options: ● OK ● Critical
Status	Object	Status of the specified leak detector resource. Options: ● Health: health status of the specified leak detector resource, including: → OK → Critical ● State: whether the specified leak detector resource is enabled. Options: → Enabled → Disabled

Chapter 7
Operations on SessionService Resources

Table of Contents

Creating a Session 512
Querying Information About the Session Service 514
Modifying Information About the Session Service 516
Querying Information About the Session Resource Collection 518
Querying Information About a Specified Session Resource 519
Deleting Information About a Specified Session Resource 521

Figure 7-1 shows the path requirements for the Redfish 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
	Status	Resource status.	GET

URL	Property	Description	Operation
/redfish/v1/SessionService/Sessions	Id	Unique ID of the newly created session resource.	POST
	Name	Name of the newly created session.	POST
	UserName	Account information about the newly created session.	POST
	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	Id	UID of the specified session resource.	GET
	Name	Name of the specified session.	GET
	UserName	Account information about the specified session.	GET

7.1 Creating a Session

Function

Create a session.

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 7-2.

Table 7-2 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 iBMC system.
password	Password of the user for the new session.	Password of the user for the iBMC 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/$metadataSessionService/Sessions",
    "@odata.etag": "W/\"1580983009\"",
    "@odata.id": "/redfish/v1/SessionService/Sessions/ccfd535bda42d5bb625eff85f4bd689a",
    "@odata.type": "#Session.v1_1_0.Session",
    "Description": "Session for user root",
    "Id": "ccfd535bda42d5bb625eff85f4bd689a",
    "Name": "root Session",
```

```
    "UserName": "root"
}
```

- Response Header Example:

```
access-control-allow-credentials Ztrue
access-control-allow-headers ZX-Auth-Token
access-control-allow-origin Z*
access-control-expose-headers ZX-Auth-Token
cache-control Zno-cache, must-revalidate
content-length Z348
content-type Zapplication/json; charset=UTF-8
date ZThu, 06 Feb 2020 09:56:49 GMT
etag ZW/"1580983009"
link Z<http://redfish.dmtf.org/schemas/v1/Session.v1_1_0.json>; rel=describedby
locationZ/redfish/v1/SessionService/Sessions/ccfd535bda42d5bb625eff85f4bd689a
odata-version Z4.0
server ZZXSAC Redfish Service
X-Auth-Token ZX+t/yUEAci2aN5VNTaqXuZGe7STrREDFVNybxw2o8y8=
```

- Status Code: 201

Output Description

For a description of the output returned when you create a session, refer to Table 7-3.

Table 7-3 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.
@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.
UserName	String	Account information about newly created session.

7.2 Querying Information About the Session Service

Function

Query information about the current session service of a server.

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 7-4.

Table 7-4 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1580873008\"",
    "@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 Code: 200

Output Description

For a description of the output returned when you query information about the session service, refer to Table 7-5.

Table 7-5 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.
Id	String	ID of the SessionService resource.
Name	String	Name of the SessionService resource.
SessionTimeout	Number	Redfish session timeout period.
Sessions	Object	Session list.
@odata.id	String	Access path of the session list.
Status	Object	Resource status. Options: ● Status: enabling status ● Health: health status

7.3 Modifying Information About the Session Service

Function

Modify the timeout period of the session service of a server.

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
}
```

Description

For a description of the parameters for modifying information about the session service, refer to Table 7-6.

Table 7-6 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 */redfish/v1/SessionService/Sessions*.
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

7.4 Querying Information About the Session Resource Collection

Function

Query information about the current session resource collection of a server.

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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1580990271\"",
```

```
    "@odata.id": "/redfish/v1/SessionService/Sessions",
    "@odata.type": "#SessionCollection.SessionCollection",
    "Members":
    [{
        "@odata.id": "/redfish/v1/SessionService/Sessions/
                                57f5ff2105218ad2df694ab94cbeba90"
    },
    {
        "@odata.id": "/redfish/v1/SessionService/Sessions/
                                ccfd535bda42d5bb625eff85f4bd689a"
    }],
    "Members@odata.count": 2,
    "Name": "Session Collection"
}
```


- 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	Session list	-
@odata.id	String	Access path of a single session resource node.

7.5 Querying Information About a Specified Session Resource

Function

Query information about a specified session resource.

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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1580990268\"",
    "@odata.id": "/redfish/v1/SessionService/Sessions/57f5ff2105218ad2df694ab94cbeba90",
    "@odata.type": "#Session.v1_1_0.Session",
    "Description": "Session for user root",
    "Id": "57f5ff2105218ad2df694ab94cbeba90",
    "Name": "Session",
    "UserName": "root"
```

```
}
```

- 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.
Id	String	UID of the specified session resource.
Name	String	Name of the session resource.
UserName	String	Username for the specified session.

7.6 Deleting Information About a Specified Session Resource

Function

Delete information about a specified session resource of a server.

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 GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

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

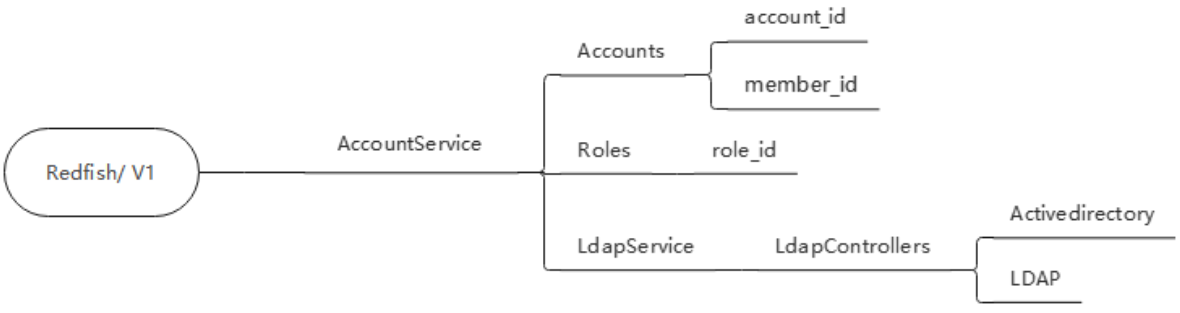
Chapter 8
Operations on AccountService Resources

Table of Contents

Querying User Service Information 528
Modifying User Service Information 531
Querying Information About the User Resource Collection 533
Querying Information About a Specified User Resource 534
Creating an Account 537
Deleting a User 541
Modifying Information About a Specified User 542
Querying Information About the Role Resource Collection 544
Querying Information About the Specified Role Resource 546
Querying Information about the LDAP Service Resource 548
Querying Information About the LDAP Domain Controller Collection 550
Querying Active Directory Information 552
Modifying Active Directory Information 555
Querying the LDAP Information 560
Modifying the LDAP Information 562

Figure 8-1 shows the path requirements for the Redfish AccountService resources supported by VANTAGEO servers.

Figure 8-1 AccountService Resource Path Requirements



For a description of properties of AccountService resources and operations supported by the properties, refer to Table 8-1.

Table 8-1 Descriptions of AccountService Resources Properties

URL	Property	Description	Operation
/redfish/v1/AccountService	Id	ID of an AccountService resource.	GET
	Name	Name of the AccountService resource.	GET
	AccountLockoutThreshold	Allowed attempts for incorrect account password input.	GET/PATCH
	AccountLockoutDuration	Account lockout duration after a user login failure.	GET/PATCH
	AccountLockoutThreshold	Number of incorrect passwords allowed. If the number of times that an incorrect password is entered exceeds this value, the user is locked. Range: 0–10.	GET
	AccountLockoutCounterResetAfter	Time after which account lockout counter is reset.	GET
	MinPasswordLength	Minimum password length.	GET
	MaxPasswordLength	Maximum password length.	GET
	Accounts	Access path of the user resource collection node.	GET
	Roles	Access path of the role resource collection node.	GET
	Status	Status of the specified resource, including: ● Status: enabling status ● Health: health status	GET
	Oem.Public	OEM object of the Account resource node.	GET

URL	Property	Description	Operation
	LdapService	Access path of the LdapService resource node.	GET
	OSUserManagementEnabled	Whether the service-side user management configuration is enabled.	GET
/redfish/v1/AccountService/Accounts	Id	ID of the specified user resource.	POST
	Name	Name of the user resource collection.	GET
	Members@odata.count	Number of user resource members.	GET
	Members	User list, which provides references for all user URLs.	GET
	UserName	Account username.	POST
	PasswordSize	Account password.	POST
	RoleId	Role resource ID in the account configuration.	POST
	Locked	• true: locked • false: unlocked	POST
	Enabled	• true: The user can log in. • false: The user cannot log in.	POST
	Links	Links to the user resource.	POST
	Roles	Links to the roles corresponding to the user.	POST
/redfish/v1/ccountService/Accounts/account_id	Id	ID of the user resource.	GET
	Name	Name of the user resource.	GET
	UserName	Username.	GET/PATCH
	Password	Password.	GET/PATCH
	RoleId	User permission.	GET/PATCH

URL	Property	Description	Operation
	Locked	Indicates that the user is locked.	GET/PATCH
	Enabled	Indicates that the user is enabled.	GET/PATCH
	Links	Links to the user resource.	GET/POST
	Roles	Links to the roles corresponding to the user.	GET/POST
/redfish/v1/AccountService/Roles	Name	Name of the role resource collection.	GET
	Members@odata.count	Number of role resource members.	GET
	Members	Role resource list, which provides references for all role type URLs.	GET
/redfish/v1/AccountService/Roles/role_id	Id	ID of the role resource.	GET
	Name	Name of the role resource.	GET
	IsPredefined	Whether the specified permissions are pre-defined.	GET
/redfish/v1/AccountService/LdapService	Id	LDAP service resource ID.	GET
	Name	LDAP service resource name.	GET
	LdapControllers	Controller list.	GET
/redfish/v1/AccountService/LdapService/LdapControllers	Name	Name of the LDAP controller collection.	GET
	Members	List of LDAP controllers.	GET
/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory	Id	ID of the Active Directory information resource.	GET/PATCH
	Name	Name of the Active directory information resource.	GET/PATCH

URL	Property	Description	Operation
	Password	Password, which is displayed as null when queried.	GET/PATCH
	ADAuthenticationEnable	Whether active directory authentication is enabled.	GET/PATCH
	ADSSLEnable	Whether SSL encryption is enabled.	GET
	DomainControllerServerAddress1	Domain Controller Server Address 1.	GET/PATCH
	DomainControllerServerAddress2	Domain Controller Server Address 2.	GET/PATCH
	DomainControllerServerAddress3	Domain Controller Server Address 3.	GET/PATCH
	UserDomain	User domain name.	GET/PATCH
	ADRoleGroups	AD role group.	GET/PATCH
	GroupDomain	Group domain name.	GET/PATCH
	GroupLoginInterface	Access permission: ● KVM ● VMedia	GET/PATCH
	GroupRole	Role group permission: ● Administrator ● Operator ● ReadOnly	GET/PATCH
	MemberId	Role group ID. Range: 0 –4.	GET/PATCH
/redfish//v1/AccountService/LdapService/LdapControllers/LDAP	Name	Name of the LDAP information resource.	GET/PATCH
	Password	Password, which is displayed as null when queried.	GET/PATCH
	BindDN	Bound DN..	GET/PATCH
	CommonNameType	Common name type: ● IP ● FQDN	GET/PATCH
	EncryptionType	Encryption type, options:	GET/PATCH

URL	Property	Description	Operation
		• NoEncryption • SSL • StartTLS	
	LDAPAuthenticationEnable	Whether LDAP authentication is enabled.	GET/PATCH
	Port	Port number.	GET/PATCH
	SearchBase	Search base.	GET/PATCH
	ServerAddress	Server.	GET/PATCH
	UserLoginAttribute	User login attribute: uid:cn	GET/PATCH
	LDAPRoleGroups	LDAP role group.	GET/PATCH
	GroupName	Group name.	GET/PATCH
	GroupDomain	Group domain name.	GET/PATCH
	GroupLoginInterface	Access permission: • KVM • VMedia	GET/PATCH
	GroupRole	Role group permission: • Administrator • Operator • ReadOnly	GET/PATCH
	MemberId	Role group ID. Range: 0–4.	GET/PATCH

8.1 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.

Syntax

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

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

- Request Message Body: None

Description

For a description of the parameters for querying the user service information, refer to Table 8-2.

Table 8-2 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1622011984\"",
    "@odata.id": "/redfish/v1/AccountService",
    "@odata.type": "#AccountService.v1_2_2.AccountService",
    "AccountLockoutCounterResetAfter": 30,
    "AccountLockoutDuration": 600,
    "AccountLockoutThreshold": 3,
    "Accounts":
    {
        "@odata.id": "/redfish/v1/AccountService/Accounts"
    },
    "Description": "BMC User Accounts",
    "Id": "AccountService",
    "MaxPasswordLength": 20,
    "MinPasswordLength": 8,
    "Name": "Account Service",
    "Oem": {
        "Public": {
```

```
        "LdapService": {
        "@odata.id": "/redfish/v1/AccountService/LdapService"
         },
         "OSUserManagementEnabled": true
     }
},
    "Roles":
    {
        "@odata.id": "/redfish/v1/AccountService/Roles"
    },
    "ServiceEnabled": true,
    "Status": {"Health": "OK", "State": "Enabled"}
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query user service information, refer to Table 8-3.

Table 8-3 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.
Id	String	ID of the AccountService resource.
Name	String	Name of the AccountService resource.
MinPasswordLength	Number	Minimum password length.
MaxPasswordLength	Number	Maximum password length.
AccountLockoutThreshold	Number	Maximum number of failed password attempts. A user is locked out if this value is reached. Range: 0–10.
AccountLockoutDuration	Number	Lockout duration after a login failure (in seconds). Range: AccountLockoutCounterResetAfter through 10000

Field	Type	Description
AccountLockoutCounterResetAfter	Number	Time after which account lockout counter is reset.
Roles	Role resources.	-
@odata.id	String	Access path of the role resource node.
Accounts	User resources.	-
@odata.id	String	Access path of the Account resource node.
Status	Object	Status of the specified resource, including: ● State: enabling status ● Health: health status
Oem.Public	Object	OEM object of the Account resource node.
LdapService	Object	Access path of the LdapService resource node.
OSUserManagementEnabled	Boolean	Whether OS user management is enabled.

8.2 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.

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:

```
{
    "AccountLockoutThreshold":count,
    "AccountLockoutDuration":time
}
```

Parameters

For a description of the parameters for modifying user service information, refer to Table 8-4.

Table 8-4 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 for requested messages	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
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.	Integer, range: 30–10000, unit: seconds.

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
If-Match: W/"bc428df5"
```

- Request Message Body:

```
{
    "AccountLockoutThreshold":8,
    "AccountLockoutDuration": 8037
}
```

- Response Example: None

- Status Code: 204

Output Description

None

8.3 Querying Information About the User Resource Collection

Function

Query information about the current user resource collection of a server.

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 8-5.

Table 8-5 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.
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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1593569280\"",
    "@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 8-6.

Table 8-6 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	User list.	-
@odata.id	String	Access path of a single account resource node.

8.4 Querying Information About a Specified User Resource

Function

Query information about a specified user resource of a server.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/AccountService/Accounts/member_id*
- Request Header:

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

- Request Message Body: None

Description

For a description of the parameters for querying information about a specified user resource, refer to Table 8-7.

Table 8-7 Parameter Descriptions for Querying Information About the Specified User 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 */redfish/v1/SessionService/Sessions*.
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/AccountService/Accounts/2
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#ManagerAccount.ManagerAccount",
    "@odata.etag": "W/\"1593678391\"",
    "@odata.id": "/redfish/v1/AccountService/Accounts/2",
    "@odata.type": "#ManagerAccount.v1_1_1.ManagerAccount",
```

```
    "Enabled": true,
    "Id": "2",
    "Links":
    {
        "Roles":
        {
            "@odata.id": "/redfish/v1/AccountService/Roles/Administrator"
        }
    },
    "Locked": false,
    "Name": "User Account",
    "PasswordSize": 20,
    "RoleId": "Administrator",
    "UserName": "root"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified user resource, refer to Table 8-8.

Table 8-8 Output Descriptions for Querying Information About the Specified User Resource

Field	Type	Description
@odata.context	String	OData description of the specified user resource model.
@odata.id	String	Access path of the specified user resource node.
@odata.type	String	Type of the specified user resource.
Id	String	ID of the specified user resource.
Name	String	Name of the account resource.
UserName	String	User name.
PasswordSize	Number	Account password size.
RoleId	String	Role resource ID in the account configuration.
Locked	Boolean	Whether the account is locked.
Enabled	Boolean	Whether the account is enabled.
Links	Object	Links to the user resource.
Roles	Object	Links to the roles corresponding to the user.

Field	Type	Description
@odata.id	String	Access path of the role resource corresponding to the user.

8.5 Creating an Account

Function

Create an account.

Syntax

- Operation Type: POST
- URL1: *https://device_ip/redfish/v1/AccountService/Accounts*
- URL2: *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,
    "PasswordSize":passwordsize,
    "RoleId": role,
    "Enabled": flag,
    "Locked": flag1
}
```

Description

For the parameter descriptions for creating an account, refer to Table 8-9.

Table 8-9 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	X-Auth-Token value contained in Request Header in the	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

Parameter	Description	Value
	POST request for authentication.	
name	User name of the new account.	● String, range: 3–16 characters. ● Value rules: → It consists of special characters, letters, and digits, and cannot contain spaces or begin with hashtags (#). → It user must start with a letter. → For special characters, only "-", "_", and "@" are allowed.
password	Password of the new account.	● If the password complexity policy is enabled on other interfaces, configured and modified passwords must comply with password complexity rules. ● If the password complexity policy is disabled on other interfaces, configured and modified passwords must comply with weak-password rules.
passwordsize	Length of the password of the new account.	Range: 16–20.
role	Role of the new account.	Available role types include: ● Administrator ● Operator ● ReadOnly
flag	Account enabling flag.	Range: ● true ● false
flag1	Account lockout flag.	Range: false
account_id	Account ID.	Range: 2–16.

Usage Guidelines

None

Example

- Request Example 1:

```
POST https://device_ip/redfish/v1/AccountService/Accounts
```

- Request Example 2:

```
POST https://device_ip/redfish/v1/AccountService/Accounts/14
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body (for both 1 and 2):

```
{
    "UserName": "root",
    "Password": "xxxxxxxxxxx",
    "PasswordSize": 20,
    "RoleId": "Administrator",
    "Enabled": true,
    "Locked": false
}
```

- Response Example 1:

```
{
    "@odata.context": "/redfish/v1/$metadata#ManagerAccount.ManagerAccount",
    "@odata.etag": "W/\"1581345923\"",
    "@odata.id": "/redfish/v1/AccountService/Accounts/2",
    "@odata.type": "#ManagerAccount.v1_1_1.ManagerAccount",
    "Enabled": true,
    "Id": "2",
    "Links": {
        "Roles": {
            "@odata.id": "/redfish/v1/AccountService/Roles/Administrator"
        }
    },
    "Locked": false,
    "Name": "User Account",
    "PasswordSize": 20,
    "RoleId": "Administrator",
    "UserName": "root"
}
```

- Response Example 2:

```
{
    "@odata.context": "/redfish/v1/$metadata#ManagerAccount.ManagerAccount",
    "@odata.etag": "W/\"1581345923\"",
    "@odata.id": "/redfish/v1/AccountService/Accounts/14",
    "@odata.type": "#ManagerAccount.v1_1_1.ManagerAccount",
    "Enabled": true,
    "Id": "14",
    "Links": {
```

```
        "Roles": {
            "@odata.id": "/redfish/v1/AccountService/Roles/Administrator"
        }
    },
    "Locked": false,
    "Name": "User Account",
    "PasswordSize": 20,
    "RoleId": "Administrator",
    "UserName": "root"
}
```


- Status Code: 201

Output Description

For a description of the output returned when you create an account, refer to Table 8-10.

Table 8-10 Output Descriptions for Creating an Account

Field	Type	Description
@odata.context	String	OData description of the specified user resource model.
@odata.id	String	Access path of the specified user resource node.
@odata.type	String	Type of the specified user resource.
Id	String	ID of the specified user resource.
Name	String	Name of the account resource.
UserName	String	User name.
PasswordSize	Number	Account password size.
RoleId	String	Role resource ID in the account configuration.
Locked	Boolean	• true: locked • false: unlocked
Enabled	Boolean	• true: The user can log in. • false: The user cannot log in.
Links	Object	Links to the user resource.
Roles	Object	Links to the roles corresponding to the user.
@odata.id	String	Access to the role resources corresponding to the user.

8.6 Deleting a User

Function

Delete a specified user.

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 the parameter descriptions for deleting a user, refer to Table 8-11.

Table 8-11 Parameter Descriptions for Deleting a User

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
account_id	User ID	It can be obtained by querying the user list.
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 */redfish/v1/SessionService/Sessions*.

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

8.7 Modifying Information About a Specified User

Function

Modify the username, password, permission, lockout status and enabling status of a specified user.

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,
    "PasswordSize":passwordsize,
    "RoleId": role,
    "Enabled": flag,
    "Locked": flag1
}
```

Description

For the parameter descriptions for modifying information about the specified user, refer to Table 8-12.

Table 8-12 Parameter Descriptions for Modifying Information About the Specified User

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
account_id	ID of the account that you want to modify.	User ID
auth_value	Authentication parameter of the request message.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

Parameter	Description	Value
header_type	Format of the request message.	application/json
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.
name	User name of the new account.	● String, range: 4–16 characters. ● Value rules: → The username must start with a letter. → For special characters, only "-", "_", and "@" are allowed.
password	Password of the new account.	● If the password complexity check function is enabled on other interfaces, configured and modified passwords must comply with the password complexity rules. ● If the password complexity check function is not enabled on other interfaces, configured and modified passwords can be any characters.
passwordsize	Length of the password of the new account.	Range: 16–20 characters.
role	Role of the new account.	Available role types include: ● Administrator ● Operator ● ReadOnly
flag	User enabling flag.	● true ● false
flag1	User lockout flag.	False.

Usage Guidelines

For a specified user, one or more properties in the requested message body can be modified at the same time.

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/AccountService/Accounts/account_id
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234e
Content-Type: application/json
```

```
If-Match: W/"1577215941"
```

- Request Message Body:

```
{
    "UserName": "username",
    "Password": "Superuser9!",
    "PasswordSize": 20,
    "RoleId": "Administrator",
    "Enabled": true,
    "Locked": false
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#ManagerAccount.ManagerAccount",
    "@odata.etag": "W/\"1581345923\"",
    "@odata.id": "/redfish/v1/AccountService/Accounts/14",
    "@odata.type": "#ManagerAccount.v1_1_1.ManagerAccount",
    "Enabled": true,
    "Id": "14",
    "Links": {
        "Roles": {
            "@odata.id": "/redfish/v1/AccountService/Roles/Administrator"
        }
    },
    "Locked": false,
    "Name": "User Account",
    "PasswordSize": 20,
    "RoleId": "Administrator",
    "UserName": "username"
}
```

- Status Code: 200

Output Description

None

8.8 Querying Information About the Role Resource Collection

Function

Query information about the current role resource collection of a server.

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 8-13.

Table 8-13 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1571460331\"",
    "@odata.id":  "/redfish/v1/AccountService/Roles",
    "@odata.type":  "#RoleCollection.RoleCollection",
    "Members":
    [{
        "@odata.id": "/redfish/v1/AccountService/Roles/Operator"
```

```
    },
    {
        "@odata.id": "/redfish/v1/AccountService/Roles/ReadOnly"
    },
    {
        "@odata.id": "/redfish/v1/AccountService/Roles/Administrator"
    }],
    "Members@odata.count": 3,
    "Name": "Roles Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the role resource collection, refer to Table 8-14.

Table 8-14 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	Session list.	-
@odata.id	String	Access path of a single role resource node.

8.9 Querying Information About the Specified Role Resource

Function

Query information about a specified role resource of a server.

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

Description

For a description of the parameters for querying information about a specified role resource, refer to Table 8-15.

Table 8-15 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 */redfish/v1/SessionService/Sessions*.
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/Accounts/Administrator
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context":
    "/redfish/v1/$metadata#Role.Role(IsPredefined,Id,AssignedPrivileges,Name,
     Description)",
    "@odata.etag": "W/\"1571460336\"",
    "@odata.id": "/redfish/v1/AccountService/Roles/Administrator",
    "@odata.type": "#Role.v1_2_1.Role",
    "AssignedPrivileges":
    [
        "ConfigureComponents",
        "ConfigureManager"
        "ConfigureSelf",
```

```
        "ConfigureUsers",
        "Login",
    ],
    "Description": "Admin User Role",
    "Id": "Administrator",
    "IsPredefined": true,
    "Name": "User Role"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified user resource, refer to Table 8-16.

Table 8-16 Output Descriptions for Querying Information About the Specified User 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 specified role resource.
Id	String	ID of the specified role resource.
Name	String	Name of the specified role resource.
IsPredefined	String	Whether the specified role is pre-defined.

8.10 Querying Information about the LDAP Service Resource

Function

Query information about the current LDAP resource of a server.

Syntax

- Operation Type: GET
- URL: *https://deviceip/redfish/v1/AccountService/LdapService*
- Request Header:

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the LDAP service resource, refer to Table 8-17.

Table 8-17 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	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1621651337\"",
    "@odata.id": "/redfish/v1/AccountService/LdapService",
    "@odata.type": "#LdapCollection.LdapServiceCollection",
    "Id": "Ldap Service",
    "LdapControllers": [
    {
        "@odata.id": "/redfish/v1/AccountService/LdapService/LdapControllers"
    }],
    "Members@odata.count": 1,
    "Name": "Ldap Service"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the LDAP service resource, refer to Table 8-18.

Table 8-18 Output Descriptions for Querying Information About the LDAP Service Resource

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.
Id	String	ID of the LDAP service resource.
Name	String	Name of the LDAP resource.
LdapControllers	Object	Controller list.
@odata.id	String	LDAP controller information.
Members@odata.count	Number	Number of members.
@odata.id	String	Access path of an LDAP controller node.

8.11 Querying Information About the LDAP Domain Controller Collection

Function

Query information about the LDAP domain controller collection of a server.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers*
- Request Header:

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the LDAP domain controller collection, refer to Table 8-19.

Table 8-19 Parameter Descriptions for Querying Information About the LDAP Domain Controller 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"946662360\"",
    "@odata.id": "/redfish/v1/AccountService/LdapService/LdapControllers",
    "@odata.type": "#LdapCollection.LdapServiceCollection.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 LDAP domain controller collection, refer to Table 8-20.

Table 8-20 Output Descriptions for Querying Information About the LDAP Domain Controller Collection

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	Access path of a member of the LDAP domain controller collection.

8.12 Querying Active Directory Information

Function

Query the information about the current active directory of a server.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/AccountService/LdapService/Ldap-Controllers/Activedirectory*
- Request Header:

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the active directory, refer to Table 8-21.

Table 8-21 Parameter Descriptions for Querying 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 GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1621492713\"",
    "@odata.id": "/redfish/v1/AccountService/LdapService/LdapControllers
                  /Activedirectory",
    "@odata.type": "#LdapCollection.LdapControllers.Activedirectory",
    "ADAuthenticationEnable": true,
    "ADRoleGroups": [
    {
        "GroupDomain": "example.com",
        "GroupLoginInterface": ["KVM"],
        "GroupName": "bsp",
        "GroupRole": "Administrator",
        "MemberId": 0
    },
    {
        "GroupDomain": "exampdle.com",
        "GroupLoginInterface": ["KVM","VMedia"],
        "GroupName": "test",
        "GroupRole": "Administrator",
        "MemberId": 2
```

```
    }
    ],
    "ADSSLEnable": false,
    "DomainControllerServerAddress1": "1.2.3.5",
    "DomainControllerServerAddress2": null,
    "DomainControllerServerAddress3": null,
    "Name": "Activedirectory",
    "Password": null,
    "UserDomain": "MyDomaintest.com",
    "UserName": "testdsf"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the active directory, refer to Table 8-22.

Table 8-22 Output Descriptions for Querying Active Directory Information

Field	Type	Description
@odata.context	String	OData description of the Active Directory Information model.
@odata.id	String	Access path of the 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	Object	Password. It is displayed as null when queried.
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 name.

Field	Type	Description
ADRoleGroups	Object	AD role group.
GroupDomain	String	Group domain name.
GroupLoginInterface	Object	Access permission: ● KVM ● VMedia
GroupRole	String	Role group permission: ● Administrator ● Operator ● ReadOnly
MemberId	Number	Role group ID. Range: 0–4.

8.13 Modifying Active Directory Information

Function

Modify the information about the current active directory of a server.

Syntax

- Operation Type: PATCH
- URL: *https://device_ip/redfish/v1/AccountService/LdapService/Ldap-Controllers/Activedirectory*
- Request Header:

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

- Request Message Body:

```
{
    "ADAuthenticationEnable": ADAuthenticationEnable_value,
    "DomainControllerServerAddress1": DomainControllerServerAddress1_value,
    "DomainControllerServerAddress2": DomainControllerServerAddress2_value,
    "DomainControllerServerAddress3": DomainControllerServerAddress3_value,
    "Password": Password_value,
    "UserDomain": UserDomain_value,
    "UserName": UserName_value,
    "ADSSLEnable": ADSSLEnable_value,
    "ADRoleGroups": [
    {
        "GroupDomain": GroupDomain_value,
        "GroupLoginInterface": GroupLoginInterface_value,
        "GroupName": GroupName_value,
```

```
        "GroupRole": GroupRole_value,
        "MemberId": MemberId_value
    }]
}
```

Description

For a description of the parameters for modifying information about the active directory, refer to Table 8-23.

Table 8-23 Parameter Descriptions for Modifying 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 */redfish/v1/SessionService/Sessions*.
ADAuthenticationEnable_value	Boolean	Whether active directory authentication is enabled: ● true ● false
DomainControllerServerAddress1_value	String	Domain Controller Server Address 1
DomainControllerServerAddress2_value	String	Domain Controller Server Address 2
DomainControllerServerAddress3_value	String	Domain Controller Server Address 3
ADSSLEnable_value	Boolean	Whether SSL encryption is enabled: ● true ● false
Password_value	String	Password.
UserDomain_value	String	User domain name.
UserName_value	String	Username.
ADRoleGroups	Object	Role set
GroupDomain_value	String	Group domain

Parameter	Description	Value
GroupLoginInter-face	Object	Group login interface: ● KVM ● VMedia
GroupNamevalue	String	Group name. If it is set to null, the role group is deleted.
GroupRole_value	String	Role group permission: ● Administrator ● Operator ● ReadOnly
MemberId_value	Number	Role group ID. Range: 0–4.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory
```

- Request Header:

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

- Request Message Body:

```
{
    "ADAuthenticationEnable": true,
    "DomainControllerServerAddress1": "2.4.3.5",
    "Password": "Superuser7!",
    "UserDomain": "MyDddidntest.com",
    "UserName": "teseddst",
    "ADRoleGroups": [
    {
        "GroupDomain": "example.com",
        "GroupLoginInterface": ["KVM"],
        "GroupName": "bsp",
        "GroupRole": "ReadOnly",
        "MemberId": 0
    },
    {
        "GroupDomain": "exampdle.com",
        "GroupLoginInterface": ["KVM","VMedia"],
        "GroupName": "testd",
```

```
        "GroupRole": "Administrator",
        "MemberId": 3
    }
    ],
}
```


- Response Example:


```
{
    "@odata.context": "/redfish/v1/$metadata#AccountService.LdapService.LdapControllers.
                       Activedirectory",
    "@odata.etag": "W/\"1621499790\"",
    "@odata.id": "/redfish/v1/AccountService/LdapService/LdapControllers
                  /Activedirectory",
    "@odata.type": "#LdapCollection.LdapControllers.Activedirectory",
    "ADAuthenticationEnable": true,
    "ADRoleGroups": [
    {
        "GroupDomain": "example.com",
        "GroupLoginInterface": ["KVM"],
        "GroupName": "bsp",
        "GroupRole": "Operator",
        "MemberId": 0
    },
    {
        "GroupDomain": "exampdle.com",
        "GroupLoginInterface": ["KVM"],
        "GroupName": "test",
        "GroupRole": "Administrator",
        "MemberId": 2
    },
    {
        "GroupDomain": "exampdle.com",
        "GroupLoginInterface": ["KVM","VMedia"],
        "GroupName": "testd",
        "GroupRole": "Administrator",
        "MemberId": 3
    }
],
    "DomainControllerServerAddress1": "2.4.3.5",
    "DomainControllerServerAddress2": null,
    "DomainControllerServerAddress3": null,
    "Name": "Activedirectory",
    "Password": null,
    "UserDomain": "MyDddidntest.com",
```

```
    "UserName": "teseddst"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you modify information about the active directory, refer to Table 8-24.

Table 8-24 Output Description for Querying Information About the Active Directory

Field	Type	Description
@odata.context	String	OData description of the Active Directory Information model.
@odata.id	String	Access path of the 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	Object	Password. It is displayed as null when queried.
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 name.
ADRoleGroups	Object	AD role group.
GroupDomain	String	Group domain name.
GroupLoginInterface	Object	Access permission: ● KVM ● VMedia
GroupRole	String	Role group permission: ● Administrator ● Operator ● ReadOnly

Field	Type	Description
MemberId	Number	Role group ID. Range: 0–4.

8.14 Querying the LDAP Information

Function

Query the current LDAP information about a server.

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 the current LDAP information, refer to Table 8-25.

Table 8-25 Parameter Descriptions for Querying the Current LDAP 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"946662360\"",
    "@odata.id": "/redfish/v1/AccountService/LdapService/LdapControllers/LDAP",
    "@odata.type": "#LdapCollection.LDAP",
    "BindDN": "cn=admin,dc=ldapdomain,dc=com",
    "CommonNameType": "IP",
    "EncryptionType": "NoEncryption",
    "LDAPAuthenticationEnable": true,
    "LDAPRoleGroups": [
    {
        "GroupDomain": "ou=testgroup,dc=ldapdomain,dc=com",
        "GroupLoginInterface": ["KVM","VMedia"],
        "GroupName": "sdf",
        "GroupRole": "Operator",
        "MemberId": 0
    }
],
    "Name": "LDAP",
    "Password": null,
    "Port": 392,
    "SearchBase": "ou=login,dc=domain,dc=com",
    "ServerAddress": "192.168.5.15",
    "UserLoginAttribute": "uid"
    }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query the current LDAP information, refer to Table 8-26.

Table 8-26 Output Descriptions for Querying the Current LDAP Information

Field	Type	Description
@odata.context	String	OData description of the LDAP information model.
@odata.id	String	Access path of the LDAP information resource node.
@odata.type	String	LDAP information resource type.

Field	Type	Description
Name	String	Name of the LDAP information resource.
Password	Object	Password. It is displayed as null when queried.
BindDN	String	Bound DN.
CommonNameType	String	Common name type: ● IP ● FQDN
EncryptionType	String	Encryption type, options: ● NoEncryption ● SSL ● StartTLS
LDAPAuthenticationEnable	Boolean	Whether LDAP authentication is enabled.
Port	Number	Port number.
SearchBase	String	Search base.
ServerAddress	String	Server.
UserLoginAttribute	String	User login attribute: uid:cn
LDAPRoleGroups	Object	LDAP role group.
GroupName	String	Group name.
GroupDomain	String	Group domain name.
GroupLoginInterface	Object	Access permission: ● KVM ● VMedia
GroupRole	String	Role group permission: ● Administrator ● Operator ● ReadOnly
MemberId	Number	Role group ID. Range: 0–4.

8.15 Modifying the LDAP Information

Function

Modify the current LDAP information about a server.

Syntax

- Operation Type: PATCH

- URL: *https://device_ip/redfish/v1/AccountService/LdapService/Ldap-Controllers/LDAP*
- Request Header:

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

- Request Message Body:

```
{
    "BindDN": BindDN_value,
    "CommonNameType": CommonNameType_value,
    "EncryptionType": EncryptionType_value,
    "LDAPAuthenticationEnable": LDAPAuthenticationEnable_value,
    "Password": Password_value,
        "Port": Port_value,
    "SearchBase": SearchBase_value,
    "ServerAddress": ServerAddress_value,
    "UserLoginAttribute": UserLoginAttribute_value
    "LDAPRoleGroups": [
    {
        "GroupDomain": GroupDomain_value,
        "GroupLoginInterface": GroupLoginInterface_value,
        "GroupName": GroupName_value,
        "GroupRole": GroupRole_value,
        "MemberId": MemberId_value
        }
    ]
}
}
```

Description

For a description of the parameters for modifying the current LDAP information, refer to Table 8-27.

Table 8-27 Parameter Descriptions for Modifying the Current LDAP 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 */redfish/v1/SessionService/Sessions*.
BindDN_value	String	Bound DN.
CommonName-Type_value	String	Common name type: ● IP

Parameter	Description	Value
		• FQDN
Encryption-Type_value	String	Encryption type, options: • NoEncryption • SSL
LDAPAuthenticatio-nEnable_value	Boolean	Whether LDAP authentication is enabled.
Password_value	String	Password.
Port_value	Number	Port number.
SearchBase_value	String	Search base.
ServerAddress_val-ue	String	Server address.
UserLoginAttribut-e_value	String	User login attribute.
LDAPRoleGroups	Object	Role set
GroupDomain_val-ue	String	Group domain
GroupLoginInter-face	Object	Role group permission: • KVM • VMedia
GroupName_value	String	Group name. If it is set to null, the role group is deleted.
GroupRole_value	String	Role group permission: • Administrator • Operator • ReadOnly • null If this parameter is set to null, null is dis-played.
MemberId_value	Number	Role group ID. Range: 0–4.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers/LDAP
```

- Request Header:

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

- Request Message Body:

```
{
    "BindDN": "cn=admin,dc=ldapdomain,dc=com",
    "CommonNameType": "IP",
    "EncryptionType": "NoEncryption",
    "LDAPAuthenticationEnable": true,
    "LDAPRoleGroups": [
    {
        "GroupDomain": "ou=testgroup,dc=ldapdomain,dc=com",
        "GroupLoginInterface": ["KVM","VMedia"],
        "GroupName": "sdf",
        "GroupRole": "Operator",
        "MemberId": 0
    }
    ],
    "Password": "Superuser9!",
    "Port": 392,
    "SearchBase": "ou=login,dc=domain,dc=com",
    "ServerAddress": "192.168.5.15",
    "UserLoginAttribute": "uid"
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#AccountService.LdapService.LdapControllers.
                       LDAP",
    "@odata.etag": "W/\"946731727\"",
    "@odata.id": "/redfish/v1/AccountService/LdapService/LdapControllers/LDAP",
    "@odata.type": "#LdapCollection.LDAP",
    "BindDN": "cn=admin,dc=ldapdomain,dc=com",
    "CommonNameType": "IP",
    "EncryptionType": "NoEncryption",
    "LDAPAuthenticationEnable": true,
    "LDAPRoleGroups": [
    {
        "GroupDomain": "ou=testgroup,dc=ldapdomain,dc=com",
        "GroupLoginInterface": ["KVM","VMedia"],
        "GroupName": "sdf",
        "GroupRole": "Operator",
```

```
        "MemberId": 0
    },
    {
        "GroupDomain": "ou=testgroup,dc=ldapdomain,dc=com",
        "GroupLoginInterface": ["KVM"],
        "GroupName": "sdfs",
        "GroupRole": "Operator",
        "MemberId": 1
    }
    ],
    "Name": "LDAP",
    "Password": null,
    "Port": 392,
    "SearchBase": "ou=login,dc=domain,dc=com",
    "ServerAddress": "192.168.5.15",
    "UserLoginAttribute": "uid"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you modify the current LDAP information, refer to Table 8-28.

Table 8-28 Output Description for Modifying the Current LDAP Information

Field	Type	Description
@odata.context	String	OData description of the LDAP information model.
@odata.id	String	Access path of the LDAP information node.
@odata.type	String	LDAP information resource type.
Name	String	Name of the LDAP information.
Password	Object	Password. It is displayed as null when queried.
BindDN	String	Bound DN.
CommonNameType	String	Common name type: ● IP ● FQDN
EncryptionType	String	Encryption type, options: ● NoEncryption ● SSL

Field	Type	Description
		• StartTLS
LDAPAuthenticationEnable	Boolean	Whether LDAP authentication is enabled.
Port	Number	Port number.
SearchBase	String	Search base.
ServerAddress	String	Server address.
UserLoginAttribute	String	User login attribute: uid:cn
LDAPRoleGroups	Object	LDAP role group.
GroupName	String	Group name.
GroupDomain	String	Group domain name.
GroupLoginInterface	Object	Access permission: • KVM • VMedia
GroupRole	String	Role group permission: • Administrator • Operator • ReadOnly
MemberId	Number	Role group ID. Range: 0–4.

Chapter 9
Operations on EventService Resources

Table of Contents

Querying the EventService Resource....574
Querying the Event Subscription Resource Collection....577
Creating an Event Subscription Resource....579
Querying an Event Subscription Resource....583
Modifying an Event Subscription Resource....585
Deleting an Event Subscription Resource....589
Querying the Alarm Resource Collection....590
Querying the Current Alarm Resource Collection....593
Querying the Current Alarm Resource....595
Deleting the Current Alarm Resource....597
Querying the Current Alarm Event Resource Collection....598
Modifying an Event Service Resource....602
Resuming an Event Subscription Resource....604
Clearing Historical Alarms in Batches....607

Figure 9-1 shows the path requirements for the Redfish EventService resources supported by VANTAGEO servers.

Figure 9-1 EventService Resource Path Requirements

For a description of properties of EventService resources and operations supported by the properties, refer to Table 9-1.

Table 9-1 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	Status of the specified EventService resource.	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
	Actions	Operations that can be performed on event resources.	GET
	#EventService.SubmitTestEvent	Submits a test event.	GET
	target	Path to send a test event operation.	GET
	Oem.Public	-	GET
	Alarms	-	GET
	CurrentAlarms	-	GET
/redfish/v1/EventService/Subscriptions	Id	ID of the specified event subscription resource.	POST
	Name	Name of the event subscription resource collection.	GET
	Destination	Valid HTTPS destination address.	POST
	EventTypes	Types of events to be monitored.	POST
	context	Event subscription context information.	POST
	protocal	Protocol used for event subscription. It must be Redfish in this version.	POST

URL	Property	Description	Operation
	MessageIds	(Optional) Message ID matching list for event subscription. Combination of valid message IDs defined in the event registry.	POST
	OriginResources	Event source list, which matches the event subscription ID list. Combination of valid resource URIs.	POST
	HttpHeaders	Event subscription HTTP header, which is displayed as null when being queried.	POST
	retry_policy	Retry policy used in case of event subscription failure, optional.	POST
	Status	Current event subscription status.	POST
	Members@odata.count	Number of event subscription resource members.	GET
	Members	Event subscription resource list.	GET
/redfish/v1/EventService/Subscriptions/subscription_id	Id	ID of the event subscription resource.	GET
	Name	Name of the event subscription resource.	GET
	Destination	Destination event service URI.	GET
	EventTypes	Type of event to be submitted.	GET
	context	Event subscription context information.	GET/ PATCH
	protocal	Protocol used for event subscription.	GET/ PATCH
	MessageIds	Submitted message ID list.	GET/ PATCH
	OriginResources	Event source list.	GET/ PATCH
	Actions	-	GET/ PATCH
	EventDestination.ResumeSubscription	Resumes event subscription.	GET/ PATCH

URL	Property	Description	Operation
	target	URL that invokes event subscription resumption.	GET/ PATCH
	HttpHeaders	HTTP Headers, for example, GET Object is empty for an authentication message.	GET/ PATCH
	DeliveryRetryPolicy	Retry policy for event subscription delivery failure.	GET/ PATCH
	Status	Current event subscription status.	GET/ PATCH
/redfish/v1/EventService/Alarms?$skip=skip_value&$top=top_value	Id	ID of the alarm resource collection.	GET
	Name	Name of the alarm resource collection.	GET
	Members@odata.count	Number of members in the alarm resource collection.	GET
	Members	List of members in the alarm resource collection.	GET
	AlarmId	Alarm ID.	GET
	AlarmCode	Code of the alarm.	GET
	AlarmLevel	Level of the alarm.	GET
	AlarmFlag	Flag of the alarm.	GET
	CrcCode	CRC of the alarm.	GET
	TimeStamp	Timestamp when an alarm is generated.	GET
	Message	Alarm information.	GET
/redfish/v1/EventService/CurrentAlarms	Id	ID of the current-alarm resource collection.	GET
	Name	Name of the current-alarm resource collection.	GET
	Members@odata.count	Number of members in the current-alarm resource collection.	GET
	Members	List of members in the current-alarm resource collection.	GET

URL	Property	Description	Operation
	AlarmId	ID of a current alarm.	GET
	AlarmCode	Code of a current alarm.	GET
	AlarmLevel	Level of a current alarm.	GET
	TimeStamp	Timestamp when a current alarm is generated.	GET
	Message	Information about a current alarm.	GET
/redfish/v1/EventService/CurrentAlarms/alarm_id	Id	ID of the specified current alarm resource.	GET
	Name	Name of the specified current alarm.	GET
	Description	Description of the specified current alarm.	GET
	AlarmCode	Code of the specified current alarm.	GET
	AlarmLevel	Level of the specified current alarm.	GET
	TimeStamp	Timestamp when the specified current alarm is generated.	GET
	Message	Information about the specified current alarm.	GET
/redfish/v1/EventService/CurrentAlertEvents	Id	ID of the current alarm event 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	List of members in the current alarm event resource collection.	GET
	EventId	Alarm event ID.	GET
	EventType	Event types.	GET
	EventTimestamp	Event occurrence time.	GET
	Severity	Alarm severity level.	GET
	Message	Alarm name.	GET
	Oem.Public	-	GET

URL	Property	Description	Operation
	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 component.	GET
	objectName	Name of the alarm component.	GET
	objectType	Type of alarm component.	GET
	locationInfo	Alarm location information.	GET
	Addinfo	Additional alarm information.	GET
/redfish/v1/EventService/Subscriptions/subscriptions_id/Actions/EventDestination.ResumeSubscription	code	ID of the specified message in the message registry.	GET
	message	Readable error message corresponding to the one in the message registry.	GET
	@odata.type	OData description of the message resource.	GET
	MessageId	Message ID.	GET
	RelatedProperties	Message-related properties.	GET
	Message	Details.	GET
	MessageArgs	Message arguments.	GET
	Severity	Severity level.	GET
	Resolution	Recommended solution.	GET

9.1 Querying the EventService Resource

Function

Query the EventService resource of a server.

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 9-2.

Table 9-2 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1596264393\"",
    "@odata.id": "/redfish/v1/EventService",
    "@odata.type": "#EventService.v1_0_6.EventService",
```

```
    "Actions":
    {
        "#EventService.SubmitTestEvent":
        {
            "EventType@Redfish.AllowableValues":
            [
                "StatusChange",
                "ResourceUpdated",
                "ResourceAdded",
                "ResourceRemoved",
                "Alert"
            ],
            "target": "/redfish/v1/EventService/Actions/EventService.SubmitTestEvent"
        }
    },
    "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"}
        }
    },
    "ServiceEnabled": true,
    "Status": {"Health": "OK", "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 9-3.

Table 9-3 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.
Id	String	ID of the EventService resource.
Name	String	Name of the EventService resource.
Status	Object	Status of the specified UpdateService resources, including: ● State: enabling status ● Health: health status
ServiceEnabled	Boolean	Whether event reporting is enabled.
DeliveryRetryAttempts	Number	Maximum number of retries for delivering event subscriptions.
DeliveryRetryIntervalSeconds	Number	Interval (in seconds) at which an event is resent upon a failure.
EventTypesForSubscription	Enumeration	Type of events that can be subscribed to. The ranges are the combinations of the following valid values: ● StatusChange: resource status change event ● ResourceUpdated: resource update event ● ResourceAdded: resource addition event ● ResourceRemoved: resource removal event ● Alert: alarming event
Subscriptions	Object	Navigation resource of the event target resource collection.
@odata.id	String	Access path of the specified event object resource.
Actions	Object	Operations that can be performed on the event service.
#EventService.SubmitTestEvent	Object	Submits a test event.

Field	Type	Description
target	String	Path to submit a test event operation.
@Redfish.ActionInfo	String	Path to query the information about the submitted test event operation.
Oem.Public	Object	-
Alarms	Object	-

9.2 Querying the Event Subscription Resource Collection

Function

Query 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 9-4.

Table 9-4 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 */redfish/v1/SessionService/Sessions*.
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.etag": "W/\"1569584551\"",
    "@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 9-5.

Table 9-5 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.
Id	String	ID of the event resource collection.
Name	String	Name of the event subscription resource collection.
Members@odata.count	Number	Number of event subscription resource members.
Members	Event subscription resource list.	-

Field	Type	Description
@odata.id	String	Access path of a single event subscription resource node.

9.3 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": protocal,
    "MessageIds": message_ids,
    "OriginResources": origin_resources
}
```

Description

For the parameter descriptions for creating an event subscription resource, refer to Table 9-6.

Table 9-6 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 */redfish/v1/SessionService/Sessions*.
event_destination	Event subscription destination address.	Valid HTTP/HTTPS destination address.

Parameter	Description	Value
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: alarm event
http_headers	Event subscription HTTP header parameters, which are carried when an event is reported.	Optional. The value shall comply with the key:value format.
context	Event subscription context information.	String
protocal	Protocol used for 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.
retry_policy	Retry policy for event subscription failure.	Optional. Options: ● TerminateAfterRetries: deletes subscription information if the number of retries exceeds the threshold. ● SuspendRetries: suspends subscription information if the number of retries exceeds the threshold. Default: SuspendRetries. ● RetryForever: continues retrying subscription all the time.

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://10.41.168.114:9001/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": "SuspendRetries",
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#EventDestination.EventDestination",
    "@odata.etag": "W/\"1581524977\"",
    "@odata.id": "/redfish/v1/EventService/Subscriptions",
    "@odata.type": "#EventDestination.v1_2_2.EventDestination",
    "Context": "event subscription context string",
    "Destination": "http://10.41.168.114:9001/redfish/test/",
    "EventTypes": [
        "Alert"
    ],
    "DeliveryRetryPolicy": "SuspendRetries",
    "HttpHeaders": null,
    "Id": 1,
    "MessageIds": [
        "iBMCEvents.2.0.PsPredicFailureInfo"
    ],
```

```
    "Name": "Subscription 1",
    "OriginResources": [
        "/redfish/v1/Chassis/1/Power#/PowerSupplies/0"
    ],
    "OriginResources@odata.count": 1,
    "Protocol": "Redfish",
    "Status": "Enabled"
}
```


- Status Code: 201

Output Description

For the output descriptions for creating the event subscription resource, refer to Table 9-7.

Table 9-7 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 specified event subscription resource.
Name	String	Name of the event subscription resource.
Destination	String	Valid http/https destination address.
EventTypes	Object Array	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: alarm event
context	String	Event subscription context information.
protocal	String	Protocol used for event subscription. It must be Redfish.

Field	Type	Description
MessageIds	Object Array	Message ID matching list of the event subscription. Optional parameter. Combination of valid message IDs defined in the event registry.
OriginResources	Object Array	Event source list. Combination of valid resource URIs.
HttpHeaders	String	Event subscription HTTP header. It is displayed as null when queried.
retry_policy	String	Retry policy for event subscription failure. Optional. Options: ● TerminateAfterRetries: deletes subscription information if the number of retries exceeds the threshold. ● SuspendRetries (default): suspends subscription information if the number of retries exceeds the threshold. ● RetryForever: continues retrying subscription all the time.
Status	String	Current event subscription status. ● Enabled ● Disabled ● StandbyOffline: suspended when the number of times that an event is reported exceeds the threshold.

9.4 Querying an Event Subscription Resource

Function

Query an event subscription resource.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/EventService/Subscriptions/id*
- Request Header:

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

- Request Message Body: None

Description

For the parameter descriptions for querying an event subscription resource, refer to Table 9-8.

Table 9-8 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1581524977\"",
    "@odata.id": "/redfish/v1/EventService/Subscriptions",
    "@odata.type": "#EventDestination.v1_2_2.EventDestination",
    "Context": "event subscription context string",
    "Destination": "https://10.41.168.114:9001/redfish/test/",
    EventTypes": [ "Alert"],
    "HttpHeaders": null,
    "Id": 1,
    "MessageIds": [ "iBMCEvents.2.0.PsPredicFailureInfo"],
    "Name": "Subscription 1",
    "OriginResources": ["/redfish/v1/Chassis/1/Power#/PowerSupplies/0"],
    "OriginResources@odata.count": 1,
    "Protocol": "Redfish"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query the event subscription resource, refer to Table 9-9.

Table 9-9 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	Event subscription destination address.
EventTypes	String	Event type for event subscription monitoring.
context	String	Event subscription context information.
protocal	String	Protocol used for event subscription.
MessageIds	Array	Message ID matching list of the event subscription.
OriginResources	Array	Event source list.
Actions	Object	-
EventDestination.ResumeSub-scription	Object	Resumes event subscription.
target	String	URL that invokes event subscription resumption.
HttpHeaders	Object	HTTP header parameters for event subscription.
DeliveryRetryPolicy	String	Retry policy for event subscription failure.
Status	String	Current event subscription status.

9.5 Modifying an Event Subscription Resource

Function

Modify an event subscription resource.

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": retry_policy
}
```

Description

For a description of the parameters for modifying an event subscription resource, refer to Table 9-10.

Table 9-10 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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
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.
http_headers	Event subscription HTTP header parameters, which are carried when an event is reported.	The value shall comply with the *key:value* format. During configuration, the previous information can be replaced directly.
context	Event subscription context information.	String

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":"RetryForever"
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#EventDestination.EventDestination",
    "@odata.etag": "W/\"1581524977\"",
    "@odata.id": "/redfish/v1/EventService/Subscriptions",
    "@odata.type": "#EventDestination.v1_2_2.EventDestination",
    "Actions": {
        "#EventDestination.ResumeSubscription": {
            "target": "/redfish/v1/EventService/Subscriptions/2/Actions/
             EventDestination.ResumeSubscription"
        }
    },
    "Context": "event subscription context string",
    "DeliveryRetryPolicy":"RetryForever"
    "Destination": "https://10.41.168.114:9001/redfish/test/",
    "EventTypes": [
        "Alert"
    ],
    "HttpHeaders": null,
    "Id": 1,
    "MessageIds": [
        "iBMCEvents.2.0.PsPredicFailureInfo"
    ],
    "Name": "Subscription 1",
    "OriginResources": [
        "/redfish/v1/Chassis/1/Power#/PowerSupplies/0"
```

```
    ],
    "OriginResources@odata.count": 1,
    "Protocol": "Redfish",
    "Status": "Enabled"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you modify an event subscription resource, refer to Table 9-11.

Table 9-11 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	Event subscription destination address.
EventTypes	String	Event type for event subscription monitoring.
context	String	Event subscription context information.
protocal	String	Protocol used for event subscription.
MessageIds	Array	Message ID matching list of the event subscription.
OriginResources	Array	Event source list.
Actions	Object	-
EventDestination.ResumeSub-scription	Object	Resumes event subscription.
target	String	URL that invokes event subscription resumption.
HttpHeaders	Object	HTTP header parameters for event subscription.
DeliveryRetryPolicy	String	Retry policy for event subscription failure.
Status	String	Current event subscription status.

9.6 Deleting an Event Subscription Resource

Function

Delete an event subscription resource.

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 9-12.

Table 9-12 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 GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.

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

9.7 Querying the Alarm Resource Collection

Function

Query the alarm resource collection.

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 the parameter descriptions for querying the alarm resource collection, refer to Table 9-13.

Table 9-13 Parameter Descriptions for Querying the Alarm Resource Collection

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 GET request for authentication.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
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 member length 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=5
```

- Request Header:

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

- Request Message Body: None
- Response Example:


```
{
    "@odata.context": "/redfish/v1/$metadata#AlarmsCollection.AlarmsCollection",
    "@odata.etag": "W/\"1596263470\"",
    "@odata.id": "/redfish/v1/EventService/Alarms",
    "@odata.type": "#AlarmsCollection.v1_0_0.AlarmsCollection",
    "Description": "Collection of Alarms",
    "Id": "Alarms",
    "Members":
    [{
        "AlarmCode": 30728,
        "AlarmFlag": 2,
        "AlarmId": "16685",
        "AlarmLevel": "Major",
        "CrcCode": 3548344972,
        "Message": "CPU1_PVCCIN is lower than lower major threshold.",
        "TimeStamp": 1596090864
    },
    {
        "AlarmCode": 23051,
        "AlarmFlag": 2,
        "AlarmId": "16684",
        "AlarmLevel": "Major",
        "CrcCode": 3725448339,
        "Message": "PSU_STATUS_01 status is absent.",
        "TimeStamp": 1596090864
    },
    {
        "AlarmCode": 30728,
        "AlarmFlag": 1,
        "AlarmId": "16683",
        "AlarmLevel": "Major",
        "CrcCode": 3548344972,
        "Message": "CPU1_PVCCIN is lower than lower major threshold.",
```

```
            "TimeStamp": 1596087424
        },
        {
            "AlarmCode": 23051,
            "AlarmFlag": 1,
            "AlarmId": "16682",
            "AlarmLevel": "Major",
            "CrcCode": 3725448339,
            "Message": "PSU_STATUS_01 status is absent.",
            "TimeStamp": 1596087420
        },
        {
            "AlarmCode": 30728,
            "AlarmFlag": 2,
            "AlarmId": "16681",
            "AlarmLevel": "Major",
            "CrcCode": 1089966855,
            "Message": "CPU1_PVCCIN is lower than lower major threshold.",
            "TimeStamp": 1596087415
        }],
        "Members@odata.count": 1000,
        "Name": "Alarms Collection"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query the alarm resource collection, refer to Table 9-14.

Table 9-14 Output Descriptions for Querying of the Alarm Resource Collection

Field	Type	Description
@odata.context	String	OData description of the alarm resource collection model.
@odata.id	String	Type of alarm resource collection.
@odata.type	String	Access path of the alarm resource collection.
Id	String	ID of the alarm resource collection.
Name	String	Name of the alarm resource collection.
Members@odata.count	Number	Number of alarm resource members.

Field	Type	Description
Members	Event subscription resource list.	-
AlarmId	String	Alarm ID.
AlarmCode	Number	Code of the alarm.
AlarmLevel	String	Level of the alarm.
AlarmFlag	Number	Flag of the alarm. ● 1: alarm event ● 2: alarm clearance event ● 3: alarm notification event
CrcCode	Number	CRC of the alarm.
TimeStamp	Number	Alarm generation timestamp.
Message	String	Alarm information.

9.8 Querying the Current Alarm Resource Collection

Function

Query the current alarm resource collection.

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 9-15.

Table 9-15 Parameter Descriptions for Querying of 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1607004360\"",
    "@odata.id": "/redfish/v1/EventService/CurrentAlarms",
    "@odata.type": "#CurrentAlarmsCollection.v1_0_0.CurrentAlarmsCollection",
    "Description": "Collection of CurrentAlarms",
    "Id": "CurrentAlarms",
    "Members":
    [{
        "@odata.id": "/redfish/v1/EventService/CurrentAlarms/2152",
        "AlarmCode": 30839,
        "AlarmId": "2152",
        "AlarmLevel": "Major",
        "Message": "Abnormal reading of ambient temperature (location:INPUT_TEMP).",
        "TimeStamp": 1607004276
    },
    {
        "@odata.id": "/redfish/v1/EventService/CurrentAlarms/2153",
        "AlarmCode": 30731,
        "AlarmId": "2153",
        "AlarmLevel": "Major",
        "Message": "CPU1_PVCCIN is more than upper major threshold.",
        "TimeStamp": 1607004280
    }],
    "Members@odata.count": 2,
    "Name": "CurrentAlarms Collection"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query the current alarm resource collection, refer to Table 9-16.

Table 9-16 Output Descriptions for Querying of 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.
Id	String	ID of the current alarm resource collection.
Name	String	Name of the current alarm resource collection.
Members@odata.count	Number	Number of alarm resource members.
Members	Event subscription resource list.	-
@odata.id	String	Access path of the specified alarm resource.
AlarmId	String	ID of the current alarm.
AlarmCode	Number	Code of the current alarm.
AlarmLevel	String	Level of the current alarm.
TimeStamp	Number	Alarm generation timestamp.
Message	String	Information about the current alarm.

9.9 Querying the Current Alarm Resource

Function

Query the current alarm resource.

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 9-17.

Table 9-17 Parameter Descriptions for Querying of 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 */redfish/v1/SessionService/Sessions*.
alarm_id	alarm_id of the current alarm.	It can be obtained from the upper-layer 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.etag": "W/\"1607004360\"",
    "@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

For a description of the output returned when you query the current alarm resource, refer to Table 9-18.

Table 9-18 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	String	ID of the current alarm resource.
Name	String	Name of the current alarm resource.
Description	String	Description of the current alarm resource.
AlarmCode	Number	Code of the current alarm.
AlarmLevel	String	Level of the current alarm.
TimeStamp	Number	Alarm generation timestamp.
Message	String	Information about the current alarm.

9.10 Deleting the Current Alarm Resource

Function

Delete the current alarm resource.

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 9-19.

Table 9-19 Parameter Descriptions for Deleting the Current 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 alarm.	-
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 */redfish/v1/SessionService/Sessions*.

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
- Status Code: 204

Output Description

None

9.11 Querying the Current Alarm Event Resource Collection

Function

Query the current alarm event resource collection.

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 9-20.

Table 9-20 Parameter Descriptions for Querying of 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1608619822\"",
    "@odata.id": "/redfish/v1/EventService/CurrentAlertEvents",
    "@odata.type":
    "#CurrentAlertEventsCollection.v1_0_0.CurrentAlertEventsCollection",
    "Description": "Collection of CurrentAlertEvents",
    "Id": "CurrentAlertEvents",
    "Members":
    [{
        "EventId": "18722",
        "EventTimestamp": "2020-12-14 11:12:19",
        "EventType": "Alert",
        "Message": "Power unit absent",
```

```
    "Oem":
    {
        "Public":
        {
            "Addinfo": "PSU_STATUS_01 status is absent.",
            "alarmStatus": 1,
            "locationInfo": "PSU 1",
            "neName": "a1",
            "neType": "server",
            "neUID": "",
            "objectName": "PSU 1",
            "objectType": "PSU",
            "objectUID": 1,
            "specificProblem": "Power unit absent",
            "specificProblemID": "23051"
        }
    },
    "Severity": "Major"
},
{
    "EventId": "18723",
    "EventTimestamp": "2020-12-14 11:12:23",
    "EventType": "Alert",
    "Message": "Voltage is lower than lower-critical threshold",
    "Oem":
    {
        "Public":
        {
            "Addinfo": "CPU1_PVCCIN is lower than lower major threshold.",
            "alarmStatus": 1,
            "locationInfo": "CPU 1",
            "neName": "a1",
            "neType": "server",
            "neUID": "",
            "objectName": "CPU 1",
            "objectType": "CPU",
            "objectUID": 1,
            "specificProblem": "Voltage is lower than lower-critical threshold",
            "specificProblemID": "30728"
        }
    },
    "Severity": "Major"
},
{
```

```
        "EventId": "18726",
        "EventTimestamp": "2020-12-22 01:22:07",
        "EventType": "Alert",
        "Message": "The hard disk is abnormal",
        "Oem":
        {
            "Public":
            {
                "Addinfo": "hard disk 1 smart is abnormal.",
                "alarmStatus": 1,
                "locationInfo": "Disk 1",
                "neName": "a1",
                "neType": "server",
                "neUID": "",
                "objectName": "Disk 1",
                "objectType": "Disk",
                "objectUID": "1",
                "specificProblem": "The hard disk is abnormal",
                "specificProblemID": "5797"
            }
    },
    "Severity": "Major"
    }],
    "Members@odata.count": 3,
    "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 9-21.

Table 9-21 Output Descriptions for Querying of 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.
Id	String	ID of the current alarm event resource collection.

Field	Type	Description
Name	String	Name of the current alarm event resource collection.
Members@odata.count	Number	Number of alarm event resource members.
Members	Event subscription resource list.	-
EventId	String	Alarm event ID.
EventType	String	Alarm type.
EventTimestamp	String	Event occurrence time.
Severity	String	Alarm level.
Message	String	Alarm name.
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).
neType	String	Type of alarm device.
objectUID	String	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.

9.12 Modifying an Event Service Resource

Function

Modify the event service resource.

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
}
```

Description

For a description of the parameters for modifying an event service resource, refer to Table 9-22.

Table 9-22 Parameter Descriptions for Modifying an Event Service Resources

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
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.
retry_attempts	Event subscription HTTP header parameters, which are carried when an event is reported.	Maximum number of event subscription retries upon failures, range: 3–1440.
retry_seconds	Event subscription context information.	Number of seconds between retry attempts to send any given event, range: 60 – 3600.

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/EventService
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body:

```
{
    "DeliveryRetryAttempts": 5,
    "DeliveryRetryIntervalSeconds": 70
}
```

- Response Example: None
- Status Code: 204

Output Description

None

9.13 Resuming an Event Subscription Resource

Function

Resume an event subscription resource.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/EventService/Subscriptions/subscriptions_id/Actions/EventDestination.ResumeSubscription*
- Request Header:

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

- Request Message Body:

```
{
    "DeliverBufferedEventDuration":set_value
}
```

Description

For a description of the parameters for resuming an event subscription resource, refer to Table 9-23.

Table 9-23 Parameter Descriptions for Resuming an Event Subscription 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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
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.
set_value	After the subscription is resumed, the server resends the unsent events buffered for the subscription. The sent events must meet the time range specified by this parameter. The events beyond the range are not sent.	ISO-8601-compliant time.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/EventService/Subscriptions/1/Actions/EventDestination.R esumeSubscription
```

- Request Header:

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

- Request Message Body:

```
{
    "DeliverBufferedEventDuration": "PT2H"
}
```

- 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.1.0.Success",
                "RelatedProperties": [],
                "Message": "Successfully Completed Request",
                "MessageArgs": [],
                "Severity": "OK",
                "Resolution": "None"
            }
        ]
     }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you resume an event subscription resource, refer to Table 9-24.

Table 9-24 Output Descriptions for Resuming an Event Subscription Resource

Field	Type	Description
code	Character string	ID of the specified message in the message registry.
message	Character string	Readable error message corresponding to the one in the message registry.
@odata.type	Character string	OData description of the message resource.
MessageId	Character string	Message ID.
RelatedProperties	Array	Message-related properties.
Message	Character string	Details.
MessageArgs	Array	Message arguments.
Severity	Character string	Severity level. Severity levels supported by Redfish, including: ● OK

Field	Type	Description
		• Warning • Critical
Resolution	Character string	Recommended solution.

9.14 Clearing Historical Alarms in Batches

Function

Clear historical alarms of a server in batches.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/EventService/Actions/EventService.ClearHistoryAlarm*
- Request Header:

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

- Request Message Body:

```
{
    "KeepSinceDatetime":set_value
}
```

Description

For a description of the parameters for clearing historical alarms in batches, refer to Table 9-25.

Table 9-25 Parameter Descriptions for Clearing Historical Alarms in Batches

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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
set_value	Time. The historical alarms generated before the specified time are cleared.	ISO-8601-compliant time.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/EventService/Actions/EventService.ClearHistoryAlarm
```

- Request Header:

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

- Request Message Body:

```
{
    "KeepSinceDatetime": "2023-09-09T12:34:56"
}
```

- Response Example: None
- Status Code: 204

Output Description

None

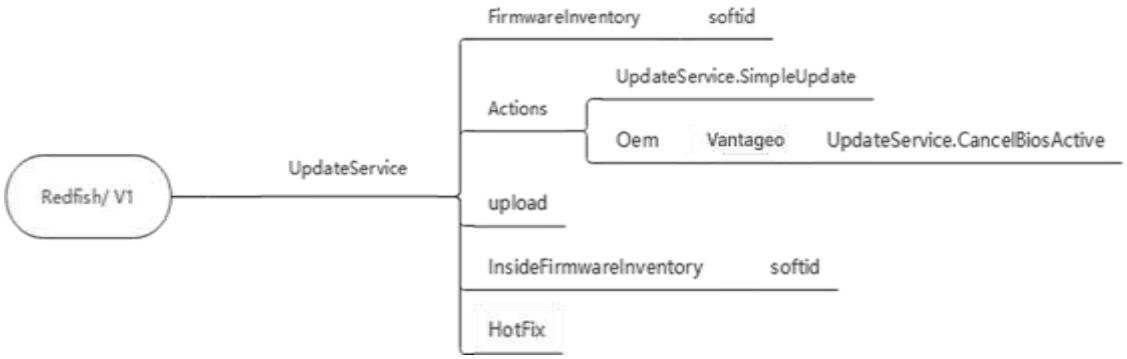
Chapter 10
Operations on UpdateService Resources

Table of Contents

Querying Information About the UpdateService Resource 613
Querying Information About the Updatable Firmware Resource Collection 616
Querying Information About a Specified Updatable Firmware Resource 618
Updating Firmware 621
Uploading a File 624
Canceling the Activation of the BIOS Changes 625
Querying Information About the Internal Firmware Resource Collection 627
Querying Information About a Specified Internal Firmware Resource of a Server 629
Querying the Information About the Hotfix Resource Collection 631
Loading or Removing Hotfixes 634

Figure 10-1 shows the path requirements for the Redfish UpdateService resources supported by VANTAGEO servers.

Figure 10-1 UpdateService Resource Path Requirements



For a description of the properties of UpdateService resources and the operations supported by the properties, refer to Table 10-1.

Table 10-1 Descriptions of UpdateService Resources Properties

URL	Property	Description	Operation
/redfish/v1/UpdateService	Id	ID of an UpdateService resource.	GET
	Name	Name of the UpdateService resource.	GET
	Description	Description of the UpdateService resource.	GET
	Status	Health status of the UpdateService resource.	GET
	ServiceEnabled	Whether the UpdateService resource is enabled.	GET
	Actions	Available actions for the UpdateService resource.	GET/POST
	#UpdateService.SimpleUpdate	Performs an 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
	Oem	Customized information about the specified firmware.	GET
	Public	Service update.	GET
	InsideFirmwareInventory	Link to the internal firmware resource list.	GET
	UpdateInformation	Update information.	GET
	UpdateComponent	Update phase.	GET
	UpdateDetail	Update details.	GET
	UpdatePercentage	Update progress.	GET
	UpdateStatus	Update status.	GET

URL	Property	Description	Operation
/redfish/v1/UpdateService/FirmwareInventory	Name	Name of the updatable firmware resource collection.	GET
	Members@odata.count	Number of updatable firmware resources.	GET
	Members	List of updatable firmware resources.	GET
	Description	Description of the updatable firmware resource collection.	GET
/redfish/v1/UpdateService/FirmwareInventory/softid	Id	ID of the specified updatable firmware resource.	GET
	Name	Name of the specified updatable firmware resource.	GET
	Status	Status of the specified updatable firmware resource.	GET
	Version	Version of the specified updatable firmware resource.	GET
	Updatable	Update status of the specified updatable firmware resource.	GET
	SoftwareId	Firmware ID.	GET
	VerAuxiliaryInfo	Auxiliary information about the version.	GET
/redfish/v1/UpdateService/Actions/UpdateService.SimpleUpdate	UpdateInformation	Firmware resource update information.	POST
	target	Path of the firmware update service.	POST
/redfish/v1/UpdateService/InsideFirmwareInventory	Name	Name of the internal firmware resource collection.	GET
	Members@odata.count	Number of internal firmware resources.	GET

URL	Property	Description	Operation
	Members	List of members in the internal firmware resource collection.	GET
/redfish/v1/UpdateService/InsideFirmwareInventory/softid	Description	Description of the internal firmware resource collection.	GET
	Id	ID of an internal firmware resource.	GET
	Name	Internal firmware resource name.	GET
	SoftwareId	Firmware ID.	GET
	Status	Status of the specified UpdateService resource.	GET
	InsideVersion	Internal firmware version.	GET
	Updateable	Whether the software can be updated.	GET
/redfish/v1/UpdateService/HotFix	Id	ID of the hotfix resource collection.	GET
	Name	Name of the hotfix resource collection.	GET
	Info	Hotfix list information.	GET
	des	Process description of a hotfix.	GET
	id	Process ID of a hotfix.	GET
	module	Process module of a hotfix.	GET
	path	File path of a hotfix.	GET
	proc	Process name of a hotfix.	GET
	HotfixStatus	Hotfix status.	GET
	Version	Version number of a hotfix.	GET
	MessageId	Message ID.	POST
	RelatedProperties	Message-related properties.	POST

URL	Property	Description	Operation
	Message	Details.	POST
	MessageArgs	Message arguments.	POST
	Severity	Severity level.	POST
	Resolution	Recommended solution.	POST

10.1 Querying Information About the UpdateService Resource

Function

Query information about the UpdateService resource.

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 about the UpdateService resource, refer to Table 10-2.

Table 10-2 Parameter Descriptions for Querying Information About the UpdateService 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"1593736964\"",
    "@odata.id": "/redfish/v1/UpdateService",
    "@odata.type": "#UpdateService.v1_2_1.UpdateService",
    "Actions": {
        "#UpdateService.SimpleUpdate": {
            "@Redfish.ActionInfo": "/redfish/v1/UpdateService/SimpleUpdateActionInfo",
            "target": "/redfish/v1/UpdateService/Actions/UpdateService.SimpleUpdate"
        }
    },
    "Description": "Redfish Update Service",
    "FirmwareInventory": {
        "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory"
    },
    "Id": "UpdateService",
    "Name": "Update Service",
    "Oem": {
        "Public": {
            "InsideFirmwareInventory": {
                "@odata.id": "/redfish/v1/UpdateService/InsideFirmwareInventory"
            },
            "UpdateInformation": {
                "UpdateComponent": "",
                "UpdateDetail": "",
                "UpdatePercentage": 0,
                "UpdateStatus": ""
            }
        }
    },
    "ServiceEnabled": true,
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about the UpdateService resource, refer to Table 10-3.

Table 10-3 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 node.
@odata.type	String	Type of specified UpdateService resource.
Id	String	ID of the specified UpdateService resource.
Name	String	Name of the specified UpdateService resource.
Status	Object	Status of the specified UpdateService resource. ● State: enabling status ● Health: health status
ServiceEnabled	Boolean	Enabling status of the UpdateService resource.
Actions	Available actions for the UpdateService resource.	-
#UpdateService.SimpleUpdate	Object	Update operation.
@Redfish.ActionInfo	String	Path to query the information about the update operation.
target	String	Update operation path.
FirmwareInventory	Object	Link to the updatable firmware resource list.
@odata.id	String	Access path of the updatable firmware resource list.
Oem	Self-defined update status.	-
Public	Object	Update service.
InsideFirmwareInventory	Object	Link to the internal firmware list.
@odata.id	String	Access path of the internal firmware list.
UpdateInformation	Object	Update information.
UpdateComponent	String	Update phase.
UpdateDetail	String	Update details.

Field	Type	Description
UpdatePercentage	String	Update progress.
UpdateStatus	String	Update status.

10.2 Querying Information About the Updatable Firmware Resource Collection

Function

Query information about the updatable firmware resource collection of a server.

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 updatable firmware resource collection, refer to Table 10-4.

Table 10-4 Parameter Descriptions for Querying Information About the Updatable Firmware 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 */redfish/v1/SessionService/Sessions*.

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.etag": "W/\"946673874\"",
    "@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/BackupBMC"
        },
        {
            "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/ActiveBIOS"
        },
        {
            "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/BackupBIOS"
        },
        {
            "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/EPLD"
        },
        {
            "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/MainBoardFRU"
        },
        {
            "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/SubCardFRU2"
        },
        {
            "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/ChassisPsu1"
        },
        {
            "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/ChassisPsu2"
        },
        {
            "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/PCIeSlot1GPU"
        }
    ],
```

```
    "Members@odata.count": 10,
    "Name": "Firmware Inventory Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the updatable firmware resource collection, refer to Table 10-5.

Table 10-5 Output Descriptions for Querying Information About the Updatable Firmware Resource Collection

Field	Type	Description
@odata.context	String	OData description of the updatable firmware resource collection model.
@odata.id	String	Access path of the updatable firmware resource collection node.
@odata.type	String	Type of updatable firmware resource collection model.
Name	String	Name of the updatable firmware resource collection.
Members@odata.count	Number	Number of updatable firmware resources.
Members	Object List	List of updatable firmware resources.
Description	String	Description of the updatable firmware resource collection.

10.3 Querying Information About a Specified Updatable Firmware Resource

Function

Query information about a specified updatable firmware resource of a server.

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 updatable firmware resource of a server, refer to Table 10-6.

Table 10-6 Parameter Descriptions for Querying Information About a Specified Updatable Firmware 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 */redfish/v1/SessionService/Sessions*.
softid	ID of the updatable firmware resource.	It can be obtained from the updatable firmware resource collection.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/UpdateService/FirmwareInventory/MainBoardFRU
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
   "@odata.context": "/redfish/v1/$metadata#UpdateService/FirmwareInventory/Members
                     /$entity",
   "@odata.etag": "W/\"946668992\"",
   "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/MainBoardFRU",
   "@odata.type": "#SoftwareInventory.v1_2_0.SoftwareInventory",
   "Description": "MainBoardFRU",
   "Id": "MainBoardFRU",
   "Name": "MainBoardFRU",
   "Oem": {
       "Public": {
           "SupportActivateType": [
               "resetbmc"
           ]
```

```
        }
    },
    "SoftwareId": "MainBoardFRU",
    "Status": {
        "Health": "OK",
        "State": "Enabled"
        },
    "Updateable": true,
    "VerAuxiliaryInfo": null,
    "Version": "01.03.0008"
}
```


- Status Code: 200

Output Description

For a description of the output returned when you query information about a specified updatable firmware resource of a server, refer to Table 10-7.

Table 10-7 Output Descriptions for Querying Information About a Specified Updatable Firmware Resource

Field	Type	Description
@odata.context	String	OData description of the updatable firmware resource model.
@odata.id	String	Access path of the updatable firmware resource node.
@odata.type	String	Type of the updatable firmware resource.
Description	String	Description of the updatable firmware resource.
Id	String	ID of the updatable firmware resource.
Name	String	Name of the updatable firmware resource.
SupportActivateType	Array	Method for the updateable firmware resource to take effect. ● none ● resetbmc ● resethost ● poweroff ● dcpowercycle ● automatic
SoftwareId	String	Firmware ID.
Status	Object	Status of the specified UpdateService resource. ● State: enabling status

Field	Type	Description
		● Health: health status
Version	String	Firmware version.
Updatable	Boolean	Whether the Update Service can update this software ● true ● false
VerAuxiliaryInfo	String	Auxiliary information about the version.

10.4 Updating Firmware

Function

Update the firmware resource information about a server.

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:

```
{
    "ImageURI": filepath,
    "TransferProtocol": protocol
}
```

Parameters

For a description of the parameters for updating the firmware resource information, refer to Table 10-8.

Table 10-8 Parameter Descriptions for Updating the Firmware Resource Information

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	Authentication parameter of the request message.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/js

Parameter	Description	Value
filepath	Path of the update package.	URL of the update package. Maximum length: 256 characters. If local update is selected, the URL is /tmp/redfishUpload/image_name.
protocol	Protocol for downloading the update package.	HTTPS is used in most cases. For local update, this field is not required.
Oem	Vendor-defined network service.	-
Public	VANTAGEO-defined service.	-
ActiveMode	BIOS validation mode. This parameter is optional for BIOS update only.	If this parameter is set to **Immediately**, the BIOS configuration takes effect immediately no matter whether the host is powered on or off. During this process, the host is powered off. If this parameter is not configured, the BIOS configuration takes effect automatically during power-off.
RestoreCfgMode	Configuration restoration mode.	● Enable: restores configurations. ● Disable: inherits configurations. If this parameter is not configured, the original configurations are inherited.
UpgradePolicy	Upgrade policy, which is valid only for PSU upgrade.	● PowerOff: PSU can be upgraded only when the host is powered off. ● PowerOn: The PSU can be upgraded when the host is powered on. If this parameter is not set, the PSU can be upgraded only when the host is powered off.

Usage Guidelines

For how to query the update progress, refer to 10.1 Querying Information About the UpdateService Resource.

Example 1

- 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:

```
{
    "ImageURI":"https://10.10.10.10/bmc/BMC_2230-RE_SPLMA_A5_R_V03.05.0010.BIN",
    "TransferProtocol":"HTTPS"
}
```

- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#SimpleUpdate.SimpleUpdate",
    "@odata.etag": "W/\"946738823\"",
    "@odata.id": "/redfish/v1/UpdateService/Actions/SimpleUpdate",
    "UpdateInformation": {
    "target": "/redfish/v1/UpdateService"
    }
}
```

- Status Code: 202

Request Example 2:

- 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:

```
{
    "ImageURI": "https://10.10.10.10/bmc/BMC_2230-RE_SPLMA_A5_R_V03.05.0010.BIN",
    "TransferProtocol": "HTTPS",
    "Oem": {
        "Public": {
            "ActiveMode": "Immediately"
        }
    }
}
```

- Response Example: None
- Status Code: 202

Output Description

For a description of the output when you update the firmware resource information, refer to Table 10-9.

Table 10-9 Output Descriptions for Updating the Firmware Resource Information

Field	Type	Description
@odata.context	String	OData description of the firmware update resource model.
@odata.id	String	Path of the firmware update resource node.
UpdateInformation	Object	Firmware resource update information.
target	String	Path of the firmware update service.

10.5 Uploading a File

Function

Upload a file through the Redfish interface to the */tmp/redfishUpload* directory.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/UpdateService/upload*
- Request Header:

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

- Request Message Body (Form):

```
<form enctype="multipart/form-data" action=" https://device_ip/redfish/v1/UpdateService
/upload" method="POST">
<input name="image_file" type="file">
</form>
```

Parameters

For a description of the parameters for uploading a file, refer to Table 10-10.

Table 10-10 Parameter Descriptions for Uploading a File

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

Parameter	Description	Value
auth_value	Authentication parameter of the request message.	It can be obtained by creating a session through */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	Supported message formats: multipart and form-data

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/UpdateService/upload
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type:  multipart/form-data
```

- Request Message Body:

```
<form enctype="multipart/form-data" action=" https://device_ip/redfish/v1/UpdateService
/upload" method="POST">
<input name="image_file" type="file">
</form>
```

- Response Example: None
- Status Code: 204

Output Description

None

10.6 Canceling the Activation of the BIOS Changes

Function

If you update the BIOS when the host is in power-on status, the changes take effect upon host power-off. If you want to power off the host but do not want to apply the changes, use this command.

Syntax

- Operation Type: POST

- URL:
  https://device_ip/redfish/v1/UpdateService/Actions/Oem/VANTAGEO/Up - dateService.CancelBiosActive
- 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/UpdateService/Actions/Oem/VANTAGEO/UpdateService.CancelBiosActive
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body:

```
{
}
```

- Response Example: None
- Status Code: 202

Output Description

For a description of the output returned when you cancel the activation of the BIOS changes, refer to Table 10-11.

Table 10-11 Output Descriptions for Canceling the Activation of the BIOS Changes

Field	Type	Description
@odata.context	String	OData description of the BIOS activation cancellation model.

Field	Type	Description
@odata.id	String	Path for canceling the activation of the BIOS changes.

10.7 Querying Information About the Internal Firmware Resource Collection

Function

Query information about the internal firmware resource collection of a server.

Syntax

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

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

- Request Message Body: None

Parameters

For a description of parameters for querying information about the internal firmware resource collection, refer to Table 10-12.

Table 10-12 Parameter Descriptions for Querying Information About the Internal Firmware 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/UpdateService/InsideFirmwareInventory
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/
                   $metadata#SoftwareInventoryCollection.SoftwareInventoryCollection",
    "@odata.etag": "W/\"1611747828\"",
    "@odata.id": "/redfish/v1/UpdateService/InsideFirmwareInventory",
    "@odata.type": "#SoftwareInventoryCollection.SoftwareInventoryCollection",
    "Description": "Collection of Inside Firmware Inventory resources available to
                    the UpdateService",
    "Members": [
        {
            "@odata.id": "/redfish/v1/UpdateService/InsideFirmwareInventory/ActiveBMC"
        },
        {
            "@odata.id": "/redfish/v1/UpdateService/InsideFirmwareInventory/BackupBMC"
        },
        {
            "@odata.id": "/redfish/v1/UpdateService/InsideFirmwareInventory/ActiveBIOS"
        },
        {
            "@odata.id": "/redfish/v1/UpdateService/InsideFirmwareInventory/BackupBIOS"
        }
    ],
    "Members@odata.count": 4,
    "Name": "Inside Firmware Inventory Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the internal firmware resource collection, refer to Table 10-13.

Table 10-13 Output Descriptions for Querying Information About the Internal Firmware Resource Collection

Field	Type	Description
@odata.context	String	OData description of the model of the internal firmware resource collection.
@odata.id	String	Access path of the internal firmware resource collection node.

Field	Type	Description
@odata.type	String	Type of internal firmware resource collection.
Name	String	Name of the internal firmware resource collection.
Members@odata.count	Number	Number of internal firmware resources.
Members	Array	List of members in the internal firmware resource collection.
@odata.id	String	Access path of an internal firmware resource node.

10.8 Querying Information About a Specified Internal Firmware Resource of a Server

Function

Query information about a specified internal firmware resource of a server.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/UpdateService/InsideFirmwareInventory/softid*
- Request Header:

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

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified internal firmware resource, refer to Table 10-14.

Table 10-14 Parameter Descriptions for Querying Information About the Specified Internal Firmware 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 */redfish/v1/SessionService/Sessions*.
softid	ID of the internal firmware resource.	It can be obtained from the internal firmware resource collection.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/UpdateService/InsideFirmwareInventory/ActiveBMC
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#UpdateService/InsideFirmwareInventory
                       /Members/$entity",
    "@odata.etag": "W/\"1611756560\"",
    "@odata.id": "/redfish/v1/UpdateService/InsideFirmwareInventory/ActiveBMC",
    "@odata.type": "#SoftwareInventory.v1_2_0.SoftwareInventory",
    "Description": "ActiveBMC",
    "Id": "ActiveBMC",
    "InsideVersion": "03.19.0300",
    "Name": "ActiveBMC",
    "SoftwareId": "ActiveBMC",
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "Updatable": true
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified internal firmware resource, refer to Table 10-15.

Table 10-15 Output Descriptions for Querying Information About the Specified Internal Firmware Resource

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

Field	Type	Description
@odata.id	String	Access path of the internal firmware resource node.
@odata.type	String	Type of internal firmware resource.
Description	String	Description of the internal firmware resource.
Id	String	ID of the internal firmware resource.
Name	String	Name of the internal firmware resource.
SoftwareId	String	Firmware ID.
Status	Object	Status of the specified UpdateService resource. ● State: enabling status ● Health: health status
InsideVersion	String	Internal firmware version.
Updatable	Boolean	Whether the Update Service can update this software ● true ● false

10.9 Querying the Information About the Hotfix Resource Collection

Function

Query information about the hotfix collection.

Syntax

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

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

- Request Message Body: None

Description

For a description of the parameters for querying information about the hotfix collection, refer to Table 10-16.

Table 10-16 Parameter Descriptions for Querying the Information About the Hotfix 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 */redfish/v1/SessionService/Sessions*.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/UpdateService/HotFix
```

- Request Header:

```
X-Auth-Token: 8574621d21b12657488c7456821c234
```

- Request Message Body: None
- Response Example:

```
{
    "@odata.context": "/redfish/v1/$metadata#HotFixCollection.HotFixCollection",
    "@odata.etag": "W/\"947037738\"",
    "@odata.id": "/redfish/v1/UpdateService/HotFix",
    "@odata.type": "#HotFixCollection.HotFixCollection",
    "Description": "HotFix",
    "Id": "HotFix",
    "Info": [
        {
            "des": "test hotpatch",
            "id": 0,
            "module": "/usr/local/lib/libipmipdkcmds.so.2.9.10",
            "path":
            2230"/mnt/nandflash1/hotfix/vantageo_oem_NetFn34_hp.o",
            "proc": "IPMIMain"
        },
        {
            "des": "test hotpatch",
            "id": 1,
            "module": "/usr/local/lib/libsafesystem.so.2.10.0",
            "path": "/mnt/nandflash1/hotfix/safesystem_hp.o",
            "proc": "IPMIMain"
        },
        {
            "des": "test spx ext",
            "id": 2,
```

```
            "module": "/usr/local/lib/libsafesystem.so.2.10.0",
            "path": "/mnt/nandflash1/hotfix/safesystem_hp.o",
            "proc": "spx_restservice_ext"
        },
        {
            "des": "test spx",
            "id": 3,
            "module": "/usr/local/lib/libsafesystem.so.2.10.0",
            "path": "/mnt/nandflash1/hotfix/safesystem_hp.o",
            "proc": "spx_restservice"
        },
        {
            "des": "test pem",
            "id": 4,
            "module": "/usr/local/bin/pem",
            "path": "/mnt/nandflash1/hotfix/vantageo_pem_alarm_hp.o",
            "proc": "pem"
        },
        {
            "des": "test mctpmain",
            "id": 5,
            "module": "/usr/local/bin/MCTPMain",
            "path": "/mnt/nandflash1/hotfix/MCTPBOProxy_hp.o",
            "proc": "MCTPMain"
        },
        {
            "des": "test blackbox",
            "id": 6,
            "module": "/usr/local/bin/blackbox",
            "path": "/mnt/nandflash1/hotfix/hppr_hp.o",
            "proc": "blackbox"
        },
        {
            "des": "test compmanager",
            "id": 7,
            "module": "/usr/local/bin/compmanager",
            "path":
            "/mnt/nandflash1/hotfix/vantageo_model_match_hp.o",
            "proc": "compmanager"
        }
    ],
    "Name": "HotFix",
    "HotfixStatus": "Load",
    "Version": "03.21.0200"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the hotfix collection, refer to Table 10-17.

Table 10-17 Output Descriptions for Querying the Information About the Hotfix Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the hotfix resource collection model.
@odata.id	Character string	Access path of the hotfix resource collection node.
@odata.type	Character string	Type of hotfix resource collection.
Description	Character string	Description of the hotfix resource collection.
Id	Number	ID of the leak detector resource collection.
Name	Character string	Name of the leak detector resource collection.
Info	Array	Hotfix list information.
des	Character string	Process description of a hotfix.
id	Number	Process ID of a hotfix.
module	Character string	Process module of a hotfix.
path	Character string	File path of a hotfix.
proc	Character string	Process name of a hotfix.
HotfixStatus	Character string	Current status of a hot patch. Options: ● Load ● Unload
Version	Character string	Version number of a hotfix.

10.10 Loading or Removing Hotfixes

Function

Load or remove hotfixes.

Syntax

- Operation Type: POST
- URL: *https://device_ip/redfish/v1/UpdateService/HotFix*
- Request Header:

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

- Request Message Body:

```
{
    "Effect":effect
}
```

Description

For a description of the parameters for loading or removing hotfixes, refer to Table 10-18.

Table 10-18 Parameter Descriptions for Loading or Removing Hotfixes

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	Chassis ID.	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 */redfish/v1/SessionService/Sessions*.
header_type	Format of the request message.	application/json
effect	Loads or removes hotfixes.	• true: loads hotfixes. • false: removes hotfixes.

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/UpdateService/HotFix
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234
Content-Type: application/json
```

- Request Message Body:

```
{
    "Effect":false
}
```

- Response Example:

```
{
```

```
    "@odata.context": "/redfish/v1/$metadata",
    "@odata.etag": "W/\"1596373630\"",
    "@odata.id": "/redfish/v1/Managers/1/Actions/Manager.RollBack",
    "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"
    }
}
```


- Status Code: 200

Output Description

For a description of the output returned when you load or remove hotfixes, refer to Table 10-19.

Table 10-19 Output Descriptions for Loading or Removing Hotfixes

Field	Type	Description
code	Character string	ID of the specified message in the message registry.
message	Character string	Readable error message corresponding to the one in the message registry.
@odata.type	Character string	OData description of the message resource.
MessageId	Character string	Message ID.
RelatedProperties	Array	Message-related properties.
Message	Character string	Details.
MessageArgs	Array	Message arguments.
Severity	Character string	Severity level. Severity levels supported by Redfish, including: ● OK ● Warning ● Critical
Resolution	Character string	Recommended solution.

Chapter 11
Redfish Installation and Use

Table of Contents

Environment Installation 637
Use Case.....637

11.1 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.getpostman.com/downloads/.
- Use the *httprequester-2.2-fx.xpi* plug-in for a version of Firefox earlier than 56.0b3 (64 bits).

11.2 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.

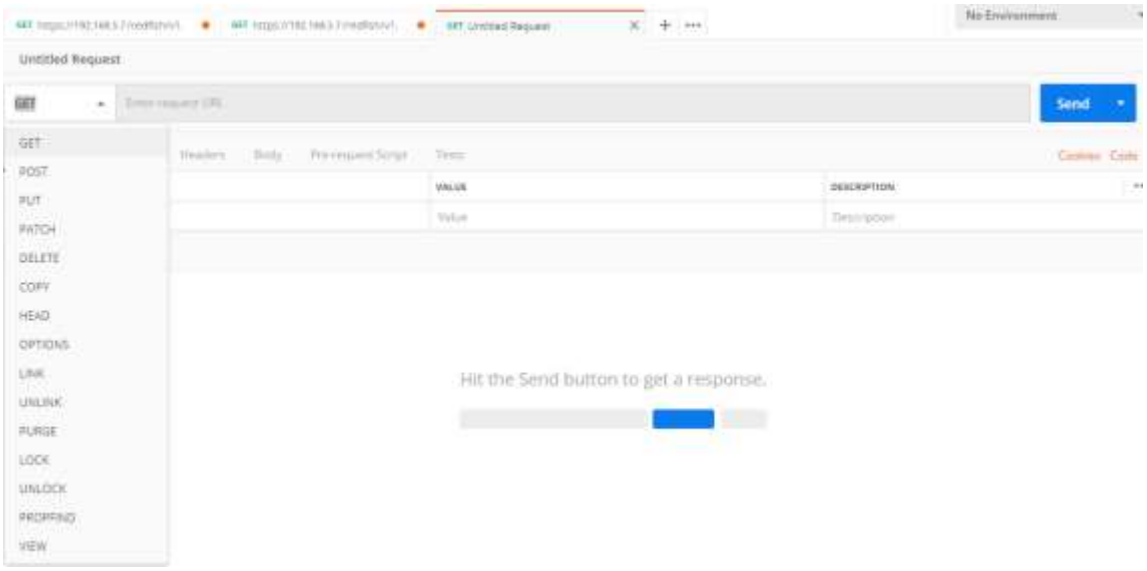
Note

For details on how to query the current root service resources, refer to "3.2 Querying the Current Root Service Resources".

Steps

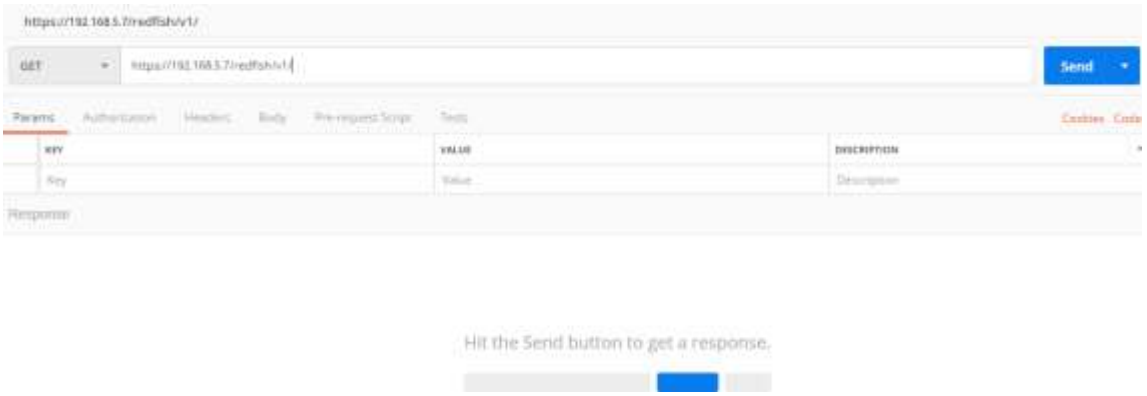
1. Open the Postman tool, create a request on the main page, and select a request action, see Figure 11-1.

Figure 11-1 Selecting a Request Action



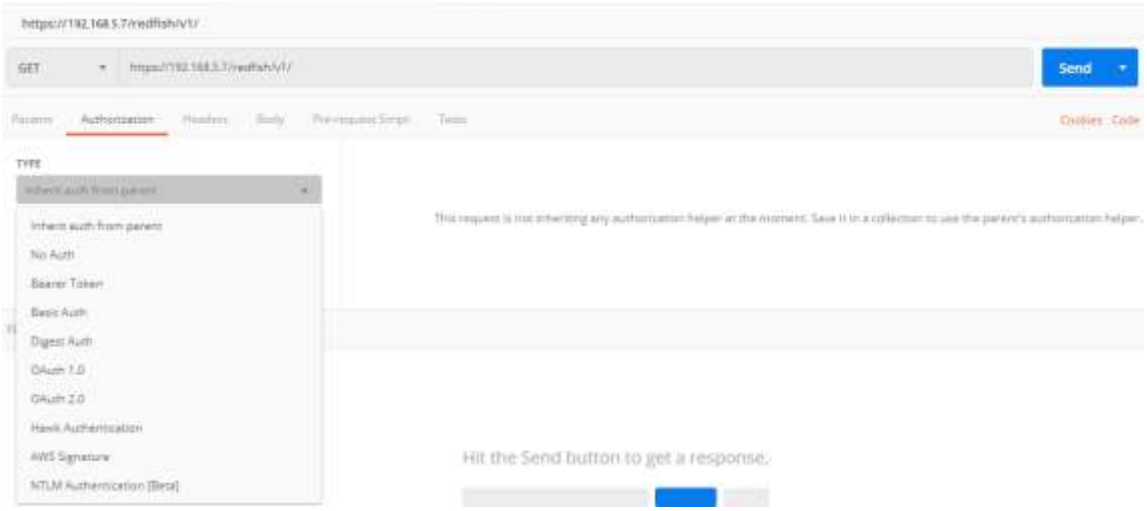
2. On the **Params** tab, set the URL of the Redfish interface, as shown in Figure 11-2.

Figure 11-2 Setting the URL



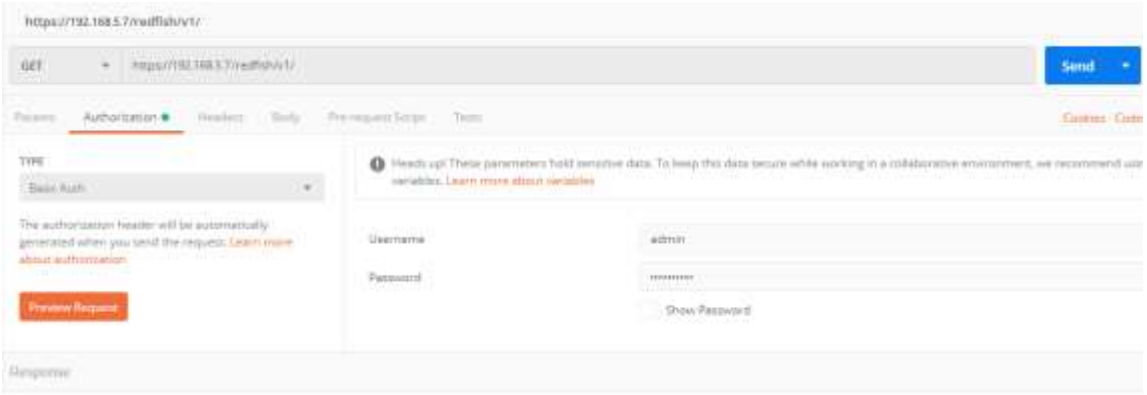
3. Select **Authorization > TYPE**. Select **Basic Auth**, see Figure 11-3.

Figure 11-3 Selecting an Authentication Type



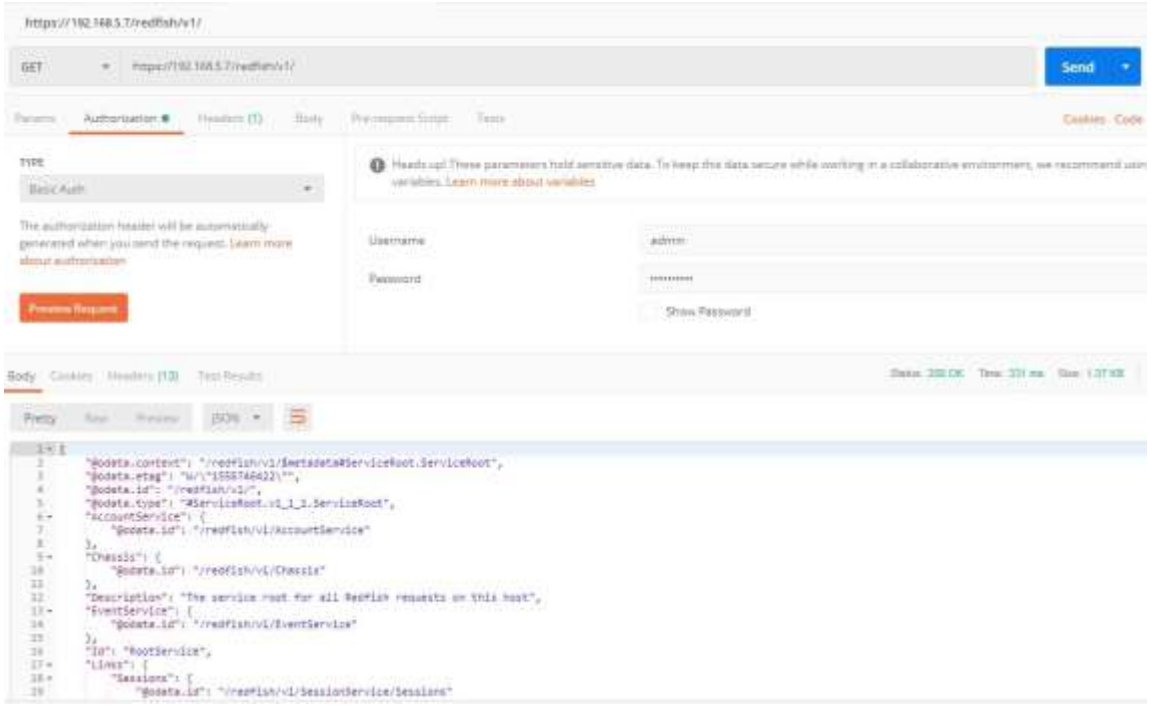
4. On the **Authorization** tab, enter the BMC username and password, see Figure 11-4.

Figure 11-4 Entering the BMC Username and Password



5. Click **Send** to send a request through the Redfish interface, see Figure 11-5.

Figure 11-5 Sending a Request



Glossary

ACPI

- Advanced Configuration and Power Interface

AD

- Administrative Domain

ADDDC

- Adaptive Double Device Data Correction

AES

- Advanced Encryption Standard

AHCI

- Advanced Host Controller Interface

API

- Application Program Interface

APIC

- Advanced Programmable Interrupt Controller

ARI

- Assist Request Instruction

ARM

- Asynchronous Response Mode

ARM

- Advanced RISC Machines

BBU

- Battery Backup Unit

BDF

- Bus/Device/Function

BF

- Beam Forming

BIOS

- Basic Input/Output System

BIST

- Built-In Self-Test

BMC

- Baseboard Management Controller

BMC

- Baseboard Management Controller

CD

- Compact Disk

CIFS

- Common Internet File System

CPU

- Central Processing Unit

CRC

- Cyclic Redundancy Check

CSRF

- Cross-Site Request Forgery

DCU

- Data Collection Unit

DDR

- Double Data Rate

DES

- Data Encryption Standard

DFX

- Design for X

DHCP

- Dynamic Host Configuration Protocol

DIMM

- Dual Inline Memory Module

DMA

- Direct Memory Access

DNS

- Domain Name System

DOS

- Disk Operating System

DRAM

- Dynamic Random Access Memory

EPB

- Energy Performance Bias

EPLD

- Erasable Programmable Logic Device

EPP

- Energy Performance Preference

FC

- Fiber Channel

FCoE

- Fibre Channel Over Ethernet

FPGA

- Field Programmable Gate Array

FQDN

- Fully Qualified Domain Name

FTP

- File Transfer Protocol

GPU

- Graphics Processing Unit

HD

- High Definition

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

IIO

- Integrated I/O Module

IP

- Internet Protocol

IPMI

- Intelligent Platform Management Interface

IPv4

- Internet Protocol Version 4

IPv6

- Internet Protocol Version 6

JSON

- Java Script Object Notation

KVM

- Keyboard, Video and Mouse

LDAP

- Lightweight Directory Access Protocol

LLC

- Logic Link Control

LLDP

- Link Layer Discovery Protocol

LMCE

- Local Machine Check Exception

MAC

- Media Access Control

MD5

- Message Digest 5 Algorithm

MMCFG

- Memory Mapped Configuration

MSI

- Multiplex Structure Identifier

MTU

- Maximum Transfer Unit

NAT

- Network Address Translation

NEO

- Native Enhanced-cloud Orchestration

NFS

- Network File System

NI

- Network Identifier

NIC

- Network Interface Card

NPS

- Net Promoter Score

NTP

- Network Time Protocol

NUMA

- Non-Uniform Memory Access Architecture

NVMe

- Non-Volatile Memory Express

OC

- Ordinary Clock

OCP

- Open Computer Project

OEM

- Original Equipment Manufacturer

OID

- Object Identifier

OPA

- Optical Pre-Amplifier

OS

- Operating System

PCB

- Printed Circuit Board

PCIe

- Peripheral Component Interconnect Express

PCS

- Policy Control Server

PECI

- Platform Environment Control Interface

PHY

- Physical layer

PM

- Power Module

PME

- Power Management Event

POR

- Population Rules

POST

- Power-On Self-Test

PPIN

- Protected Processor Identification Number

PPR

- Privacy Profile Register

PSD

- Protection Switching Duration

PSU

- Power Supply Unit

PXE

- Preboot eXecution Environment

RAID

- Redundant Array of Independent Disks

RMT

- Remote Maintenance Terminal

RPM

- Rotations Per Minute

SAS

- Serial Attached SCSI

SATA

- Serial ATA

SEL

- System Event Log

SFTP

- Secure File Transfer Protocol

SHA

- Secure Hash Algorithm

SMB

- Server Message Block

SMI

- System Management Interruption

SMR

- Switching Mode Rectifier

SMTP

- Simple Message Transfer Protocol

SNC

- Sub-Network Connection

SNMP

- Simple Network Management Protocol

SPI

- Serial Peripheral Interface

SR-IOV

- Single-Root I/O Virtualization

SSD

- Solid State Drive

SSDP

- Simple Service Discovery Protocol

SSH

- Secure Shell

SSL

- Secure Sockets Layer

SST

- Subsystem Status Test

TCP

- Transmission Control Protocol

TDP

- Trigger Detection Point

TLS

- Transport Layer Security

TDT

- Trusted Execution Technology

UDP

- User Datagram Protocol

UHCI

- Universal Host Controller Interface

UID

- User Identifier

UID

- Unique Identifier

UMA

- Unified Message Application

UPI

- Ultra Path Interconnect

URI

- Uniform Resource Identifier

URL

- Uniform Resource Locator

USB

- Universal Serial Bus

UUID

- Universal Unique Identifier

VLAN

- Virtual Local Area Network

VMD

- Volume Management Device

VT

- Virtual Tributary

WHEA

- Windows Hardware Error Architecture

WWNN

- World Wide Node Name

WWPN

- World Wide Port Name

XML

- Extensible Markup Language

eDPC

- Enhanced Downstream Port Containment

eMCA

- Enhanced Machine Check Architecture

iBMC

- intelligent Board Management Controller

iSCSI

- Internet Small Computer System Interface