



NETAŞ Server

Redfish Interface Description (BMC V4)

Version: R1.2

NETAŞ TELEKOMÜNİKASYON A.Ş
Yenişehir Mahallesi Osmanlı Bulvarı Aeropark Sitesi
B Blok No:11B İç Kapı No:40
Postcode: 34912
Tel: +90 (216) 522 20 00
URL: <https://destek.netas.com.tr>
E-mail: info@netas.com.tr info@netas.com.tr

LEGAL INFORMATION

Copyright 2024 NETAŞ CORPORATION.

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 NETAŞ CORPORATION is prohibited. Additionally, the contents of this document are protected by con-

tractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of NETAŞ CORPORATION 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. NETAŞ CORPORATION and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

NETAŞ CORPORATION 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 NETAŞ CORPORATION and its licensee, the user of this document shall not acquire any license to the subject matter herein.

NETAŞ CORPORATION reserves the right to upgrade or make technical change to this product without further notice.

Users may visit the NETAŞ technical support website <https://support.NETAŞ.com.cn> to inquire for related information.

The ultimate right to interpret this product resides in NETAŞ CORPORATION.

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 NETAŞ, 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. NETAŞ will provide technical support for the embedded software of this product.

Revision History

Revision No.	Revision Date	Revision Reason
R1.2	2024-07-01	Updated "Chapter 4, Operations on Manager Resources".
R1.1	2024-05-30	Added "Chapter 10, Operations on AccountService Resources". Updated "Chapter 4, Operations on Manager Resources".
Revision No.	Revision Date	Revision Reason
R1.0	2023-07-31	First edition.

Serial Number: SJ-20230907115354-009

Publishing Date: 2024-07-01 (R1.2)

Contents

1 Redfish Overview.....	1
1.1 Basic Concepts.....	1
1.2 General Descriptions.....	1 2
Redfish Resource Tree.....	6 3
Operations on Public Fixed Resources.....	10
3.1 Querying the Redfish Version Information.....	11
3.2 Querying the Current Root Service Resources.....	12 4
Operations on Manager Resources.....	17
4.1 Querying Information About the Manager Resource Collection.....	21
4.2 Querying Information About a Specified Manager Resource.....	23
4.3 Modifying Information About a Specified Manager Resource.....	29
4.4 Querying Information About the Syslog Configuration.....	30
4.5 Configuring Information About the Syslog Server.....	33
4.6 Submitting a Syslog Test Log.....	38
4.7 Querying Information About the NtpService Configuration Resource.....	39
4.8 Modifying Properties of the NTP Resource.....	41
4.9 Querying Information About the BMC Service.....	43
4.10 Modifying Information About a Specified BMC Service.....	47
4.11 Querying the BMC Management Interface Resource Collection.....	52
4.12 Querying Information About a Specified BMC Management Interface Resource.....	54
4.13 Modifying a Specified BMC Management Interface Resource.....	61
4.14 Restarting the BMC.....	67
4.15 Querying Information About the LLDP Service Configuration Resource.....	69
4.16 Modifying Properties of the LLDP Service Resource.....	71
4.17 Querying Information About the SNMP Resource.....	73
4.18 Modifying Properties of the SNMP Resource.....	78
4.19 Submitting an SNMP Trap Test Event.....	84
4.20 Querying the Virtual Media Resource Collection.....	85
4.21 Querying a Virtual Media Resource.....	87
4.22 Connecting to the Virtual Media.....	90
4.23 Disconnecting the Virtual Media.....	92
4.24 Sending a One-Click Collection Request.....	94

4.25 Querying the One-Click Collection Progress.....	96
4.26 Exporting Logs.....	99
4.27 Querying the KVM Service Resource.....	101
4.28 Modifying Information About the KVM Resource.....	103
4.29 Querying Information About a Specified SEL Log Service Resource.....	105
4.30 Capturing the Screen Manually.....	108
4.31 Downloading the Manually Captured Screen Image.....	109
4.32 Querying Information About the ISDT Resource.....	110
4.33 Modifying Properties of the ISDT Service Resource.....	112
4.34 Mounting and Dismounting Navigation Disks.....	113
Operations on System Resources.....	116
5.1 Querying Information About the System Resource Collection.....	122
5.2 Querying Information About a Specified System Resource.....	124
5.3 Remotely Powering On, Powering Off, and Resetting a System Resource.....	132
5.4 Modifying Properties of a Specified System Resource.....	134
5.5 Querying Information About the CPU Resource Collection.....	138
5.6 Querying Information About a Specified CPU Resource.....	140
5.7 Querying Information About All CPU Resources.....	144
5.8 Querying Information About the Memory Resource Collection.....	147
5.9 Querying Information About a Specified Memory Resource.....	149
5.10 Querying Information About All Memory Resources.....	152
5.11 Querying Information About the Storage Resource Collection.....	155
5.12 Querying Information About a Specified Storage Controller Resource.....	157
5.13 Querying Information About All Storage Controller Resources.....	161
5.14 Querying Information About the Logical Volume Resource Collection.....	166
5.15 Querying Information About a Specified Logical Volume Resource.....	168
5.16 Creating a Logical Volume.....	172
5.17 Deleting a Logical Volume.....	176
5.18 Querying Properties of the BIOS Resource.....	178
5.19 Querying Information About the BIOS Settings.....	181
5.20 Modifying the BIOS Settings.....	184
5.21 Setting the BIOS Password.....	185
5.22 Restoring the Default BIOS Settings.....	186
Operations on Chassis Resources.....	188
6.1 Querying Information About the Chassis Resource Collection.....	197

6.2 Querying Information About a Specified Chassis Resource.....	199
6.3 Modifying the Position Indicator Status of a Chassis.....	204
6.4 Querying Information About the Network Adapter Resource Collection.....	205
6.5 Querying Information About a Specified Network Adapter Resource.....	208
6.6 Querying Information About All Network Adapter Resources.....	212
6.7 Querying Information About a Specified Network Port Resource.....	218
6.8 Querying Information About the Optical Module Resource Connected to a Network Port.....	222
6.9 Modifying the LLDP Switch of a Specified Network Port.....	226
6.10 Querying Information About the PCIe Device Resource Collection.....	230
6.11 Querying Information About a Specified PCIe Device Resource.....	233
6.12 Querying Information About All PCIe Device Resources.....	237
6.13 Querying Information About the Drive Resource Collection.....	241
6.14 Querying Information About a Specified Drive Resource.....	243
6.15 Querying Information About All Drive Resources.....	247
6.16 Querying the Power Supply Information About a Specified Chassis.....	251
6.17 Collecting Information About Power Statistics.....	260
6.18 Modifying Properties of a Specified Power Supply.....	263
6.19 Querying Cooling Resource Information About a Specified Chassis.....	274
6.20 Querying Information About the Expansion Board Resource Collection.....	279
6.21 Querying Information About the Hard Disk Backplane Resource Collection.....	281
6.22 Querying Information About a Specified Hard Disk Backplane Resource.....	283
6.23 Querying Information About the Riser Card Resource Collection.....	285
6.24 Querying Information About a Specified Riser Card Resource.....	287
6.25 Querying Information About a Specified PCIe Device Function Resource.....	289
Operations on SessionService Resources.....	293
7.1 Querying Information About the Session Service.....	294
7.2 Modifying Information About the Session Service.....	296
7.3 Creating Information About a Session.....	297
7.4 Querying Information About the Session Resource Collection.....	299
7.5 Querying Information About a Specified Session Resource.....	301
7.6 Deleting Information About a Specified Session Resource.....	303
Operations on EventService Resources.....	305
8.1 Querying Information About the EventService Resource.....	307
8.2 Querying Information About the Event Subscription Resource Collection.....	310
8.3 Creating an Event Subscription Resource.....	312

8.4 Querying Information About an Event Subscription Resource.....	316
8.5 Modifying Information About an Event Subscription Resource.....	318
8.6 Deleting an Event Subscription Resource.....	321
8.7 Reporting an Event.....	322
8.8 Querying Information About the Event Resource Collection.....	324
8.9 Deleting All Event Resources.....	327
8.10 Querying Information About the Current Alarm Resource Collection.....	328
8.11 Querying Information About the Current Alarm Resource.....	332
8.12 Deleting the Current Alarm Resource.....	334
8.13 Deleting All Current Alarm Resource.....	335
8.14 Querying Information About the Current Alarm Event Resource Collection.....	336
8.15 Modifying Event Service Resource Information.....	340
Operations on UpdateService Resources.....	342
9.1 Querying Information About an UpdateService Resource.....	344
9.2 Querying Information About an Updateable Firmware Resource Collection.....	346
9.3 Querying Information About a Specified Updateable Firmware Resource.....	348
9.4 Updating Firmware.....	351
9.5 Querying Information About the Internal Firmware Resource Collection.....	354
9.6 Querying Information About a Specified Internal Firmware Resource.....	356
9.7 Updating Firmware Remotely.....	358
10 Operations on AccountService Resources.....	362
10.1 Querying User Service Information.....	365
10.2 Modifying User Service Information.....	367
10.3 Querying Information About the User Resource Collection.....	369
10.4 Querying Information About a Specified Account Resource.....	371
10.5 Creating an Account.....	373
10.6 Deleting an Account.....	376
10.7 Modifying Information About a Specified Account.....	377
10.8 Querying Information About the Role Resource Collection.....	380
10.9 Querying Information About a Specified Role Resource.....	382
10.10 Querying Information About the LDAP Service Resource.....	384
10.11 Querying Information About the Collection of LDAP Domain Controller Resources....	386
10.12 Querying the Active Directory Information.....	388
10.13 Modifying the Active Directory Information.....	391
11 Redfish Installation and Use.....	397

11.1 Environment Installation.....	397
11.2 Use Case.....	397
Glossary.....	401

About This Manual

Purpose

This manual describes the **iBMC** Redfish interfaces of the NETAŞ 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 EventService Resources	Describes the operations on EventService resources on a Redfish interface.
Chapter 9, Operations on UpdateService Resources	Describes the operations on UpdateService resources on a Redfish interface.

Chapter 10, Operations on AccountService Resources	Describes the operations on AccountService 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.....	1
General Descriptions.....	1

1.1 Basic Concepts

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

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

1.2 General Descriptions

Resource Operations

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

Table 1-1 Resource Operation Descriptions

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

The URI described in this manual is in the following format:

https://device_ip/redfish/v1/path, which is divided into three parts:

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

**Note**

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

Resource Functions

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

Table 1-2 Resource Function Descriptions

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

Request Headers

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

Table 1-3 Request Header Descriptions

Request Header	Description
----------------	-------------

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

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

Response Headers

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

Table 1-4 Response Header Descriptions

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

Response Header	Description
	- Services shall set Content-Type to application/xml when returning metadata as XML. ;charset=utf-8 shall be appended to the Content-Type if Content-Type is specified in the selected media type in the Accept header for the request.
Content-Length	Describes the size of the message body. To indicate the size of the body, a client preferentially uses the Transfer-Encoding: chunked header instead of the Content Length header, because the Transfer-Encoding: chunked header allows the length of the currently transmitted message to be repeatedly sent. If a service does not support Transfer-Encoding and needs to use Content-Length , the service shall return status code 411 .
ETag	Identifier for a specified version of a resource, which is usually a message digest. The ETag header shall be included in responses to GET requests for 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.
400	The request is illegal. An error occurs on the client and an error message is returned.

Status Code	Description
401	Invalid user request.
403	The server rejects the request.
404	The requested resource does not exist.
405	The operation is not supported.
406	The Accept header is specified in the request. The resource identified in the request cannot generate a resource representation corresponding to a media type contained in the Accept header.
409	The request causes a conflict in the current state of the resources.
410	The requested resource is unavailable to the service, and no forwarding address is known. This condition is considered permanent. Clients with hyperlink editing capabilities shall delete references to the URI in the client request after user approval. If the service does not know, or has no facility to determine, whether or not the condition is permanent, the status code 404 (Not Found) is used instead. Unless otherwise specified, this response can be cached.
411	The request does not specify the length of its content using the Content-Length header (perhaps Transfer-Encoding: chunked was used instead). The addressed resource requires the Content-Length header.
412	The precondition (such as OData-Version or If-Match) check fails.
415	The request specifies a Content-Type for an unsupported message body.

500	An internal error occurs on the server.
501	The requested function is not available.
503	The service is temporarily overloaded or in maintenance, so it cannot process requests. ● A service may use this response to indicate that the request URI is valid but the service is performing initialization or other maintenance on the resource. ● The service can also use this response to indicate that the service itself is in maintenance. For example, the service is being initialized after reboot.

Others

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

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

Chapter 2

Redfish Resource Tree

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

Table 2-1 Redfish Resource Tree

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

/redfish/v1/Managers/manager_id/VirtualMediae	GET
/redfish/v1/Managers/manager_id/VirtualMedia/Media_type	GET

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

/redfish/v1/Systems/system_id/Storages?\$expand=.	GET
/redfish/v1/Systems/system_id/Storages/storage_id/Volumes	GET/POST
/redfish/v1/Systems/system_id/Storages/storage_id/Volumes/volume_id	GET/DELETE
/redfish/v1/Systems/system_id/Bios	GET
/redfish/v1/Systems/system_id/Bios/SD	GET/PATCH
/redfish/v1/Systems/system_id/Bios/Actions/Bios.ChangePassword	POST
/redfish/v1/Systems/system_id/Bios/Actions/Bios.ResetBios	POST
Chassis resources	

URL	Operation
/redfish/v1/redfish/v1/Chassis	GET
/redfish/v1/redfish/v1/Chassis/chassis_id	GET/PATCH
/redfish/v1/Chassis/chassis_id/NetworkAdapters	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters?\$expand=.	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/NetworkPorts	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/Network-Ports/networkports_id	GET/PATCH
/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/Network-Ports/networkports_id/OpticalModule	GET
/redfish/v1/Chassis/chassis_id/PCleDevices	GET
/redfish/v1/Chassis/chassis_id/PCleDevices/pciedevices_id	GET
/redfish/v1/Chassis/chassis_id/PCleDevices/pciedevices_id/Functions/functions_id	GET
/redfish/v1/Chassis/chassis_id/PCleDevices?\$expand=.	GET
/redfish/v1/Chassis/chassis_id/Drives	GET
/redfish/v1/Chassis/chassis_id/Drives/drives_id	GET

/redfish/v1/Chassis/chassis_id/Drives?\$expand=.	GET
/redfish/v1/Chassis/chassis_id/Power	GET/PATCH
/redfish/v1/Chassis/Chassis_id/Power/Actions/Power.CollectHistoryData	POST
/redfish/v1/Chassis/chassis_id/Thermal	GET/PATCH
/redfish/v1/Chassis/chassis_id/Boards	GET
/redfish/v1/Chassis/Chassis_id/Boards/DiskBackplanes	GET
/redfish/v1/Chassis/Chassis_id/Boards/DiskBackplanes/DiskBackplaneId	GET
/redfish/v1/Chassis/Chassis_id/Boards/Risercard	GET
/redfish/v1/Chassis/Chassis_id/Boards/Risercard/RisercardId	GET
/redfish/v1/Chassis/chassis_id/PCleDevices/pciedevices_id/Functions/functions_	GET
SessionService resources	
/redfish/v1/SessionService	GET/PATCH
/redfish/v1/SessionService/Sessions	GET/POST
/redfish/v1/SessionService/Sessions/Session_id	GET/DELETE

URL	Operation
EventService resources	
/redfish/v1/EventService	GET/PATCH
/redfish/v1/EventService/Subscriptions	GET/POST
/redfish/v1/EventService/Subscriptions/id	GET/PATCH/ DELETE
/redfish/v1/EventService/Alarms?\$skip=skip_value&\$top=top_value	GET
/redfish/v1/EventService/DeleteAlarmsAll	DELETE
redfish/v1/EventService/CurrentAlarms	GET
/redfish/v1/EventService/CurrentAlarms/alarm_id	GET/DELETE

/redfish/v1/EventService/DeleteCurrentAlarmsAll	DELETE
/redfish/v1/EventService/CurrentAlertEvents	GET
UpdateService resources	
/redfish/v1/UpdateService	GET
/redfish/v1/UpdateService/FirmwareInventory	GET
/redfish/v1/UpdateService/FirmwareInventory/softid	GET
/redfish/v1/UpdateService/upload	POST
/redfish/v1/UpdateService/InsideFirmwareInventory	GET
/redfish/v1/UpdateService/InsideFirmwareInventory/softid	GET
/redfish/v1/UpdateService/Actions/UpdateService.SimpleUpdat	POST
AccountService resources	
/redfish/v1/AccountService	GET/PATCH
/redfish/v1/AccountService/Accounts	GET/POST
/redfish/v1/AccountService/Accounts/account_id	GET/DELETE/ PATCH
/redfish/v1/AccountService/Roles	GET
/redfish/v1/AccountService/Roles/role_id	GET
/redfish/v1/AccountService/LdapService	GET
/redfish/v1/AccountService/LdapService/LdapControllers	GET
/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory	GET/PATCH

Chapter 3

Operations on Public Fixed Resources

Table of Contents

Querying the Redfish Version Information.....11

Querying the Current Root Service Resources..... 12

Figure 3-1 shows the path requirements for the public fixed resources supported by NETAŞ

URL	Property	Description	Operation
/redfish	v1	Redfish version information.	GET
/redfish/v1	Id	ID of the root server.	GET
	Name	Name of the root service resource.	GET
	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
	Tasks	TaskService resources.	GET
	SessionService	SessionService resources.	GET
	AccountService	AccountService resources.	GET

Figure 3-1 Public Fixed Resources Path Requirements



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

URL	Property	Description	Operation
	UpdateService	UpdateService resources.	GET
	EventService	EventService resources.	GET
	Registries	Message registry resources.	GET
	Description	Root service description.	GET
	Links	-	GET
	Sessions	SessionService resources.	GET

Table 3-1 Descriptions for Properties of Public Fixed Resources

3.1 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
Message v1	String	Redfish version information.

3.2 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/\"1269454979\"",
    "@odata.id": "/redfish/v1/",
    "@odata.type":
"#ServiceRoot.v1_7_0.ServiceRoot",
    "AccountService":
    {
        "@odata.id":
"/redfish/v1/AccountService"
    },
    "CertificateService":
    {
        "@odata.id":
"/redfish/v1/CertificateService"
    },
    "Chassis":
    {
        "@odata.id":
"/redfish/v1/Chassis"
    },
    "CompositionService":
    {
        "@odata.id":
"/redfish/v1/CompositionService"
    },
    "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",
    "Oem":
    {
        "Ami":
        {
            "@odata.type":
"#AMIServiceRoot.v1_0_0.AMIServiceRoot",
            "Configurations":
            {
                "@odata.id":
"/redfish/v1/Oem/Ami/Configurations"
            },
            "InventoryDataStatus":
            {
                "@odata.id":
"/redfish/v1/Oem/Ami/InventoryData/Status"
            },
            "RtpVersion": "13.04"
        }
    },
    "Product": "AMI Redfish Server",
    "ProtocolFeaturesSupported":
    {
        "DeepOperations":
        {
            "DeepPATCH": true,
            "DeepPOST": false,
            "MaxLevels": 6
        },
        "ExcerptQuery": true,
        "ExpandQuery":
        {
            "ExpandAll": true,
            "Levels": true,
            "Links": true,
            "MaxLevels": 5,
            "NoLinks": true
        },
        "FilterQuery": true,
        "OnlyMemberQuery": true,
        "SelectQuery": true
    },
    "RedfishVersion": "1.11.0",

```

```

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

```

- 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.

Field	Type	Description
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

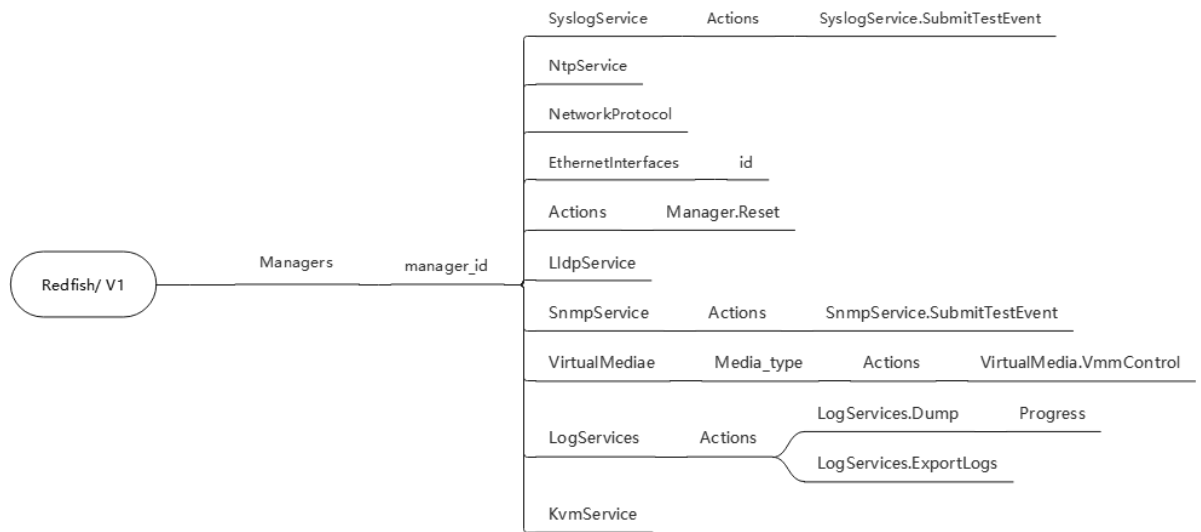
Table of Contents

Querying Information About the Manager Resource Collection.....	21
Querying Information About a Specified Manager Resource.....	23
Modifying Information About a Specified Manager Resource.....	29
Querying Information About the Syslog Configuration.....	30
Configuring Information About the Syslog Server.....	33
Submitting a Syslog Test Log.....	38
Querying Information About the NtpService Configuration Resource.....	39
Modifying Properties of the NTP Resource.....	41
Querying Information About the BMC Service.....	43
Modifying Information About a Specified BMC Service.....	47
Querying the BMC Management Interface Resource Collection.....	52
Querying Information About a Specified BMC Management Interface Resource.....	54
Modifying a Specified BMC Management Interface Resource.....	61
Restarting the BMC.....	67
Querying Information About the LLDP Service Configuration Resource.....	69
Modifying Properties of the LLDP Service Resource.....	71
Querying Information About the SNMP Resource.....	73
Modifying Properties of the SNMP Resource.....	78
Submitting an SNMP Trap Test Event.....	84
Querying the Virtual Media Resource Collection.....	85
Querying a Virtual Media Resource.....	87
Connecting to the Virtual Media.....	90
Disconnecting the Virtual Media.....	92
Sending a One-Click Collection Request.....	94
Querying the One-Click Collection Progress.....	96
Exporting Logs.....	99
Querying the KVM Service Resource.....	101
Modifying Information About the KVM Resource.....	103

Querying Information About a Specified SEL Log Service Resource.....	105
Capturing the Screen Manually.....	108
Downloading the Manually Captured Screen Image.....	109
Querying Information About the ISDT Resource.....	110
Modifying Properties of the ISDT Service Resource.....	112
Mounting and Dismounting Navigation Disks.....	113

Figure 4-1 shows the path requirements for the Managers resources supported by NETAŞ 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/1	Id	ID of the Manager resource.	GET

	Name	Name of the Manager resource.	GET
	ManagerType	Type of Manager resource.	GET

URL	Property	Description	Operation
	FirmwareVersion	Firmware version of the Manager resource.	GET
	UUID	UUID of the Manager resource.	GET
	Model	Model of the Manager resource.	GET
	DateTime	System time of the Manager resource.	GET
	DateTimeLocalOffset	Time zone of the Manager resource.	GET/PATCH
	NetworkProtocol	Access path of the network protocol supported by the specified Manager resource.	GET
	EthernetInterfaces	Access path of the Ethernet interface information about the specified Manager resource.	GET
	Links	Links to the related resources.	GET
/redfish/v1/Managers/1/SyslogService	ServiceEnabled	Syslog service enabled.	GET/PATCH
	ServerIdentitySource	- Board serial number: BoardSN - Asset tag: ProductAssetTag - Host name: HostName	GET/PATCH
	TransmissionProtocol	Transmission protocol: - UDP - TCP	GET/PATCH
	SyslogServers	Syslog servers.	GET/PATCH
	Enabled	Channel enabled.	GET/PATCH
	Address	Server address.	GET/PATCH
	Port	Server port number.	GET/PATCH

	LogType	Log type.	GET/PATCH
/redfish/v1/Managers/1/NtpService	ServiceEnabled	NTP service enabled.	GET/PATCH
	AlternateNtpServer	Address of the alternate NTP server.	GET/PATCH
	PreferredNtpServer	Address of the preferred NTP server.	GET/PATCH
	ExtraNtpServer	Address of the extra NTP server.	GET/PATCH
	MinPollingInterval	Minimum polling interval.	GET
	MaxPollingInterval	Maximum polling interval.	GET

URL	Property	Description	Operation
	CurrentPollingInterval	Current polling interval.	GET/PATCH
/redfish/v1/Managers/1/Actions/Manager.Reset	ResetType	Reset type.	POST
/redfish/v1/Managers/1/LldpService	Description	Description of the LLDP resource.	GET
	Id	ID of the LLDP resource.	GET
	Name	Name of the LLDP resource.	GET
	LldpEnabled	LLDP enabled.	GET/PATCH
	WorkMode	LLDP operation mode.	GET/PATCH
/redfish/v1/Managers/manager_id/LogServices/SEL/Entries/entries_id	Created	Time when the SEL log instance is created.	GET
	Description	Log resource description information.	GET

	EntryCode	Type of SEL log instance.	GET
	EntryType	Type of SEL log instance.	GET
	EventTimestamp	Timestamp of the SEL log instance information.	GET
	Id	ID of the SEL log instance.	GET
	Message	Message content of the SEL log instance information.	GET
	Name	Name of the SEL log instance.	GET
	SensorNumber	ID of the sensor that creates the SEL log instance.	GET
	SensorType	Type of the sensor that creates the SEL log instance.	GET
	Message	Details.	GET
	Severity	Log severity level of the SEL log instance information.	GET
/redfish/v1/Managers/manager_id/ISDTSERVICE	ImageInstalled	Whether there is a navigation disk image.	GET
	Actions	Available actions for	GET

		the ISDT resource.	
URL	Property	Description	Operation
	#ISDTService.VmmControl	Control operation on the navigation disk.	GET
	target	Path of the control operation on the navigation disk.	GET
	ServiceEnabled	Whether service is enabled.	PATCH
/redfish/v1/Managers/manager_id/ISDTService/Actions/ISDTService.VmmControl	Information	-	POST
	target	Access path of the current ISDT resource.	POST

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/v1/Managers` • Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

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

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

Parameter	Description	Value
-----------	-------------	-------

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#ManagerCollection.ManagerCollection",
  "@odata.etag": "\"1269405217\"",
  "@odata.id": "/redfish/v1/Managers",
  "@odata.type":
    "#ManagerCollection.ManagerCollection",
  "Description": "The collection for Managers",
  "Members":
    [{
      "@odata.id":
        "/redfish/v1/Managers/1"
    }],
  "Members@odata.count": 1,
  "Name": "Manager
Collection"
}
```

- Status Code: 200

Output Description

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

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

Field	Type	Description
-------	------	-------------

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

4.2 Querying Information About a Specified Manager Resource

Function

Query information about a specified Manager resource of a server.



Note

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

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 <i>/redfish/v1/SessionService/Sessions.</i>

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None
- Response Example:


```

{
  "@odata.context":
"/redfish/v1/$metadata#Manager.Manager",
  "@odata.etag": "\"1269405264\"",
  "@odata.id": "/redfish/v1/Managers/1",
  "@odata.type": "#Manager.v1_13_0.Manager",
  "Actions": {
    "Oem": {
      "#Manager.EffectFactory": {
"@Redfish.ActionInfo":
"/redfish/v1/Managers/1/EffectFactoryActionInfo",
"target":
"/redfish/v1/Managers/1/Actions/Oem/NETAS/Manager.EffectFactory"
      },
      "#Manager.ExportConfiguration": {
"@Redfish.ActionInfo":
"/redfish/v1/Managers/1/ExportConfigurationActionInfo",
"target":
"/redfish/v1/Managers/1/Actions/Oem/NETAS/Manager.ExportConfiguration"
      },
      "#Manager.FactoryReset": {
"target":
"/redfish/v1/Managers/1/Actions/Manager.FactoryReset",
"FactoryResetType@Redfish.AllowableValues": [
"ResetAll"
      ],
      "#Manager.ImportConfiguration": {
"@Redfish.ActionInfo":
"/redfish/v1/Managers/1/ImportConfigurationActionInfo",
"target":
"/redfish/v1/Managers/1/Oem/NETAS/Manager.ImportConfiguration"
      },
      "#Manager.Rollback": {

```

```

        "target":
"/redfish/v1/Managers/1/Actions/Manager.Rollback",
"RollBackType@Redfish.AllowableValues": [
        "RollBack"
    ]
    },
    "#Manager.Reset": {
        "target":
"/redfish/v1/Managers/1/Actions/Manager.Reset",
"ResetType@Redfish.AllowableValues": [
"ForceRestart"
    ]
    },
    "#Manager.CaptureScreenShot": {
        "target":
"/redfish/v1/Managers/1/Actions/Manager.CaptureScreenShot"
    },
    "#Manager.DownloadScreenShot": {
        "target":
"/redfish/v1/Managers/1/Actions/Manager.DownloadScreenShot"
    }
},
"CommandShell": {
"ConnectTypesSupported": [
    "SSH",
    "IPMI"
],
"MaxConcurrentSessions": 36,
"ServiceEnabled": true
},
"DateTime": "2010-03-24T12:34:27+08:00",
"DateTimeLocalOffset": "+08:00",
"Description": "BMC",
"EthernetInterfaces": {
"@odata.id":
"/redfish/v1/Managers/1/EthernetInterfaces"
},
"GraphicalConsole": {
"ConnectTypesSupported": [
    "KVMIP"
],
"MaxConcurrentSessions": 4,
"ServiceEnabled": true
},
"Id": "1",
"ManagerType": "BMC",
"Model": "43707000",

```



```

    "Name": "Manager",
    "NetworkProtocol": {
      "@odata.id":
"/redfish/v1/Managers/1/NetworkProtocol"
    },
    "SerialConsole": {
      "ConnectTypesSupported": [
        "IPMI"
      ],
      "MaxConcurrentSessions": 3,
      "ServiceEnabled": true
    },
    "Status": {
      "Health": "OK",
      "State": "Enabled"
    },
    "VirtualMedia": {
      "@odata.id":
"/redfish/v1/Managers/1/VirtualMedia"
    },
    "Links": {
      "ManagerForChassis": [
        {
          "@odata.id":
"/redfish/v1/Chassis/1"
        }
      ],
      "ManagerForServers": [
        {
          "@odata.id":
"/redfish/v1/Systems/1"
        }
      ],
      "ManagerInChassis": [
        {
          "@odata.id":
"/redfish/v1/Chassis/1"
        }
      ],
      "NtpService": {
        "@odata.id":
"/redfish/v1/Managers/1/NtpService"
      },
      "LogServices": {
        "@odata.id":
"/redfish/v1/Managers/1/LogServices"
      },
      "LldpService": {
        "@odata.id":
"/redfish/v1/Managers/1/LldpService"
      }
    }
  },

```

```

    "SyslogService": {          "@odata.id":
"/redfish/v1/Managers/1/SyslogService"
    },
    "KvmService": {            "@odata.id":
"/redfish/v1/Managers/1/KvmService"
    },
    "SnpService": {            "@odata.id":
"/redfish/v1/Managers/1/SnpService"
    },
    "FirmwareVersion": "04.22.01.01",
    "UUID": "30e72400-0000-1000-0000-000000000000",
    "ServiceEntryPointUUID": "30e72400-0000-1000-0000-000000000000",
    "Oem": {
        "NAT": {
"@odata.id":"/redfish/v1/Managers/1/NAT"
        },
        "Public":{
"FirmwareVersionDate": "May 09 2024",
            "IfMatchEnabled": false,
"USB0InterfaceEnabled": false,
            "ISDTSservice":{                                "@odata.id":
"/redfish/v1/Managers/1/ISDTSservice"
            },
            "FirewallService":{                                "@odata.id":
"/redfish/v1/Managers/1/SecurityService"
            }
        }
    }
}

```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	String	OData description of the specified Manager resource collection model.
@odata.id	String	Access path of the specified Manager resource node.

@odata.type	String	Type of the specified Manager resource.
-------------	--------	---

Field	Type	Description
Id	String	ID of the Manager resource.
Name	String	Name of the Manager resource.
ManagerType	String	Type of Manager resource.
FirmwareVersion	String	Firmware version of the Manager resource.
UUID	String	UUID of the Manager resource.
Model	String	Model of the Manager resource.
DateTime	String	System time of the Manager resource.
DateTimeLocalOffset	String	Time zone of the Manager resource, in time zone format, for example, +08:00, or time zone/region format, for example, Asia/Shanghai or America/New_York.
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.
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.
LdpService	Object	Access path of the LIDP service of the specified Manager resource.
VirtualMedia	Object	Access path of the virtual media service of the specified Manager resource.

Links	Object	Links to the related resources.
Actions	Object	Available actions for the specified Manager resource.
Oem	Object	Customized properties.
#Manager.Rollback	Object	OS operation.
RollBackType@Redfish.AllowableValues	Array	OS operations allowed through the Redfish interface, including: RollBack
target	String	Operation path.
Field	Type	Description
Manager.Rollback	Object	Switches BMC versions.
Manager.ImportConfiguration	Object	Imports configurations.
Manager.ExportConfiguration	Object	Exports configurations.
Manager.FactoryReset	Object	Restores the factory default settings.
Oem.Public	Object	Customized field.
FirmwareVersionDate	String	BMC firmware version date.

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:**

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

Parameters

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

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

- Response Example: None
- Response Code: 204

Output Description

None

4.4 Querying Information About the Syslog Configuration

Function

Query information about the Syslog configuration.

Syntax

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

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

- Request Message Body: None

Parameters

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#SyslogService.SyslogService",
  "@odata.id": "/redfish/v1/Managers/Self/SyslogService",
  "@odata.type": "#SyslogService.v1_2_0.SyslogService",
  "Actions": {
    "#SyslogService.SubmitTestEvent": {
      "target":
        "/redfish/v1/Managers/Self/SyslogService/Actions/SyslogService.SubmitTestEvent"
    }
  },
  "Id": "SyslogService",
  "Name": "SyslogService",
  "ServerIdentitySource": "BoardSN",
  "ServiceEnabled": true,
  "SyslogServers": [
    {

```

```

        "Address": "10.228.34.159",
        "Enabled": false,
        "LogType": [
            "SecurityLog",
            "OperationLog",
            "EventLog"
        ],
        "MemberId": "0",
        "Port": 111
    },
    {
        "Address":
"10.228.34.157",
        "Enabled": false,
        "LogType": [
            "EventLog"
        ],
        "MemberId": "1",
        "Port": 222
    },
    {
        "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 4-8](#).

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

Field	Type	Description
@odata.context	String	OData description of the Syslog resource model.
@odata.id	String	Access path of the Syslog resource.
@odata.type	String	Type of Syslog resource.
Id	String	ID of the Syslog resource.
Name	String	Name of the Syslog resource.
ServiceEnabled	Boolean	Syslog service enabled.
ServerIdentitySource	String	Host ID: - Board serial number: BoardSN - Asset tag: ProductAssetTag - Host name: HostName
TransmissionProtocol	String	Transmission protocol. - UDP - TCP
SyslogServers	Object	Syslog servers.
MemberId	String	Member ID: "0" "1" "2" "3"
Enabled	Boolean	Channel enabled: - true - false
Address	String	Server address.
Port	Number	Server port number.
LogType	Array.	Log type: - OperationLog - SecurityLog - EventLog

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

Parameters

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

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

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

header_type	Format of the request message.	application/json
ServerIdentitySource	Host ID.	Host ID:

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

enabled_value	Whether the channel is enabled.	Whether the channel is enabled: ● true ● false
add_value	Server address format.	Server address format: ● IP address. ● FQDN format.
Parameter	Description	Value
		When enabled_value of a channel is set to true in SyslogServers, add_value of the corresponding channel must be unique.
port_value	Server port number.	Server port number, range: 1–65535.
logtype_value	Log type.	Log type: ● OperationLog ● SecurityLog ● EventLog

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```

{
  "ServerIdentitySource":
  "ProductAssetTag",
  "TransmissionProtocol": "UDP",
  "ServiceEnabled": true,
  "SyslogServers": [
    {
      "Address":
      "ABCD:9A8C:39A0:FE80:02D0:BCFF:FEA6:6C01",
      "Enabled": false,
      "LogType":
      ["EventLog", "OperationLog", "SecurityLog"],
      "Port": 1
    }, {
      "Address": "2020::12a",
      "Enabled": false,
      "LogType":
      ["EventLog", "SecurityLog", "OperationLog"],
      "Port":
      65535
    }, {
      "Address":
      "ABCD:9A8C:39A0:FE80:02D0",
      "Enabled": false,
      "LogType": ["EventLog", "OperationLog", "SecurityLog"],
      "Port": 1
    }, {
      "Address":
      "10.228.34.156",
      "Enabled": true,
      "LogType": ["SecurityLog"], "Port": 444
    }
  ]
}

```

Configure the Syslog function separately:

```

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

```

Configure the Syslog Server separately:


```
{
  "SyslogServers": [
    {
      "Address":
"ABCD:9A8C:39A0:FE80:02D0:BCFF:FEA6:6C01",
      "Enabled": false,
      "LogType":
["EventLog","OperationLog","SecurityLog"],
      "Port": 1
    }, {
      "Address": "2020::12a",
      "Enabled": false,
      "LogType":
["EventLog","SecurityLog","OperationLog"],
      "Port":
65535
    }, {
      "Address":
"ABCD:9A8C:39A0::FE80:02D0",
      "Enabled": false,
      "LogType":
["EventLog","OperationLog","SecurityLog"],
      "Port": 1
    }, {
      "Address":
"10.228.34.156",
      "Enabled": true,
      "LogType": ["SecurityLog"],
      "Port": 444
    }
  ]
}
```

- Response Example: None
- Status Code: 204

Output Description

None

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.SubmitTestEvent

- Request Header:

x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

Content-Type:application/json

- Request Message Body:

{

}

- Response Example: None
- Status Code: 204

Output Description

None

4.7 Querying Information About the NtpService Configuration Resource

Function

Query information about the NtpService configuration resource.

Syntax

- Operation Type: GET

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

x-auth-token:auth_value

- **Request Message Body:** None

Parameters

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

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

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

Usage Guidelines

None

Example

- **Request Example:**

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

- **Request Header:**

x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- **Request Message Body:** None • **Response Example:**

```

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

```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	String	OData description of the NTP resource model.
@odata.id	String	Access path of the NTP resource.
@odata.type	String	Type of NTP resource.
ServiceEnabled	Boolean	NTP enabled.
AlternateNtpServer	String	Alternate NTP server address.
CurrentPollingInterval	Number	Current synchronization interval. Range: MinPollingInterval through MaxPollingInterval .
Description	String	Description of the NTP resource.
ExtraNtpServer	String	Address of the extra NTP server.
Field	Type	Description

MaxPollingInterval	Number	Maximum synchronization interval.
MinPollingInterval	Number	Minimum synchronization interval.
PreferredNtpServer	String	Address of the preferred NTP server.
ServerAuthenticationEnabled	Boolean	Whether server authentication is enabled.
ServiceEnabled	Boolean	Whether the NTP service is enabled: • true • false

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
```

- Request Message Body:

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

Parameters

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

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

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

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 PATCH request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
ServiceEnabled	Boolean	Whether the NTP service is enabled: • true • false
AlternateNtpServer	String	Alternate NTP server address.
PreferredNtpServer	String	Preferred NTP server address.
ExtraNtpServer	String	Address of the extra NTP server.
CurrentPollingInterval	Number	Current polling interval. Range: Min-PollingInterval through MaxPollingInterval.
NtpAddressOrigin	Address mode.	Address mode: • static • IPv4: not supported in this version. • IPv6: not supported in this version.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

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

- Response Example: None
- Status Code: 204

Output Description

None

4.9 Querying Information About the BMC Service

Function

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

Syntax

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

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

- Request Message Body: None

Parameters

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None • Response Example:


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

```

    }
    "VNC": {
        "Port": 5900,
        "ProtocolEnabled": true,
    "SecurePort": 5901
    },
    "SSDP": {
    "NotifyEnabled": true
    }
    },
    "SNMP": {
    "ProtocolEnabled": true,
    "Port": 161
    },
    "SSH": {
    "ProtocolEnabled": true,
    "Port": 22
    },
    "VirtualMedia": {
    "ProtocolEnabled": true
    },
    "SSDP": {
    "ProtocolEnabled": true,
        "Port": 1900,
    "NotifyMulticastIntervalSeconds": 600,
    "NotifyIPv6Scope": "Site"
    }
}

```

- Status Code: 200

Output Description

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

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

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

@odata.id	String	Access path of the BMC service resource collection.
-----------	--------	---

Field	Type	Description
@odata.type	String	Type of BMC service resource collection.
Description	String	Description of the BMC resource.
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.
Oem.Public	Customized field.	-
VirtualMedia-CD/VirtualMedia-HD	Object	-
Timeout	Number	Service timeout period. Unit: seconds.
ProtocolEnabled	Boolean	Service enabling status: true/false
Port	Number	Service port number.
Instance	Number	Number of instances.
NotifyMulticastIntervalSeconds	Number	SSDP notification multicast interval.

NotifyIPv6Scope	String	IPv6 multicast range of SSDP messages: ● link: local link ● Site: local site ● Organization: local organization
NotifyEnabled	Boolean	Whether SSDP multicast is enabled.
VNC	Object	VNC service.
SecurePort	Number	Secure port.

4.10 Modifying Information About a Specified BMC Service

Function

Modify the information about 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": time,
  "NotifyIPv6Scope": scope
},
  "Oem": {
    "Public":
      {
        "OEMServerType": {
          "Port": oem_port_value,
          "ProtocolEnabled": oem_protocolEnabled_value,
          "Timeout": oem_timeout_value
        },
        "SSDP": {
          "NotifyEnabled": state
        }
      }
  }
}

```

Parameters

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

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

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

Service_type	Specified BMC services of the server.	• HTTPS • KVMIP • VirtualMedia • SSH • SNMP
protocolenabled_value	Whether the service is enabled.	Boolean: • true • false
port_value	Modifies the server port number.	Integer type: 1–65535.
Oem.Public	Customized field.	-
OEMServerType	OEM service type to be set.	Modifiable service type: • VirtualMedia-CD • VirtualMedia-HD

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
  "HTTPS": {
    "Port": 443
  }
}
```

```

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

```

- **Response Example:**

```

{
  "@odata.context":
    "/redfish/v1/$metadata#ManagerNetworkProtocol.ManagerNetworkProtocol",
  "@odata.id": "/redfish/v1/Managers/1/NetworkProtocol",
  "@odata.type": "#ManagerNetworkProtocol.v1_6_0.ManagerNetworkProtocol",
  "Description": "Network Protocol Details",
  "Id": "NetworkProtocol",

```



```

    "Name": "Manager Network Protocol",
    "HostName": "iSAC26C4F96B1676",
    "HTTPS": {
    "ProtocolEnabled": true,
    "Port": 443
    },
    "KVMIP": {
    "ProtocolEnabled": true,
    "Port": 7578
    },
    "Oem": {
        "Public": {
            "HTTPS": {
    "Timeout": 30
            },
            "KVMIP": {
    "Timeout": 30
            },
            "VirtualMedia-CD": {
    "ProtocolEnabled": true,
            "Port": 5120,
    "Instance": 1
            },
            "VirtualMedia-HD": {
    "ProtocolEnabled": false,
            "Port": 5123,
    "Instance": 0
            },
            "VNC": {
            "Port": 5900,
            "ProtocolEnabled": true,
    "SecurePort": 5901
            },
            "SSDP": {
    "NotifyEnabled": true
            }
        }
    },
    "SSH": {
    "ProtocolEnabled": true,
    "Port": 22
    },
    "SNMP": {
        "ProtocolEnabled": true,

```

```

        "Port": 161
    },
    "IPMI": {
        "Port": 623,
        "ProtocolEnabled": true
    },
    "VirtualMedia": {
        "ProtocolEnabled": true
    },
    "SSDP": {
        "ProtocolEnabled": true,
        "Port": 1900,
        "NotifyMulticastIntervalSeconds": 600,
        "NotifyIPv6Scope": "Site"
    }
}

```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	String	OData description of the BMC service resource collection model.
@odata.id	String	Access path of the BMC service resource collection.
@odata.type	String	Type of BMC service resource collection.
Description	String	Description of the BMC resource.
Id	String	BMC network protocol resource ID.
Name	String	BMC network protocol resource name.

HostName	String	BMC hostname.
HTTPS/KVMIP/SNMP/SSH/VirtualMedia/IPMI	Object	Service information supported by BMC.
Field	Type	Description
ProtocolEnabled	Boolean	Service enabling status: true/false
Port	Number	Service port number.
Oem.Public	Customized field.	-
VirtualMedia-CD/VirtualMedia-HD	Object	-
Timeout	Number	Service timeout period. Unit: seconds.
ProtocolEnabled	Boolean	Service enabling status: true/false
Port	Number	Service port number.
Instance	Number	Number of instances.
NotifyMulticastIntervalSeconds	Number	SSDP notification multicast interval.
NotifyIPv6Scope	String	IPv6 multicast range of SSDP messages: ● link: local link ● Site: local site ● Organization: local organization
NotifyEnabled	Boolean	Whether SSDP multicast is enabled.
VNC	Object	VNC service
SecurePort	Number	Secure port.

4.11 Querying the BMC Management Interface Resource Collection

Function

Query the management port resource collection supported by the current 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

Parameters

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None • Response Example:

```

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

```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	String	OData description of the BMC management interface resource collection model.
@odata.id	String	Type of BMC management interface resource collection.
@odata.type	String	Access path of the BMC management interface resource collection.
Description	String	Description of the BMC management interface resource collection.
Name	String	Name of the BMC management interface resource collection.
Members@odata.count	Number	Number of members in the BMC management interface resource collection.

Members	Object	List of members in the BMC management interface resource collection.
@odata.id	String	Access path of a single BMC management interface resource node.

4.12 Querying Information About a Specified BMC Management Interface Resource

Function

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

Syntax

- Operation Type: GET

- URL:

```
https://device_ip/redfish/v1/Managers/manager_id/EthernetInterfaces/  
id
```

- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#EthernetInterface.EthernetInterface",
  "@odata.id": "/redfish/v1/Managers/1/EthernetInterfaces/D64FE89CE17C",
  "@odata.type": "#EthernetInterface.v1_6_2.EthernetInterface",
}
```

```

    "Id": "D64FE89CE17C",
    "Name": "D64FE89CE17C",
    "MACAddress": "D6:4F:E8:9C:E1:7C",
    "PermanentMACAddress": "BE:0B:64:49:40:C0",
    "InterfaceEnabled": true,
    "MTUSize": 1500,
    "AutoNeg": true,
    "FullDuplex": true,
    "SpeedMbps": 1000,
    "Description":
    "Ethernet Interface D64FE89CE17C",
    "HostName":
    "iSACD64FE89CE17C",
    "IPv4Addresses": [
        {
            "Address": "192.168.5.7",
            "Gateway": "0.0.0.0",
            "SubnetMask": "255.255.255.0",
            "AddressOrigin": "Static"
        }
    ],
    "IPv6DefaultGateway": "::",
    "IPv6Addresses": [
        {
            "Address": "fe80::4e09:b4ff:fe07:622",
            "AddressOrigin": "LinkLocal",
            "PrefixLength": 64
        },
        {
            "Address": "::",
            "PrefixLength": 80,
            "AddressOrigin": "DHCPv6"
        }
    ],
    "IPv6StaticAddresses": [
        {
            "Address": "::",
            "PrefixLength": 0
        }
    ],
    "Oem": {
        "Public": {
            "IPStacks": "IPv4AndIPv6",
            "DNSServiceEnabled": true,
            "DNSDhcpEnabled": true,
            "PatchInProgress": false,

```



```

        "DoMain": "",
        "VLANPriority": 0,
        "NetworkPortMode": "Automatic",
        "NCSIModeSelect": null,
    "ManagementNetworkPort": [
        {
            "Type": "Dedicated",
            "CardNumber": null,
            "PortNumber": 0
        }
    ],
    "ManagementNetworkPort@Redfish.AllowableValues": [
        {
            "Type": "Dedicated",
            "CardNumber": null,
            "PortNumber": 0
        },
        {
            "Type": "ShareLink",
            "CardNumber": 1,
            "PortNumber": 1
        },
        {
            "Type": "ShareLink",
            "CardNumber": 1,
            "PortNumber": 2
        },
        {
            "Type": "ShareLink",
            "CardNumber": 2,
            "PortNumber": 1
        },
        {
            "Type": "ShareLink",
            "CardNumber": 2,
            "PortNumber": 2
        }
    ]
},
    "NameServers": [
        ":",
        "0.0.0.0",
        ":"
    ]

```

```

    },
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "VLAN": {
        "VLANEnable": false,
        "VLANId": 0
    }
}

```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	String	OData description of the specified BMC management interface resource model.
@odata.id	String	Access path of the specified BMC management interface resource node.
@odata.type	String	Type of the specified BMC management interface resource.
Id	String	ID of the specified BMC management interface resource.
Name	String	Name of the specified BMC management interface resource.
PermanentMACAddress	String	Permanent MAC address allocated to the interface.
InterfaceEnabled	Boolean	Whether the interface is enabled.
MTUSize	Number	MTU configured on the current interface (in bytes).
AutoNeg	Boolean	Whether auto-negotiation is enabled. including: ● true ● false

FullDuplex	Boolean	Whether full-duplex mode is used. including: ● true ● false
------------	---------	--

Field	Type	Description
SpeedMbps	Number	Current rate (in Mbps).
Description	String	Description of the specified BMC management interface resource.
HostName	String	DNS hostname, which does not contain any domain information.
IPv4Addresses	Array	IPv4 information object.
Address	String	IPv4 address.
AddressOrigin	String	Origin of the IPv4 address. including: ● Static ● DHCP
Gateway	String	IPv4 gateway address.
SubnetMask	String	IPv4 subnet mask.
IPv6DefaultGateway	String	Default IPv6 gateway.
IPv6Addresses	Array	IPv6 information object.
Address	String	IPv6 address.
AddressOrigin	String	Origin of the IPv6 address. including: ● Static ● DHCP
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.
Oem.Public	Object	OEM object.

IPStacks	String	IPv4/IPv6 enabling switch: ● null: interface not enabled ● IPv4: IPv4 enabled only ● IPv6: IPv6 enabled only ● IPv4AndIPv6: IPv4 and IPv6 both enabled
DNSServiceEnabled	Boolean	Whether the DNS service is enabled.
DNSDhcpEnabled	Boolean	Manual or automatic DNS switch: ● true: automatic ● false: manual
PatchInProgress	Boolean	Configuration validity flag:

Field	Type	Description
		● true: being configured ● false: applied successfully
DoMain	String	Domain name.
VLANPriority	Number	VLAN priority, range: 0–7.
NetworkPortMode	String	Network port mode: ● Automatic ● Fixed ● Standalone
NCSIModeSelect	String	NCSI mode: ● Automatic ● Manual ● null: default setting when NetworkPortMode is set to Fixed.
ManagementNetworkPort	Array	In fixed mode of the specified management network port, there is only one group of BMC management network port data. In automatic mode and standalone mode, the data is dedicated port data and shared port data respectively.
Type	String	● Dedicated: dedicated network port ● ShareLink: shared network port

CardNumber	Number	The default value of the dedicated network port is null, and the default value of the shared network port is: 1: NIC 1 2: NIC 2
PortNumber	Number	For a dedicated network port, the default serial number is set to 0. For a shared network port, the silkscreen number of the network port is set to 1 through 4.
ActualPortNumber	Number	Actual silk screen number of the network interface, range: 1–4. This field is displayed only when the network port mode is set to standalone or automatic (the selected network port is not a dedicated port) and the NCSI mode is set to automatic.
ManagementNetworkPort @Redfish.AllowableValues	Array	All available network ports of the BMC.
NameServers	Array	Domain name server list.
Field	Type	Description
Status	Object	Status information about the specified BMC management interface resource. - State: whether the BMC management interface is enabled. - Health: health status of the BMC management interface.
VLAN	Object	VLAN information object.
VLANEnable	Boolean	Whether VLAN is enabled: - true: enabled - false: disabled
VLANId	Number	Configured VLAN ID, range: 2–4094.

4.13 Modifying a Specified BMC Management Interface Resource

Function

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

Syntax

- Operation Type: PATCH

- **URL:**

*https://device_ip/redfish/v1/Managers/manager_id/EthernetInterfaces/
id*

- **Request Header:**

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

- **Request Message Body:** → **IPv4** configuration:

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

→ **IPv6** configuration:

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

→ **VLAN** configuration:

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

→ **HostName configuration:**

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

→ **NameServers configuration:**

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

→ **Network port mode configuration:**

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

Parameters

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

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

Parameter	Description	Value
hostname	Hostname.	Customized hostname: ● Cannot exceed 64 characters. ● Consists of digits, letters, and hyphens (-). ● Cannot begin or end with a hyphen.
ipv4_address	IPv4 IP address	String, valid IPv4 address.
ipv4_address_origin	Origin of the IPv4 address.	● "Static": configures a static IPv4 address. ● "DHCP": assigns the address through DHCP.
ipv4_subnet_mask	IPv4 subnet mask.	String, valid IPv4 address.
ipv4_gateway	IPv4 gateway.	String, valid IPv4 gateway.
ipv6_address	IPv6 address.	String, valid IPv6 address.
ipv6_address_origin	Origin of the IPv4 address.	● "Static": configures a static IPv6 address. ● "DHCPv6": assigns the address through DHCP.

Parameter	Description	Value
ipv6_prefix	Prefix length of the IPv6 address.	Integer type, range: 1–128.
Gw_value	Default IPv6 gateway.	In IPv6 format.
nameserver	Domain name server.	One primary server and two secondary servers are included. Valid IPv4 or IPv6 addresses are used. The domain and nameservers must be set together.

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

card_number	Number	The value of the dedicated network port does not need to be reported. The value of the shared network port is as follows: • 1: NIC 1 • 2: NIC 2
port_number	Number	For a dedicated network port, the default value is 0. For a shared network port, the silkscreen number of the network port is used. Range: 1–4.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: → IPv4 configuration:

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

→ IPv6 configuration:

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

→ **VLAN configuration:**

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

→ **HostName configuration:**

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

→ **NameServers configuration:**

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

→ **Network port mode configuration:**

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

- Response Example: None
- Status Code: 204

Output Description

None

4.14 Restarting the BMC

Function

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

Syntax

- Operation Type: POST
- [URL](#):
`https://device_ip/redfish/v1/Managers/manager_id/Actions/Manager.Reset`
- Request Header:

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

- Request Message Body:

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

Parameters

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

Table 4-22 Parameter Descriptions for Restarting the BMC

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

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

- Response Example:

```
{
  "@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"
  },
}
```

- Response Code: 200

Output Description

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

Table 4-23 Output Descriptions for Restarting the BMC

Field	Type	Description
code	String	String indicating the specified message ID in the message registry.
message	String	Readable 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 interface. • OK • Warning • Critical
Resolution	String	Solution.

4.15 Querying Information About the LLDP Service Configuration Resource

Function

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

Syntax

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

x-auth-token:auth_value

- Request Message Body: None

Parameters

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#LldpService.LldpService",
  "@odata.etag": "\"1596405264\"",
  "@odata.id": "/redfish/v1/Managers/1/LldpService",
  "@odata.type": "#LldpService.v1_0_0.LldpService",
  "Description": "LLDP Service",

  "Id": "LldpService",
  "LldpEnabled": true,
  "Name": "LldpService",
  "WorkMode": "TxRx"
}
```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	String	OData description of the LLDP resource model.
@odata.id	String	Access path of the LLDP resource.
@odata.type	String	Type of LLDP resource.
Description	String	Description of the LLDP resource.
Id	String	ID of the LLDP resource.
Name	String	Name of the LLDP resource.
LldpEnabled	Boolean	Whether LLDP is enabled: • true: enabled • false: disabled

WorkMode	String	LLDP operation mode: ● TxRx: both transmitting and receiving ● Rx: receiving ● Disabled: neither sending nor receiving
----------	--------	--

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
}
```

Parameters

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

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

Parameter	Description	Value
manager_id	ID of the Manager resource.	For a rack server, the value is 1 or Self.
enable_value	Whether LLDP is enabled.	● true: enabled ● false: disabled
workmode_value	String	LLDP operation mode: ● TxRx: both transmitting and receiving ● Rx: receiving When LLDP is enabled, the default setting is TxRx. If LLDP is disabled, workmode_value is unavailable.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

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

- Response Example:

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

- Status Code: 200

Output Description

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

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

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

Id	String	ID of the LLDP resource.
Name	String	Name of the LLDP resource.
LldpEnabled	Boolean	Whether LLDP is enabled: ● true: enabled ● false: disabled
WorkMode	String	LLDP operation mode: ● TxRx: both transmitting and receiving ● Rx: receiving ● Disabled: neither sending nor receiving

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:

x-auth-token:auth_value

- Request Message Body: None

Parameters

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#SnmpService.SnmpService",
  "@odata.id":
    "/redfish/v1/Managers/1/SnmpService",
  "@odata.type": "#SnmpService.v1_2_0.SnmpService",
  "Actions": {
    "#SnmpService.SubmitTestEvent":
      {
        "target":
```

```

        "/redfish/v1/Managers/1/SnmpService/Actions/SnmpService.SubmitTestEvent"
    },
    "Id": "SnmpService",
    "Name": "SnmpService",
    "ComplexPwEnable": true,
    "ReadOnlyCommunity": null,
    "ReadWriteCommunity": null,
    "SnmpServiceEnable": true,
    "SnmpServicePort": 161,
    "SnmpTrapNotification": {
"TrapServer": [
    {
        "MemberId": "0",
        "TrapServerAddress": "1.2.3.4",
        "TrapServerEnable": true,
"TrapServerPort": 110
    }, {
        "MemberId": "1",
        "TrapServerAddress": "1.2.3.4",
        "TrapServerEnable": false,
"TrapServerPort": 111
    }, {
        "MemberId": "2",
        "TrapServerAddress": "2.3.4.5",
        "TrapServerEnable": false,
"TrapServerPort": 111
    }
],
    "AlarmSeverity": "Normal",
    "TrapHostIdentify": "BoardSN",
    "TrapV3User": "",
    "TrapVersion": "V2C",
    "TrapServer@odata.count": 3,
    "snmpTrapCommunity": "public",
    "snmpTrapEnable": true
},
    "SnmpV3AuthUser": [
    {
        "snmpV3AuthProtocol": "SHA",
        "snmpV3PrivProtocol": "AES",
"UserName": "Administrator"
    }
],

```

```
"SnmpV3AuthUser@odata.count": 1,
"SnmpV3EngineID": "0x80000f3e035ed7580e2ddd"
}
```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	Character string	OData description of the resource model.
@odata.id	Character string	Access path of the SNMP resource.
@odata.type	Character string	Type of SNMP resource.
Actions	Object	Operations that can be performed on the SNMP resource.
SnmpService.SubmitTestEvent	Object	Sends an SNMP trap test event.
target	Character string	Access path for sending the SNMP trap test event.
Id	Character string	ID of the SNMP resource.
Name	Character string	Name of the SNMP resource.
ComplexPwdEnable	Boolean	Complex password switch: ● true: on. ● false: off.
ReadOnlyCommunity	Character string	Name of the SNMP read-only community. This attribute contains sensitive information and is displayed as null. The PATCH operation is supported.
ReadWriteCommunity	Character string	Name of the SNMP read/write community. This attribute contains sensitive information and is displayed as null. The PATCH operation is supported.
SnmpServiceEnable	Boolean	SNMP switch: ● true: on. ● false: off.

SnmpServicePort	Digit	SNMP service port.
SnmpTrapNotification	Object	SNMP Trap properties.
TrapServer	Array	SNMP Trap server information.
MemberId	Character string	SNMP Trap group member ID.

Field	Type	Description
TrapServerAddress	Character string	SNMP Trap server address.
TrapServerEnable	Boolean	Current Trap Server status: ● true: enabled ● false: disabled
TrapServerPort	Digit	SNMP Trap server port number.
AlarmSeverity	Character string	Event severity: ● Critical ● Major ● Minor ● Normal
TrapHostIdentify	Character string	Trap host ID: ● BoardSN: board serial number. ● ProductAssetTag: product asset tag. ● HostName: hostname.
TrapV3User	Character string	SNMPv3 username.
TrapVersion	Character string	SNMP Trap version number.: ● V1 ● V2C ● V3
TrapServer@odata.count	Digit	Number of SNMP Trap servers.
snmpTrapCommunity	Character string	SNMP Trap community name.
snmpTrapEnable	Boolean	SNMP Trap switch: ● true: on. ● false: off.

SnmpV3AuthUser	Array	This array lists the information about all users with the SNMP permission.
snmpV3AuthProtocol	Character string	SNMPv3 user authentication algorithm: • SHA • MD5 • SHA256 • SHA384 • SHA512
snmpV3PrivProtocol	Character string	SNMPv3 user encryption algorithm: • DES • AES
UserName	Character string	Username of the account with the SNMP permission.
Field	Type	Description
SnmpV3AuthUser@oda-ta.count	Digit	Number of users with the SNMP permission.
SnmpV3EngineID	Character string	SNMPv3 engine ID.

4.18 Modifying Properties of the SNMP Resource

Function

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

Syntax

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

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

- Request Message Body:

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

```
        "TrapServerAddress": TrapServerAddress,
        "TrapServerEnable": TrapServerEnable,
  "TrapServerPort": TrapServerPort
      }
    ]
  }
}
```

Parameters

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

Table 4-30 Parameter Descriptions for Modifying the SNMP Resource

Field	Type	Description
-------	------	-------------

ComplexPwdEnable	Character string	Complex password switch: ● true: on. ● false: off. If SnmpServiceEnable is set to true, this parameter must be set. If SnmpServiceEnable is set to false, no verification is performed.
ReadWriteCommunity	Character string	This parameter can be configured when SnmpServiceEnable is set to true. SNMP read-write community name. The naming rule for this parameter is as follows: ● Community name rule when the complex password switch is on: The name supports 8– 32 characters, including at least letters, digits, and one special character, which can be any visible characters except for a space (" "), single quotation mark ("'"), or backslash("\"). The name cannot begin with a pound sign ("#"). ● Community name rule when the complex password switch is off: The name supports 1 –32 characters including digits, letters, and special characters. Allowed special characters: visible characters except for a space (" "), single quotation mark ("'"), or backslash("\"). The name cannot begin with a pound sign ("#"). ReadWriteCommunity is not required. If it is set, verification is performed. If it is not set, no verification is performed.

Field	Type	Description
-------	------	-------------

ReadOnlyCommunity	Character string	This parameter can be configured when SnmpServiceEnable is set to true. SNMP read-only community name. The naming rule for this parameter is as follows: - Community name rule when the complex password switch is on: The name supports 8– 32 characters, including at least letters, digits, and one special character, which can be any visible characters except for a space (" "), single quotation mark ("'"), or backslash("\"). The name cannot begin with a pound sign ("#"). - Community name rule when the complex password switch is off: The name supports 1 –32 characters including digits, letters, and special characters. Allowed special characters: visible characters except for a space (" "), single quotation mark ("'"), or backslash("\"). The name cannot begin with a pound sign ("#"). ReadOnlyCommunity is not required, and will be checked only if there is a value.
SnmpServiceEnable	Boolean	SNMP switch: - true: on. - false: off.
SnmpServicePort	Digit	SNMP port number, range: 1–65535, which cannot be null. If SnmpServiceEnable is set to true, this parameter must be set. If SnmpServiceEnable is set to false, no verification is performed.
snmpTrapCommunity	Character string	SNMP Trap community name, which is a string of 1–18 characters including digits, letters, and special characters. Allowed special characters: visible characters except for a space (" "), single quotation mark ("'"), or backslash("\"). The name cannot begin with a pound sign ("#"). If TrapVersion is set to V1 or V2C, this parameter must be set. If TrapVersion is set to V3, no verification is performed.

snmpTrapEnable	Boolean	SNMP Trap switch:
----------------	---------	-------------------

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
  "ComplexPwdEnable": true,
  "SnmpServiceEnable": true,
  "SnmpServicePort": 161,
  "ReadWriteCommunity": "7654321b&",
  "ReadOnlyCommunity": "1234567a$",
  "SnmpTrapNotification": {
    "snmpTrapEnable": true,
    "snmpTrapCommunity": "public",
    "AlarmSeverity": "Normal",
    "TrapHostIdentify": "BoardSN",
    "TrapVersion": "V2C", "TrapServer": [
      {
        "MemberId": "0",
        "TrapServerAddress": "1.2.3.4",
        "TrapServerEnable": false,
        "TrapServerPort": 110
      },
      {
```

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

Separate SNMP instance configuration:

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

Separate SNMP Trap instance configuration:

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

Separate SNMP Trap Server instance configuration:

```
{
  "SnmpTrapNotification": {
  "TrapServer": [
    {
      "MemberId": "0",
      "TrapServerAddress": "1.2.3.4",
      "TrapServerEnable": false,

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

- Response Example: None
- Response Code: 204

Output Description

None

4.19 Submitting an SNMP Trap Test Event

Function

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

Syntax

- Operation Type: POST
- [URL](#):
`https://device_ip/redfish/v1/Managers/manager_id/SnmpService/Actions/SnmpService.SubmitTestEvent`
- Request Header:

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

- Request Message Body:

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

Parameters

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

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

Parameter	Description	Value
MemberId	Trap group member ID .	Range: 1–4.

Usage Guidelines

None

Example

- Request Example:

POST https://device_ip/redfish/v1/Managers/1/SnmpService/Actions/SnmpService.SubmitTestEvent
- Request Header:

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

Request Message Body:

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

- Response Example: None
- Response Code: 204

Output Description

None

4.20 Querying the Virtual Media Resource Collection

Function

Query the virtual media resource collection.

Syntax

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

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

- Request Message Body: None

Parameters

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#VirtualMediaCollection.VirtualMediaCollection",
  "@odata.id": "/redfish/v1/Managers/1/VirtualMedia",
  "@odata.type": "#VirtualMediaCollection.VirtualMediaCollection",
  "Description": "Virtual Media Services Settings",
  "Members": [
    {
      "@odata.id":
"/redfish/v1/Managers/1/VirtualMedia/CD"
    },
    {
      "@odata.id":
"/redfish/v1/Managers/1/VirtualMedia/CD1"
    },
    {
      "@odata.id":
"/redfish/v1/Managers/1/VirtualMedia/USBStick"
    },
    {
      "@odata.id":
"/redfish/v1/Managers/1/VirtualMedia/USBStick1"
    }
  ],
  "Members@odata.count": 2, "Name": "Virtual Media Services",
  "@odata.etag": "W/\\"d771a360c6bf8c1b015153492a0abf76\\""
}
```

- Status Code: 200

Output Description

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

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

Field	Type	Description
-------	------	-------------

@odata.context	Character string	OData description of the virtual media resource collection model.
@odata.id	Character string	Access path of the virtual media resource collection.
@odata.type	Character string	Type of virtual media resource collection.
Description	Character string	Description
Members	Object	Virtual media resource list. The CD1 and USBStick1 resources can be queried and used only when the number of entities is set to two.
@odata.id	Character string	Access path of the virtual media resource collection.
Members@odata.count	Number	Number of virtual media resource members that can be connected currently.
Name	Character string	Name of the virtual media resource collection.

4.21 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

Parameters

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

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#VirtualMedia.VirtualMedia",
  "@odata.id": "/redfish/v1/Managers/1/VirtualMedia/CD",
  "@odata.type": "#VirtualMedia.v1_2_0.VirtualMedia",
  "Description": "CD VirtualMedia",
  "ConnectedVia": "NotConnected",
  "Id": "CD",
  "Name": "VirtualMedia",
  "Image": null,
}
```

```

    "ImageName": null,
    "Inserted": false,
    "MediaTypes": null,
    "TransferMethod": null,
    "TransferProtocolType": null,
    "Oem": {
        "Public": {
            "Actions": {
                "#VirtualMedia.VmmControl": {
"@Redfish.ActionInfo":
"/redfish/v1/Managers/1/VirtualMedia/CD/VmmControlActionInfo",
"target":
"/redfish/v1/Managers/1/VirtualMedia/CD/Actions/
VirtualMedia.VmmControl"
                }
            }
        }
    },
    "@odata.etag":
"W/\\"0d1832b8465870af53e53e44961eacdd\\"
}

```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	Character string	OData description of the virtual media resource model.
@odata.id	Character string	Access path of the virtual media resource.
@odata.type	Character string	Type of virtual media resource.
Description	Character string	Description.
ConnectedVia	Character string	Connection method.
Id	Character string	ID of the virtual media resource.
Name	Character string	Name of the virtual media resource.

MediaTypes	Object	Media plane type: - CD - CD1 - USBStick
Field	Type	Description
		USBStick1
TransferProtocolType	Character string	Transmission protocol type: - NFS - CIFS - HTTPS
TransferMethod	Character string	Transfer method: stream
Image	Character string	Image path.
ImageName	Character string	Image name.
ConnectedVia	Character string	Connection method.
Inserted	Boolean	Connection status: - true: mounting (inserted) - false: Uninstalled (removed)
Oem	Object	Customized properties of a specified session.

4.22 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/Actions/VirtualMedia.VmmControl`

- Request Header:

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

- Request Message Body:

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

Parameters

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

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

- Response Example:

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

- Status Code: 200

Output Description

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

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

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

4.23 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/Actions/VirtualMedia.VmmControl`
- Request Header:

x-auth-token:auth_value

Content-Type:header_type

- Request Message Body:

{

"VmmControlType":value

}

Parameters

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

Table 4-38 Parameter Descriptions for Disconnecting the Virtual Media

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

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

- Response Example:

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

- Status Code: 200

Output Description

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

Table 4-39 Output Descriptions for Disconnecting the Virtual Media

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

4.24 Sending a One-Click Collection Request

Function

Send a one-click collection request.

Syntax

- Operation Type: POST

- URL:

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

- Request Header:

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

- Request Message Body:

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

Parameters

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

Table 4-40 One-Click Collection Request Parameter Descriptions

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

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

- Response Example:

```
{
  "error": {
    "code": "Base.1.8.1.Success",
    "message": "Successfully Completed Request",
    "@Message.ExtendedInfo": [
      {
        "@odata.type": "#Message.v1_1_1.Message",
        "MessageId": "Base.1.8.1.Success",
        "Message": "Successfully Completed Request",
        "Severity": "OK",
        "Resolution": "None."
      }
    ]
  },
  "@odata.context": "/redfish/v1/$metadata",
  "@odata.id":
  "/redfish/v1/Managers/Self/LogServices/Actions/LogServices.Dump"
}
```

- Status Code: 200

Output Description

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

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

Field	Type	Description
code	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 supported by Redfish. Options: • OK • Warning • Critical
Resolution	Character string	Solution.

4.25 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/LogServices/Actions/LogServices.Dump/Progress`

- **Request Header:**

x-auth-token:auth_value

- Request Message Body: None

Parameters

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.content": "/redfish/v1/$metadata",
  "@odata.id": "/redfish/v1/Managers/Self/LogServices/Actions/
    LogServices.Dump/Progress",
  "@odata.type": "#PCIeDevice.v1_4_0.PCIeDevice",
  "Message": "SUCCEEDED",
  "Percentage": "100",
  "State": "STATE_SUCCEEDED",
  "TarName": "bmcinfo_UnknownProductSN.tar.gz",
  "TarPath": "/var/bmcdata/bmcinfo_UnknownProductSN.tar.gz",
  "Type": "Logs"
}
```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	Character string	OData description for the query of the one-click log collection progress.
@odata.id	Character string	Access path for the query of the one-click log collection progress.
@odata.type	Character string	Type of query of the one-click log collection progress.
Percentage	Character string	Task progress percentage.

State	Character string	Status, options: ● STATE_FAILED ● STATE_SUCCEEDED ● STATE_RUNNING ● STATE_SILENT
Type	Character string	Type. Only the Logs type is available in this version.
Message	Character string	Task progress status, including: ● SILENT: indicates that collection is triggered. ● RUNNING: indicates that collection is in progress. ● SUCCEEDED: indicates that collection is completed and successful. ● FAILED: indicates that an error occurs during collection.
TarName	Character string	File name of the compressed package, in which UnknownProductSN varies with the actual SN . If the actual SN is not obtained, UnknownProductSN is used.
TarPath	Character string	Storage path of the local compressed package.

4.26 Exporting Logs

Function

Export the log information about a server.

Syntax

- Operation Type: POST
- [URL](#):
`https://device_ip/redfish/v1/Managers/manager_id/LogServices/Actions/LogServices.ExportLogs`
- Request Header:

x-auth-token:auth_value

Content-Type:header_type

- Request Message Body:

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

Parameters

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

Table 4-44 Log Export Parameter Descriptions

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

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

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

- Response Example:

```
{
  "error": {
    "code": "Base.1.8.1.Success",      "message": "Successfully
Completed Request",
    "@Message.ExtendedInfo": [
      {
        "@odata.type": "#Message.v1_1_1.Message",
        "MessageId": "Base.1.8.1.Success",      "Message":
"Successfully Completed Request",
        "Severity": "OK",
        "Resolution": "None."
      }
    ]
  },
  "@odata.context": "/redfish/v1/$metadata",
  "@odata.id": "/redfish/v1/Managers/1/LogServices/Actions/LogServices.ExportLogs"
}
```

- Status Code: 200

Output Description

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

Table 4-45 Log Export Descriptions

Field	Type	Description
code	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. The Redfish supports the following severity levels: • OK • Warning • Critical
Resolution	Character string	Solution.

4.27 Querying the KVM Service Resource

Function

Query [KVM](#) resource information.

Syntax

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

x-auth-token:auth_value

- Request Message Body: None

Parameters

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45pPFIC8QG2lp2F0=
```

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#KvmService.KvmService",
  "@odata.id": "/redfish/v1/Managers/Self/KvmService",
  "@odata.type": "#KvmService.v1_0_0.KvmService",
  "ActivatedSessionsType": "Private",
  "EncryptionEnabled": true,
  "Description": "KvmService",      "KvmUrl":
    "https://192.168.5.7/viewer.html?&token=IywH3U7qkcKzW8aKb",
  "MaximumNumberOfSessions": 4,
  "NumberOfActivatedSessions": 0,
  "SessionTimeoutMinutes": 30,
  "@odata.etag":
    "w/\\"8dd4d65018cdc6ed251faeac4fdd27c5\\""}

```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	Character string	OData description of the KVM service resource model.
@odata.id	Character string	Access path of the KVM resource.
@odata.type	Character string	Type of KVM service resource.
MaximumNumberOfSessions	Number	Maximum number of KVM sessions.
KvmUrl	Character string	URL for accessing the KVM resource. When the URL is used for access, the Web session is automatically logged out.
NumberOfActivatedSessions	Number	Number of current KVM sessions.

ActivatedSessionsType	Character string	KVM session type. Options: • Shared: Shared • Private: Exclusive
EncryptionEnabled	Boolean	Enables or disables KVM encryption. Options: • true: enabled. • false: disabled.
SessionTimeoutMinutes	Number	Session timeout time, range: 1–60, unit: minutes.

4.28 Modifying Information About the KVM Resource

Function

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

Syntax

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

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

- Request Message Body:

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

Parameters

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

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

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

EncryptionEnabled_value	Whether KVM encryption is enabled.	• true: enabled • false: disabled
SessionTimeout-Minutes_value	Session timeout period.	Range: 1–60, unit: minutes.

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

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

- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#KvmService.KvmService",
  "@odata.id": "/redfish/v1/Managers/Self/KvmService",
  "@odata.type": "#KvmService.v1_0_0.KvmService",
  "ActivatedSessionsType": "Private",

  "EncryptionEnabled": true,
  "Description": "KvmService",
  "MaximumNumberOfSessions": 4,
  "NumberOfActivatedSessions": 0,
  "SessionTimeoutMinutes": 10
}
```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	Character string	OData description of the KVM service resource model.
@odata.id	Character string	Access path of the KVM resource.
@odata.type	Character string	Type of KVM service resource.
MaximumNumberOfSessions	Number	Maximum number of KVM sessions.
NumberOfActivatedSessions	Number	Number of current KVM sessions.
ActivatedSessionsType	Character string	KVM session type. Options: • Shared: shared. • Private: exclusive.
EncryptionEnabled	Boolean	Enables or disables KVM encryption. Options: • true: enabled. • False: disabled.
SessionTimeoutMinutes	Number	Session timeout time, range: 1–60.

4.29 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 4-50](#).

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#LogEntry.LogEntry",
  "@odata.etag": "\"1267901780\"",
  "@odata.id":
"/redfish/v1/Managers/Self/LogServices/SEL/Entries/631",
  "@odata.type": "#LogEntry.v1_4_3.LogEntry",
  "Created": "2010-03-04T14:56:23+08:00",
  "Description": "SEL LOG info",
  "EntryCode": "Assert",
  "EntryType": "SEL",
  "EventTimestamp": "2010-03-04T14:56:23+08:00",
```



```

    "Id": "631",      "Message":
"Initiated By Warm Reset",
    "MessageId": "0x02FFFF",
    "Name": "SEL 1221",
    "SensorNumber": 128,
    "SensorType": "SystemBoot/Restart",
    "Severity": "OK"
}

```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	String	OData description of the specified SEL log service resource model.
@odata.id	String	Access path of the specified SEL log service resource node.
@odata.type	String	Type of the specified SEL log service resource.
Created	String	Time when the SEL log instance is created.
Description	String	Log resource description information.
EntryCode	String	Type of SEL log instance.
EntryType	String	Type of SEL log instance. ● SEL ● Oem
EventTimestamp	String	Timestamp of the SEL log instance information.
Id	String	ID of the SEL log instance.
Message	String	Message content of the SEL log instance information.
Name	String	Name of the SEL log instance.
SensorNumber	Number	ID of the sensor that creates the SEL log instance.

SensorType	String	Type of the sensor that creates the SEL log instance.
Message	String	Details.
Severity	String	Log severity level of the SEL log instance information. OK
Field	Type	Description
		- Warning - Critical - Non-recoverable

4.30 Capturing the Screen Manually

Function

Capture the screen manually.

Syntax

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

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

- Request Message Body: None

Description

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

Table 4-52 Parameter Descriptions for Capturing the Screen Manually

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

header_type	Format of the request message.	application/json
-------------	--------------------------------	------------------

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

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

Output Description

None

4.31 Downloading the Manually Captured Screen Image

Function

Download the manually captured screen image.

Syntax

- Operation Type: POST

- URL:

```
https://device_ip/redfish/v1/Managers/manager_id/Actions/Manager.DownloadScreenShot
```

- Request Header:

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

- Request Message Body: None

Description

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

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

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

- Request Header:

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

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

Output Description

Return the image data of the manually captured screen image.

4.32 Querying Information About the ISDT Resource

Function

Query the information about the ISDT resource of a server.

Syntax

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

X-Auth-Token:auth_value

- Request Message Body: None

Description

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None • Response Example:

```

{
    "@odata.context":
    "/redfish/v1/$metadata#ISDTSERVICE.ISDTSERVICE",
    "@odata.id": "/redfish/v1/Managers/1/ISDTSERVICE",
    "@odata.type": "#ISDTSERVICE.v1_0_0.ISDTSERVICE",
    "ImageInstalled": false,
    "Actions": {
        "#ISDTSERVICE.VmmControl": {
            "@Redfish.ActionInfo":
            "/redfish/v1/Managers/1/ISDTSERVICE/VmmControlActionInfo",
            "target":
            "/redfish/v1/Managers/1/ISDTSERVICE/Actions/ISDTSERVICE.VmmControl"
        }
    },
    "@odata.etag":
    "W/\"53019246fb266788a65ac6a5aecf2b6d\""
}

```

- Status Code: 200

Output Description

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

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

Field	Type	Description
@odata.context	String	OData description of the DNS resource model.
@odata.id	String	Access path of the SNMP resource node.
@odata.type		Type of the ISDT resource.
ImageInstalled	Boolean	Whether there is a navigation disk image.
Actions	Object	Available actions for the ISDT resource.
#ISDTSERVICE.VmmControl	Object	Control operation on the navigation disk.
target	String	Path of the control operation on the navigation disk.

4.33 Modifying Properties of the ISDT Service Resource

Function

Modify properties of the ISDT Service resource.

Syntax

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

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

- Request Message Body:

```
{
  "ServiceEnabled":
  ServiceEnabled_value
}
```

Description

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

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

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
  "ServiceEnabled":
  true
}
```

- Response Example: None
- Status Code: 204

Output Description

None

4.34 Mounting and Dismounting Navigation Disks

Function

Mount and dismount navigation disks.

Syntax

- Operation Type: POST

- URL

https://device_ip/redfish/v1/Managers/manager_id/ISDTSservice/Actions/ISDTSservice.VmmControl

- Request Header:

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

- Request Message Body:

```
{
  "VmmControlType":
  VmmControlType_value
}
```

Description

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

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

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

auth_value	During the execution of the PATCH request, the "Headers" field must carry the "X-Auth-Token" value for authentication.	It can be obtained when a session is created through <i>/redfish/v1/SessionService/Sessions.</i>
VmmControlType	Type of Vmm control.	● Connect: connected ● Disconnect: disconnected

Usage Guidelines

None

Use Cases

- Request Example:

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

- Request Header:

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

- Request Message Body:

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

- Response Example:

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

- Status Code: 200

输出说明

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

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

字段	类型	说明
@odata.context	String	OData description of the ISDT resource model.

@odata.id	String	Access path of the ISDT resource node.
@odata.type	String	Type of ISDT resource.
Information	Object	-
target	String	Access path of the current ISDT resource.

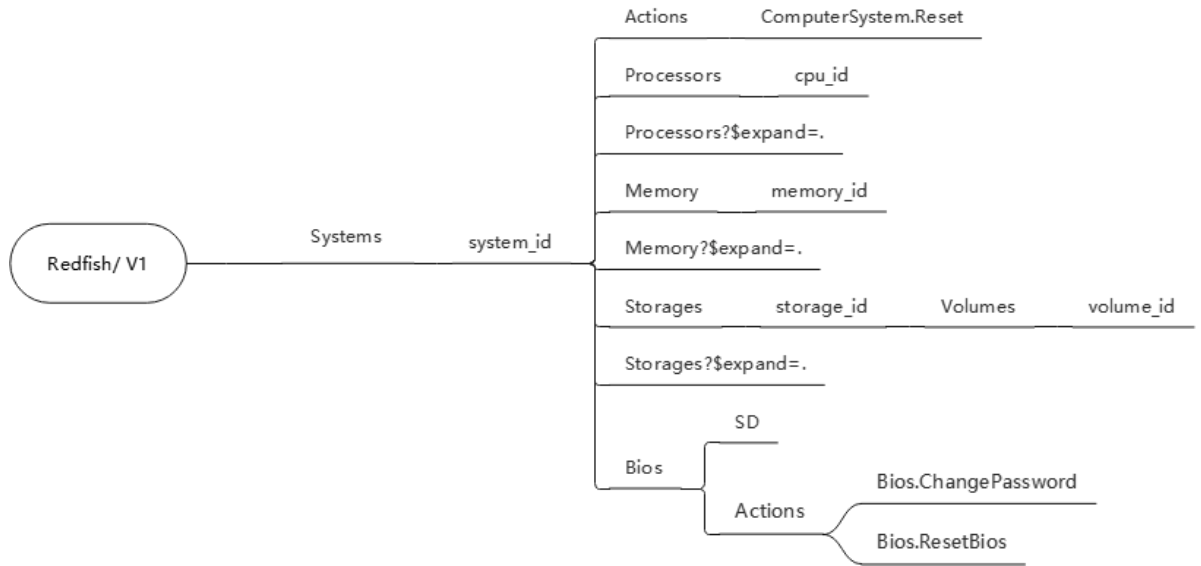
Chapter 5

Operations on System Resources

Table of Contents

Querying Information About the System Resource Collection.....	122
Querying Information About a Specified System Resource.....	124
Remotely Powering On, Powering Off, and Resetting a System Resource.....	132
Modifying Properties of a Specified System Resource.....	134
Querying Information About the CPU Resource Collection.....	138
Querying Information About a Specified CPU Resource.....	140
Querying Information About All CPU Resources.....	144
Querying Information About the Memory Resource Collection.....	147
Querying Information About a Specified Memory Resource.....	149
Querying Information About All Memory Resources.....	152
Querying Information About the Storage Resource Collection.....	155
Querying Information About a Specified Storage Controller Resource.....	157
Querying Information About All Storage Controller Resources.....	161
Querying Information About the Logical Volume Resource Collection.....	166
Querying Information About a Specified Logical Volume Resource.....	168
Creating a Logical Volume.....	172
Deleting a Logical Volume.....	176
Querying Properties of the BIOS Resource.....	178
Querying Information About the BIOS Settings.....	181
Modifying the BIOS Settings.....	184
Setting the BIOS Password.....	185
Restoring the Default BIOS Settings.....	186

Figure 5-1 shows the path requirements for the Systems resources supported by NETAŞ 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	UUID 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
	Boot	Boot parameters of the specified System resource.	GET/PATCH
	BiosVersion	BIOS versions of the specified System resource.	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
	Oem	Customized properties of the System resource.	GET/PATCH

	Actions	Operations that can be performed for the specified System resource.	GET/POST
/redfish/v1/ Systems/system_id/Processors	Name	Name of the CPU resource collection.	GET
	Members@odata.count	Number of CPU resource members.	GET
	Members	CPU resource list, which provides references for all CPU resource URL s.	GET

URL	Property	Description	Operation
/redfish/v1/ Systems/system_id/Processors/cpu_id	Name	CPU name.	GET
	Id	UID of CPU in the iBMC system.	GET
	ProcessorArchitecture	CPU architecture.	GET
	Manufacturer	CPU manufacturer.	GET
	Model	CPU type.	GET
	MaxSpeedMHz	Maximum CPU speed.	GET
	TotalCores	Total number of CPU cores.	GET
	TotalThreads	Total number of CPU threads.	GET
	Socket	CPU socket ID.	GET
	Status	CPU status.	GET
	SerialNumber	Serial number of the specified CPU resource.	GET
	Oem	Customized properties of the 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
	OperatingSpeedMhz	Speed of the specified memory resource.	GET
	SerialNumber	Serial number of the specified memory resource.	GET

URL	Property	Description	Operation
	MemoryDeviceType	Type of the specified memory resource.	GET
	PartNumber	Part number of the specified memory resource.	GET
	DeviceLocator	Screen printing of the specified memory resource.	GET
	BaseModuleType	Basic module type of the specified memory resource.	GET
	MemoryLocation	Location of the specified memory resource.	GET
	Status	Status of the specified memory resource.	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
	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

URL	Property	Description	Operation
	SupportedDeviceProtocols	Protocol type supported by the storage controller.	GET
	Manufacturer	Manufacturer of the storage controller.	GET
	SerialNumber	Serial number of the storage controller.	GET
	Drives@odata.count	Number of drives managed by	GET

			the storage controller.	
	Drives		Drive list.	GET
	Oem		Customized properties of the storage controller.	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
/redfish/v1/ Systems/system_id/Storages/storage_id/Volumes/volume_id	Name		Name of a logical volume.	GET
	VolumeType		Redundancy type of the logical volume.	GET
	RaidControllerID		Controller ID of the logical volume.	GET
	VolumeRaidLevel		RAID level of the logical volume.	GET
	NumDrive		Number of physical disk members.	GET
	Links		Resources link.	GET
	Status		Status of the logical volume.	GET
/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
URL	Property	Description	Operation
/redfish/v1/ Systems/system_id/Bios/SD	Id	ID of the BIOS setting resource.	GET
	Name	Name of the BIOS setting resource.	GET
	AttributeRegistry	Registry resource ID for BIOS properties.	GET
	Attributes	Property list of the current BIOS setting resource.	GET/PATCH

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 <code>/redfish/v1/SessionService/Sessions</code> .
------------	---	---

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
x-auth-token:QnaWfqvKOY0ZGc2LK5Ay6+CaSYWjEYcxE6GcWKNFyjU=
```

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#ComputerSystemCollection.ComputerSystemCollection",
  "@odata.etag": "\"1631391578\"",
  "@odata.id": "/redfish/v1/Systems",      "@odata.type":
"#ComputerSystemCollection.ComputerSystemCollection",
  "Description": "Collection of Computer Systems",      "Members":
  [{
    "@odata.id":
"/redfish/v1/Systems/1"
  }],
  "Members@odata.count": 1,
  "Name": "Systems Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the System resource collection, refer to [Table 5-3](#).

Table 5-3 Output Descriptions for Querying Information About the System resource Collection

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

@odata.id	String	Access path of the System resource collection.
@odata.type	String	Type of System resource collection.
Name	String	Name of the System resource collection.
Members@odata.count	Number	Number of System resource members.
Members	Object	System resource list.
@odata.id	String	Access path of a single System resource node.

5.2 Querying Information About a Specified System Resource

Function

Query information about a specified System resource of a server.



Note

Only the System resource information about the server itself can be queried.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Systems/system_id` • Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified System resource, refer to [Table 5-4](#).

Table 5-4 Parameter Descriptions for Querying Information About the Specified System Resource

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

```
x-auth-token:QnaWfqvKOY0ZGc2LK5Ay6+CaSYWjEYcxE6GcWKNFyjU=
```

- Request Message Body: None
- Response Example:

[illegible]

```

    "Description": "System 1",
    "EthernetInterfaces": {
      "@odata.id":
"/redfish/v1/Systems/1/EthernetInterfaces"
    },
    "HostName":
    "iSACE2814D77795F",
    "Id": "1",
    "IndicatorLED": "Blinking",
    "Links": {
      "Chassis": [
        {
          "@odata.id":
"/redfish/v1/Chassis/1"
        }
      ],
      "CooledBy": [
        {
          "@odata.id":
"/redfish/v1/Chassis/1/Thermal"
        }
      ],
      "ManagedBy": [
        {
          "@odata.id":
"/redfish/v1/Managers/1"
        }
      ],
      "PoweredBy": [
        {
          "@odata.id":
"/redfish/v1/Chassis/1/Power"
        }
      ]
    },
    "LogServices": {
      "@odata.id":
"/redfish/v1/Systems/1/LogServices"
    },
    "Manufacturer": "NETAŞ",
    "Memory": {
      "@odata.id":
"/redfish/v1/Systems/1/Memory"
    },
    "MemoryDomains": {
      "@odata.id":
"/redfish/v1/Systems/1/MemoryDomains"
    },
    "Model": "",
    "Name": "System",
    "NetworkInterfaces": {
      "@odata.id":
"/redfish/v1/Systems/1/NetworkInterfaces"
    },

```



```

    "Oem": {
      "Public": {
        "CPUUsagePercent": 0,
        "IOUsagePercent": 0,
        "MemoryUsagePercent": 0,
        "PowerOnDelayEnabled": true,
        "PowerOnDelayMode": "RandomDelay",
        "PowerOnDelaySeconds": 120,
        "ConfigurationModel": "20220905"
      }
    },
    "ProductSpecificIdentity": "R5300G5E,MI05102A,Intel",
    "BiosVersionDate": "Dec 12 2012",
    "ProductVersion": "?/",
    "ProductName": "a6",
    "ProductExtra": "q6n dtHiGUC12TK6npW6HSjKEiJiuQE
5H791PVoffbKxe2f6f8j5qjxmy2Pe6J4fzaFbmwMojynG
5nocSqPD bnYEV76KGxa2bmqFJOBW8XY7joaOMJOK
PeDtEokxqq7R3law1S68nToFlhGey9fCX03hH9532RjV
uuu8tYn7p 5QwE9s48wL3gVCP3yW6mCv7lHXoM2VQ
N2O1GWA vX9f2c2MHCWk7DxBdH2qbCfYhqpiWFH7
8MNVow15hu5gO29vKrpLk",
    "PartitionLists": [
      {
        "DiskIndex": 1,
        "PartitionName": "/",
        "UsagePercent": 13,
        "TotalCapacityGB": 50
      },
      {
        "DiskIndex": 2,
        "PartitionName": "/boot",
        "UsagePercent": 17,
        "TotalCapacityGB": 1
      },
      {
        "DiskIndex": 3,
        "PartitionName": "/boot/efi",
        "UsagePercent": 5,
        "TotalCapacityGB": 0.2
      },
      {
        "DiskIndex": 4,
        "PartitionName": "/home",
        "UsagePercent": 0,
        "TotalCapacityGB": 2896.9
      }
    ]
  }

```

```
        }
    ],
}

},
"PartNumber": "",
"PowerState": "On",
"Processors": {          "@odata.id":
"/redfish/v1/Systems/1/Processors"
},
"SecureBoot": {          "@odata.id":
"/redfish/v1/Systems/1/SecureBoot"
},
"SerialNumber": "",
"SimpleStorage": {       "@odata.id":
"/redfish/v1/Systems/1/SimpleStorage"
},
"Status": {
    "Health": "OK",
    "HealthRollup": "OK",
"State": "Enabled"
},
"Storage": {             "@odata.id":
"/redfish/v1/Systems/1/Storage"
},
"Storages": {            "@odata.id":
"/redfish/v1/Systems/1/Storages"
},
"SystemType": "Physical",    "UUID":
"30e72400-0000-1000-0000-000000000000",
"Bios": {                 "@odata.id":
"/redfish/v1/Systems/1/Bios"
}
}
```

- Status Code: 200

Output Description

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

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

Field	Type	Description
-------	------	-------------

@odata.context	String	OData description of the specified System resource model.
@odata.id	String	Access path of the specified System resource.
@odata.type	String	Type of System resource.
Actions	Object	Operations that can be performed for the specified System resource through the Redfish interface.
#ComputerSystem.Reset	Object	OS operation.
target	String	Access path of the restart operation properties.
ResetType@Redfish. AllowableValues	Object	OS operations allowed through the Redfish interface, including: ● On ● ForceOff ● GracefulShutdown ● ForceRestart ● ForcePowerCycle
AssetTag	String	Asset tag of the specified System resource.
BiosVersion	String	BIOS version of the specified System resource.
Boot	Object	Boot parameters of the specified System resource.
BootSourceOverrideEnabled	String	Mode for applying the current boot settings of the System.
BootSourceOverrideMode	String	System boot mode.
BootSourceOverrideTarget	String	Current boot settings of the System.
BootSourceOverrideEnabled@Redfish.AllowableValues	Object	Options of the mode for applying the current boot settings of the System, including: ● Once: effective only once

		Continuous: effective permanently
BootSourceOverrideTarget@Redfish.AllowableValues	Object	Range of the boot devices defined by Redfish, including:

Field	Type	Description
		- None - PXE - Floppy - CD - HDD - BiosSetup
Description	String	Description of the specified System resource.
EthernetInterfaces	Object	Access path of the Ethernet interfaces of the host.
HostName	String	Hostname of the specified System resource.
Id	String	ID of the specified System resource.
IndicatorLED	String	Position indicator status of the specified Chassis resource, including:
Links	Object	System resource links.
Chassis	Object	Access path of the Chassis resource node.
CooledBy	Object	Access path of the fan resource node.
ManagedBy	Object	Access path of the Manager resource node.
PoweredBy	Object	Access path of the power resource.
LogServices	Object	Access path of the log service resource node.

Manufacturer	String	Manufacturer of the specified System resource.
Memory	Object	Access path of the memory resource node.
MemoryDomains	Object	V3 field.
Model	String	Model of the specified System resource.
Name	String	Name of the specified System resource.
NetworkInterfaces	Object	Access path of the network interfaces.
Oem.Public	Object	Customized properties.
CPUUsagePercent	Number	Dynamic CPU usage detected by CUPS.

Field	Type	Description
IOUsagePercent	Number	Dynamic I/O usage detected by CUPS.
MemoryUsagePercent	Number	Dynamic memory usage detected by CUPS.
PowerOnDelayEnabled	Boolean	Whether to enable power-on delay: ● true ● false
PowerOnDelayMode	String	Power-on delay mode: ● CustomDelay: custom delay mode. ● RandomDelay: random delay mode.
PowerOnDelaySeconds	Number	Power-on delay.
ConfigurationModel	String	Year + typical configuration model. The configuration value must be in dictionary format.
ProductSpecificIdentity	String	Internally defined product name.
BiosVersionDate	String	BIOS version date.
ProductVersion	String	Product version.
ProductName	String	Product name.

ProductExtra	String	Additional product information.
PartNumber	String	Part number of the specified System resource.
PartNumber	String	Part number of the specified System resource.
PowerState	String	Power-on status of the specified System resource: ● On ● Off
Processors	Object	Access path of the processor resource node.
SerialNumber	String	Serial number of the specified System resource.
Status	Object	Status of the specified System resource: ● Health: The System resource is healthy. ● Status: The System resource is enabled.
Field	Type	Description
Storage	Object	Access path of the storage resource node.
Storages	Object	Access path of the storage resource node.
UUID	String	Globally unique ID of the specified System resource.
Bios	Object	Access path of the BIOS resource node.
DiskIndex	Number	Disk partition number.
PartitionName	String	Disk partition name.
TotalCapacityGB	Number	Total disk partition capacity.
UsagePercent	Number	Disk partition usage.

5.3 Remotely Powering On, Powering Off, and Resetting a System Resource

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 System resource.	For a rack server, the value is 1 or Self.
Parameter	Description	Value
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
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:

```
{
  "error": {
    "code": "Base.1.8.1.Success", "message":
    "Successfully Completed Request",
    "@Message.ExtendedInfo": [{
      "@odata.type": "#Message.v1_1_1.Message",
      "MessageId": "Base.1.8.1.Success",
      "Message": "Successfully Completed Request",
      "Severity": "OK",
      "Resolution": "None."
    }]
  },
  "@odata.context": "/redfish/v1/$metadata",
  "@odata.id": "/redfish/v1/Systems/Self/Actions/ComputerSystem.Reset"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you perform a remote operation, refer to [Table 5-7](#).

Table 5-7 Output Descriptions for Remote Operations

Field	Type	Description
code	String	ID of the specified message in the message registry.
message	String	Error message corresponding to the message in the message registry.
@odata.type	String	OData description of the message resource.
MessageId	String	Message ID.
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, host name, 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": "zichanbiaoqian-001",
  "HostName": "iSAC-20221022",
  "Oem": {
    "Public": {
      "ConfigurationModel": "2022C2",
      "PowerOnDelayEnabled": true,
      "PowerOnDelayMode": "CustomDelay",
      "PowerOnDelaySeconds": 100
    }
  },
  "Boot": {
    "BootSourceOverrideMode": "Legacy",
    "BootSourceOverrideEnabled": "Continuous",
    "BootSourceOverrideTarget": "Pxe"
  }
}
```

→ Separate asset tag configuration:

```
{
  "AssetTag": "zichanbiaoqian-001"
}
```

→ Separate hostname configuration:

```
{
  "HostName": "iSAC-20221022"
}
```

→ Separate typical configuration model configuration:

```
{
  "Oem": {
    "Public": {
      "ConfigurationModel": "2022C2"
    }
  }
}
```

→ Separate power-on delay configuration:

```
{
  "Oem": {
    "Public": {
      "PowerOnDelayEnabled": true,

```

```

        "PowerOnDelayMode": "CustomDelay",
        "PowerOnDelaySeconds": 100
    }
}

```

Parameters

For a description of the parameters for properties of the specified System resource, refer to [Table 5-8](#).

Table 5-8 Parameter Descriptions for Properties of the Specified System Resource

Parameter	Description	Value
tag	Customized asset tags.	- Length: 2–63 characters. - Consists of digits or letters, case-sensitive. - Allowed special characters: hyphen, underscore, space, and at (@). The tag cannot start or end with a hyphen, an underscore, or a space.
name	Customized host name.	- The length cannot exceed 63 characters. - The name can only contain letters, digits, and the minus signs. No blank or space is allowed. The name is not case-sensitive. - The first character must be a letter, and the last character cannot be a minus sign.
model	Customized typical configuration model.	Year + typical configuration model. The configuration value must be in dictionary format, for example 2019C1, and the string length is 1–63.
powerondealy_enable	Whether to enable power-on delay:	- true - false
powerondelay_mode	Power-on delay mode:	- RandomDelay: random delay mode. - CustomDelay: custom delay mode.
powerondealy_seconds	Delay duration.	Delay duration, range: 1–120 s.

bootsourceoverride_mode	Boot mode.	- Legacy - UEFI
Parameter	Description	Value
bootsourceoverride_state	Mode for applying the boot settings.	- Once: effective only once - Continuous: effective permanently
bootsourceoverride_target	Type of boot mode.	Boot devices defined by Redfish: - None: no override - Pxe: network - Cd: CD-ROM - Floppy: Usb - Hdd: hard disk - BiosSetup: BIOS

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": "my test",
  "HostName": "my test",
  "Oem": {
    "Public": {"ConfigurationModel": "2019C1"}
  }
}
```

- 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 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.
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.
------------	--------	-----------

5.5 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 5-10](#).

Table 5-10 Parameter Descriptions for Querying Information About the CPU Resource Collection

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

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Systems/1/Processors

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

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

- Status Code: 200

Output Description

For a description of the output returned when you query information about the CPU resource collection, refer to [Table 5-11](#).

Table 5-11 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.

5.6 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

Parameters

For a description of the parameters for querying information about the specified CPU resources, refer to [Table 5-12](#).

Table 5-12 Parameter Descriptions for Querying Information About the Specified CPU Resource

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

Usage Guidelines

None

Example

- Request Example:

GET : *https://device_ip/redfish/v1/Systems/1/Processors/0*

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None • Response Example:


```
{
  "@odata.context": "/redfish/v1/$metadata#Processor.Processor",
  "@odata.id": "/redfish/v1/Systems/1/Processors/0",
  "@odata.type": "#Processor.v1_10_0.Processor",
  "Name": "Intel Processor 1",
  "Id": "1",
  "InstructionSet": "X86,X86-64",
  "Manufacturer": "Intel (R) Corporation",
  "MaxSpeedMHz": 3600,
  "Model": "Genuine Intel(R) CPU 0000%",
  "Oem": {
    "Public": {
      "FrequencyMHz": 1700,
      "L1CacheKiB": 4480,
      "L2CacheKiB": 114688,
      "L3CacheKiB": 107520,
      "SerialNumber": "2F8A6BEB959A73D6"
    }
  },
  "Voltage": "1.6",
  "OperatingSpeedMHz": 2000,
  "ProcessorArchitecture": "x86",
  "ProcessorId": {
    "IdentificationRegisters": "f2-06-08-00-ff-fb-eb-bf"
  },
  "ProcessorType": "CentralProcessor",
  "Socket": 1,
  "Status": {
    "State": "Enabled",
    "Health": "OK"
  },
  "TDPWatts": 350,
  "TotalCores": 56,
  "TotalThreads": 112
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified CPU resource, refer to [Table 5-13](#).

Table 5-13 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.
@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

Field	Type	Description
		● 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.
TotalCores	Number	Total number of cores of the specified CPU resource.
TotalThreads	Number	Total number of threads of the specified CPU resource.

Socket	Number	Slot ID of the specified CPU resource.
Status	Object	Status of the specified CPU resource, including: ● State: whether the CPU is isolated ● Health: CPU resource health status
Oem.Public	Object	Customized vendor properties.
L1CacheKiB	Number	Level I cache of the specified CPU resource.
L2CacheKiB	Number	Level II cache of the specified CPU resource.
L3CacheKiB	Number	Level III cache of the specified CPU resource.
FrequencyMHz	Number	Frequency of the specified CPU resource.
SerialNumber	String	Serial number of the specified CPU resource.
Voltage	String	Voltage of the specified CPU resource.
OperatingSpeedMHz	Number	Current speed of the specified CPU resource.
TDPWatts	Number	TDP(W) of the specified CPU resource.
Voltage	String	Voltage of the specified CPU resource.

5.7 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

Parameters

For a description of the parameters for querying information about all CPU resources, refer to [Table 5-14](#).

Table 5-14 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 <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
GET : https://10.43.211.250/redfish/v1/Systems/1/Processors?$expand=.
```

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
```

```

    "@odata.context":
"/redfish/v1/$metadata#ProcessorCollection.ProcessorCollection",
    "@odata.id": "/redfish/v1/Systems/1/Processors",
    "@odata.type": "#ProcessorCollection.ProcessorCollection",
    "Description": "Collection of processors for this system",
    "Name": "Processors Collection",
    "Members@odata.count": 2,
    "Members": [
        {
            "@odata.id": "/redfish/v1/Systems/1/Processors/0",
            "@odata.type": "#Processor.v1_10_0.Processor",
            "Name": "Intel Processor 1",
            "Id": "1",
            "InstructionSet": "X86,X86-64",
            "Manufacturer": "Intel(R) Corporation",
            "MaxSpeedMHz": 3300,
            "Model": "Genuine Intel(R) CPU 0000%@",
            "Oem": {
                "Public": {
                    "FrequencyMHz": 1500,
                    "L1CacheKiB": 3840,
                    "L2CacheKiB": 98304,
                    "L3CacheKiB": 92160,
                }
            },
            "SerialNumber": "B65FD4F4B77D6755"
            "Voltage": "1.6"
        },
        {
            "OperatingSpeedMHz": 2000,
            "ProcessorArchitecture": "x86",
            "ProcessorId": {
                "IdentificationRegisters": "f3-06-08-00-ff-fb-eb-bf"
            },
            "ProcessorType": "CentralProcessor",
            "Socket": 1,
            "Status": {
                "State": "Enabled",
            },
            "Health": "OK"
        },
        {
            "TDPWatts": 350,
            "TotalCores": 48,
            "TotalThreads": 96
        },
        {
            "@odata.id": "/redfish/v1/Systems/1/Processors/1",
            "@odata.type": "#Processor.v1_10_0.Processor",

```

```
        "Name": "Intel Processor 2",
        "Id": "2",
        "InstructionSet": "X86,X86-64",
        "Manufacturer": "Intel(R) Corporation",
        "MaxSpeedMHz": 3300,
        "Model": "Genuine Intel(R) CPU 0000%@",
        "Oem": {
            "Public": {
                "FrequencyMHz": 1500,
                "L1CacheKiB": 3840,
                "L2CacheKiB": 98304,
                "L3CacheKiB": 92160,
            }
        },
        "SerialNumber": "B65FA8F41D9829E7"
    },
    "Voltage": "1.6"
},
{
    "OperatingSpeedMHz": 2000,
    "ProcessorArchitecture": "x86",
    "ProcessorId": {
        "IdentificationRegisters": "f3-06-08-00-ff-fb-eb-bf"
    },
    "ProcessorType": "CentralProcessor",
    "Socket": 2,
    "Status": {
        "State": "Enabled",
    },
    "Health": "OK"
},
{
    "TDPWatts": 350,
    "TotalCores": 48,
    "TotalThreads": 96
}
]
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all CPU resources, refer to [Table 5-15](#).

Table 5-15 Output Descriptions for Querying Information About All CPU Resources

Field	Type	Description
-------	------	-------------

@odata.context	String	OData description of the CPU resource collection model.
Field	Type	Description
@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	Information about all CPU resources.

For a description of the parameters of the CPU resource information, refer to [Table 5-13](#).

5.8 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 5-16](#).

Table 5-16 Parameter Descriptions for Querying Information About the Memory Resource Collection

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

auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
------------	---	---

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Systems/1/Memory

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#MemoryCollection.MemoryCollection",
  "@odata.id": "/redfish/v1/Systems/1/Memory",
  "@odata.type": "#MemoryCollection.MemoryCollection",
  "Description": "Collection of Memories for this system",
  "Name": "Memory
Collection",
  "Members@odata.count":1,
  "Members":
    [{
      "@odata.id":
        "/redfish/v1/Systems/1/Memory/DIMM1"
    }],
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the memory resource collection, refer to [Table 5-17](#).

Table 5-17 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.

5.9 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

Parameters

For a description of the parameters for querying information about the specified memory resource, refer to [Table 5-18](#).

Table 5-18 Parameter Descriptions for Querying Information About the Specified Memory Resource

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/1/Memory/DIMM1
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Memory.Memory",
  "@odata.id": "/redfish/v1/Systems/1/Memory/CPU1_A0",
  "@odata.type": "#Memory.v1_11_0.Memory",
  "AllowedSpeedsMHz": 4800,
  "BaseModuleType": "RDIMM",
  "CapacityMiB": 65536,
  "DataWidthBits": 64,
  "DeviceLocator": "CPU1_A0",
  "ECCType": "Multi-bit ECC",
  "Id": "CPU1_A0",
  "Manufacturer": "Samsung",
  "MemoryDeviceType": "DDR5",
  "MemoryLocation": {
    "Channel": 0,
    "Controller": 0,
    "Slot": 0,
  },
  "Socket": 1
},
{
  "Name": "CPU1_A0",
  "OperatingSpeedMhz": 4800,
  "PartNumber": "M321R8GA0BB0-CQKEG",
  "RankCount": 2,
  "SerialNumber": "01E2FC6C",
  "Status": {
    "State": "Enabled",
  },
  "Health": "OK"
},
{
  "Oem": {
    "Public": {
      "VoltageVolt": 1.1,
    },
  },
  "Temperature": null
}
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified memory resource, refer to [Table 5-19](#).

Table 5-19 Output Descriptions for Querying Information About the Specified Memory Resource

Field	Type	Description
@odata.context	String	OData description of the specified memory resource model.
@odata.id	String	Access path of the specified memory resource.
@odata.type	String	Type of the specified memory resource.
Name	String	Name of the specified memory resource.
Id	String	ID of the specified memory resource.
AllowedSpeedsMHz	Number	Maximum frequency of the specified memory resource, unit: MHz.
CapacityMiB	Number	Capacity of the specified memory resource, in MB.
Manufacturer	String	Manufacturer of the specified memory device.
OperatingSpeedMhz	Number	Operating speed of the specified memory resource.
SerialNumber	String	Serial number of the specified memory resource.
MemoryDeviceType	String	Type of the specified memory resource. The value should be in dictionary type, such as DDR4 and DDR3 .
DataWidthBits	Number	Data bandwidth of the specified memory resource.
RankCount	Number	Number of ranks of the specified memory resource.
PartNumber	String	Part number of the specified memory resource.
DeviceLocator	String	Screen printing of the specified memory resource.

BaseModuleType	String	Basic module type of the specified memory resource, including: ● RDIMM ● UDIMM ● SO_DIMM ● LRDIMM ● Mini_RDIMM ● Mini_UDIMM ● SO_RDIMM_72b ● SO_UDIMM_72b ● SO_DIMM_16b ● SO_DIMM_32b
MemoryLocation	Object	Location of the specified memory device.
Field	Type	Description
Socket	Number	Slot ID of the CPU of the specified memory resource.
Controller	Number	Controller ID of the specified memory resource.
Channel	Number	Channel ID of the specified memory resource.
Slot	Number	Slot ID of the specified memory resource.
Status	Object	Status of the specified memory resource, including: ● Health: health status of the specified memory resource ● State: whether the specified memory resource is enabled
Oem.Public	Object	Customized field.
VoltageVolt	Number	Voltage of the specified memory resource, unit: Volt.
Temperature	数字	Temperature of the specified memory resource, unit: °C.

5.10 Querying Information About All Memory Resources

Function

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

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 5-20](#).

Table 5-20 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.
Parameter	Description	Value
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- **Request Example:**

GET https://device_ip/redfish/v1/Systems/1/Memory?\$expand=.

- **Request Header:**

X-Auth-Token: 8574621d21b84756218c7456821c234

- **Request Message Body:** None • **Response Example:**

```
"@odata.id": "/redfish/v1/Systems/Self/Memory",
  "@odata.type": "#MemoryCollection.MemoryCollection",
  "Description": "Collection of Memories for this system",
  "Name": "Memory Collection",
  "Members@odata.count": 2,
  "Members": [
    {
      "@odata.id":
"/redfish/v1/Systems/Self/Memory/DIMM9",
      "@odata.type": "#Memory.v1_11_0.Memory",
      "BaseModuleType": "RDIMM",
      "CapacityMiB": 16384,
      "DataWidthBits": 64,
      "DeviceLocator": "DIMM9",
      "ECCType": "Multi-bit ECC",
      "Id": "9",
      "Manufacturer": "Hynix",
      "MemoryDeviceType": "DDR5",
      "MemoryLocation": {
        "Channel": 0,
        "Controller": 0,
        "Slot": 0,
      },
      "Socket": 1
    },
    {
      "Name": "DIMM9",
```

```

        "OperatingSpeedMhz": 4800,
    "PartNumber": "HMC78MEBRA115N",
        "RankCount": 1,
    "SerialNumber": "137A8358",
        "Status": {
            "State": "Enabled",
    "Health": "OK"
        }
    },
    {
        "@odata.id":
"/redfish/v1/Systems/Self/Memory/DIMM25",
    "@odata.type": "#Memory.v1_11_0.Memory",
        "BaseModuleType": "RDIMM",
        "CapacityMiB": 16384,
        "DataWidthBits": 64,
        "DeviceLocator": "DIMM25",
    "ECCType": "Multi-bit ECC",
        "Id": "25",
        "Manufacturer": "Hynix",
        "MemoryDeviceType": "DDR5",
        "MemoryLocation": {
            "Channel": 0,
            "Controller": 0,
            "Slot": 0,
    "Socket": 2
        },
        "Name": "DIMM25",
        "OperatingSpeedMhz": 4800,
    "PartNumber": "HMC78MEBRA115N",
        "RankCount": 1,
    "SerialNumber": "138B9C40",
        "Status": {
            "State": "Enabled",
    "Health": "OK"
        }
    }
]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all memory resource, refer to [Table 5-21](#).

Table 5-21 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.

For a description of the parameters of the memory resource information, refer to [Table 5-19](#).

5.11 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 5-22](#).

Table 5-22 Parameter Descriptions for Querying Information About the Storage Resource Collection

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

auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
------------	---	---

Usage Guidelines

None

Example

- Request Example:

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.Storage
Collection",
  "@odata.id":
  "/redfish/v1/Systems/1/Storages",
  "@odata.type":
  "#StorageCollection.StorageCollection",
  "Name": "Storage Collection",
  "Members@odata.count": 2,
  "Members": [
    {
      "@odata.id":
      "/redfish/v1/Systems/1/Storages/RAIDStorage19"
    },
    {
      "@odata.id":
      "/redfish/v1/Systems/1/Storages/RAIDStorage5"
    }
  ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the storage resource collection, refer to [Table 5-23](#).

Table 5-23 Output Descriptions for Querying Information About the Storage Resource Collection

Field	Type	Description
-------	------	-------------

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

5.12 Querying Information About a Specified Storage Controller Resource

Function

Query information about the specified storage controller resource of a server.

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

Parameters

For a description of the parameters for querying information about a specified storage controller resource, refer to [Table 5-24](#).

Table 5-24 Parameter Descriptions for Querying Information About the Specified Storage Controller Resource

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

auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
storage_id	ID of the specified storage resource.	It can be obtained by querying the information about the storage resource collection.

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Systems/1/Storages/RAIDStorage5

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```

{
  "@odata.context":
"/redfish/v1/$metadata#Storage.Storage",      "@odata.id":
"/redfish/v1/Systems/1/Storages/RAIDStorage5",
"@odata.type": "#Storage.v1_9_0.Storage",      "Drives":
  [{
    "@odata.id":
"/redfish/v1/Chassis/1/Drives/HDDPlaneDisk16"
  },
  {
    "@odata.id":
"/redfish/v1/Chassis/1/Drives/HDDPlaneDisk18"
  },
  {
    "@odata.id":
"/redfish/v1/Chassis/1/Drives/HDDPlaneDisk20"
  },
  {
    "@odata.id":
"/redfish/v1/Chassis/1/Drives/HDDPlaneDisk22"
  }
],
  "Drives@odata.count": 4,
  "Name": "RAIDStorage5",
  "StorageControllers": [
    {
      "Description": "RAID Controller",
      "FirmwareVersion": "3.22",
      "Manufacturer": "Microchip",
      "MemberId": "RAIDStorage5",
      "Model": "PM8236",
      "CardManufacturer": "NETAS",
      "CardModel": "RS241-18i 2G",
      "Name": "RS241-18i 2G(RAIDStorage5)",

```

```

        "Oem": {
            "Public": {
                "CapacitanceName": null,
                "CapacitanceStatus": {
                    "Health": null,
                    "State": "Absent"
                },
                "MemorySizeMiB": 2048,
                "OBSupport": true,
                "SASAddress": null,
                "SupportedRAIDLevels": [
                    "RAID0",
                    "RAID1",
                    "RAID5",
                    "RAID6",
                    "RAID10",
                    "RAID50",
                    "RAID60"
                ]
            },
            "SerialNumber":
"743551500214",
            "SpeedGbps": 12,
            "status": {
                "Health": "OK",
                "State": "Enabled"
            },
            "SupportedDeviceProtocols": [
                "SAS",
                "SATA"
            ]
        },
        "StorageControllers@odata.count": 1,
        "Volumes": {
            "@odata.id":
"/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes"
        }
    }

```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about a specified storage controller resource, refer to [Table 5-25](#).

Table 5-25 Output Descriptions for Querying Information About the Specified Storage Controller Resource

Field	Type	Description
@odata.context	String	OData description of the specified storage controller model.
@odata.id	String	Access path of the specified storage controller.
@odata.type	String	Type of the specified storage controller.
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 • SFTP
Manufacturer	String	Chip manufacturer of the specified storage controller.
Model	String	Chip model of the specified storage controller.
Field	Type	Description
Manufacturer	String	Manufacturer of the specified storage controller.
Model	String	Model of the specified storage controller.
CardManufacturer	String	Manufacturer of the specified storage controller.
CardModel	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. • Health: BBU health status • State: BBU presence status

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. - State: whether the specified storage controller is enabled. - Health: health status of the specified storage controller.
Description	String	Information about the specified storage controller.

5.13 Querying Information About All Storage Controller Resources

Function

Query information about all current storage controller 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 controller resources, refer to [Table 5-26](#).

Table 5-26 Parameter Descriptions for Querying Information About All Storage Controller Resources

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/s1/Storages?$expand=.
```

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#StorageCollection.StorageCollection",
  "@odata.id": "/redfish/v1/Systems/1/Storages",
  "@odata.type": "#StorageCollection.StorageCollection",
  "Name": "Storage Collection",
  "Members@odata.count": 2,
  "Members": [
    {
      "@odata.id":
"/redfish/v1/Systems/1/Storages/RAIDStorage19",
      "@odata.type": "#Storage.v1_9_0.Storage",
      "Drives": [],
      "Drives@odata.count": 0,
      "Name": "RAIDStorage19",
      "StorageControllers": [
```

```

        {
            "Description": "RAID Controller",
            "FirmwareVersion": "3.22",
            "Manufacturer": "Microchip",
            "MemberId": "RAIDStorage19",
            "Model": "PM8236",
            "CardManufacturer": "NETAS",
            "CardModel": "RS241-18i 2G",
            "Name": "RS241-18i 2G(RAIDStorage19)",
            "Oem": {
                "Public": {
                    "CapacitanceName": null,
                    "CapacitanceStatus": {
                        "Health": null,
                    },
                    "State": "Absent"
                },
                "MemorySizeMiB": 2048,
                "OOBSupport": true,
                "SASAddress": null,
                "SupportedRAIDLevels": [
                    "RAID0",
                    "RAID1",
                    "RAID5",
                    "RAID6",
                    "RAID10",
                    "RAID50",
                    "RAID60"
                ]
            },
            "SerialNumber": "743551500696",
            "SpeedGbps": 12,
            "status": {
                "Health": "OK",
            },
            "State": "Enabled"
        },
        "SupportedDeviceProtocols": [
            "SAS",
            "SATA"
        ]
    },
    "StorageControllers@odata.count": 1,
    "Volumes": {

```



```

        "@odata.id":
"/redfish/v1/Systems/1/Storages/RAIDStorage19/Volumes"
    },
    {
        "@odata.id":
"/redfish/v1/Systems/1/Storages/RAIDStorage5",
"@odata.type": "#Storage.v1_9_0.Storage",
        "Drives": [
            {
                "@odata.id":
"/redfish/v1/Chassis/1/Drives/HDDPlaneDisk16"
            },
            {
                "@odata.id":
"/redfish/v1/Chassis/1/Drives/HDDPlaneDisk18"
            },
            {
                "@odata.id":
"/redfish/v1/Chassis/1/Drives/HDDPlaneDisk20"
            },
            {
                "@odata.id":
"/redfish/v1/Chassis/1/Drives/HDDPlaneDisk22"
            }
        ],
        "Drives@odata.count": 4,
        "Name": "RAIDStorage5",
        "StorageControllers": [
            {
                "Description": "RAID Controller",
                "FirmwareVersion": "3.22",
                "Manufacturer": "Microchip",
                "MemberId": "RAIDStorage5",
                "Model": "PM8236",
                "CardManufacturer": "NETAŞ",
                "CardModel": "RS241-18i 2G",
                "Name": "RS241-18i 2G (RAIDStorage5)",
                "Oem": {
                    "Public": {
                        "CapacitanceName": null,
                        "CapacitanceStatus": {
                            "Health": null,
                            "State": "Absent"
                        },
                        "MemorySizeMiB": 2048,
                        "OOBSupport": true,
                        "SASAddress": null,
                        "SupportedRAIDLevels": [

```

```

        "RAID0",
        "RAID1",
        "RAID5",
        "RAID6",
        "RAID10",
        "RAID50",
"RAID60"
    ]
    },
    },
    "SerialNumber": "743551500214",
    "SpeedGbps": 12,
    "status": {
        "Health": "OK",
"State": "Enabled"
    },
    "SupportedDeviceProtocols": [
        "SAS",
"SATA"
    ]
    }
    ],
    "StorageControllers@odata.count": 1,
    "Volumes": {
"@odata.id":
"/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes"
    }
    ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all storage controller resources, refer to [Table 5-27](#).

Table 5-27 Output Descriptions for Querying Information About All Storage Controller Resources

Field	Type	Description
@odata.context	String	OData description of the storage controller resource collection model.

Field	Type	Description
@odata.id	String	Access path of the storage controller resource collection.
@odata.type	String	Type of storage controller resource collection.
Name	String	Name of the storage controller resource collection.
Members@odata.count	Number	Number of storage controller resource members.
Members	Object	Storage resource list.

For a description of the parameters of the storage controller resource information, refer to [Table 5-25](#).

5.14 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 5-28](#).

Table 5-28 Parameter Descriptions for Querying Information About the Logical Volume Resource Collection

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

auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
------------	---	---

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes
```

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#VolumeCollection.VolumeCollection",      "@odata.id":
"/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes",      "@odata.type":
"#VolumeCollection.VolumeCollection",      "Members":
  [{
    "@odata.id":
"/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes/LogicalDrive0"
  },
  {
    "@odata.id":
"/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes/LogicalDrive1"
  },
  {
    "@odata.id":
"/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes/LogicalDrive2"
  }
],
  "Members@odata.count": 3,
  "Name": "Volume Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the logical volume resource collection, refer to [Table 5-29](#).

Table 5-29 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.
Field	Type	Description
@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.

5.15 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

Parameters

For a description of the parameters for querying information about the specified logical volume resource, refer to [Table 5-30](#).

Table 5-30 Parameter Descriptions for Querying Information About the Specified Logical Volume Resource

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

system_id	ID of the System resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions.</i>
storage_id	ID of the specified storage resource.	It can be obtained from the storage resource collection.
Parameter	Description	Value
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/RAIDStorage5/Volumes/LogicalDrive2
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```

{
  "@odata.context": "/redfish/v1/$metadata#Volume.Volume",
  "@odata.id":
  "/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes/LogicalDrive0",
  "@odata.type": "#Volume.v1_0_3.Volume",
  "Links": {
    "Drives": [
      {
        "@odata.id":
        "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk19"
      }
    ],
    "Drives@odata.count": 1
  },
  "Id": "LogicalDrive0",
  "Name": "2223",
  "Oem": {
    "Public": {
      "AccessPolicy": null,
      "IoPolicy": null,
      "ReadPolicy": null,
      "WritePolicy": null,
      "DriveCachePolicy": null,
      "NumDrive": 1,
      "RaidControllerID": 5,
      "State": "Optimal",
      "VolumeName": "2223",
      "VolumeRaidLevel": "RAID0"
    }
  },
  "OptimumIOSizeBytes": 1048576,
  "CapacityBytes": 1919850381312,
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  },
  "VolumeType": "NonRedundant",
  "NumDriveperspan": null,
  "SpanNumber": null
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified logical volume resource, refer to [Table 5-31](#).

Table 5-31 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.
@odata.type	String	Type of the specified logical volume.
Name	String	Name of the specified logic volume resource.
Id	String	ID of the specified logical volume ID.
VolumeType	String	Redundancy type of the specified logical volume: ● RawDevice ● NonRedundant ● Mirrored ● StripedWithParity ● SpannedMirrors ● SpannedStripesWithParity
CapacityBytes	Number	Capacity of the logical volume.
OptimumIOSizeBytes	Number	Stripe size of the logical volume.
Links	Object	Member logical volume list.
Drives	Object	Drive list managed by the current specified controller.

Field	Type	Description
@odata.id	String	Access path of the specified drive.
Drives@odata.count	Number	Number of member physical disks included in the RAID .
Status	Object	Status of the specified logical volume resource, including: ● State: whether the logical volume is enabled. ● Health: health status of the logical volume.

Oem.Public	Object	Customized logical volume information.
RaidControllerID	Number	Controller ID of the logical volume.
VolumeRaidLevel	String	RAID level of the logical volume. The value must be in dictionary format, including: ● RAID0 ● RAID1 ● RAID5 ● RAID6 ● RAID00 ● RAID10 ● RAID50 ● RAID60
DriveCachePolicy	String	Hard disk Cache policy: ● Unchanged ● Enabled ● Disabled
NumDrive	Number	Number of physical disk members.
ReadPolicy	String	Read policy of the logical volume: ● NoReadAhead ● ReadAhead
WritePolicy	String	Write policy of the logical volume: ● WriteThrough ● WriteBack ● AlwaysWriteBack
AccessPolicy	String	Access policy of the logical volume: ● ReadWrite ● ReadOnly ● Blocked
IoPolicy	String	IO policy of the logical volume: ● DirectIO
Field	Type	Description
		● CachedIO
VolumeName	String	Name of the logical volume.

State	String	Status of the logical volume: ● Offline ● Partially ● Degraded ● Optimal ● Initializing
NumDriveperspan	Number	Number of drive members in a span.
SpanNumber	Number	Number of spans of a volume.

5.16 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 5-32](#).

Table 5-32 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 POST request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
OptimumIOSize-Bytes	Number	Stripe size of the logical volume, optional, in bytes. Options: ● 65536 ● 131072 ● 262144 ● 524288 ● 1048576
VolumeName	String	Name of the logical volume, required, consisting of 1–15 characters, including letters, digits, minus, and underscores, and cannot be the same as the original logical volume name.
VolumeRaidLevel	String	RAID level of the logical volume, required, including: ● RAID0 ● RAID1 ● RAID5 ● RAID6

ReadPolicy	String	Read policy of the logical volume, optional, including: • NoReadAhead • ReadAhead
------------	--------	--

Parameter	Description	Value
WritePolicy	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.
AccessPolicy	String	Access policy of the logical volume, optional, including: • ReadWrite • ReadOnly • Blocked
IoPolicy	String	IO policy of the logical volume, optional, including: • DirectIO • CachedIO
DriveCachePolicy	String	Caching policy of the logical volume, optional, including: • Unchanged • Enabled • Disabled
InitializationMode	String	Initiation mode of the logical volume, optional, including: • UnInit: no initialization • QuickInit: quick initialization • FullInit: full initialization

SpanNumber	Number	Number of logical volume subgroups, optional, default:1. The value can be set to 1 only.
drives	Array	Member volume list, required. The format of the drives field is: [HDDPlaneDiskid1,HD- DPlaneDiskid2,...,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/RAIDStorage5/Volumes
```

- Request Header:

```
Content-Type: application/json
X-Auth-Token: 8574621d21b84756218c7456821c234
```

- Request Message Body:

```
{
  "OptimumIOSizeBytes":
  1048576,
  "Oem": {
    "Public": {
      "VolumeName":
      "2222",
      "VolumeRaidLevel":
      "RAID0",
      "ReadPolicy":
      "ReadAhead",
      "WritePolicy":
      "WriteThrough",
      "AccessPolicy": "ReadWrite",
      "IoPolicy":
      "CachedIO",
      "DriveCachePolicy":
      "Enabled",
      "InitializationMode": "UnInit",
      "SpanNumber": 2,
      "Drives": ["HDDPlaneDisk19"]
    }
  }
}
```

--	--

- **Response Example:**

```
{
  "@odata.context": "/redfish/v1/$metadata",      "@odata.id":
"/redfish/v1/Systems/1/Storages/RAIDStorage5/Volumes",
  "error": {
    "@Message.ExtendedInfo": [
      {
        "@odata.type": "#Message.v1_1_1.Message",
        "Message": "Successfully Completed Request",
        "MessageArgs": [],

        "MessageId": "Base.1.0.Success",
        "RelatedProperties": [],
        "Resolution": "None",

        "Severity": "OK"
      }
    ],
    "code": "Base.1.0.Success",
    "message": "Successfully Completed Request"
  }
}
```

- **Status Code: 202**

Output Description

For a description of the output returned when you create the logical volume, refer to [Table 5-33](#).

Table 5-33 Output Descriptions for Creating 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.

5.17 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 5-34](#).

Table 5-34 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.
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 <i>/redfish/v1/SessionService/Sessions</i> .
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/RAIDStorage5/Volumes/LogicalDrive0
```

- 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/RAIDStorage5/Volumes/LogicalDrive0",
  "error":
  {
    "@Message.ExtendedInfo":
```

```
[{
  "@odata.type": "#Message.v1_1_1.Message",
  "Message": "Successfully Completed Request",
  "MessageArgs": [],
  "MessageId": "Base.1.0.Success",
  "RelatedProperties": [],
  "Resolution": "None",
  "Severity": "OK"
}],
"code": "Base.1.0.Success",
"message": "Successfully Completed Request"
}
```

- Status Code: 202

Output Description

For a description of the output returned when you delete the logical volume, refer to [Table 5-35](#).

Table 5-35 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.

5.18 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

Parameters

For a description of the parameters for querying properties of the BIOS resource, refer to [Table 5-36](#).

Table 5-36 Parameter Descriptions for Querying Properties of the BIOS Resource

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

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Systems/1/Bios

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None • Response Example:

```

{
  "@Redfish.Settings": {
"@odata.type": "#Settings.v1_2_2.Settings",
    "SettingsObject": {
"@odata.id": "/redfish/v1/Systems/1/Bios/SD"
      }
    },
    "@odata.context": "/redfish/v1/$metadata#Bios.Bios",
    "@odata.etag": "\"1626875188\"",
    "@odata.id": "/redfish/v1/Systems/1/Bios",
    "@odata.type": "#Bios.v1_1_0.Bios",
    "Actions": {
      "#Bios.ChangePassword": {
"@Redfish.ActionInfo":
        "/redfish/v1/Systems/1/Bios/ChangePasswordActionInfo",
      "target": "/redfish/v1/Systems/1/Bios/Actions/Bios.ChangePassword"
      },
      "#Bios.ResetBios": {
        "target":
"/redfish/v1/Systems/1/Bios/Actions/Bios.ResetBios"
      }
    },
    "AttributeRegistry":
BiosAttributeRegistryEGSG5.0.56.0",
    "Attributes": {
      "BootMode": "UEFI Only",
      "C1E": "Enabled",
      "EIST": "Disabled",
      "EnergyPerformanceBIAS": "Balanced Performance",
      "HardwarePStates": "Native Mode",
      "HyperThreading": "Enabled",
      "LoadBIOSDefault": "Disabled",
      "MonitorMWAIT": "Enabled",
      "NUMA": "Enabled",
      "PackageCState": "C0/C1 state",
      "PowerPerformanceTuning": "OS controls EPB",
      "PowerPolicySelect": "Custom",
      "TurboMode": "Enabled"
    },
    "Description": "Current BIOS
Settings",
    "Id": "Bios",
    "Name":
"Current BIOS Settings"
  }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query properties of the BIOS resource, refer to [Table 5-37](#).

Table 5-37 Output Descriptions for Querying Properties of the BIOS Resource

Field	Type	Description
@odata.context	String	OData description of the BIOS resource model.
Field	Type	Description
@odata.id	String	Access path of the BIOS resource.
@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	Object	BIOS attribute.
Actions	Object	Operations that can be performed on the BIOS resource.
@Redfish.Settings	Object	Information about BIOS settings.

5.19 Querying Information About the BIOS Settings

Function

Query information about the current [BIOS](#) settings of a server.

Syntax

- Operation Type: GET

- [URL](#):

`https://device_ip/redfish/v1/Systems/system_id/Bios/(SD|Settings)`

- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the BIOS settings, refer to [Table 5-38](#).

Table 5-38 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 <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Systems/1/Bios/SD
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#Bios.Bios",
  "@odata.etag": "W/\"1589902226\"",
"@odata.id": "/redfish/v1/Systems/1/Bios/Settings",
"@odata.type": "#Bios.v1_0_3.Bios",    "Attributes":
{
  "BootType": "LegacyBoot",
  "BootTypeOrder0": "DVDROMDrive",
"BootTypeOrder1": "HardDiskDrive",
  "BootTypeOrder2": "PXE",
  "BootTypeOrder3": "None",
  "CREnable": "Enabled",
  "CustomPowerPolicy": "Performance",
  "GlobalBaudRate": "Rate9600",
  "IPv4PXESupport": "Enabled",
  "IPv6PXESupport": "Disabled",
  "MainBoardLOMPort1": "Disabled",
  "MainBoardLOMPort2": "Disabled",
  "MainBoardLOMPort3": "Enabled",
"MainBoardLOMPort4": "Disabled",
  "Numa": "Enabled",
"PCIEsRIOVSupport": "Disabled",
  "PXEOnly": "Enabled",
"ProcessorHyperThreading": "Enabled",
  "TurboMode": "Enabled",
  "VTdSupport": "Enabled",
  "VTxSupport": "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"
    },
    "Description": "Future BIOS
Settings",
    "Id": "Settings",
    "Name": "Future BIOS Settings"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the BIOS settings, refer to [Table 5-39](#).

Table 5-39 Output Descriptions for Querying Information About the BIOS Settings

Field	Type	Description
@odata.context	String	OData description of the BIOS setting resource model.
@odata.id	String	Access path of the BIOS setting resource.
@odata.type	String	Type of BIOS setting resource.
@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	Object	BIOS attribute.
Actions	Object	Operations that can be performed on the BIOS resource.

@Redfish.Settings	Object	Information about BIOS settings.
-------------------	--------	----------------------------------

5.20 Modifying the BIOS Settings

Function

Modify the BIOS settings.

Syntax

- Operation Type: PATCH
- URL:
https://device_ip/redfish/v1/Systems/system_id/Bios/(SD|Settings)
- Request Header:

Content-Type: header_type If-Match: ifmatch_value

- Request Message Body:

```
{
  "Attributes":
    {
      "EIST": set_value,
      "C1E": set_value,
      ...
    }
}
```

Parameters

None

Usage Guidelines

None

Example

- Request Example:

PATCH https://device_ip/redfish/v1/Systems/1/Bios/SD

- Request Header:

Content-Type: application/json If-Match: "1626878215"

- Request Message Body:

```
{
  "Attributes":
    {
      "EIST": "Disabled",
      "ClE": "Enabled"
    }
}
```

- Response Example: None
- Status Code: 204

Output Description

None

5.21 Setting the BIOS Password

Function

Set the [BIOS](#) password.

Syntax

- Operation Type: POST
- [URL](#):
`https://device_ip/redfish/v1/Systems/system_id/Bios/Actions/Bios.ChangePassword`
- Request Header:

```
Content-Type: header_type If-
Match: ifmatch_value
```

- Request Message Body:

```
{
  "PasswordName": set_value,
  "OldPassword": set_value,
  "NewPassword": set_value
}
```

Parameters

For a description of the parameters for setting the BIOS password, refer to [Table 5-40](#).

Table 5-40 Parameter Descriptions for Setting the BIOS Password

Parameter	Description	Value
PasswordName	BIOS password type.	• AdministratorPassword • UserPassword

OldPassword	Current password.	Character string. If this parameter is set to "", it indicates that there is no password.
Parameter	Description	Value
NewPassword	New password.	Character string. If this parameter is set to "", it indicates that the password is to be cleared.

Usage Guidelines

None

Example

- Request Example:

POST https://device_ip/redfish/v1/Systems/1/Bios/Actions/Bios.ChangePassword

- Request Header:

Content-Type: application/json
If-Match: "1626878215"

- Request Message Body:

```
{
  "PasswordName": "AdministratorPassword",
  "OldPassword": "test",
  "NewPassword": ""
}
```

- Response Example: None
- Response Code: 204

Output Description

None

5.22 Restoring the Default BIOS Settings

Function

Restore the default BIOS settings.

Syntax

- Operation Type: POST

- **URL:**
`https://device_ip/redfish/v1/Systems/system_id/Bios/Actions/Bios.ResetBios`
- **Request Header:**

Content-Type: header_type

- **Request Message Body:**

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

Parameters

For a description of the parameters for restoring the default BIOS settings, refer to [Table 5-41](#).

Table 5-41 Descriptions of BIOS Default Settings

Parameter	Description	Value
value	Operation type.	Character string: ResetBios

Usage Guidelines

None

Example

- **Request Example:**

POST https://device_ip/redfish/v1/Systems/1/Bios/Actions/Bios.ResetBios
- **Request Header:**

Content-Type: application/json
- **Request Message Body:**

```
{
  "ResetType":"ResetBios"
}
```
- **Response Example:** None
- **Response Code:** 204

Output Description

None

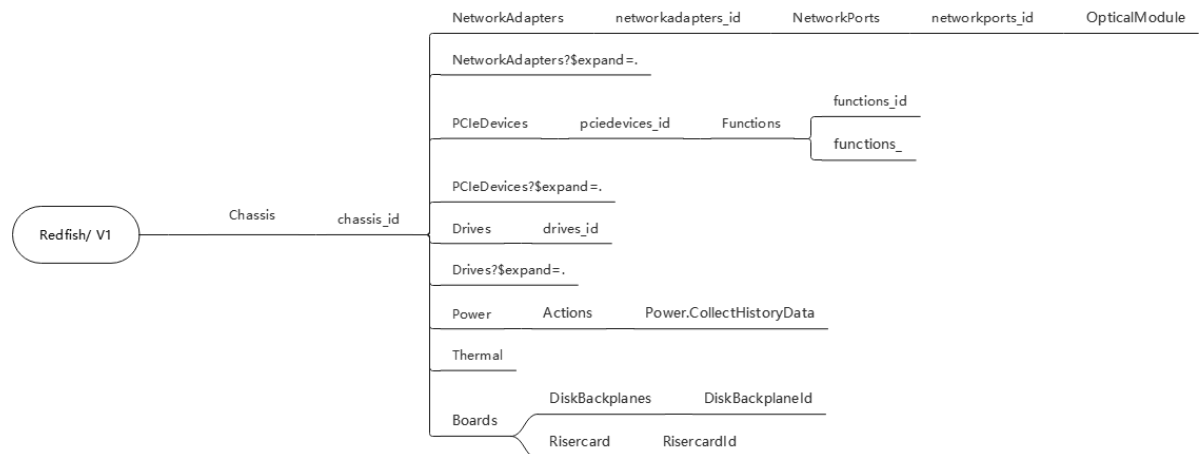
Chapter 6

Operations on Chassis Resources

Table of Contents

Querying Information About the Chassis Resource Collection.....	197
Querying Information About a Specified Chassis Resource.....	199
Modifying the Position Indicator Status of a Chassis.....	204
Querying Information About the Network Adapter Resource Collection.....	205
Querying Information About a Specified Network Adapter Resource.....	208
Querying Information About All Network Adapter Resources.....	212
Querying Information About a Specified Network Port Resource.....	218
Querying Information About the Optical Module Resource Connected to a Network Port.....	222
Modifying the LLDP Switch of a Specified Network Port.....	226
Querying Information About the PCIe Device Resource Collection.....	230
Querying Information About a Specified PCIe Device Resource.....	233
Querying Information About All PCIe Device Resources.....	237
Querying Information About the Drive Resource Collection.....	241
Querying Information About a Specified Drive Resource.....	243
Querying Information About All Drive Resources.....	247
Querying the Power Supply Information About a Specified Chassis.....	251
Collecting Information About Power Statistics.....	260
Modifying Properties of a Specified Power Supply.....	263
Querying Cooling Resource Information About a Specified Chassis.....	274
Querying Information About the Expansion Board Resource Collection.....	279
Querying Information About the Hard Disk Backplane Resource Collection.....	281
Querying Information About a Specified Hard Disk Backplane Resource.....	283
Querying Information About the Riser Card Resource Collection.....	285
Querying Information About a Specified Riser Card Resource.....	287
Querying Information About a Specified PCIe Device Function Resource.....	289

Figure 6-1 shows the path requirements for the Chassis resources supported by NETAŞ 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
	IndicatorLED	Position indicator status of the Chassis resource.	GET/PATCH
	Oem	OEM field.	GET
	Thermal	Access path of the cooling resource node of the specified Chassis.	GET
	Mainboard	Mainboard information about the server.	GET

	Power	Access path of the power resource node of the specified Chassis.	GET
--	-------	--	-----

URL	Property	Description	Operation
	NetworkAdapters	Access path of the network adapter resource of the specified Chassis.	GET
	Status	Status of the specified System resource.	GET
	Links	Resources links.	GET
/redfish/v1/Chassis/chassis_id/Thermal	FanSummary	Information about the specified fan sensors.	GET
	Count	Number of fan sensors.	GET
	Fans	Fan sensor list.	GET
	@odata.id	Access path of the specified fan sensor.	GET
	FanName	Name of the specified fan sensor.	GET
	Status	Status of the specified fan sensor.	GET
	SerialNumber	Serial number of the fan.	GET
	LowerThresholdCritical	Critical warning threshold for low speed rotation of the specified fan sensor.	GET
	LowerThresholdFatal	Fatal warning threshold for low speed rotation of the specified fan sensor.	GET
	LowerThresholdNonCritical	Noncritical warning threshold for low speed rotation of the specified fan sensor.	GET
	UpperThresholdCritical	Critical warning threshold for high speed rotation of the specified fan sensor.	GET

	UpperThresholdFatal	Fatal warning threshold for high speed rotation of the specified fan sensor.	GET
	UpperThresholdNonCritical	Noncritical warning threshold for high speed rotation of the specified fan sensor.	GET
	MaxReadingRange	Maximum rotation speed reading for the specified fan sensor.	GET
	MemberId	ID of the specified fan sensor.	GET

URL	Property	Description	Operation
	MinReadingRange	Minimum rotation speed reading for the specified fan sensor.	GET
	Reading	Current reading of the specified fan sensor.	GET
	ReadingUnits	Unit of the fan rotation speed reading for the fan sensor, including: RPM and Percent.	GET
	Temperatures	Temperature sensor list.	GET
	@odata.id	Access path of a specified temperature sensor.	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	Noncritical 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	Noncritical warning threshold for high temperature of the specified temperature sensor.	GET
	MaxReadingRangeTemp	Maximum temperature reading for the specified temperature sensor.	GET
	MinReadingRangeTemp	Minimum temperature reading for the specified temperature sensor.	GET
	Name	Name of the specified temperature sensor.	GET
	PhysicalContext	Area or device used for temperature measurement.	GET

URL	Property	Description	Operation
	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: whether the fan sensor is enabled - Health: health status of the fan sensor	GET
/redfish/v1/Chassis/chassis_id/Power	Id	ID of the power resource.	GET
	Name	Name of the power resource.	GET
	PowerControl	Power control list.	GET

	@odata.id	Access path of the specified power control.	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
	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
	@odata.id	Access path of a 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

URL	Property	Description	Operation
	LineInputVoltage	Input voltage of the specified power supply.	GET
	PowerCapacityWatts	Rated 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
@odata.id	Access path of a specified power redundancy group.	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
@odata.id	Access path of the specified voltage sensor.	GET
Name	Name of the specified voltage sensor.	GET
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	Noncritical warning threshold for high voltage of the specified voltage sensor.	GET

URL	Property	Description	Operation
-----	----------	-------------	-----------

	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	Noncritical 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 reading for the specified voltage sensor.	GET
	MaxReadingRange	Maximum voltage reading for the specified voltage sensor.	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters	Name	Name of the network adapter resource.	GET
	Members@odata.count	Number of network adapter	GET

			resource members.	
	Members		Access path of a single network adapter resource node.	GET
/redfish/v1/Chassis/chassis_id/NetworkAdapters/NetworkAdapters_id	Id		ID of the specified network adapter resource.	GET
	Name		Name of the specified network adapter resource.	GET
	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

URL	Property
	NetworkPorts
	Status
	Oem

	/redfish/v1/Chassis/chassis_id/NetworkAdapters/NetworkAdapters_id/NetworkPorts/NetworkPorts_id	
		Id
		Name
		PhysicalPortNumber
		LinkStatus
		AssociatedNetworkA
	/redfish/v1/Chassis/chassis_id/Drives	Oem
		Name
		Members@odata.co
	/redfish/v1/Chassis/chassis_id/Drives/Drives_id	Members
		Id
		Name

	Model
	Manufacturer
	Status
	CapacityBytes
	MediaType
	Protocol

URL	Property	Description	Op
	PredictedMediaLifeLeftPercent	Percentage of the remaining service life of the specified drive.	GE
	CapableSpeedGbs	Maximum speed of the interface of the specified drive.	GE
	NegotiatedSpeedGbs	Negotiated speed of the interface of the specified drive.	GE
	SerialNumber	Serial number of the specified drive.	GE
	Location	Screen printing of the specified drive.	GE
	Revision	Version information about the	GE

		specified drive.	
/redfish/v1/ Chassis/chassis_id/PCleDevices	Name	Name of the PCle device resource collection.	GE
	Members@odata.count	Number of PCIe device resource members.	GE
	Members	Access path of the specified PCIe device resource node.	GE
/redfish/v1/ Chassis/chassis_id/PCleDevices/PCleDevices_id	Id	ID of the specified PCIe device resource.	GE
	Name	Name of the specified PCIe device resource.	GE
	Description	Description of the specified PCIe device resource.	GE
	Manufacturer	Manufacturer of the specified PCIe device resource.	GE
	Model	Model of the specified PCIe device resource.	GE
	Links	Resources links.	GE
	Status	Status of the specified PCIe device resource.	GE
/redfish/v1/ Chassis/chassis_id/PCleDevices/pciedevices_id/Functions/functions_	DeviceClass	Class of the specified PCIe device function resource.	GE
	DeviceId	DID of the specified PCIe device.	GE

URL	Property	Description	Op
	Id	UID of the specified PCIe device function resource in the iBMC system.	GE
	Links	Links to the related resources.	GE
	PCleDevice	PCIe device resource list.	GE
	Name	Name of the specified PCIe device function resource.	GE
	Oem	Customized properties.	GE
	Public	Customized properties.	GE
	AssociatedResource	Associated resource of the specified PCIe device function resource.	GE
	BusNumber	Bus number of the specified PCIe device root port.	GE
	DeviceNumber	Device number of the specified PCIe device root port.	GE
	FunctionNumber	Function number of the specified PCIe device root port.	GE
	SubsystemId	SDID of the specified PCIe device root port.	GE
	SubsystemVendorId	SVID of the specified PCIe device root port.	GE
	VendorId	VID of the specified PCIe device root port.	GE

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 <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

x-auth-token: `QnaWfqvKOY0ZGc2LK5Ay6+CaSYWjEYcxE6GcWKNFyjU=`

- Request Message Body: None • Response Example:

```

{
    "@odata.context":
"/redfish/v1/$metadata#ChassisCollection.ChassisCollection",
    "@odata.etag": "\"1269454623\"",
    "@odata.id": "/redfish/v1/Chassis",
    "@odata.type": "#ChassisCollection.ChassisCollection",
    "Description": "The Collection for Chassis",
    "Members": [
        {
            "@odata.id":
"/redfish/v1/Chassis/1"
        }
    ],
    "Members@odata.count": 1,
    "Name": "Chassis Collection"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the Chassis resource collection, refer to [Table 6-3](#).

Table 6-3 Output Descriptions for Querying Information About the Chassis Resource Collection

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

6.2 Querying Information About a Specified Chassis Resource

Function

Query information about the specified Chassis resource of a server.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id` • Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

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

Table 6-4 Parameter Descriptions for Querying Information About the Specified Chassis Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
chassis_id	ID of the Chassis resource.	• For a rack server, the value is 1 or Self. • For a high-density server, the value is BladeN (where N indicates slot number of the node), for example, "Blade1". • For a blade server, the value is BladeN (where N indicates the slot number of the computing node) or SwiN (where N 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": "\"1266678241\"",
  "@odata.id": "/redfish/v1/Chassis/1",
"@odata.type": "#Chassis.v1_14_0.Chassis",
  "AssetTag": "1234",
  "ChassisType": "RackMount",
  "Description": "Chassis Self",
  "Drives": {
    "@odata.id":
"/redfish/v1/Chassis/1/Drives"
  },
  "Id": "1",
```



```

        "IndicatorLED": "Blinking",
    "IndicatorLED@Redfish.AllowableValues": [
        "Lit",
        "Blinking",
        "Off"
    ],
    "Links": {
    "ComputerSystems": [
        {
            "@odata.id":
"/redfish/v1/Systems/1"
        }
    ],
    "ManagedBy": [
        {
            "@odata.id":
"/redfish/v1/Managers/1"
        }
    ]
    },
    "LogServices": {
        "@odata.id":
"/redfish/v1/Chassis/1/LogServices"
    },
    "Manufacturer": "NETAŞ",
    "Model": "MBI65G50A",
    "Name": "Computer System Chassis",
    "NetworkAdapters": {
        "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters"
    },
    "Oem": {
        "Public": {
            "DeviceMaxNum": {
                "CPUNum": 2,
                "DiskNum": 25,
                "FanNum": 12,
                "MemoryNum": 32,
                "PCIeNum": 32,
            "PowerSupplyNum": 4
            },
            "Mainboard": {
                "Manufacturer": "NETAŞ",
                "BoardName": "MBI65G50A",
            "SerialNumber": ""
            }
        }
    },

```

```

    "PCIeDevices": {
        "@odata.id":
"/redfish/v1/Chassis/1/PCIeDevices"
    },
    "PCIeSlots": {
        "@odata.id":
"/redfish/v1/Chassis/1/PCIeSlots"
    },
    "PartNumber": " ",
    "Power": {
        "@odata.id":
"/redfish/v1/Chassis/1/Power"
    },
    "PowerState": "On",
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "Thermal": {
        "@odata.id":
"/redfish/v1/Chassis/1/Thermal"
    }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified Chassis resource, refer to [Table 6-5](#).

Table 6-5 Output Descriptions for Querying Information About the Specified Chassis Resource

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

Field	Type	Description
IndicatorLED	String	Position indicator status of the specified Chassis resource, including: ● 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: whether the Chassis is enabled ● Health: health status of the Chassis
PowerState	String	The power-on status of the specified System resource, including ● On ● Off
Oem.Public	Object	Manufacturer-customized properties.
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.
PCleNum	Number	Maximum number of PCIe cards.
PowerSupplyNum	Number	Maximum number of power supplies.
Mainboard	Object	Mainboard information.
BoardName	String	Mainboard name.

SerialNumber	String	Serial number of the mainboard.
PartNumber	String	Part number of the board.
BoardDate	String	Manufacturing date of the board.
Links	Object	Links related to the Chassis resource.
ComputerSystems	Object array	Link to System resources.
ManagedBy	Object array	Link to Manager resources.
PCleDevices	Object	Navigation of the PCIe device resources.
Drives	Object	Navigation of the drive resources.
Field	Type	Description
NetworkAdapters	Object	Information about the related network adapters.
Power	Object	Information about the related power supplies.
Thermal	Object	Chassis cooling resource information.
Boards	Object	Board-level resource links.
SerialNumber	String	Serial number of the chassis.
ProductName	String	Product name.
BoardProductVer	String	Product version of the board.
PartNumber	String	Material code.
ChassisHeight	String	Chassis size.

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
}
```

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.
Parameter	Description	Value
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
state	Position indicator status of the Chassis resource.	Including: ● Lit ● Blinking ● Off

Usage Guidelines

After configuration, you can view the result through **GET** `https://device_ip/redfish/v1/Chassis/1`.

Example

- Request Example:

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

- Request Header:

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

- Request Message Body:

```
{
  "IndicatorLED": "Lit"
}
```

- Response Example: None
- Status Code: 204

Output Description

None

6.4 Querying Information About the Network Adapter Resource Collection

Function

Query information about the network adapter resource collection of a server.

Syntax

- Operation Type: GET
- URL: *https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters*
 - Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the network adapter resource collection, refer to [Table 6-7](#).

Table 6-7 Parameter Information of Querying Information About the Network Adapter Resource Collection

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/NetworkAdapters
```

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#NetworkAdaptersCollection.NetworkAdaptersCollection",
  "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters",
  "@odata.type": "#NetworkAdapterCollection.NetworkAdapterCollection",
  "Description": "Collection of Network Adapters for this Manager",
  "Name": "Network Adapters Collection",
  "Members@odata.count": 4,
  "Members": [
    {
      "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard7"
    },
    {
      "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard8"
    },
    {
      "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1"
    },
    {
      "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2"
    }
  ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the network adapter resource collection, refer to [Table 6-8](#).

Table 6-8 Output Descriptions for Querying Information About the Network Adapter Resource Collection

Field	Type	Description
@odata.context	String	OData description of the network adapter resource collection model.
@odata.id	String	Access path of the network adapter resource collection.
@odata.type	String	Type of network adapter resource collection.
Name	String	Name of the network adapter resource collection.
Name	String	Name of the network adapter resource collection.
Members@odata.count	Number	Number of network adapter resource members.
Members	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

Parameters

For a description of the parameters for querying information about the specified network adapter resource, refer to [Table 6-9](#).

Table 6-9 Parameter Descriptions for Querying Information About the Specified Network Adapter Resource

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/NetworkAdapters/mainboardLOM1
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```

{
  "@odata.context": "/redfish/v1/$metadata#NetworkAdapter.NetworkAdapter",
  "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2",
  "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
  "Id": "mainboardOCPCard2",
  "Name": "mainboardOCPCard2",
  "NetworkPorts": {
    "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2/NetworkPorts"
  },
  "Manufacturer":
"Mellanox",
  "Model": "CX5",
  "Controllers": [
    {
      "FirmwarePackageVersion":
"16.30.1004",
      "Links": {
        "NetworkPorts": [
          {
            "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2/NetworkPorts/1"
          },
          {
            "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2/NetworkPorts/2"
          }
        ]
      },
      "NetworkPorts@odata.count": 2
    }
  ],
  "Oem": {
    "Public": {
      "CardManufacturer": "Mellanox",
      "Name": "MCX562A-ACAB",
      "CardModel": "2*25GE",
      "CardType": "fiber",
      "DriverVersion": null,
      "NetworkTechnology": [
        "Ethernet"
      ]
    }
  }
}

```

```

      "DeviceLocator": "mainboardOCPCard2",
      "SlotNumber": 2,
    "RootBDF": "0000:18:00.0"
  },
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  },
  "SerialNumber":
    "MT2030X11548"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about 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.
@odata.type	String	Type of the specified network adapter resource.
Id	String	Unique ID of the network adapter resource in the iBMC system.
Name	String	Name of the specified network adapter resource.
NetworkPorts	Object	Network port resource list.
@odata.id	String	Access path of a single network port resource.
Manufacturer	String	Manufacturer of the specified network adapter.
Model	String	Model of the specified network adapter.
Controllers	Array	Information about adapter controllers.
FirmwarePackageVersion	String	Firmware version of the specified network adapter.

Links	Object	Links to the related resources.
NetworkPorts	Object	Network port resource information.
@odata.id	String	Access path of the network port resource collection.

Field	Type	Description
NetworkPorts@odata.count	Number	Number of network port resources.
Oem.Public	Object	Manufacturer-customized properties.
CardManufacturer	String	Manufacturer of the specified network adapter.
Name	String	Name of the specified network adapter.
CardModel	String	Interface mode of the specified network adapter.
CardType	String	Type of the specified network adapter.
DriverVersion	String	Driver version of the specified network adapter.
NetworkTechnology	Array	Network protocol of the specified network adapter: • Ethernet • FC • iSCSI • FCoE • OPA • IB
DeviceLocator	String	Screen printing of the specified network adapter.
SlotNumber	String	Slot number of the specified network adapter.
RootBDF	String	Root, port, and BDF of the specified network adapter.
AlarmTmp	Number	Alarm temperature of the network adapter. Query is not supported. By default, null is displayed.
CurrentTmp	Number	Main chip temperature of the network adapter. Query is not supported. By default, null is displayed.

FpgaStatus	Number	FPGA status of the network adapter: 0: The FPGA status of the network adapter is normal. 1: The FPGA status of the network adapter is abnormal. This field is displayed only for an FPGA card.
HistoryMaxTmp	Number	Maximum historical temperature of the network adapter. This field is displayed only for an FPGA card.
NicMemory	Object	Memory information of the network adapter. This field is displayed only for an FPGA card.
CapacityGb	Number	Memory capacity of the network adapter. This field is displayed only for an FPGA card.
Field	Type	Description
Model	String	Memory model of the network adapter. Default: DDR4_2400MHz. This field is displayed only for an FPGA card.
Status	Number	Memory status of the specified network adapter, options: 0: normal memory status of the network adapter 1: abnormal memory status of the network adapter
Status	Object	Status of the network adapter, including: - Health: health status of the network adapter - State: enabling status of the network adapter
SerialNumber	String	Serial number of the specified network adapter.

6.6 Querying Information About All Network Adapter Resources

Function

Query information about all network adapter resources of a server.

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 <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Chassis/1/NetworkAdapters?\$expand=.

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```
{
    "@odata.context":
"/redfish/v1/$metadata#NetworkAdaptersCollection.NetworkAdaptersCollection",
    "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters?$expand=",
    "@odata.type": "#NetworkAdapterCollection.NetworkAdapterCollection",
    "Description": "Collection of Network Adapters for this Manager",
    "Name": "Network Adapters Collection",
    "Members@odata.count": 4,
    "Members": [
        {
            "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard7",
            "@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
            "Id": "mainboardPCIECard7",
            "Name": "mainboardPCIECard7",
            "NetworkPorts": {
                "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard7/NetworkPorts"
            },
            "Manufacturer": "Mellanox",
            "Model": "CX4",
            "Controllers": [
                {
                    "FirmwarePackageVersion": null,
                    "Links": {
                        "NetworkPorts": [
                            {
                                "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard7/NetworkPorts/1"
                            }
                        ]
                    }
                }
            ]
        }
    ]
}
```

```

        {
"@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard7/NetworkPorts/2"
        }
    ],
    "NetworkPorts@odata.count": 2
    }
    }
    ],
    "Oem": {
        "Public": {
    "CardManufacturer": "NETAŞ",
        "Name": "NS212",
        "CardModel": "2*10GE",
        "CardType": "fiber",
        "DriverVersion": null,
        "NetworkTechnology": [
    "Ethernet"
        ],
    "DeviceLocator": "mainboardPCIECard7",
        "SlotNumber": 7,
    "RootBDF": "0000:27:00.0"
        }
    },
    "Status": {
        "Health": "OK",
    "State": "Enabled"
    },
    "SerialNumber": "733320500068"
    },
    {
"@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard8",
"@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
        "Id": "mainboardPCIECard8",
    "Name": "mainboardPCIECard8",
        "NetworkPorts": {
            "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard8/NetworkPorts"
        },
        "Manufacturer": "Intel",
        "Model": "X710",
    "Controllers": [
        {

```



```

        "FirmwarePackageVersion": "8.40",
        "Links": {
"NetworkPorts": [
                {
"@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard8/NetworkPorts/1"
                },
                {
"@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard8/NetworkPorts/2"
                }
            ],
"NetworkPorts@odata.count": 2
        }
    },
    "Oem": {
        "Public": {
"CardManufacturer": "Intel",
            "Name": "X710T2L",
            "CardModel": "2*10GE",
            "CardType": "copper",
            "DriverVersion": null,
            "NetworkTechnology": [
"Ethernet"
            ],
"DeviceLocator": "mainboardPCIECard8",
            "SlotNumber": 8,
"RootBDF": "0000:38:00.0"
        }
    },
    "Status": {
        "Health": "OK",
"State": "Enabled"
    },
    "SerialNumber":
"014613ffff132000"
    },
    {
"@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1",
"@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
        "Id": "mainboardOCPCard1",
"Name": "mainboardOCPCard1",
        "NetworkPorts": {

```



```

        "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1/NetworkPorts"
    },
    "Manufacturer": "Mellanox",
    "Model": "CX5",
    "Controllers": [
        {
            "FirmwarePackageVersion": "16.31.1014",
            "Links": {
                "NetworkPorts": [
                    {
                        "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1/NetworkPorts/1"
                    },
                    {
                        "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1/NetworkPorts/2"
                    }
                ],
                "NetworkPorts@odata.count": 2
            }
        }
    ],
    "Oem": {
        "Public": {
            "CardManufacturer": "Mellanox",
            "Name": "MCX562A-ACAB",
            "CardModel": "2*25GE",
            "CardType": "fiber",
            "DriverVersion": null,
            "NetworkTechnology": [
                "Ethernet"
            ],
            "DeviceLocator": "mainboardOCPCard1",
            "SlotNumber": 1,
            "RootBDF": "0000:ba:00.0"
        },
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        },
        "SerialNumber": "MT2144J28308"
    },

```



```

    {
"@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2",
"@odata.type": "#NetworkAdapter.v1_4_0.NetworkAdapter",
        "Id": "mainboardOCPCard2",
        "Name": "mainboardOCPCard2",
        "NetworkPorts": {
"@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2/NetworkPorts"
        },
        "Manufacturer": "Mellanox",
        "Model": "CX5",
        "Controllers": [
            {
                "FirmwarePackageVersion": "16.30.1004",
                "Links": {
                    "NetworkPorts": [
                        {
"@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2/NetworkPorts/1"
                        },
                        {
"@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard2/NetworkPorts/2"
                        }
                    ],
                    "NetworkPorts@odata.count": 2
                }
            }
        ],
        "Oem": {
            "Public": {
                "CardManufacturer": "Mellanox",
                "Name": "MCX562A-ACAB",
                "CardModel": "2*25GE",
                "CardType": "fiber",
                "DriverVersion": null,
                "NetworkTechnology": [
                    "Ethernet"
                ],
                "DeviceLocator": "mainboardOCPCard2",
                "SlotNumber": 2,
                "RootBDF": "0000:18:00.0"
            }
        }
    }

```

```
    },
    "Status": {
      "Health": "OK",
      "State": "Enabled"
    },
    "SerialNumber": "MT2030X11548"
  }
]
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all network adapter resources, refer to [Table 6-12](#).

Table 6-12 Output Descriptions for Querying Information About All Network Adapter Resources

Field	Type	Description
@odata.context	String	OData description of the network adapter resource collection model.
@odata.id	String	Access path of the network adapter resource collection.
@odata.type	String	Type of network adapter resource collection.
Name	String	Name of the network adapter resource collection.
Members@odata.count	Number	Number of network adapter resource members.
Members	Object array	Network adapter resource information.

For a description of the parameters of the network adapter resource information, refer to [Table 6-10](#).

6.7 Querying Information About a Specified Network Port Resource

Function

Query the information about a single network port resource of a specified Chassis of a server. The information includes the network port name, status, [MAC](#) address, network port type, and network port [BDF](#) information.

Syntax

- Operation Type: GET

- URL:

`https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/NetworkPorts/networkports_id` • Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified network port resource, refer to [Table 6-13](#).

Table 6-13 Parameter Descriptions for Querying Information About the Specified Network Port Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
networkadapters_id	ID of the specified network adapter resource.	It can be obtained by querying the information about the network adapter resource collection.
networkports_id	ID of the network port resource.	It can be obtained by querying the information about the network port resource collection.

Usage Guidelines

None

Example

- Request Example:

GET `https://device_ip/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCleCard8/NetworkPorts/2`

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#EthernetInterface.EthernetInterface",      "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1/NetworkPorts/1",
"@odata.type": "#NetworkPort.v1_4_0.NetworkPort",
  "AssociatedNetworkAddresses": [
    "08:c0:eb:84:cb:d3"
  ],
  "AutoNeg": true,
  "Id": "1",
  "LinkStatus": "Up",
  "Name": "1",
  "Oem": {
    "Public": {
      "BDF": "0000:ba:00.1",
      "CurrentSpeed": "1000Mb/s",
      "DriverVersion": null,
      "FirmwarePackageVersion": "16.31.1014",
      "PortMaxSpeed": "25000Mb/s",
      "PortType": "OpticalPort",
      "LldpService": {
        "LldpEnabled": false,
        "WorkMode": null
      },
      "SupportSpeed": [
        "10Mb/s",
        "100Mb/s",
        "1000Mb/s",
        "10000Mb/s",
        "40000Mb/s",
        "25000Mb/s",
        "100000Mb/s"
      ]
    }
  },
  "PhysicalPortNumber": "1"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified network port resource, refer to [Table 6-14](#).

Table 6-14 Output Descriptions for Querying Information About the Specified Network Port Resource

Field	Type	Description
@odata.context	String	OData description of the specified network port resource model.
@odata.id	String	Access path of the specified network port resource.
@odata.type	String	Type of the specified network port resource.
Id	String	UID of the specified network port resource in the iBMC system.
Name	String	Name of the specified network port resource.
AutoNeg	Boolean	Negotiation mode: ● true: automatic ● false: forced
LinkStatus	String	Status of the specified network port, including: ● Up: connected ● Down: disconnected
AssociatedNetworkAddresses	Array	Network address of the specified network port.
Oem.Public	Object	Manufacturer-customized properties.
PortMaxSpeed	String	Port speed of the specified network port, unit: Mb/s.
PortType	String	Type of the specified network port, including: ● Optical port: OpticalPort ● Electrical port: ElectricalPort ● Location: N/A
BDF	String	BDF of the specified network port.
CurrentSpeed	Number	Current speed.

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
ServiceEnabled	Boolean	Whether the specified network port supports LLDP information query. ● true: LLDP query is supported. ● false: LLDP query is not supported. If this parameter is set to false, only the default values of LldpEnabled and WorkMode are displayed, making no sense.
WorkMode	String	LLDP operation mode.
SupportSpeed	Array	Supported speed of the specified network port.
OpticalModule	Object	Indicates the optical module resources connected to the network port.
PhysicalPortNumber	String	Physical screen printing of the specified network port.

6.8 Querying Information About the Optical Module Resource Connected to a Network Port

Function

Query the information about the optical module resource connected to a network port of a specified server chassis.

Syntax

- Operation Type: GET

- **URL:**

`https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/NetworkPorts/networkports_id/OpticalModule`

- **Request Header:**

`x-auth-token:auth_value`

- **Request Message Body:** None

Parameters

For a description of the parameters for querying the information about the optical module resource connected to a network port, refer to [Table 6-15](#).

Table 6-15 Parameter Descriptions for Querying Information About the Optical Module Resource Connected to the Network Port

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

Usage Guidelines

None

Example

- **Request Example:**

```
GET
https://device_ip/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCleCard8/NetworkPorts/2/OpticalModule
```

- **Request Header:**

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None ● Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#OpticalModule.OpticalModule",
  "@odata.id": "/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCIECard4/
    NetworkPorts/1/OpticalModule",
```

```

    "@odata.type": "#OpticalModule.v1_0_0.OpticalModule",
    "Id": "OpticalModule",
    "Manufacturer": "Hisense",
    "Name": "OpticalModule",
    "PartNumber": "LTF8502-BC+",
    "ProductionDate": "2020-11-09",
    "RXPower": [
        {
            "LowerThresholdCritical": -9.9,
            "ReadingMilliWatts": [
                -40
            ],
            "UpperThresholdCritical": 0.49
        }
    ],
    "SerialNumber":
    "UHYABJ09852",
    "Status": {
        "State": "Enabled"
    },
    "BR_Nominal": 10300,
    "TXBiasCurrent": [
        {
            "LowerThresholdCritical": 0, "
            ReadingMilliWatts": [
                6.24
            ],
            "UpperThresholdCritical": 12
        }
    ],
    "TXPower": [
        {
            "LowerThresholdCritical": -5.5,
            "ReadingMilliWatts": [
                -2.53
            ],
            "UpperThresholdCritical": -1
        }
    ],
    "Temperature": {
        "LowerThresholdCritical": -10,
        "ReadingCelsius": 30.32,
        "UpperThresholdCritical": 75
    },
    "Voltage": {

```

```

        "LowerThresholdCritical": 3.1,
        "ReadingVolts": 3.29,
        "UpperThresholdCritical": 3.5
    },
    "WaveLengthNanometer": 850,    "@odata.etag":
    "W/\\"3e786cf2a931385c3bff00cb24919751\\"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the optical module resource connected to the network port, refer to [Table 6-16](#).

Table 6-16 Output Descriptions for Querying Information About the Optical Module Resource Connected to the Network Port

Field	Type	Description
@odata.context	Character string	OData description of the specified network port resource model.
@odata.id	Character string	Access path of the specified network port resource model.
@odata.type	Character string	Resource type of the specified network port resource model.
@odata.etag	Character string	Whether the interface is changed.
Id	Character string	ID of the optical module resource.
Name	Character string	Name of the optical module resource.
Status	Object	Status of the optical module, including: ● Enabled: enabled state.
Manufacturer	Character string	Name of the manufacturer of the optical module.
PartNumber	Character string	Part number of the optical module.
SerialNumber	Character string	Serial number of the optical module.
ProductionDate	Character string	Manufacturing date of the optical module.
WaveLengthNanometer	Number	Wavelength of the optical module.

BR_Nominal	Number	Rate supported by the optical module.
Voltage	Object	Voltage information about the optical module.
ReadingVolts	Number	Current voltage reading of the optical module.
LowerThresholdCritical	Number	Critical alarm threshold for low voltage.
Field	Type	Description
UpperThresholdCritical	Number	Critical alarm threshold for high voltage.
RXPower	Object	Receiving power of the optical module.
ReadingMilliWatts	Array	Current reading of the receiving power of the optical module.
LowerThresholdCritical	Number	Critical alarm threshold for low receiving power.
UpperThresholdCritical	Number	Critical alarm threshold for high receiving power.
TXPower	Object	Transmission power of the optical module.
ReadingMilliWatts	Array	Current reading of the transmission power of the optical module.
LowerThresholdCritical	Number	Critical alarm threshold for low transmission power.
UpperThresholdCritical	Number	Critical alarm threshold for high transmission power.
TxBiasCurrent	Object	Transmission bias current of the optical module.
ReadingMilliAmperes	Array	Current reading of the bias current of the optical module.
LowerThresholdCritical	Number	Critical alarm threshold for low bias current.
UpperThresholdCritical	Number	Critical alarm threshold for high temperature.
Temperature	Object	Temperature of the optical module.
ReadingCelsius	Number	Current temperature reading of the optical module.
LowerThresholdCritical	Number	Critical alarm threshold for low temperature.
UpperThresholdCritical	Number	Critical alarm threshold for high temperature.

6.9 Modifying the LLDP Switch of a Specified Network Port

Function

Modify the [LLDP](#) switch of a specified network port.

Syntax

- Operation Type: PATCH

- [URL](#):

`https://device_ip/redfish/v1/Chassis/chassis_id/NetworkAdapters/networkadapters_id/NetworkPorts/networkports_id`

- Request Header:

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

- Request Message Body:

```
{
  "Oem":
    {
      "Public":
        {
          "LldpService":
            {
              "LldpEnabled": enable_value,
              "WorkMode": workmode_value
            }
        }
    }
}
```

Parameters

For a description of the parameters for modifying the LLDP switch of a network port, refer to [Table 6-17](#).

Table 6-17 Parameter Descriptions for Modifying the LLDP Switch of the Network Port

Parameter	Description	Value
chassis_id	ID of the chassis resource.	For a rack server, the value is 1 or Self.
networkadapters_id	ID of the specified network adapter resource.	It can be obtained by querying the information about the network adapter resource collection.

networkports_id	ID of the network port resource.	-
enable_value	Whether LLDP is enabled.	● true: enabled ● false: disabled
workmode_value	LLDP operation mode.	● TxRx (default): both the transmitting and receiving modes. If LLDP is disabled, workmode_value is unavailable. ● Rx: receiving mode ● Tx: transmitting mode

Usage Guidelines

None

Example

- Request Example:

PATCH https://device_ip/redfish/v1/Chassis/1/NetworkAdapters/mainboardPCleCard7/NetworkPorts/1

- Request Header:

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

- Request Message Body:

```
{
  "Oem":
  {
    "Public":
    {
      "LldpService":
      {
        "LldpEnabled": true,
        "WorkMode": workmode_value
      }
    }
  }
}
```

- Response Example:

```

{
  "@odata.context":
"/redfish/v1/$metadata#EthernetInterface.EthernetInterface",      "@odata.id":
"/redfish/v1/Chassis/1/NetworkAdapters/mainboardOCPCard1/NetworkPorts/1",
"@odata.type": "#NetworkPort.v1_4_0.NetworkPort",
  "AssociatedNetworkAddresses": [
    "08:c0:eb:84:cb:d3"
  ],
  "AutoNeg": true,
  "Id": "1",
  "LinkStatus": "Up",
  "Name": "1",
  "Oem": {
    "Public": {
      "BDF": "0000:ba:00.1",
      "CurrentSpeed": "1000Mb/s",
      "DriverVersion": null,
      "FirmwarePackageVersion": "16.31.1014",
      "PortMaxSpeed": "25000Mb/s",
      "PortType": "OpticalPort",
      "LldpService": {
        "LldpEnabled": false,
        "WorkMode": null
      },
      "SupportSpeed": [
        "10Mb/s",
        "100Mb/s",
        "1000Mb/s",
        "10000Mb/s",
        "40000Mb/s",
        "25000Mb/s",
        "100000Mb/s"
      ]
    }
  },
  "PhysicalPortNumber": "1"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you modify the LLDP switch of the network port, refer to [Table 6-18](#).

Table 6-18 Output Descriptions for Modifying the LLDP Switch of the Network Port

Field	Type	Description
@odata.context	String	OData description of the specified network port resource model.
@odata.id	String	Access path of the specified network port resource.
@odata.type	String	Type of the specified network port resource.
Id	String	UID of the specified network port resource in the iBMC system.
Name	String	Name of the specified network port resource.
AutoNeg	Boolean	Negotiation mode: ● true: automatic ● false: forced
Field	Type	Description
LinkStatus	String	Status of the specified network port, including: ● Up ● Down
AssociatedNetworkAddresses	Array	Network address of the specified network port.
Oem.Public	Object	Manufacturer-customized properties.
PortMaxSpeed	String	Port speed of the specified network port, unit: Mb/s.
PortType	String	Type of the specified network port, including: ● Optical port: OpticalPort ● Electrical port: ElectricalPort ● Location: N/A
BDF	String	BDF of the specified network port.
CurrentSpeed	Number	Current speed.

FirmwarePackageVersion	String	Firmware version of the specified network port.
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.
PhysicalPortNumber	String	Physical screen printing of the specified network port.

6.10 Querying Information About the PCIe Device Resource Collection

Function

Query information about the [PCIe](#) device resources of a server.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Chassis/chassis_id/PCIeDevices`
 - Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the PCIe device resource collection, refer to [Table 6-19](#).

Table 6-19 Parameter Descriptions for Querying Information About the PCIe Device Resource Collection

Parameter	Description	Value
-----------	-------------	-------

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/PCleDevices
```

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context": "/redfish/v1/
$metadata#PCleDevicesCollection.PCleDbDevicesCollection",
  "@odata.etag": "\"1267642969\"",
  "@odata.id": "/redfish/v1/Chassis/Self/PCleDbDevices",
  "@odata.type": "#PCleDbDeviceCollection.PCleDbDeviceCollection",
}
```

```

    "Description": "PCIe Device Collection",
    "Members": [
      {
        "@odata.id":
"/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard22"
      },
      {
        "@odata.id":
"/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard5"
      },
      {
        "@odata.id":
"/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard19"
      },
      {
        "@odata.id":
"/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard8"
      }
    ],
    "Members@odata.count": 4,
    "Name": "PCIe Device Collection"
  }

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the PCIe device resource collection, refer to [Table 6-20](#).

Table 6-20 Output Descriptions for Querying Information About the PCIe Device Resource Collection

Field	Type	Description
@odata.context	String	OData description of the PCIe device resource collection model.
@odata.id	String	Access path of the PCIe device resource collection.
@odata.type	String	Type of PCIe device resource collection.
Description	String	Description of the PCIe device resource collection.
Name	String	Name of the PCIe device resource collection.
Members@odata.count	Number	Number of PCIe device resource members.
Members	Object array	PCIe device resource list.

6.11 Querying Information About a Specified PCIe Device Resource

Function

Query information about a specified [PCIe](#) device resource of a server.

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

Parameters

For a description of the parameters for querying information about the specified PCIe device resource, refer to [Table 6-21](#).

Table 6-21 Parameter Descriptions for Querying Information About the Specified PCIe Device Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
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/PCIeCard5

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#PCIeDevices.PCIeDevices",
  "@odata.id": "/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard5",
  "@odata.type": "#PCIeDevice.v1_4_0.PCIeDevice",
  "CardManufacturer": "NETAS",
  "CardModel": null,
  "Description": "RS241-18i 2G",
  "FirmwareVersion": "3.22",
  "Id": "mainboardPCIeCard5",
  "Links": {
    "PCIeFunctions": [
      {
        "@odata.id":
"/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard5/Functions/1"
      }
    ]
  },
  "Oem": {
    "Public": {
      "DeviceLocator": "PCIeCard5",
      "LinkSpeed": "3GT/s",
      "MaxLinkSpeed": "3GT/s",
      "MemorySizeMiB": 2097152,
      "PCIeCardType": "Storage Card",
      "PowerCapacityWatts": null,
      "PowerWatts": null,
      "SlotNumber": 5
    }
  },
  "Manufacturer": null,
  "Model": "RAID_SAS8236",
  "Name": "Storage Card5",
  "PCIeInterface": {
    "LanesInUse": 8,
    "MaxLanes": 8
  },
  "SerialNumber":
"743551500214",
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  }
}
```

}

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified PCIe device resource, refer to [Table 6-22](#).

Table 6-22 Output Descriptions for Querying Information About the Specified PCIe Device Resource

Field	Type	Description
@odata.context	String	OData description of the specified PCIe device resource model.
@odata.id	String	Access path of the specified PCIe device resource.
@odata.type	String	Type of the specified PCIe device resource.
CardManufacturer	String	PCIe device manufacturer, which is the same as the CardManufacturer value of the storage controller and NIC.
CardModel	String	PCIe device model, which is the same as the CardModel of the storage controller and the Oem.Public.Name of the NIC.
Name	String	Name of the specified PCIe device resource.
Id	String	UID of the specified PCIe device resource in the iBMC system.
Description	String	Description of the specified PCIe device resource.
Manufacturer	String	Manufacturer of the specified PCIe device.
Model	String	Model of the specified PCIe device resource.
Links	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: whether the specified PCIe device is enabled
PCIeInterface	Object	Interface information about the specified PCIe device.
LanesInUse	Number	Number of currently negotiated PCIe lanes of the specified PCIe device.

Field	Type	Description
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.
DeviceBDF	String	Device BDF of the specified PCIe device.
DeviceLocator	String	Screen printing of the specified PCIe device.
MemorySizeMiB	String	Total memory capacity of the specified PCIe device.
MemoryBandWidth	String	Bandwidth of the display memory data of the specified GPU or NPU when PCIeCardType is GPU or NPU, unit: GB/s.
PowerCapacityWatts	Number	Maximum Thermal Design Power (TDP) of the specified GPU, unit: W.
PowerConsumedWatts	Number	Actual power consumed by the specified GPU, unit: W.
ReadingCelsius	Number	Actual temperature of the specified GPU, unit: centigrade.
PCIeCardType	String	Type of the specified PCIe device.
PowerWatts	Number	Power of the specified PCIe device, unit: W.

RootPortBDF	String	Root port BDF of the specified PCIe device.
SlotNumber	Number	Slot number of the specified PCIe device.
Oem.Public.GpuCore	Memory resource list of the specified PCIe device.	-
BuildTime	String	Production date of the memory of the specified PCIe device.
CapacityGB	Number	Memory capacity of the specified PCIe device, unit: GB.
MemberId	Number	Memory index of the specified PCIe device.
PartNum	String	Memory part number of the specified PCIe device.
Power	String	Power of the specified PCIe device, unit: W.
Field	Type	Description
Temperature	Number	Temperature of the specified PCIe device, unit: centigrade.
Oem.Public.NVMeAIC	Object	-
CapacityGB	Number	Storage capacity of the specified PCIe device.

6.12 Querying Information About All PCIe Device Resources

Function

Query information about all **PCIe** device resources of a server.

Syntax

- Operation Type: GET
- **URL**:
`https://device_ip/redfish/v1/Chassis/chassis_id/PCIeDevices?$expand=.`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For the parameter descriptions for querying information about all PCIe device resources, refer to [Table 6-23](#).

Table 6-23 Parameter Descriptions for Querying Information About All PCIe Device Resources

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/PCleDevices?$expand=.
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```

{
  "@odata.context":
"/redfish/v1/$metadata#PCIeDevicesCollection.PCIeDevicesCollection",
  "@odata.etag": "\"1264523258\"",
  "@odata.id": "/redfish/v1/Chassis/Self/PCIeDevices",
  "@odata.type": "#PCIeDeviceCollection.PCIeDeviceCollection",
  "Description": "PCIe Device Collection",
  "Members": [
    {
      "@odata.id":
"/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard5",
      "@odata.type": "#PCIeDevice.v1_4_0.PCIeDevice",
      "CardManufacturer": "Nvidia",
      "CardModel": "NVIDIA A10",
      "Description": "NVIDIA A10",
      "FirmwareVersion": "94.02.5C.00.04",
      "Id": "mainboardPCIeCard5",
      "Links": {
        "PCIeFunctions": [
          {
            "@odata.id":
"/redfish/v1/Chassis/Self/PCIeDevices/PCIeCard5/Functions/1"
          }
        ]
      },
      "Oem": {
        "Public": {
          "DeviceLocator": "mainboardPCIeCard5",
          "GpuCore": [
            {
              "BuildTime": "2021/06/26",
              "CapacityGB": 24,
              "MemberId": 1,
              "PartNum": null,
              "Power": null,
              "Temperature": 40
            }
          ]
        }
      }
    }
  ],

```

```

        "LinkSpeed": "16.0GT/s",
        "MaxLinkSpeed": "16.0GT/s",
        "MemoryBandWidth": "600GB/s",
        "MemorySizeMiB": 24576,
        "PCIECardType": "GPU",
        "PowerCapacityWatts": 150,
        "PowerWatts": null,
        "PowerConsumedWatts": null,
        "ReadingCelsius": 40,
"SlotNumber": 5
    },
    "Manufacturer": "Nvidia",
    "Model": "NVIDIA A10",
    "Name": "GPU5",
    "PCIEInterface": {
        "LanesInUse": 16,
"MaxLanes": 16
    },
    "SerialNumber":
"1322521044226",
    "Status": {
        "Health": "OK",
"State": "Enabled"
    }
},
{
    "@odata.id":
"/redfish/v1/Chassis/Self/PCIEDevices/PCIECard7",
"@odata.type": "#PCIEDevice.v1_4_0.PCIEDevice",
    "CardManufacturer": "Memblaze",
    "CardModel": "P5916CH0320M00",
    "Description": "AIC",
    "FirmwareVersion": "21300BA0",
"Id": "mainboardPCIECard7",
    "Links": {
"PCIEFunctions": [
        {
            "@odata.id":
"/redfish/v1/Chassis/Self/PCIEDevices/PCIECard19/Functions/1"
        }
    ],
    "Oem": {
        "Public": {
            "DeviceBDF": "a8:0.0",

```

```
        "DeviceLocator": "mainboardPCIECard7",
        "LinkSpeed": "8.0GT/s",
        "MaxLinkSpeed": "8.0GT/s",
        "MemorySizeMiB": 3200,
        "PCIECardType": "NVMe AIC",
        "PowerCapacityWatts": null,
        "PowerWatts": null,
        "PowerConsumedWatts": null,
        "RootPortBDF": "a7:1.0",
    "SlotNumber": 7
    },
    {
        "Manufacturer": "Memblaze",
        "Model": "P5916CH0320M00",
        "Name": "NVMe AIC7",
        "PCIEInterface": {
            "LanesInUse": 4,
            "MaxLanes": 8
        },
        "SerialNumber": "SH193800164",
        "Status": {
            "Health": "OK",
            "State": "Enabled"
        }
    },
    {
        "Members@odata.count": 2,
        "Name": "PCIe Device Collection"
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all PCIe device resources, refer to [Table 6-24](#).

Table 6-24 Output Descriptions for Querying Information About All PCIe Device Resources

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

@odata.type	String	Type of PCIe device resource collection.
Description	String	Description of the PCIe device resource collection.
Field	Type	Description
Name	String	Name of the PCIe device resource collection.
Members@odata.count	Number	Number of PCIe device resource members.
Members	Object array	PCIe device resources.

For a description of the parameters of the PCIe device resource information, refer to [Table 6-22](#).

6.13 Querying Information About the Drive Resource Collection

Function

Query information about the drive resource collection of a server.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Chassis/chassis_id/Drives` • **Request Header:**

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the drive resource collection, refer to [Table 6-25](#).

Table 6-25 Parameter Descriptions for Querying Information About the Drive Resource Collection

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Drives
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#DrivesCollection.DrivesCollection",
  "@odata.id": "/redfish/v1/Chassis/1/Drives",
  "@odata.type": "#DriverCollection.DriverCollection",
  "Description": "Drivers Collection",
  "Name": "Drivers Collection",
  "Members@odata.count": 4,
  "Members": [
    {
      "@odata.id":
"/redfish/v1/Chassis/1/Drives/HDDPlaneDisk16"
    },
    {
      "@odata.id":
"/redfish/v1/Chassis/1/Drives/HDDPlaneDisk17"
    },
    {
      "@odata.id":
"/redfish/v1/Chassis/1/Drives/HDDPlaneDisk19"
    },
    {
      "@odata.id":
"/redfish/v1/Chassis/1/Drives/HDDPlaneDisk21"
    }
  ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the drive resource collection, refer to [Table 6-26](#).

Table 6-26 Output Descriptions for Querying Information About the Drive Resource Collection

Field	Type	Description
-------	------	-------------

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

6.14 Querying Information About a Specified Drive Resource

Function

Query information about a specified drive resource of a server.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Chassis/chassis_id/Drives/drives_id`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified drive resource, refer to [Table 6-27](#).

Table 6-27 Parameter Descriptions for Querying Information About the Specified Drive Resource

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

auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
drives_id	ID of the specified disk.	It can be obtained from the drive list managed by the current specified controllers

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Chassis/1/Drives/HDDPlaneDisk17

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```

{
  "@odata.context": "/redfish/v1/$metadata#Drives.Drives",
  "@odata.id": "/redfish/v1/Chassis/1/Drives/HDDPlaneDisk17",
  "@odata.type": "#Drive.v1_1_0.Drive",
  "CapableSpeedGbs": 12,
  "CapacityBytes": 644245094400,
  "FailurePredicted": null,
  "HotspareType": null,
  "Id": "HDDPlaneDisk17",
  "IndicatorLED": "Off",
  "Location": [
    {
      "Info": "Disk17",
      "InfoFormat": "DeviceName"
    }
  ],
  "Manufacturer": "TOSHIBA",
  "MediaType": "HDD",
  "Model": "AL14SEB060N",
  "Name": "Disk17",
  "NegotiatedSpeedGbs": 12,
  "Oem": {
    "Public": {
      "SASAddress": "30015EBE04B2B93F",
      "RotationSpeedRPM": null,
      "SATAPort": {
        "BelongCPU": null,
        "ControllerBDF": null,
        "ControllerPortNum": null
      }
    }
  },
  "PartNumber": null,
  "PredictedMediaLifeLeftPercent": null,
  "Protocol": "SAS",
  "Revision": "0103",
  "SerialNumber": "38Q0A03LFV7B",
  "SlotNumber": 17,
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  }
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified drive resource, refer to [Table 6-28](#).

Table 6-28 Output Descriptions for Querying Information About the Specified Drive Resource

Field	Type	Description
@odata.context	String	OData description of the specified drive resource model.
@odata.id	String	Access path of the specified drive resource.
@odata.type	String	Type of the specified drive resource.
Id	String	ID of the specified drive resource.
Name	String	Name of the specified drive resource.
Model	String	Model of the specified drive.
Revision	String	Version information about the specified drive.
Status	Object	Status of the specified drive, including: ● State: whether drives are enabled ● Health: health status of the drives
CapableSpeedGbs	Number	Maximum interface speed of the specified drive.
NegotiatedSpeedGbs	Number	Negotiated rate of the specified drive. The value for NVMe is null.

Field	Type	Description
Oem.Public	Object	-
BackpanelId	Number	Backplane ID of the specified drive.
BackPanelLocation	String	Backplane position of the specified drive.
SASAddress	Object	-

CapacityBytes	Number	Capacity of the specified drive, in bytes.
FailurePredicted	Boolean	Pre-failure status of the specified drive, including: ● true ● false
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
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.
Field	Type	Description
PartNumber	String	Part number of the specified drive.
SlotNumber	Number	Slot number of the specified drive.

IndicatorLED	String	Positioning indicator status of the specified drive: • Lit • Off • UnKnown
Location	Object array	Screen printing of the specified drive.
Info	String	Screen printing information about the specified drive.
InfoFormat	String	Screen printing format of the specified drive.
RotationSpeedRPM	Number	Rotation speed of the specified drive, unit: RPM.
BelongCPU	String	CPU of the controller of the specified drive.
ControllerBDF	String	Controller BDF of the specified drive.
ControllerPortNum	Number	Controller port number of the specified drive.

6.15 Querying Information About All Drive Resources

Function

Query information about the drive resource collection of a server.

Syntax

- Operation Type: GET
- [URL](#): `https://device_ip/redfish/v1/Chassis/chassis_id/Drives?$expand=.`
- Request Header: None

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about all drive resources, refer to [Table 6-29](#).

Table 6-29 Parameter Descriptions for Querying Information About All Drive Resources

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Drives?$expand=.
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#DrivesCollection.DrivesCollection",
  "@odata.id": "/redfish/v1/Chassis/Self/Drives",
  "@odata.type": "#DriverCollection.DriverCollection",
  "Description": "Drivers
Collection",      "Name": "Drivers
Collection",
  "Members": [
    {
      "@odata.id":
"/redfish/v1/Chassis/Self/Drives/HDDPlaneDisk30",
      "@odata.type": "#Drive.v1_1_0.Drive",
      "CapableSpeedGbs": 3,
      "CapacityBytes": 2000000000000,
      "FailurePredicted": null,
      "HotspareType": null,
      "Id": "HDDPlaneDisk30",
      "IndicatorLED": null,
```

```

        "Location": [
            {
                "Info": "",
                "InfoFormat": "DeviceName"
            }
        ],
        "Manufacturer": "ATA",
        "MediaType": "HDD",
        "Model": "WDC WD2000FYYZ-01UL1B0",
        "Name": "Disk30",
        "NegotiatedSpeedGbs": 3,
        "Oem": {
            "Public": {
                "SASAddress": null,
                "SATAPort": {
                    "BelongCPU": "CPU0",
                }
            }
        },
        "ControllerBDF": "0000:00:17.0",
        "ControllerPortNum": 2
    },
    "RotationSpeedRPM": 7200
},
{
    "PartNumber": null,
    "PredictedMediaLifeLeftPercent": null,
    "Protocol": "SATA",
    "Revision": "01.x1Kx2",
    "SerialNumber": "WD-WCC1P0458212",
    "SlotNumber": 30,
    "Status": {
        "Health": null,
    },
    "State": null
},
{
    "@odata.id":
"/redfish/v1/Chassis/Self/Drives/HDDPlaneDisk9",
"@odata.type": "#Drive.v1_1_0.Drive",
    "CapableSpeedGbs": 8,
    "CapacityBytes": 3840755982336,
    "FailurePredicted": false,
    "HotspareType": null,
    "Id": "HDDPlaneDisk9",
    "IndicatorLED": "Off",
    "Location": [
        {

```

```

        "Info": "Disk9",
    "InfoFormat": "DeviceName"
    },
    "Manufacturer": "Intel",
    "MediaType": "SSD",
    "Model": "INTEL SSDPF2KX038T1",
    "Name": "Disk9",
    "NegotiatedSpeedGbs": null,
    "Oem": {
        "Public": {
            "BackpanelId": 10,
    "BackPanelLocation": "Front"
        }
    },
    "PartNumber": null,
    "PredictedMediaLifeLeftPercent": 100,
    "Protocol": "NVMe",
    "Revision": "9CV10200",
    "SerialNumber": "PHAX2170001D3P8CGN",
    "SlotNumber": 9,
    "Status": {
        "Health": "OK",
    "State": "Enabled"
    }
    },
    "Members@odata.count": 2,
    "@odata.etag":
    "W/\\"392843a2add75f249962c003c4b05fe9\\"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about all drive resources, refer to [Table 6-30](#).

Table 6-30 Output Descriptions for Querying Information About All Drive Resources

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

@odata.type	String	Type of drive resource collection.
Field	Type	Description
Name	String	Name of the drive resource collection.
Members@odata.count	Number	Number of drive resource members.
Members	Object array	All drive resources.

For a description of the parameters of the drive resource information, refer to [Table 6-28](#).

6.16 Querying the Power Supply Information About a Specified Chassis

Function

Query power supply information about a specified Chassis.

Syntax

- Operation Type: GET
- **URL:** `https://device_ip/redfish/v1/Chassis/Chassis_id/Power` • **Request Header:**

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

Parameters

For a description of the parameters for querying the power supply information about the specified Chassis, refer to [Table 6-31](#).

Table 6-31 Parameter Descriptions for Querying Information About the Specified Chassis Power Supply

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Power
```

- Request Header:

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

- Request Message Body: None • Response Example:

```

{
  "@odata.context":
"/redfish/v1/$metadata#Power.Power",
  "@odata.etag": "\"946660584\"",
  "@odata.id": "/redfish/v1/Chassis/1/Power",
  "@odata.type": "#Power.v1_5_4.Power",
  "Description": "Power sensor readings",
  "Id": "Power",
  "Name": "Power",
  "PowerSupplies": [
    {
      "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/1",
      "FirmwareVersion": "DC:1.01 PFC:1.00",
      "LineInputVoltage": 217,
      "Manufacturer": "Great Wall",
      "Model": "CRPS1200D",
      "Name": "PSU1",
      "PowerCapacityWatts": 1200,
      "PowerInputWatts": 26,
      "PowerOutputWatts": 5,
      "PowerSupplyType": "AC",
      "SerialNumber": "22M010020400",
      "Status": {
        "Health": "OK",
      },
      "State": "Enabled",
      "Oem": {
        "Public": {
          "SlotNumber": 1,
        },
      },
      "ActiveStandby": "Active",
      "MemberId": "1"
    },
    {
      "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/2",
      "FirmwareVersion": "N/A",
      "LineInputVoltage": 0,

```

```

        "Manufacturer": "N/A",
        "Model": "N/A",
        "Name": "PSU2",
        "PowerCapacityWatts": 65535,
        "PowerInputWatts": 65535,
        "PowerOutputWatts": 65535,
        "PowerSupplyType": "N/A",
    "SerialNumber": "N/A",
        "Status": {
            "Health": "Warning",
    "State": "Disabled"
        },
        "Oem": {
            "Public": {
                "SlotNumber": 2,
    "ActiveStandby": "Standby"
            }
        },
    "MemberId": "2"
    },
    {
        "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/3",
        "FirmwareVersion": "N/A",
        "LineInputVoltage": 0,
        "Manufacturer": "N/A",
        "Model": "N/A",
        "Name": "PSU3",
        "PowerCapacityWatts": 65535,
        "PowerInputWatts": 65535,
        "PowerOutputWatts": 65535,
        "PowerSupplyType": "N/A",
    "SerialNumber": "N/A",
        "Status": {
            "Health": "Warning",
    "State": "Disabled"
        },
        "Oem": {
            "Public": {
                "SlotNumber": 3,
    "ActiveStandby": "Standby"
            }
        },
    "MemberId": "3"
    },

```



```

        {
            "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/4",
"FirmwareVersion": "DC:1.01 PFC:1.00",
    "LineInputVoltage": 0,
    "Manufacturer": "Great Wall",
    "Model": "CRPS1200D",
    "Name": "PSU4",
    "PowerCapacityWatts": 1200,
    "PowerInputWatts": 0,
    "PowerOutputWatts": 0,
    "PowerSupplyType": "AC",
"SerialNumber": "22M010020399",
    "Status": {
        "Health": "Warning",
"State": "Enabled"
    },
    "Oem": {
        "Public": {
            "SlotNumber": 4,
"ActiveStandby": "Active"
        }
    },
"MemberId": "4"
    },
],
"PowerSupplies@odata.count": 4,
"PowerControl": [
    {
        "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerControl/1",
        "MemberId": "1",
        "Name": "Chassis Power Control",
"PhysicalContext": "Intake",
        "PowerLimit": {
            "CorrectionInMs": 1000,
            "LimitInWatts": 500,
"LimitException": "NoAction"
        },
        "PowerMetrics": {
            "AverageConsumedWatts": 0,
            "IntervalInMin": 0,
            "MaxConsumedWatts": 0,
"MinConsumedWatts": 0
        },
        "RelatedItem@odata.count": 0,

```



```

        "PowerConsumedWatts": 29,
        "Oem": {
            "Public": {
                "ExpectedActivePSU": [
                    {
                        "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/1"
                    },
                    {
                        "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/4"
                    }
                ]
            }
        }
    ],
    "PowerControl@odata.count": 1,
    "Voltages": [
        {
            "@odata.id":
"/redfish/v1/Chassis/1/Power#/Voltages/1",
            "LowerThresholdCritical": 2.643,
            "LowerThresholdFatal": 0,
            "LowerThresholdNonCritical": 0,
            "MaxReadingRange": 4.463,
            "MemberId": "1",
            "MinReadingRange": 0,
            "Name": "RGM_VCC3.3V",
            "Oem": {
                "Ami": {
                    "@odata.type":
"#AMIDChassisPowerThermal.v1_0_0.AMIDChassisPowerThermal",
                    "OwnerLUN": 0
                }
            },
            "PhysicalContext": "VoltageRegulator",
            "RelatedItem@odata.count": 0,
            "SensorNumber": 1,
            "Status": {
                "State": "Absent"
            },
            "UpperThresholdCritical": 3.955,
            "UpperThresholdFatal": 0,
            "UpperThresholdNonCritical": 0
        },
        {
            "@odata.id": "/redfish/v1/Chassis/1/Power#/Voltages/2",

```



```

        "LowerThresholdCritical": 0.802,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 1.811,
        "MemberId": "2",
        "MinReadingRange": 0,
    "Name": "CPU1_PVNN_MAIN",
        "Oem": {
            "Ami": {
                "@odata.type":
"#AMICHassisPowerThermal.v1_0_0.AMICHassisPowerThermal",
                "OwnerLUN": 0
            }
        },
        "PhysicalContext":
"VoltageRegulator",
        "ReadingVolts": 0.014,
    "RelatedItem@odata.count": 0,
        "SensorNumber": 2,
        "Status": {
            "Health": "Critical",
    "State": "Enabled"
        },
        "UpperThresholdCritical": 1.2,
        "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
    },
    {
        "@odata.id":
"/redfish/v1/Chassis/1/Power#/Voltages/3",
        "LowerThresholdCritical": 0.802,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 1.811,
        "MemberId": "3",
        "MinReadingRange": 0,
    "Name": "CPU0_PVNN_MAIN",
        "Oem": {
            "Ami": {
                "@odata.type":
"#AMICHassisPowerThermal.v1_0_0.AMICHassisPowerThermal",
                "OwnerLUN": 0
            }
        },
        "PhysicalContext": "VoltageRegulator",
    "RelatedItem@odata.count": 0,
        "SensorNumber": 3,
        "Status": {

```

```

        "State": "Absent"
    },
    "UpperThresholdCritical": 1.2,
    "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
    },
    {
        "@odata.id":
"/redfish/v1/Chassis/1/Power#/Voltages/4",
        "LowerThresholdCritical": 2.3,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 3.621,
        "MemberId": "4",
        "MinReadingRange": 0,
    "Name": "CPU1_PVPP_HBM",
        "Oem": {
            "Ami": {
                "@odata.type":
"#AMiChassisPowerThermal.v1_0_0.AMiChassisPowerThermal",
                "OwnerLUN": 0
            }
        },
        "PhysicalContext": "VoltageRegulator",
    "RelatedItem@odata.count": 0,
        "SensorNumber": 4,
        "Status": {
    "State": "Absent"
        },
        "UpperThresholdCritical": 2.797,
        "UpperThresholdFatal": 0,
    "UpperThresholdNonCritical": 0
        }
    ],
    "Voltages@odata.count": 4,
    "Redundancy": [
        {
            "@odata.id":
"/redfish/v1/Chassis/1/Power#/Redundancy/1",
            "Mode": "Sharing",
            "Name":
"PowerSupply Redundancy Group 1"
        }
    ]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the power supply information about the specified Chassis, refer to [Table 6-32](#).

Table 6-32 Output Descriptions for Querying the Power Supply Information About the Specified Chassis

Field	Type	Description
@odata.context	String	OData description of the power supply resource model.
@odata.id	String	Access path of the power resource.
@odata.type	String	Type of power supply resource.
Description	String	Description.
Id	String	ID of the power supply resource.
Name	String	Name of the power supply resource.
PowerControl	Array	Power control list.
@odata.id	String	Access path of the specified power control.
Name	String	Name of the specified power control.
MemberId	String	ID of the specified power control. The ID is the unique identifier of the power control in the power control list.
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.
PowerLimitEnable	Boolean	Whether power capping is enabled.
LimitException	String	Action to be taken when power capping becomes invalid. Value: NoAction (no action).
PowerConsumedWatts	Number	Current power of the device.
Oem.Public	Object	Customized properties.

ExpectedActivePSU	Object	Active power supply list.
@odata.id	String	Access path of a specified power supply.
CurrentCPUPowerWatts	Number	Current CPU power consumption.
CurrentFanPowerWatts	Number	Current fan power consumption.

Field	Type	Description
CurrentMemoryPowerWatts	Number	Current memory power consumption.
CurrentHDDPowerWatts	Number	Current hard disk power consumption.
PowerSupplies	Array	Power supply list. The Status field indicates whether or not the corresponding power module is present.
FirmwareVersion	String	Firmware version of the specified power supply.
LineInputVoltage	Number	Input voltage of the specified power supply.
Manufacturer	String	Manufacturer of the specified power supply.
Model	String	Model of the specified power supply.
Name	String	Name 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.
PowerSupplyType	String	Type of the specified power supply.
ProductionDate	String	Production date of the specified power module.
SerialNumber	String	Serial number of the specified power supply.
Status	Object	Power supply status, including: ● State: whether the power supply is enabled. ● Health: health status of the power supply.
Oem.Public	Object	Customized properties.

ActiveStandby	String	Active or standby power supply mode. Active: active mode. Standby: standby mode.
SlotNumber	Number	Slot number of the specified power supply.
MemberId	String	ID of the specified power supply. The ID is the unique identifier of the power supply in the power supply list.
PowerSupplies@odata.count	Number	Number of power supplies.
Voltages	Array	Voltage sensor list.
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.
Field	Type	Description
LowerThresholdNonCritical	Number	Noncritical warning threshold for low voltage of the specified voltage sensor.
MaxReadingRange	Number	Maximum voltage reading for the specified voltage sensor.
MinReadingRange	Number	Minimum voltage reading for the specified voltage sensor.
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: whether the voltage sensor is enabled. ● Health: health status of the voltage sensor.
ReadingVolts	Number	Current reading of the specified voltage sensor. If no voltage value is obtained from the current voltage sensor, this field will be not displayed.
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	Noncritical warning threshold for low voltage of the specified voltage sensor.
@odata.id	String	Access path of the specified voltage sensor.
Redundancy	Array	Power redundancy group list.
@odata.id	String	Access path of a specified power redundancy group.
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.
Actions	Object	Power operations.
#Power.CollectHistoryData	Object	Collected historical power statistics.

6.17 Collecting Information About Power Statistics

Function

Collect the information about the power statistics of the last 24 hours.

Syntax

- Operation Type: POST

- URL:

https://device_ip/redfish/v1/Chassis/Chassis_id/Power/Actions/Power.CollectHistoryData

- Request Header: None

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

- Request Message Body:

```
{
  "Type":type_value,
  "Content":content_value
  "Range":range_value,
  "Cycle":cycle_value
}
```

Parameters

For a description of the parameters for collecting the information about the power statistics of the last 24 hours, refer to [Table 6-33](#).

Table 6-33 Parameter Descriptions for Querying Information About Power Statistics

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self .
auth_value	When the post request is executed, the "X-Auth-Token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
header_type	Format of the request message.	application/json
type_value	URI for collecting power statistics files.	URI
content_value	Path of power statistics files.	Remote export: "File transfer protocol://ip address/directory/file name". The file transfer protocol is TFTP.
range_value	Power statistics collection range.	- Day: daily statistics. - Week: weekly statistics.
cycle_value	Power statistics collection period.	- Hour: Statistics are collected once an hour (applicable to daily statistics). - Day: Statistics are collected once a day (applicable to weekly statistics).

Usage Guidelines

When the TFTP protocol is used for transmission, the TFTP server needs to be enabled on the server end, for example, through the 3CD software.

Example

- Request Example:

```
POST https://device_ip/redfish/v1/Chassis/1/Power/Actions/Power.CollectHistoryData
```

- Request Header:

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

- Request message body 1: The Range and Cycle fields are not reported.

```
{
  "Type": "URI",
  "Content": "tftp://192.168.5.7/test/powerstatistics.csv"
}
```

- Request message body2: The Type and Content fields are not reported, indicating that the default local download mode is used.

```
{
  "Range": "Day",
  "Cycle": "Hour"
}
```

- Response Example 1:

```
{
  "error": {
    "code": "Base.1.8.1.Success",
    "message": "Successfully Completed Request",
    "@Message.ExtendedInfo": [
      {
        "@odata.type": "#Message.v1_1_1.Message",
        "MessageId": "Base.1.8.1.Success",
        "Message": "Successfully Completed Request",
        "Severity": "OK",
        "Resolution": "None."
      }
    ]
  },
  "@odata.context": "/redfish/v1/$metadata",
  "@odata.id": "/redfish/v1/Chassis/1/Power/Actions/Power.CollectHistoryData"
}
```

- Response example 2: If Postman is used, select a path to save the CSV file.
- Response code:
 - Range and Cycle fields not reported: 202
 - Type and Content fields not reported: 200

Output Description

None.

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"
            }]
        }
      }
    }]
}
```

Parameters

For a description of the parameters for modifying properties of the specified power supply, refer to [Table 6-34](#).

Table 6-34 Parameter Descriptions for Modifying Properties of the Specified Power Supply

Parameter	Description	Value
-----------	-------------	-------

device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self.
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
limit_value	Server power capping value	- Integer: Power capping is enabled and the capping values are set. Range: 1–32767 - null: Power capping is disabled
power_id	Slot number of the power supply.	Set it in accordance with the number of power supplies of different models. Range: 1–4.
redundancy_type	Power redundancy type.	Power redundancy type. Options: - Sharing: If redundancy_type is set to Sharing, Oem does not need to be configured. - Failover

Usage Guidelines

None

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/Chassis/1/Power
```

- Request Header:

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

- Request Message Body1:

```
{
  "PowerControl":
    [{
      "PowerLimit":
        {
          "LimitInWatts": 700
        }
    }]
}
```

- Request Message Body2:

```
{
  "Redundancy":
    [{
      "Mode":
        "Failover"
    }],
  "PowerControl":
    [{
      "Oem": {
        "Public": {
          "ExpectedActivePSU":
            [{
              "@odata.id":
                "/redfish/v1/Chassis/1/Power#/PowerSupplies/1"
            }]
        }
      }
    }]
}
```

- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#Power.Power",
  "@odata.etag": "\"946660584\"",
}
```

```

    "@odata.id": "/redfish/v1/Chassis/1/Power",
    "@odata.type": "#Power.v1_5_4.Power",
    "Description": "Power sensor readings",
    "Id": "Power",
    "Name": "Power",
    "PowerSupplies": [
        {
            "FirmwareVersion":
"DC:1.01 PFC:1.00",
            "LineInputVoltage": 217,
            "Manufacturer": "Great Wall",
            "Model": "CRPS1200D",
            "Name": "PSU1",
            "PowerCapacityWatts": 1200,
            "PowerInputWatts": 26,
            "PowerOutputWatts": 5,
            "PowerSupplyType": "AC",
            "SerialNumber": "22M010020400",
            "Status": {
                "Health": "OK",
            "State": "Enabled"
            },
            "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/1",
            "Oem": {
                "Public": {
                    "SlotNumber": 1,
                "ActiveStandby": "Active"
                }
            },
            "MemberId": "1"
        },
        {
            "FirmwareVersion": "N/A",
            "LineInputVoltage": 0,
            "Manufacturer": "N/A",
            "Model": "N/A",
            "Name": "PSU2",
            "PowerCapacityWatts": 65535,
            "PowerInputWatts": 65535,
            "PowerOutputWatts": 65535,
            "PowerSupplyType": "N/A",
            "SerialNumber": "N/A",
            "Status": {
                "Health": "Warning",
                "State": "Disabled"
            }
        }
    ]

```



```

        },
        "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/2",
        "Oem": {
            "Public": {
                "SlotNumber": 2,
                "ActiveStandby": "Standby"
            }
        },
        "MemberId": "2"
    },
    {
        "FirmwareVersion": "N/A",
        "LineInputVoltage": 0,
        "Manufacturer": "N/A",
        "Model": "N/A",
        "Name": "PSU3",
        "PowerCapacityWatts": 65535,
        "PowerInputWatts": 65535,
        "PowerOutputWatts": 65535,
        "PowerSupplyType": "N/A",
        "SerialNumber": "N/A",
        "Status": {
            "Health": "Warning",
            "State": "Disabled"
        },
        "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/3",
        "Oem": {
            "Public": {
                "SlotNumber": 3,
                "ActiveStandby": "Standby"
            }
        },
        "MemberId": "3"
    },
    {
        "FirmwareVersion":
"DC:1.01 PFC:1.00",
        "LineInputVoltage": 0,
        "Manufacturer": "Great Wall",
        "Model": "CRPS1200D",
        "Name": "PSU4",
        "PowerCapacityWatts": 1200,
        "PowerInputWatts": 0,
        "PowerOutputWatts": 0,
        "PowerSupplyType": "AC",

```



```

        "SerialNumber": "22M010020399",
        "Status": {
            "Health": "Warning",
"State": "Enabled"
        },
        "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/4",
        "Oem": {
            "Public": {
                "SlotNumber": 4,
"ActiveStandby": "Active"
            }
        },
        "MemberId": "4"
    }
],
"PowerSupplies@odata.count": 4,
"PowerControl": [
    {
        "Name": "Chassis Power Control",
"PhysicalContext": "Intake",
        "PowerLimit": {
            "CorrectionInMs": 1000,
            "LimitInWatts": 500,
"LimitException": "NoAction"
        },
        "PowerMetrics": {
            "AverageConsumedWatts": 0,
            "IntervalInMin": 0,
            "MaxConsumedWatts": 0,
"MinConsumedWatts": 0
        },
        "RelatedItem@odata.count": 0,
        "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerControl/1",
        "MemberId": "1",
"PowerConsumedWatts": 29,
        "Oem": {
            "Public": {
"ExpectedActivePSU": [
                {
                    "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/1"
                },
                {
                    "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/4"
                }
            ]
        }
    }
]

```



```

        ]
    }
}
],
"PowerControl@odata.count": 1,
    "Voltages": [
        {
            "@odata.id":
"/redfish/v1/Chassis/1/Power#/Voltages/1",
            "LowerThresholdCritical": 2.643,
            "LowerThresholdFatal": 0,
            "LowerThresholdNonCritical": 0,
            "MaxReadingRange": 4.463,
            "MemberId": "1",
            "MinReadingRange": 0,
            "Name": "RGM_VCC3.3V",
            "Oem": {
                "Ami": {
                    "@odata.type":
"#AMiChassisPowerThermal.v1_0_0.AMiChassisPowerThermal",
                    "OwnerLUN": 0
                }
            },
            "PhysicalContext": "VoltageRegulator",
            "RelatedItem@odata.count": 0,
            "SensorNumber": 1,
            "Status": {
                "State": "Absent"
            },
            "UpperThresholdCritical": 3.955,
            "UpperThresholdFatal": 0,
            "UpperThresholdNonCritical": 0
        },
        {
            "@odata.id":
"/redfish/v1/Chassis/1/Power#/Voltages/2",
            "LowerThresholdCritical": 0.802,
            "LowerThresholdFatal": 0,
            "LowerThresholdNonCritical": 0,
            "MaxReadingRange": 1.811,
            "MemberId": "2",
            "MinReadingRange": 0,
            "Name": "CPU1_PVNN_MAIN",
            "Oem": {
                "Ami": {
                    "@odata.type":
"#AMiChassisPowerThermal.v1_0_0.AMiChassisPowerThermal",

```



```

        "OwnerLUN": 0
    },
    "PhysicalContext":
"VoltageRegulator",
    "ReadingVolts": 0.014,
"RelatedItem@odata.count": 0,
    "SensorNumber": 2,
    "Status": {
        "Health": "Critical",
"State": "Enabled"
    },
    "UpperThresholdCritical": 1.2,
    "UpperThresholdFatal": 0,
"UpperThresholdNonCritical": 0
    },
    {
        "@odata.id":
"/redfish/v1/Chassis/1/Power#/Voltages/3",
        "LowerThresholdCritical": 0.802,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 1.811,
        "MemberId": "3",
        "MinReadingRange": 0,
"Name": "CPU0_PVNN_MAIN",
        "Oem": {
            "Ami": {
                "@odata.type":
"#AMICHassisPowerThermal.v1_0_0.AMICHassisPowerThermal",
                "OwnerLUN": 0
            }
        },
        "PhysicalContext": "VoltageRegulator",
"RelatedItem@odata.count": 0,
        "SensorNumber": 3,
        "Status": {
"State": "Absent"
    },
        "UpperThresholdCritical": 1.2,
        "UpperThresholdFatal": 0,
"UpperThresholdNonCritical": 0
    },
    {
        "@odata.id":
"/redfish/v1/Chassis/1/Power#/Voltages/4",
        "LowerThresholdCritical": 2.3,
        "LowerThresholdFatal": 0,

```



```

        "LowerThresholdNonCritical": 0,
        "MaxReadingRange": 3.621,
        "MemberId": "4",
        "MinReadingRange": 0,
        "Name": "CPU1_PVPP_HBM",
        "Oem": {
            "Ami": {
                "@odata.type":
"#AMICHassisPowerThermal.v1_0_0.AMICHassisPowerThermal",
                "OwnerLUN": 0
            }
        },
        "PhysicalContext": "VoltageRegulator",
        "RelatedItem@odata.count": 0,
        "SensorNumber": 4,
        "Status": {
        "State": "Absent"
        },
        "UpperThresholdCritical": 2.797,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0
    }
],
    "Voltages@odata.count": 4,
    "Redundancy": [
        {
            "@odata.id":
"/redfish/v1/Chassis/1/Power#/Redundancy/1",
            "Mode": "Sharing",
            "Name":
"PowerSupply Redundancy Group 1"
        }
    ]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you modify properties of the specified power supply, refer to [Table 6-35](#).

Table 6-35 Output Descriptions for Modifying Properties of the Specified Power Supply

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

@odata.id	String	Access path of the power resource.
-----------	--------	------------------------------------

Field	Type	Description
@odata.type	String	Type of power supply resource.
Description	String	Description.
Id	String	ID of the power supply resource.
Name	String	Name of the power supply resource.
PowerControl	Array	Power control list.
@odata.id	String	Access path of the specified power control.
Name	String	Name of the specified power control.
MemberId	String	ID of the specified power control. The ID is the unique identifier of the power control in the power control list.
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.
PowerLimitEnable	Boolean	Whether power capping is enabled.
LimitException	String	Action to be taken when power capping becomes invalid. Value: NoAction (no action).
PowerConsumedWatts	Number	Current power of the device.
Oem.Public	Object	Customized properties.
ExpectedActivePSU	Object	Active power supply list.
@odata.id	String	Access path of a specified power supply.
CurrentCPUPowerWatts	Number	Current CPU power consumption.
CurrentFanPowerWatts	Number	Current fan power consumption.

CurrentMemoryPowerWatts	Number	Current memory power consumption.
CurrentHDDPowerWatts	Number	Current hard disk power consumption.
PowerSupplies	Array	Power module list.
FirmwareVersion	String	Firmware version of the specified power supply.
LineInputVoltage	Number	Input voltage of the specified power supply.
Manufacturer	String	Manufacturer of the specified power supply.
Model	String	Model of the specified power supply.
Name	String	Name of the specified power supply.

Field	Type	Description
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.
PowerSupplyType	String	Type of the specified power supply.
SerialNumber	String	Serial number of the specified power supply.
Status	Object	Power supply status, including: ● State: whether the power supply is enabled. ● Health: health status of the power supply.
Oem.Public	Object	Customized properties.
ActiveStandby	String	Active or standby power supply mode. ● Active: active mode. ● Standby: standby mode.
SlotNumber	Number	Slot number of the specified power supply.
MemberId	String	ID of the specified power supply. The ID is the unique identifier of the power supply in the power supply list.
PowerSupplies@odata.count	Number	Number of power supplies.

Voltages	Array	Voltage sensor list.
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.
LowerThresholdNonCritical	Number	Noncritical warning threshold for low voltage of the specified voltage sensor.
MaxReadingRange	Number	Maximum voltage reading for the specified voltage sensor.
MinReadingRange	Number	Minimum voltage reading for the specified voltage sensor.
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: whether the voltage sensor is enabled. ● Health: health status of the voltage sensor.
Field	Type	Description
ReadingVolts	Number	Current reading of the specified voltage sensor. If there is no reading, this field is not displayed.
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.
UpperThresholdNonCritical	Number	Noncritical warning threshold for high voltage of the specified voltage sensor.
@odata.id	String	Access path of the specified voltage sensor.
Redundancy	Array	Power redundancy group list.
@odata.id	String	Access path of a specified power redundancy group.
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.
------	--------	--

6.19 Querying 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 6-36](#).

Table 6-36 Parameter Descriptions for Querying the Temperature and Fan Sensor Resource Information About the Specified Chassis

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Thermal
```

- Request Header:

x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None ● Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#Thermal.Thermal",
  "@odata.etag": "\"946656065\"",
  "@odata.id": "/redfish/v1/Chassis/1/Thermal",
  "@odata.type": "#Thermal.v1_5_3.Thermal",
  "Description": "Thermal sensor readings",
  "Id": "Thermal",
  "Name": "Thermal",
  "Oem": {
    "Public": {
      "FanSpeedAdjustmentMode": "Manual",
      "SpeedRatio": 30
    }
  },
  "FanSummary": {
    "Count": 2
  },
  "Fans": [
    {
      "@odata.id": "/redfish/v1/Chassis/1/Thermal#/Fans/156",
```

```

        "Name": "FAN_SPEED_03",
        "LowerThresholdCritical": 1500,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MemberId": "3",
        "ReadingUnits": "RPM",
        "Status": {
            "State": "Enabled",
        },
        "Health": "OK",
        "UpperThresholdCritical": 16500,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0,
        "SerialNumber": "20150305",
        "Oem": {
            "Public": {
                "SlotNumber": 3,
            },
        },
        "SpeedRatio": 30,
        "MinReadingRange": 1500,
        "MaxReadingRange": 16500,
        "Reading": 4599,
        {
            "@odata.id":
"/redfish/v1/Chassis/1/Thermal#/Fans/157",
        "Name": "FAN_SPEED_04",
        "LowerThresholdCritical": 1500,
        "LowerThresholdFatal": 0,
        "LowerThresholdNonCritical": 0,
        "MemberId": "4",
        "ReadingUnits": "RPM",
        "Status": {
            "State": "Enabled",
        },
        "Health": "OK",
        "UpperThresholdCritical": 16500,
        "UpperThresholdFatal": 0,
        "UpperThresholdNonCritical": 0,
        "SerialNumber": "20150305",
        "Oem": {
            "Public": {
                "SlotNumber": 4,
                "SpeedRatio": 30
            }
        }
    }

```

```

        }
    },
    "MinReadingRange": 1500,
    "MaxReadingRange": 16500,
    "Reading": 4552
  }
]
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the temperature and fan sensor resource information about the specified Chassis, refer to [Table 6-37](#).

Table 6-37 Output Descriptions for Querying the Temperature and Fan Sensor Resource Information About the Specified Chassis

Field	Type	Description
Description	String	Description of the cooling resource.
Id	String	ID of the cooling resource.
Name	String	Name of the cooling resource.
Oem.Public	Object	Customized information about the cooling resource.
FanSpeedAdjustmentMode	String	Fan speed adjustment mode, including: • Automatic mode • Manual mode
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 terms.
Temperatures	Object	Temperature sensor list.
LowerThresholdCritical	Number	Critical warning threshold for low speed rotation of the specified fan sensor.
LowerThresholdFatal	Number	Fatal warning threshold for high speed rotation of the specified fan sensor.

LowerThresholdNonCritical	Number	Noncritical warning threshold for low speed rotation of the specified fan sensor.
MemberId	String	ID of the specified temperature sensor.

Field	Type	Description
Name	String	Name of the specified temperature sensor.
PhysicalContext	String	Area or device to which the temperature measurement applies.
ReadingCelsius	Number	Current reading of the specified temperature sensor.
SensorNumber	String	Serial number of the specified temperature sensor.
Status	Object	Status of the specified temperature sensor. Options: ● State: whether the temperature sensor is enabled. ● Health: health status of the temperature sensor.
UpperThresholdCritical	Number	Critical warning threshold for high speed rotation of the specified fan sensor.
UpperThresholdFatal	Number	Fatal warning threshold for high speed rotation of the specified fan sensor.
UpperThresholdNonCritical	Number	Noncritical warning threshold for low speed rotation of the specified fan sensor.
MinReadingRange	Number	Minimum rotation speed reading for the specified fan sensor.
MaxReadingRange	Number	Maximum rotation speed reading for the specified fan sensor.
FanSummary	Object	Information about the specified fan sensor.
Count	Number	Number of fan sensors.
Fans	Array	Fan sensor list.
Name	String	Name of the specified fan sensor.

Status	Object	Status of the specified fan sensor, including: • State: whether the fan sensor is enabled. • Health: health status of the fan sensor.
MemberId	String	ID of the specified fan sensor.
ReadingUnits	String	Unit of the fan rotation speed reading for the fan sensor, including: • RPM • Percent
Oem.Public	Object	Customized information about the cooling resource.
SlotNumber	Number	Slot number of the specified fan sensor.
SpeedRatio	Number	Current reading of the specified fan sensor, in percentage.
Field	Type	Description
MaxReadingRangeTemp	Number	Maximum temperature reading for the specified temperature sensor.
MinReadingRangeTemp	Number	Minimum temperature reading for the specified temperature sensor.
Reading	Number	Current reading of the specified fan sensor.
Model	Number	Fan model.

6.20 Querying Information About the Expansion Board Resource Collection

Function

Query the information about the expansion board resource collection.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/chassis_id/Boards` • Request Header:

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

Parameters

For a description of the parameters for querying the information about the expansion board resource collection, refer to [Table 6-38](#).

Table 6-38 Parameter Descriptions for Querying Information About the Expansion Board Resource Collection

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

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Chassis/1/Boards

Request Header:

X-Auth-Token: 8574621db1284756218c7564821c234

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#BoardInformation.BoardInformation",
  "@odata.id": "/redfish/v1/Chassis/1/Boards",
  "@odata.type":
    "#BoardInformation.BoardInformation",
  "Description": "Board Information",
  "DiskBackplanes": {
    "@odata.id":
      "/redfish/v1/Chassis/1/Boards/DiskBackplanes"
  },
  "Risercard": {
    "@odata.id":
      "/redfish/v1/Chassis/1/Boards/Risercard"
  },
  "Id":
    "Boards",
  "Name": "Board
  Information"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the expansion board resource collection, refer to [Table 6-39](#).

Table 6-39 Output Descriptions for Querying Information About the Expansion Board Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the expansion board resource collection module.
@odata.id	Character string	Access path of the expansion board resource collection.

@odata.type	Character string	Type of expansion board resource collection.
Description	Character string	Description of the expansion board resource collection.

Field	Type	Description
DiskBackplanes	Object	Hard disk backplanes.
Risercard	Object	Riser card collection information.
Id	Character string	ID of the expansion board resource collection.
@odata.id	Character string	Access path of the riser card.
Name	Character string	Board name.

6.21 Querying Information About the Hard Disk Backplane Resource Collection

Function

Query the information about the hard disk backplane resource collection of a server.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/Chassis_id/Boards/DiskBackplanes`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the information about the hard disk backplane resource collection, refer to [Table 6-40](#).

Table 6-40 Parameter Descriptions for Querying Information About the Hard Disk Backplane Resource Collection

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

Example

- Request Example:

auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

GET https://device_ip/redfish/v1/Chassis/1/Boards/DiskBackplanes

Request Header:

x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#DiskBackplanesCollection.DiskBackplanesCollection",
  "@odata.id": "/redfish/v1/Chassis/1/Boards/DiskBackplanes",
  "@odata.type": "#DiskBackplanesCollection.DiskBackplanesCollection",
  "Description": "DiskBackplanes Collection",
  "Name": "DiskBackplanes Collection",
  "Members": [
    {
      "@odata.id":
"/redfish/v1/Chassis/1/Boards/DiskBackplanes/DiskBackplanes10"
    },
    {
      "@odata.id":
"/redfish/v1/Chassis/1/Boards/DiskBackplanes/DiskBackplanes11"
    }
  ]
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the hard disk backplane resource collection, refer to [Table 6-41](#).

Table 6-41 Output Descriptions for Querying Information About the Hard Disk Backplane Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the hard disk backplane resource collection model.
@odata.id	Character string	Access path of the hard disk backplane resource collection.
@odata.type	Character string	Type of hard disk backplane resource collection.

Field	Type	Description
Name	Character string	Name of the hard disk backplane resource collection.
Members@odata.count	Number	Current number of hard disk backplane resources.
Members	Array	Hard disk backplane resources list.
@odata.id	Character string	Access path of a hard disk backplane resource node.

6.22 Querying Information About a Specified Hard Disk Backplane Resource

Function

Query information about a specified hard disk backplane resource of a server.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/Chassis/Chassis_id/Boards/DiskBackplanes/DiskBackplaneId`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the information about the specified hard disk backplane resource, refer to [Table 6-42](#).

Example

- Request Example:

Table 6-42 Parameter Descriptions for Querying Information About the Specified Hard Disk Backplane Resource

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

Usage Guidelines

None

GET https://device_ip/redfish/v1/Chassis/1/Boards/DiskBackplanes/DiskBackplane8

Request Header:

x-auth-token:LXlrQPHHOPTz6k4rrPB/UfABUd45p9PFIC8QG2lp2F0=

- Request Message Body: None
- Response Example:


```
{
  "@odata.context": "/redfish/v1/$metadata#DiskBackplane.DiskBackplane",
  "@odata.id": "/redfish/v1/Chassis/1/Boards/DiskBackplanes/DiskBackplanes8",
  "@odata.type": "#DiskBackplane.v1_0_0.DiskBackplane",
  "Name": "SBF24MB",
  "CPLDVersion": null,
  "MaxDiskCountSupported": 24,
  "PartNumber": "19020100",
  "Location": "Front",
  "Manufacturer": "NETAŞ",
  "PortCount": "SLIMSAS*2 + SLIMLINE*4",
  "SerialNumber": null,
  "Type": "3.5
SAS/SATA*24,U.2*8,Expander",
  "OnlineDiskCount": 0,
  "ID": 10,
  "PcbID": 1
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the specified hard disk backplane resource, refer to [Table 6-43](#).

Table 6-43 Output Descriptions for Querying Information About the Specified Hard Disk Backplane Resource

Field	Type	Description
@odata.context	Character string	OData description of the hard disk backplane resource collection model.
@odata.id	Character string	Access path of the hard disk backplane resource collection.
@odata.type	Character string	Type of hard disk backplane resource collection.

Field	Type	Description
Name	Character string	Name of the hard disk backplane resource collection.
CPLDVersion	Character string	CPLD version of the specified hard disk backplane.
MaxDiskCountSupported	Number	Maximum number of hard disks supported by the specified hard disk backplane.

Example

- Request Example:

-

PartNumber	Character string	Part number of the specified hard disk backplane.
Location	Character string	Lcation of the specified hard disk backplane.
Manufacturer	Character string	Manufacturer of the specified hard disk backplane.
PortCount	Character string	Number of ports supported by the specified hard disk backplane.
SerialNumber	Character string	Serial number of the specified hard disk backplane.
Type	Character string	Type of the specified hard disk backplane.
OnlineDiskCount	Number	Number of present hard disks supported by the specified hard disk backplane.
ID	Number	Serial number of the specified hard disk backplane.
PcbID	Number	PCB ID of the specified hard disk backplane.

6.23 Querying Information About the Riser Card Resource Collection

Function

Query information about the Riser card resource collection of a server.

Syntax

- Operation Type: GET
- URL:
`https://device_ip/redfish/v1/Chassis/Chassis_id/Boards/Risercard`
- Request Header:

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

Parameters

For a description of the parameters for querying information about the Riser card resource collection, refer to [Table 6-44](#).

Table 6-44 Parameter Descriptions for Querying Information About the Riser Card Resource Collection

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Boards/Risercard
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#RisercardCollection.RisercardCollection",
  "@odata.id": "/redfish/v1/Chassis/1/Boards/Risercard",
  "@odata.type": "#RisercardCollection.RisercardCollection",
  "Description": "Risercard Collection",
  "Name": "Risercard Collection",
  "Members": [
    {
      "@odata.id":
"/redfish/v1/Chassis/1/Boards/Risercard/Risercard6"
    }
  ],
  "Members@odata.count": 1
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the riser card resource collection, refer to [Table 6-45](#).

Table 6-45 Output Descriptions for Querying Information About the Riser Card Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the riser card resource collection model.
@odata.id	Character string	Access path of the riser card resource collection.
@odata.type	Character string	Type of riser card resource collection.
Description	Character string	Description of the riser card resource collection.
Name	Character string	Name of the riser card resource collection.
Members@odata.count	Number	Current number of riser card resources.
Members	Object array	Riser card resource list.
@odata.id	Character string	Access path of a riser card resource node.

6.24 Querying Information About a Specified Riser Card Resource

Function

Query the information about a specified riser card resource of a server.

Syntax

- Operation Type: GET

- URL:

`https://device_ip/redfish/v1/Chassis/Chassis_id/Boards/Risercard/RisercardId` • Request Header:

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

- Request Message Body: None

Parameters

For a description of the parameters for querying the information about the specified riser card resource, refer to [Table 6-46](#).

Table 6-46 Parameter Descriptions for Querying Information About the Specified Riser Card Resource

Parameter	Description	Value
-----------	-------------	-------

device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
chassis_id	ID of the Chassis resource.	For a rack server, the value is 1 or Self .

Parameter	Description	Value
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
RisercardId	ID of the specified riser card.	Obtained from the information about the slot of the riser card.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/Chassis/1/Boards/Risercard/Risercard6
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Risercard.Risercard",
  "@odata.id": "/redfish/v1/Chassis/1/Boards/Risercard/Risercard6",
  "@odata.type": "#Risercard.v1_0_0.Risercard",
  "Manufacturer": "NETAŞ",
  "Name": "Risercard6",
  "PartNumber": "",
  "SerialNumber": "208540654320"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the specified riser card resource, refer to [Table 6-47](#).

Table 6-47 Output Descriptions for Querying Information About the Specified Riser Card Resource

Field	Type	Description
-------	------	-------------

@odata.context	Character string	OData description of the specified riser card resource.	
@odata.id	Character string	Access path of the specified riser card resource.	
Field	Type	Description	
@odata.type	Character string	Type of the specified riser card resource.	
Manufacturer	Character string	Manufacturer of the specified riser card.	
Name	Character string	Name of the specified riser card resource.	
PartNumber	Character string	Part number of the specified riser card resource.	
SerialNumber	Character string	Serial number of the specified riser card resource.	

6.25 Querying Information About a Specified PCIe Device Function Resource

Function

Query information about a specified [PCIe](#) device function resource of a server.

Syntax

- Operation Type: GET
- [URL](#) :
`https://device_ip/redfish/v1/Chassis/chassis_id/PCIeDevices/pciedevices_id/Functions/functions_`
 - Request Header:

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

Parameters

For a description of the parameters for querying the information about the specified PCIe device function resource, refer to [Table 6-48](#).

Table 6-48 Parameter Descriptions for Querying Information About the Specified PCIe Device Function Resource

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

auth_value		When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions.</i>
pciedevices_id		ID of the specified PCIe device resource.	This parameter can be queried through the specified resource set.

Parameter	Description	Value
functions_id	ID of the PCIe device function resource.	This parameter can be queried through the specified resource set.

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/Chassis/1/PCleDevices/PCleCard64/Functions/1

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:


```
{
  "@odata.context": "/redfish/v1/$metadata#PCIeFunction.PCIeFunction",
  "@odata.id": "/redfish/v1/Chassis/1/PCIeDevices/PCIeCard64/Functions/1",
  "@odata.type": "##PCIeFunction.v1_2_3.PCIeFunction",      "DeviceClass":
  "NetworkController",      "DeviceId": "0x1017",
  "Id": "1",
  "Links": {
    "PCIeDevice": [
      {
        "@odata.id":
"/redfish/v1/Chassis/1/PCIeDevices/PCIeCard64"
      }
    ]
  },      "Name":
  "Function1",
  "Oem": {
    "Public": {
      "AssociatedResource": "CPU1",
      "BusNumber": "0xb8",
      "DeviceNumber": "0x00",
      "FunctionNumber": "0x00"
    }
  },
  "SubsystemId": "0x0052",
  "SubsystemVendorId": "0x15b3",
  "VendorId": "0x15b3",

  "@odata.etag": "W/\"1ae394128c6b9056e8d6da3cde35c220\""
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the specified PCIe device function resource, refer to [Table 6-49](#).

Table 6-49 Output Descriptions for Querying Information About the Specified PCIe Device Function Resource

字段	类型	说明
@odata.context	String	OData description of the specified PCIe device function resource.

@odata.id	String	Access path of the specified PCIe device function resource.
@odata.type	String	Type of the specified PCIe device function resource.
DeviceClass	String	Class of the specified PCIe device function resource, including: - UnclassifiedDevice - MassStorageController - NetworkController - DisplayController - MultimediaController - MemoryController - Bridge - CommunicationController - GenericSystemPeripheral - InputDeviceController - DockingStation - Processor - SerialBusController - WirelessController - IntelligentController - SatelliteCommunicationsController - EncryptionController - SignalProcessingController - ProcessingAccelerators - NonEssentialInstrumentation - Coprocessor - UnassignedClass - Other

字段	类型	说明
DeviceId	String	DID of the specified PCIe device.
Id	String	UID of the specified PCIe device function resource in the iBMC system.
Links	Object	Links to the related resources.
PCIeDevice	Array	PCIe device resource list.
Name	String	Name of the specified PCIe device function resource.

Oem	Object	Customized properties.
Public	Object	Customized properties.
AssociatedResource	String	Associated resource of the specified PCIe device function resource.
BusNumber	String	Bus number of the specified PCIe device root port.
DeviceNumber	String	Device number of the specified PCIe device root port.
FunctionNumber	String	Function number of the specified PCIe device root port.
SubsystemId	String	SDID of the specified PCIe device root port.
SubsystemVendorId	String	SVID of the specified PCIe device root port.
VendorId	String	VID of the specified PCIe device root port.

Chapter 7

Operations on SessionService Resources

Table of Contents

Querying Information About the Session Service.....294

Modifying Information About the Session Service..... 296

Creating Information About a Session.....297

Querying Information About the Session Resource Collection.....299

Querying Information About a Specified Session Resource.....301

Deleting Information About a Specified Session Resource..... 303

Figure 7-1 shows the path requirements for the SessionService resources supported by NETAŞ servers.

Figure 7-1 SessionService Resource Path Requirements



For a description of properties of SessionService resources and operations supported by the properties, refer to Table 7-1.

Table 7-1 Descriptions of SessionService Resources Properties

URL	Property	Description	Operation
/redfish/v1/SessionService	Id	ID of the SessionService resource.	GET
	Name	Name of the SessionService resource.	GET
	SessionTimeout	Session service timeout period.	GET/PATCH
	Sessions	Access path of the session list.	GET

URL	Property	Description	Operation
/redfish/v1/SessionService/Sessions	Name	Name of the session resource.	GET
	Members@odata.count	Number of session members.	GET
	Members	Session resource list, which provides references for all session resource URLs .	GET
/redfish/v1/SessionService/Sessions/session_id	-	Specified session resource.	DELETE
	Id	UID of the specified session resource.	GET
	Name	Name of the specified session.	GET
	UserName	Account information about the specified session.	GET

7.1 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 7-2](#).

Table 7-2 Parameter Descriptions for Querying Information About the Session Service

Parameter	Description	Value
-----------	-------------	-------

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

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/SessionService

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#SessionService.SessionService",
  "@odata.etag": "W/\"1606215253\"",
  "@odata.id":
    "/redfish/v1/SessionService",
  "@odata.type":
    "#SessionService.v1_1_3.SessionService",
  "Description": "Session Service",
  "Id": "SessionService",
  "Name": "Session Service",
  "ServiceEnabled": true,
  "SessionTimeout": 180,
  "Sessions": {
    "@odata.id":
      "/redfish/v1/SessionService/Sessions"
  },
  "Status": {

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

- Status Code: 200

Output Description

For a description of the output returned when you query information about the session service, refer to [Table 7-3](#).

Table 7-3 Output Descriptions for Querying Information About the Session Service

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

7.2 Modifying Information About the Session Service

Function

Modify the timeout period of the current 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
}
```

Parameters

For a description of the parameters for modifying information about the session service, refer to [Table 7-4](#).

Table 7-4 Parameter Descriptions for Modifying Information About the Session Service

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

7.3 Creating Information About 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 7-5](#).

Table 7-5 Parameter Descriptions for Creating a Session

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
header_type	Format of the request message.	application/json
name	User for the new session.	User of the iBMC system.
password	Password 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 "XAuth-Token" value can be obtained through this operation.

Example

- **Request Example:**

POST https://device_ip/redfish/v1/SessionService/Sessions

- **Request Header:**

Content-Type: application/json

- **Request Message Body:**

```
{
  "UserName": "username",
  "Password": "password"
}
```

- **Response Example:**

```
{
  "@odata.context": "/redfish/v1/$metadata#SessionService.Sessions",
  "@odata.id": "/redfish/v1/SessionService/Sessions/q1xUU91KqyADxiLlJcq9jdygXUZ",
  "@odata.type": "#Session.v1_1_0.Session",
  "Name": "User Session",
  "Id":
    "q1xUU91KqyADxiLlJcq9jdygXUZr0Hwe",
  "UserName": "Administrator"
}
```

- Response Header Example:

Location: /redfish/v1/SessionService/Sessions/1
X-Auth-Token: YzAhv2WCq5ZMDJUq7JJ3ELEpNF3eoOab

- Status Code: 201

Output Description

For a description of the output returned when you create a session, refer to [Table 7-6](#).

Table 7-6 Output Descriptions for Session Creation

Field	Type	Description
@odata.context	String	OData description of the newly created session resource model.
@odata.id	String	Access path of the newly created session resource. The detailed information about the session can be obtained.
@odata.type	String	Type of the newly created session resource.
Id	String	UID of the newly created session resource.
Name	String	Name of the newly created session.
Description	String	Description of the new session.
UserName	String	Account information about newly created session.

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 <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/SessionService/Sessions

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None • Response Example:

```

{
    "@odata.context":
"/redfish/v1/$metadata#SessionCollection.SessionCollection",
    "@odata.id": "/redfish/v1/SessionService/Sessions",
    "@odata.type": "#SessionCollection.SessionCollection",
    "Name": "Session Collection",
    "Members": [
        {
            "@odata.id":
"/redfish/v1/SessionService/Sessions/
iZoEEcrx8c2uOzFefkA8pFD0XnSqDqaG"
        },
        {
            "@odata.id":
"/redfish/v1/SessionService/Sessions/
sf3I8CJsQrpwCumCR9niUTcpFVeaz2Wx"
        }
    ],
    "Members@odata.count": 2
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the session resource collection, refer to [Table 7-8](#).

Table 7-8 Output Descriptions for Querying Information About the Session Resource Collection

Field	Type	Description
@odata.context	String	OData description of the session resource model.
@odata.id	String	Access path of the session resource node.
@odata.type	String	Type of session resource.
Name	String	Name of the session resource.
Members@odata.count	Number	Number of session members.
Members	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 <code>/redfish/v1/SessionService/Sessions</code> .

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/SessionService/Sessions/57f5ff2105218ad2df694ab94cbeba90
```

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Session.Session",
  "@odata.id":
  "/redfish/v1/SessionService/Sessions/iZoEEcrx8c2uOzFefkA8pFD0XnSqDqaG",
  "@odata.type": "#Session.v1_1_0.Session",
  "Description": "Session for user Administrator",
  "UserName": "Administrator",
  "Name": "Session",      "Id":
  "iZoEEcrx8c2uOzFefkA8pFD0XnSqDqaG"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the specified session resource, refer to [Table 7-10](#).

Table 7-10 Output Descriptions for Querying Information About the Specified Session Resource

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

Parameter	Description	Value
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 <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

DELETE https://device_ip/redfish/v1/SessionService/Sessions/57f5ff2105218ad2df694ab94cbeba90

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

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

Output Description

None

Chapter 8

Operations on EventService Resources

Table of Contents

Querying Information About the EventService Resource.....307

Querying Information About the Event Subscription Resource Collection.....310

Creating an Event Subscription Resource.....312

Querying Information About an Event Subscription Resource.....316

Modifying Information About an Event Subscription Resource.....318

Deleting an Event Subscription Resource..... 321

Reporting an Event..... 322

Querying Information About the Event Resource Collection.....324

Deleting All Event Resources..... 327

Querying Information About the Current Alarm Resource Collection.....328

Querying Information About the Current Alarm Resource.....332

Deleting the Current Alarm Resource.....334

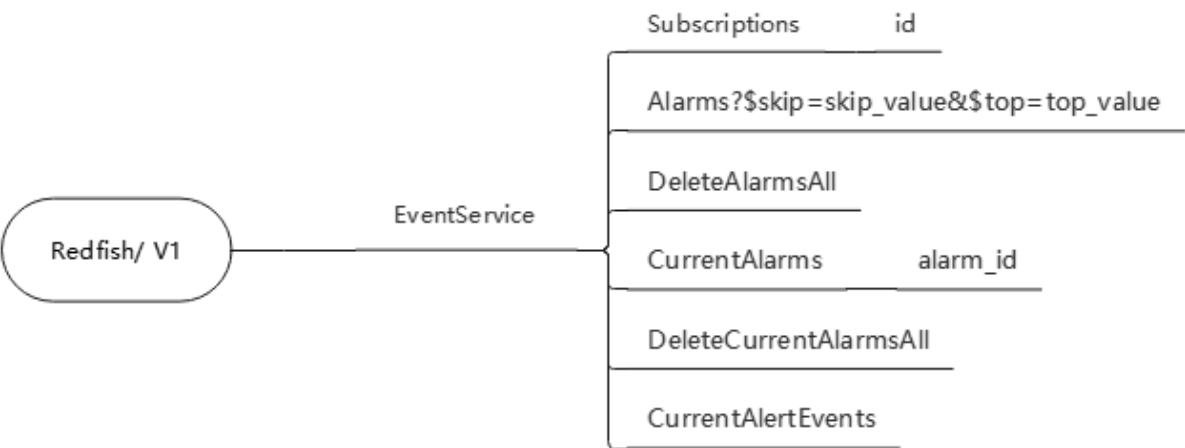
Deleting All Current Alarm Resource.....335

Querying Information About the Current Alarm Event Resource Collection.....336

Modifying Event Service Resource Information.....340

Figure 8-1 shows the path requirements for the EventService resources supported by NETAŞ servers.

Figure 8-1 EventService Resource Path Requirements



For a description of properties of EventService resources and operations supported by the properties, refer to [Table 8-1](#).

Table 8-1 Descriptions of EventService Resources Properties

URL	Property	Description	Opera - tion
/redfish/v1/EventService	Id	ID of an event resource.	GET
	Name	Name of the event resource.	GET
	ServiceEnabled	Whether event reporting is enabled.	GET
	DeliveryRetryAttempts	Maximum number of retries for delivering event subscription s.	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	GET

		target resource collection.	
	Actions	Operations that can be performed on event resources.	GET
/redfish/v1/EventService/Subscriptions	Name	Name of the event subscription resource collection.	GET
	Members@odata.count	Number of event subscription resource members.	GET
	Members	Event subscription resource list.	GET
	-	Creates event subscription.	POST

URL	Property	Description	Operation
/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
	HttpHeaders	HTTP Headers, for example, GET Object is empty for an authentication message.	GET
	Protocol	Protocol connected to the event.	GET

	Context	String provided by the client and stored together with the event target subscription.	GET
	MessageIds	Submitted message ID list.	GET
	OriginResources	Submits the event-related resource list.	GET
	-	Modifies the event subscription resource.	PATCH
	-	Deletes the event subscription resource.	DELETE

8.1 Querying Information About the EventService Resource

Function

Query the information about 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 8-2](#).

Table 8-2 Parameter Descriptions for Querying the Event Service Resource

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None • Response Example:

```
{  "@odata.context": "/redfish/v1/$metadata#EventService.EventService",
  "@odata.etag": "\"1268462761\"",
  "@odata.id": "/redfish/v1/EventService",
  "@odata.type": "#EventService.v1_5_0.EventService",
  "Actions": {
    "#EventService.SubmitTestEvent": {
      "EventType@Redfish.AllowableValues": [
        "StatusChange",
        "ResourceUpdated",
        "ResourceAdded",
        "ResourceRemoved",
        "Alert"
      ],
      "target":
        "/redfish/v1/EventService/Actions/EventService.SubmitTestEvent"
    }
  },
  "DeliveryRetryAttempts": 3,
  "DeliveryRetryIntervalSeconds": 60,
```

```

    "Description": "Event Service",
    "EventTypesForSubscription": [
        "StatusChange",
        "ResourceUpdated",
        "ResourceAdded",
        "ResourceRemoved",
        "Alert"
    ],
    "Id": "EventService",
    "Name": "Event Service",
    "ServiceEnabled": true,
    "Status": {
    "State": "Enabled"
    },
    "Subscriptions": {
        "@odata.id":
"/redfish/v1/EventService/Subscriptions"
    }
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the event service resource, refer to [Table 8-3](#).

Table 8-3 Output Descriptions for Querying the Event Service Resource

Field	Type	Description
@odata.context	String	OData description of the EventService resource model.
@odata.id	String	Access path of the EventService resource node.
@odata.type	String	Type of EventService resource.
Id	String	ID of the EventService resource.
Name	String	Name of the EventService resource.
Status	Object	Status of the specified EventService resources, including: ● Status: enabling status ● Health: health status
ServiceEnabled	Boolean	Whether event reporting is enabled.

DeliveryRetryAttempts	Number	Maximum number of retries for delivering event subscriptions.
-----------------------	--------	---

Field	Type	Description
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.

8.2 Querying Information About the Event Subscription Resource Collection

Function

Query the information about the event subscription resource collection.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/EventService/Subscriptions`
 - Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For the parameter descriptions for querying the event subscription resource collection, refer to [Table 8-4](#).

Table 8-4 Parameter Descriptions for Querying the Event Subscription Resource Collection

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/EventService/Subscriptions
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#EventDestinationCollection.EventDestinationCollection",
  "@odata.etag": "\"1267581807\"",
  "@odata.id": "/redfish/v1/EventService/Subscriptions",
  "@odata.type": "#EventDestinationCollection.EventDestinationCollection",
  "Members": [
    {
      "@odata.id":
"/redfish/v1/EventService/Subscriptions/1"
    }
  ],
  "Members@odata.count": 1,
  "Name":
"Event Subscriptions Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the event subscription resource collection, refer to [Table 8-5](#).

Table 8-5 Output Descriptions for Querying the Event Subscription Resource Collection

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

8.3 Creating an Event Subscription Resource

Function

Create an event subscription resource.

Syntax

- Operation Type: POST
- URL: `https://device_ip/redfish/v1/EventService/Subscriptions`
 - Request Header:

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

- Request Message Body:


```
{
  "Destination": event_destination,
  "EventTypes": event_types,
  "HttpHeaders": http_headers,
  "Context": context,
  "Protocol": protocol,
  "MessageIds": message_ids,
  "OriginResources": origin_resources
}
```

Parameters

For the parameter descriptions for creating an event subscription resource, refer to [Table 8-6](#).

Table 8-6 Parameter Descriptions for Creating the Event Subscription Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
header_type	Format of the request message.	application/json
auth_value	X-Auth-Token value contained in Request Header in the POST request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
event_destination	Event subscription destination address.	Valid HTTPS destination address.
event_types	Event type for event subscription monitoring.	A combination of the following values: ● StatusChange: resource status change event ● ResourceUpdated: resource update event ● ResourceAdded: resource addition event ● ResourceRemoved: resource removal event ● Alert: alarming event
http_headers	Event subscription HTTP header parameters, which are carried when an event is reported.	Optional parameter. The value shall comply with the key:value format, and is displayed as null when being queried.
context	Event subscription context information.	String
protocol	Protocol used by the event subscription.	It must be Redfish.

message_ids	Message ID matching list of the event subscription.	Optional parameter. Combination of valid message IDs defined in the event registry.
origin_resources	Event source list.	Combination of valid resource URIs .

Usage Guidelines

The specified event destination address used for creating a subscription cannot be the same as any existing subscription destination address.

Example

- Request Example:

POST https://device_ip/redfish/v1/EventService/Subscriptions

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234 Content-Type: application/json

- Request Message Body:

```
{
  "Destination":
  "https://10.228.34.200/redfish/test/",
  "EventTypes": [ "Alert" ],
  "HttpHeaders": {
    "Content-Type":
    "Application/JSON",
    "OData-Version": "4.0",
    "X-Auth-Token": "5ac44e4c36db20ee69f661f42239b6f5" },
  "Context": "event subscription context string",
  "Protocol": "Redfish",
  "MessageIds": [ "iBMCEvents.2.0.PsPredicFailureInfo" ],
  "OriginResources": [ {
    "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/0" } ]
}
```

- Response Example:

```

{
  "@odata.context":
"/redfish/v1/$metadata#EventDestination.EventDestination",
  "@odata.etag": "W/\"1267581807\"",
  "@odata.id": "/redfish/v1/EventService/Subscriptions",
"@odata.type": "#EventDestination.v1_7_0.EventDestination",
  "Context": "event subscription context string",
"Destination": "https://10.228.34.200/redfish/test/",
  "EventTypes": [
    "Alert"
  ],
  "Id": 1,
  "MessageIds": [
    "iBMCEvents.2.0.PsPredicFailureInfo"
  ],
  "Name": "Subscription 1",
  "OriginResources": [
    "/redfish/v1/Chassis/1/Power#/PowerSupplies/0"
  ],
  "OriginResources@odata.count":
1,
  "Protocol": "Redfish",
  "HttpHeaders": null
}

```

- Status Code: 201

Output Description

For a description of the output returned when you create the event subscription resource, refer to [Table 8-7](#).

Table 8-7 Output Descriptions for Creating the Event Subscription Resource

Field	Type	Description
@odata.context	String	OData description of the event subscription resource model.
@odata.id	String	Access path of the event subscription resource node.
@odata.type	String	Type of event subscription resource.
Id	String	ID of the event subscription resource.
Name	String	Name of the event subscription resource.
Destination	Event subscription destination address.	Valid HTTPS destination address.

EventTypes	Event type for event subscription monitoring.	A combination of the following values: ● StatusChange: resource status change event ● ResourceUpdated: resource update event ● ResourceAdded: resource addition event ● ResourceRemoved: resource removal event ● Alert: alarming event
context	Event subscription context information.	String
protocol	Protocol used by the event subscription.	It must be Redfish.
MessageIds	Message ID matching list of the event subscription.	Optional parameter. Combination of valid message IDs defined in the event registry.
OriginResources	Event source list.	Combination of valid resource URIs
OriginResources@odata.count	Number	Number of event sources.
HttpHeaders	Event subscription HTTP header.	It is displayed as "null" when being queried.

8.4 Querying Information About an Event Subscription Resource

Function

Query the information about 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

Parameters

For the parameter descriptions for querying an event subscription resource, refer to [Table 8-8](#).

Table 8-8 Parameter Descriptions for Querying the Event Subscription Resource

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

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": "\"1267581807\"",
}
```

```

    "@odata.id": "/redfish/v1/EventService/Subscriptions/1",
"@odata.type": "#EventDestination.v1_7_0.EventDestination",
    "Context": "event subscription context string",
"Destination": "https://10.228.34.200/redfish/test/",
    "EventTypes": [
        "Alert"
    ],
    "Id": "1",
    "MessageIds": [
        "iBMCEvents.2.0.PsPredicFailureInfo"
    ],
    "Name": "Subscription 1",
"OriginResources": [
    {
        "@odata.id":
"/redfish/v1/Chassis/1/Power#/PowerSupplies/0"
    }
],
"OriginResources@odata.count":
1,
    "Protocol": "Redfish",
"SubscriptionType": "RedfishEvent",
"HttpHeaders": null
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query the event subscription resource, refer to [Table 8-9](#).

Table 8-9 Output Descriptions for Querying the Event Subscription Resource

Field	Type	Description
@odata.context	String	OData description of the event subscription resource model.
@odata.id	String	Access path of the event subscription resource node.
@odata.type	String	Type of event subscription resource.
Id	String	ID of the specified event subscription resource.
Name	String	Name of the event subscription resource.
Destination	String	Valid HTTP/HTTPS destination address.

EventTypes	String	Types of events to which a client can subscribe. ● StatusChange: resource status change event ● ResourceUpdated: resource update event
Field	Type	Description
		● ResourceAdded: resource addition event ● ResourceRemoved: resource removal event ● Alert: alarming event
Context	String	Event subscription context information.
Protocol	String	Protocol used for event subscription.
MessageIds	Array	Message ID matching list of the event subscription.
OriginResources	Array	Event source list.
OriginResources@odata.count	Number	Number of event sources.
HttpHeaders	Object	Event subscription HTTP header, which is displayed as "null" when being queried.

8.5 Modifying Information About 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
}
```

Parameters

For the parameter descriptions for modifying an event subscription resource, refer to [Table 8-10](#)

Table 8-10 Parameter Descriptions for Modifying the Event Subscription Resource

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

Parameter	Description	Value
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 <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
http_headers	Event subscription HTTP header parameters, which are carried when an event is reported.	The value shall comply with the <i>key:value</i> 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

- Request Message Body:

```
{
  "HttpHeaders":
    {
      "Content-Type":
        "Application/JSON",
      "OData-Version": "4.0",
      "X-Auth-Token":
        "5ac44e4c36db20ee69f661f42239b6f5"
    },
    "Context": "event subscription
context string"
}
```

- Response Example:

<pre>{ "@odata.context": "/redfish/v1/\$metadata#EventDestination.EventDestination", "@odata.etag": "\"1268164049\"", "@odata.id": "/redfish/v1/EventService/Subscriptions/2", "@odata.type": "#EventDestination.v1_7_0.EventDestination", "Context": "Event_2", </pre>
<pre> "Destination": "https://10.228.34.158:9002/redfish/test/", "EventTypes": ["Alert"], "Id": "2", "MessageIds": ["iBMCEvents.2.0.PsPredicFailureInfo"], "Name": "Subscription 2", "OriginResources": [{ "@odata.id": "/redfish/v1/Chassis/1/Power#/PowerSupplies/4" }], "OriginResources@odata.count": 1, "Protocol": "Redfish", "SubscriptionType": "RedfishEvent", "HttpHeaders": null }</pre>

- Status Code: 200

Output Description

For a description of the output returned when you modify an event subscription resource, refer to [Table 8-11](#).

Table 8-11 Output Descriptions for Modifying the Event Subscription Resource

Field	Type	Description
@odata.context	String	OData description of the event subscription resource model.
@odata.id	String	Access path of the event subscription resource node.
@odata.type	String	Type of event subscription resource.
Id	String	ID of the specified event subscription resource.
Name	String	Name of the event subscription resource.

Destination	String	Valid HTTP/HTTPS destination address.
EventTypes	Array	Types of events to which a client can subscribe. ● StatusChange: resource status change event ● ResourceUpdated: resource update event ● ResourceAdded: resource addition event ● ResourceRemoved: resource removal event ● Alert: alarming event

Field	Type	Description
Context	String	Event subscription context information.
Protocol	String	Protocol used for event subscription, It must be Redfish in this version.
MessageIds	Array	(Optional) Message ID matching list of the event subscription. Combination of valid message IDs defined in the event registry.
OriginResources	Array	Mapping between event subscriptions and event sources.
OriginResources@odata.count	Number	Number of event sources.
HttpHeaders	Object	Event subscription HTTP header, which is displayed as "null" when being queried.

8.6 Deleting an Event Subscription Resource

Function

Delete an event subscription resource.

Syntax

- Operation Type: DELETE
- URL: `https://device_ip/redfish/v1/EventService/Subscriptions/id`
 - Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for deleting an event subscription resource, refer to [Table 8-12](#).

Table 8-12 Parameter Descriptions for Deleting the Event Subscription Resource

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

Usage Guidelines

None

Example

- Request Example:

DELETE https://device_ip/redfish/v1/EventService/Subscriptions/1

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

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

Output Description

None

8.7 Reporting an Event

Function

Report an event.

Syntax

- Operation Type: POST
- URL: `https://event_destination`

Parameters

For the parameter descriptions for reporting an event, refer to [Table 8-13](#).

Table 8-13 Parameter Descriptions for Reporting an Event Parameters

Field	Type	Description
@odata.context	String	OData description of the root service resource model.
@odata.id	String	Access path of the root service resource node.
@odata.type	String	Type of root service resource.
Id	String	ID of the root service resource. Set it to alert_id.
Name	String	Root service resource name, which is fixed to Event Array.
Events	Object	Set of events.

Field	Type	Description
EventType	String	Event type. Options: ● StatusChange: resource status change event ● ResourceUpdated: resource update event ● ResourceAdded: resource addition event ● ResourceRemoved: resource removal event ● Alert: alarm event
EventId	String	ID of this alarm event, that is, the serial number of the alarm event. The ID is incremented when a new alarm caused by the same fault is raised. The ID of the active alarm is the same as that of the cleared alarm.
EventTimestamp	String	Event occurrence time. ● Active alarm: alarm occurrence time. ● Cleared alarm: time when the alarm is cleared.

Severity	String	Alarm severity level. ● 1: Critical ● 2: Major ● 3: Minor ● 4: Warning. The OrigSeverity value of an active alarm is the same as that of the corresponding cleared alarm. This field does not need to be specified for notifications of event type, and needs to be set to Inform for notifications of internal alarm type.
Message	Object	Manufacturer-customized alarm event or title.
Oem	Object	Customized properties.
alarmStatus	String	Alarm status. ● 1: active. ● 0: cleared.
specificProblemID	String	Alarm classification description.
neUID	String	Alarm server ID, which is set to the SerialNumber value of the server.
neName	String	Alarm server name, which is set to the asset number of the server.
neType	String	Type of alarm device, which is set to server.
objectUID	String	Alarm object ID, which is defined by the manufacturer.

Field	Type	Description
objectName	String	Alarm object name, which is defined by the manufacturer.

objectType	String	Alarm object type, which corresponds to the manufacturer-customized tAlarmPublic.DeviceType. • {ALARM_DEVICE_TYPE_MAINBOARD, "Main-Board"} • {ALARM_DEVICE_TYPE_PSU, "PSU"} • {ALARM_DEVICE_TYPE_FAN, "Fan"} • {ALARM_DEVICE_TYPE_CPU, "CPU"} • {ALARM_DEVICE_TYPE_DISK, "Disk"} • {ALARM_DEVICE_TYPE_MEMORY, "Memory"} • {ALARM_DEVICE_TYPE_IOMODULE, "IOMoudle"} • {ALARM_DEVICE_TYPE_GPU, "GPU"} • {ALARM_DEVICE_TYPE_NIC_CARD, "NIC_Card"}
locationInfo	String	Alarm positioning information, which is defined by the manufacturer.
Addinfo	String	Detailed information about the alarm, including multiple Key-Value pairs, which are defined by the manufacturer. A key and its value are separated by a colon. Multiple Key-Value pairs are separated by semicolons. Keys and values cannot include colons or semicolons.
Name	String	Name of the alarm event, format: Log entry

8.8 Querying Information About the Event Resource Collection

Function

Query the information about the event 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 a description of the parameters for querying the event resource collection, refer to [Table 8-14](#).

Table 8-14 Parameter Descriptions for Querying the Event Resource Collection

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
skip_value	Integer that indicates the number of members in the resource collection to be skipped before the first resource is retrieved.	0 and positive integers
top_value	Integer that indicates the maximum number of members to be included in the response.	0-100

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/EventService/Alarms?$skip=10&$top=3
```

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#AlarmsCollection.AlarmsCollection",
  "@odata.id": "/redfish/v1/EventService/Alarms",
  "@odata.type": "#AlarmsCollection.v1_0_0.AlarmsCollection",
  "Description": "Collection of Alarms",
  "Id": "Alarms",
  "Members": [
    {
      "AlarmCode": "0x1a000016",
      "AlarmLevel": "Major",

```

```

      "Message": "Disk22 is missing(SN:unknown).",
    "TimeStamp": "2010-05-23 02:56:09"
  },
  {
    "AlarmCode": "0x1a000016",
    "AlarmLevel": "Major",
    "Message": "Disk20 is missing(SN:unknown).",
    "TimeStamp": "2010-05-23 02:56:09"
  },
  {
    "AlarmCode": "0x1a000016",
    "AlarmLevel": "Major",
    "Message": "Disk18 is missing(SN:unknown).",
    "TimeStamp": "2010-05-23 02:56:09"
  }
],
"Members@odata.count": 131,
"Name": "Alarms Collection"
}

```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the event resource collection, refer to [Table 8-15](#).

Table 8-15 Output Descriptions for Querying the Event Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the event resource collection.
@odata.id	Character string	Access path of the event resource collection.
@odata.type	Character string	Type of event resource collection.
Description	Character string	Description of the event resource collection.
Id	Character string	Operations that can be performed on the event resource collection.
Name	Character string	Name of the event resource collection.
Members@odata.count	Number	Number of event resources.
Members	Array	Event resource list.

AlarmCode	Character string	Event Code
AlarmLevel	Character string	Event level.
Field	Type	Description
TimeStamp	Character string	Event generation time.
Message	Character string	Event information.

8.9 Deleting All Event Resources

Function

Delete all event resources.

Syntax

- Operation Type: DELETE
- URL: `https://device_ip/redfish/v1/EventService/DeleteAlarmsAll`
 - Request Header:

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

- Request Message Body: None

Parameters

For a description of the parameters for deleting all event resources, refer to [Table 8-16](#).

Table 8-16 Parameter Descriptions for Deleting All Event Resources

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

Usage Guidelines

None

Example

- Request Example:

```
DELETE https://device_ip/redfish/v1/EventService/DeleteAlarmsAll
```

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

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

Output Description

None

8.10 Querying Information About the Current Alarm Resource Collection

Function

Query the information about 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 8-17](#).

Table 8-17 Parameter Descriptions for Querying the Current Alarm Resource Collection

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

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/EventService/CurrentAlarms

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#CurrentAlarmsCollection.CurrentAlarmsCollection",
  "@odata.id": "/redfish/v1/EventService/CurrentAlarms",
  "@odata.type": "#CurrentAlarmsCollection.v1_0_0.CurrentAlarmsCollection",
  "Description": "Collection of CurrentAlarms",      "Id": "CurrentAlarms",
  "Actions": {
    "Oem": {
      "#EventService.DeleteCurrentAlarmsAll": {
"target": "/redfish/v1/EventService/DeleteCurrentAlarmsAll"
      }
    }
  },
  "Members": [
    {
      "@odata.id":
"/redfish/v1/EventService/CurrentAlarms/94",
      "AlarmCode": "0x03010109",
      "AlarmId": 94,
      "AlarmLevel": "Major",
      "Message": "CPU1_Temp CPU Temperature (86.000 degrees C)
Upper Critical - Going High (86.000 degrees C) assert.",
      "TimeStamp": "2010-05-23 03:01:07"
    },
    {
      "@odata.id":
"/redfish/v1/EventService/CurrentAlarms/92",
      "AlarmCode": "0x1a000016",
      "AlarmId": 92,
      "AlarmLevel": "Major",
      "Message": "Disk22 is missing(SN:unknown).",
      "TimeStamp": "2010-05-23 02:56:09"
    },
    {
      "@odata.id":
"/redfish/v1/EventService/CurrentAlarms/91",
      "AlarmCode": "0x1a000016",
      "AlarmId": 91,
      "AlarmLevel": "Major",
      "Message": "Disk20 is missing(SN:unknown).",
      "TimeStamp": "2010-05-23 02:56:09"
    },
  ],
}
```

```

    {
        "@odata.id":
"/redfish/v1/EventService/CurrentAlarms/90",
"AlarmCode": "0x1a000016",
        "AlarmId": 90,
        "AlarmLevel": "Major",
"Message": "Disk18 is missing(SN:unknown).",
"TimeStamp": "2010-05-23 02:56:09"
    },
    {
        "@odata.id":
"/redfish/v1/EventService/CurrentAlarms/89",
"AlarmCode": "0x1a000016",
        "AlarmId": 89,
        "AlarmLevel": "Major",
"Message": "Disk16 is missing(SN:unknown).",
"TimeStamp": "2010-05-23 02:56:09"
    },
    {
        "@odata.id":
"/redfish/v1/EventService/CurrentAlarms/88",
"AlarmCode": "0x0a000012",
        "AlarmId": 88,
        "AlarmLevel": "Minor",
        "Message": "PSU4 Input
Undervoltage Warning (SN:22M010020399).",
        "TimeStamp": "2010-
05-23 02:45:43"
    },
    {
        "@odata.id":
"/redfish/v1/EventService/CurrentAlarms/87",
"AlarmCode": "0x0a000011",
        "AlarmId": 87,
        "AlarmLevel": "Major",
        "Message": "PSU4 Input
Undervoltage Fault (SN:22M010020399).",
        "TimeStamp": "2010-
05-23 02:45:43"
    },
    {
        "@odata.id":
"/redfish/v1/EventService/CurrentAlarms/86",
"AlarmCode": "0x0a000015",
        "AlarmId": 86,
        "AlarmLevel": "Major",
        "Message": "PSU4 Output
Undervoltage Fault (SN:22M010020399).",
        "TimeStamp": "2010-
05-23 02:45:43"
    },
    {
        "@odata.id":
"/redfish/v1/EventService/CurrentAlarms/85",
"AlarmCode": "0x0a6f0803",
        "AlarmId": 85,

```

```
      "AlarmLevel": "Major",      "Message":
"PSU4_Status POWER SUPPLY Power Supply input lost (AC/DC) assert.",
"TimeStamp": "2010-05-23 02:45:42"
    },
    {
      "@odata.id":
"/redfish/v1/EventService/CurrentAlarms/84",
"AlarmCode": "0x0a6f0802",
      "AlarmId": 84,
      "AlarmLevel": "Minor",      "Message": "PSU4_Status
POWER SUPPLY Predictive Failure assert.",      "TimeStamp": "2010-
05-23 02:45:42"
    },
    {
      "@odata.id":
"/redfish/v1/EventService/CurrentAlarms/83",
"AlarmCode": "0x0a6f0801",
      "AlarmId": 83,
      "AlarmLevel": "Critical",      "Message": "PSU4_Status POWER
SUPPLY Power Supply Failure detected assert.",      "TimeStamp": "2010-05-23
02:45:42"
    },
    {
      "@odata.id":
"/redfish/v1/EventService/CurrentAlarms/82",
"AlarmCode": "0xa0010209",
      "AlarmId": 82,
      "AlarmLevel": "Major",      "Message": "SYS_5V RESERVED
Voltage (5.084 Volts) Upper Critical -
      Going High (2.542 Volts) assert.",
"TimeStamp": "2010-05-23 02:44:31"
    }
  ],
  "Members@odata.count": 12,
  "Name": "CurrentAlarms Collection"
}
```

- Status Code: 200

Output Description

a description of the output returned when you query the current alarm resource collection, refer to [Table 8-18](#).

Table 8-18 Output Descriptions for Querying the Current Alarm Resource Collection

Field	Type	Description
-------	------	-------------

@odata.context	Character string	OData description of the current alarm resource collection model.
@odata.id	Character string	Access path of the current alarm resource collection.
@odata.type	Character string	Type of alarm resource collection.
Description	Character string	Description of the current alarm resource collection.
Actions	Object	Operations that can be performed on the current alarm resource collection.
Oem	Object	Customized properties.
EventService.DeleteCurrentAlarmsAll	Object	Deletes all current alarms.
target	Character string	Operation path.
Name	Character string	Name of the current alarm resource collection.
Members@odata.count	Digit	Number of alarm resource members.
Members	Array	Event subscription resource list.
@odata.id	Character string	Access path of the specified alarm resource.
AlarmId	Character string	ID of the current alarm.
AlarmCode	Digit	Code of the current alarm.
AlarmLevel	Character string	Level of the current alarm.
TimeStamp	Digit	Alarm generation timestamp.
Message	Character string	Information about the current alarm.

8.11 Querying Information About the Current Alarm Resource

Function

Query the information about 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 8-19](#).

Table 8-19 Parameter Descriptions for Querying the Current Alarm Resource

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

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/EventService/CurrentAlarms/2152

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:


```
{
  "@odata.context": "/redfish/v1/$metadata#CurrentAlarm.CurrentAlarm",
  "@odata.id": "/redfish/v1/EventService/CurrentAlarms/2152",
  "@odata.type": "#CurrentAlarm.v1_0_0.CurrentAlarm",
  "AlarmCode": 30839,
  "AlarmLevel": "Major",
  "Description": "Current Alarm",
  "Id": "2152",      "Message": "Abnormal reading of ambient temperature
(location:INPUT_TEMP).",
  "Name": "CurrentAlarm",
  "TimeStamp": 1607004276
}
```

- Status Code: 200

Output Description

a description of the output returned when you query the current alarm resource, refer to [Table 8-20](#).

Table 8-20 Output Descriptions for Querying the Current Alarm Resource

Field	Type	Description
@odata.context	Character string	OData description of the current alarm resource model.
@odata.id	Character string	Access path of the current alarm resource.
@odata.type	Character string	Type of alarm resource.
Id	Character string	ID of the current alarm resource.
Name	Character string	Name of the current alarm resource.
Description	Character string	Description of the current alarm resource.
AlarmCode	Digit	Code of the current alarm.
AlarmLevel	Character string	Level of the current alarm.
TimeStamp	Digit	Alarm generation timestamp.
Message	Character string	Information about the current alarm.

8.12 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 8-21](#).

Table 8-21 Parameter Descriptions for Deleting an Active Alarm Resource

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
alarm_id	ID of the current alarms	-
auth_value	When the DELETE request is executed, the "X-AuthToken" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- Request Example:

DELETE https://device_ip/redfish/v1/EventService/CurrentAlarms/2152

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

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

Output Description

None

8.13 Deleting All Current Alarm Resource

Function

Delete all current alarm resources.

Syntax

- Operation Type: DELETE
- URL: `https://device_ip/redfish/v1/EventService/DeleteCurrentAlarmsAll`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For the parameter descriptions for deleting all current alarm resources, refer to [Table 8-22](#).

Table 8-22 Parameter Descriptions for Deleting All Current Alarm Resources

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

Usage Guidelines

None

Example

- Request Example:

DELETE https://device_ip/redfish/v1/EventService/DeleteCurrentAlarmsAll

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

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

Output Description

None

8.14 Querying Information About the Current Alarm Event Resource Collection

Function

Query the information about 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 8-23](#).

Table 8-23 Parameter Descriptions for Querying the Current Alarm Event Resource Collection

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

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/EventService/CurrentAlertEvents
- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234
- Request Message Body: None • Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#CurrentAlertsCollection.CurrentAlertEventsCollection",
"@odata.id": "/redfish/v1/EventService/CurrentAlertEvents",    "@odata.type":
"#CurrentAlertEventsCollection.v1_0_0.CurrentAlertEventsCollection",
"Description": "Collection of CurrentAlertEvents",    "Id":
"CurrentAlertEvents",    "Members":
  [{
    "EventId": "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

a description of the output returned when you query the current alarm event resource collection, refer to [Table 8-24](#).

Table 8-24 Output Descriptions for Querying the Current Alarm Event Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the current alarm event resource collection model.
@odata.id	Character string	Access path of the current alarm event resource collection.
@odata.type	Character string	Type of alarm event resource collection.
Description	Character string	Description of the current alarm event resource collection.
Id	Character string	ID of the current alarm event resource collection.

Name	Character string	Name of the current alarm event resource collection.
Members@odata.count	Digit	Number of alarm event resource members.

Field	Type	Description
Members	Array	Event subscription resource list
EventId	Digit	Alarm event ID.
EventType	Character string	Alarm type.
EventTimestamp	Character string	Event occurrence time.
Severity	Character string	Alarm level.
Message	Character string	Alarm name.
Oem.Public	Object	-
alarmStatus	Digit	Alarm status.
specificProblemID	Character string	Alarm classification ID (alarm code).
specificProblem	Character string	Alarm classification description (alarm name).
neUID	Character string	Alarm server ID (serial number of the server).
neName	Character string	Alarm server name (asset number of the server).
neType	Character string	Type of the device where the alarm is raised.
objectUID	Digit	ID of the alarm part.
objectName	Character string	Name of the alarm part.
objectType	Character string	Type of alarm part.
locationInfo	Character string	Alarm positioning information.

Addinfo	Character string	Additional alarm information.
---------	------------------	-------------------------------

8.15 Modifying Event Service Resource Information

Function

Modify event service resource information.

Syntax

- Operation Type: PATCH
- URL: `https://device_ip/redfish/v1/EventService` • Request Header:

`x-auth-token:auth_value`

`Content-Type:header_type`

- Request Message Body:

```
{
  "DeliveryRetryAttempts" : retry_attempts,
  "DeliveryRetryIntervalSeconds" : retry_seconds
}
```

Parameters

For a description of the parameters for modifying event service resource information, refer to [Table 8-25](#).

Table 8-25 Parameter Descriptions for Modifying Event Service Resource Information

Parameter	Description	Value
retry_attempts	Maximum number of event subscription retries upon a failure.	Number, range: 3–1440.
retry_seconds	Interval (in seconds) at which an event is resent upon a failure.	Number, range: 60–3600.

Usage Guidelines

None

Example

- Request Example:

`PATCH https://device_ip/redfish/v1/EventService`

- Request Header:

`X-Auth-Token: 8574621d21b84756218c7456821c234`

- Request Message Body:

```
{
  "DeliveryRetryAttempts" : 40,
  "DeliveryRetryIntervalSeconds" : 60
}
```

- Response Example: None
- Response Code: 204

Output Description

None

Chapter 9

Operations on UpdateService Resources

Table of Contents

Querying Information About an UpdateService Resource.....344

Querying Information About an Updateable Firmware Resource Collection.....346

Querying Information About a Specified Updateable Firmware Resource.....348

Updating Firmware.....351

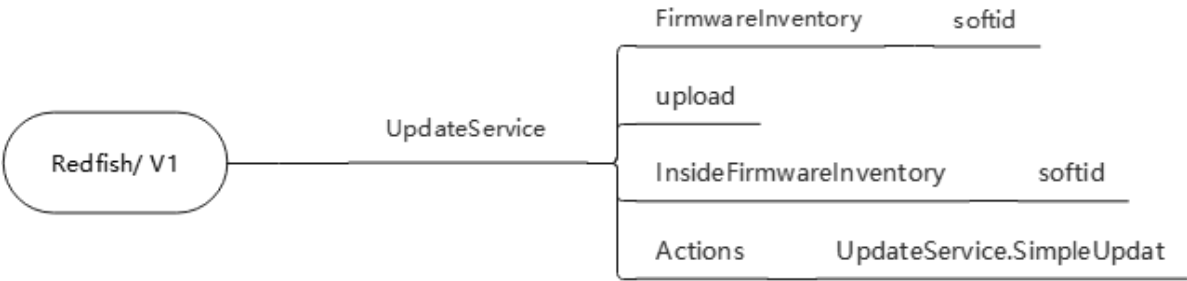
Querying Information About the Internal Firmware Resource Collection.....354

Querying Information About a Specified Internal Firmware Resource.....356

Updating Firmware Remotely.....358

Figure 9-1 shows the path requirements for the UpdateService resources supported by **NETAŞ** servers.

Figure 9-1 UpdateService Resource Path Requirements



For a description of the properties of UpdateService resources and the operations supported by the properties, refer to [Table 9-1](#).

Table 9-1 Descriptions of UpdateService Resources Properties

URL	Property	Description	Operation
/redfish/v1/UpdateService	Id	ID of an UpdateService resource.	GET
	Name	Name of the UpdateService resource.	GET

URL	Property	Description	Operation
-----	----------	-------------	-----------

	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
	FirmwareInventory	Access path of the firmware information resource node.	GET
	Oem	Customized information about the specified firmware.	GET
/redfish/v1/UpdateService/FirmwareInventory	Name	Name of the updateable firmware resource collection.	GET
	Members@odata.count	Number of updateable firmware resources.	GET
	Members	List of updateable firmware resources.	GET
	Description	Description of the updateable firmware resource collection.	GET
/redfish/v1/UpdateService/FirmwareInventory/softid	Id	ID of the specified updateable firmware resource.	GET
	Name	Name of the specified updateable firmware resource.	GET

		Status	Status of the specified updateable firmware resource.	GET
		Version	Version of the specified updateable firmware resource.	GET
	URL	Property	Description	Operation
		Updateable	Update status of the specified updateable firmware resource.	GET
		SoftwareId	Firmware ID.	GET

9.1 Querying Information About an UpdateService Resource

Function

Query information about an 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 the UpdateService resource, refer to [Table 9-2](#).

Table 9-2 Parameter Descriptions for Querying Information About the UpdateService Resource

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

Usage Guidelines

None

Example

- Request Example:

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

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#UpdateService.UpdateService",
  "@odata.etag": "\"946668445\"",
  "@odata.id": "/redfish/v1/UpdateService",
  "@odata.type": "#UpdateService.v1_6_0.UpdateService",
  "Actions": {
    "#UpdateService.SimpleUpdate": {
      "@Redfish.ActionInfo":
"/redfish/v1/UpdateService/SimpleUpdateActionInfo",
      "target":
"/redfish/v1/UpdateService/Actions/SimpleUpdate"
    }
  },
  "Description": "Redfish Update
Service",
  "FirmwareInventory": {
    "@odata.id":
"/redfish/v1/UpdateService/FirmwareInventory"
  },
  "Id": "UpdateService",
  "Name": "Update Service",
  "ServiceEnabled": true,
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  }
}
```

- Response Code: 200

Output Description

For a description of the output returned when you query information about the UpdateService resource, refer to [Table 9-3](#).

Table 9-3 Output Descriptions for Querying Information About the UpdateService Resource

Field	Type	Description
@odata.context	String	OData description of a specified UpdateService resource model.

@odata.id	String	Access path of the specified UpdateService resource.
@odata.type	String	Type of the specified UpdateService resource.
Id	String	ID of the specified UpdateService resource.
Name	String	Name of the specified UpdateService resource.

Field	Type	Description
Status	Object	Status and health of the specified UpdateService resource. - State: status of the specified UpdateService resource. - Health: health of the specified UpdateService resource.
ServiceEnabled	Boolean	Whether the UpdateService is enabled.
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 updateable firmware resource list.
@odata.id	String	Access path of the updateable firmware resource list.

9.2 Querying Information About an Updateable Firmware Resource Collection

Function

Query information about an updateable firmware resource collection of a server.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/UpdateService/FirmwareInventory`
 - Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the updateable firmware resource collection, refer to [Table 9-4](#).

Table 9-4 Parameter Descriptions for Querying Information About the Updateable Firmware Resource Collection

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

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/UpdateService/FirmwareInventory

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None
- Response Example:


```
{
  "@odata.context":
"/redfish/v1/$metadata#SoftwareInventoryCollection.SoftwareInventoryCollection",
  "@odata.etag": "\"946656063\"",
  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory",
  "@odata.type": "#SoftwareInventoryCollection.SoftwareInventoryCollection",
  "Description": "Collection of Firmware Inventory resources available to the
UpdateService",
  "Members": [
    {
      "@odata.id":
"/redfish/v1/UpdateService/FirmwareInventory/ActiveBMC"
    },
    {
      "@odata.id":
"/redfish/v1/UpdateService/FirmwareInventory/ActiveBIOS"
    },
    {
      "@odata.id":
"/redfish/v1/UpdateService/FirmwareInventory/EPLD"
    },
    {
      "@odata.id":
"/redfish/v1/UpdateService/FirmwareInventory/MainBoardFRU"
    },
    {
      "@odata.id":
"/redfish/v1/UpdateService/FirmwareInventory/SubCardFRU2"
    }
  ],
  "Members@odata.count": 5,
  "Name": "Firmware Inventory Collection"
}
```

- Response Code: 200

Output Description

For a description of the output returned when you query information about the updateable firmware resource collection, refer to [Table 9-5](#).

Table 9-5 Output Descriptions for Querying Information About the Updateable Firmware Resource Collection

Field	Type	Description
@odata.context	String	OData description of the updateable firmware resource collection model.

@odata.id	String	Access path of the updateable firmware resource collection model.
@odata.type	String	Type of updateable firmware resource collection model.
Description	String	Description of the updateable firmware resource collection.
Name	String	Name of the updateable firmware resource collection.
Members@odata.count	Number	Number of updateable firmware resources.
Members	Session list.	-
@odata.id	String	Access path of an updateable firmware resource.

9.3 Querying Information About a Specified Updateable Firmware Resource

Function

Query information about a specified updateable firmware resource of a server.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/UpdateService/FirmwareInventory/softid`
- Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying information about a specified updateable firmware resource of a server, refer to [Table 9-6](#).

Table 9-6 Parameter Descriptions for Querying Information About a Specified Updateable Firmware Resource

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

auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
softid	ID of the updateable firmware resource.	It can be obtained from the updateable firmware resource collection.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/UpdateService/FirmwareInventory/ActiveBMC
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#SoftwareInventory.SoftwareInventory",
  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/ActiveBMC",
  "@odata.type": "#SoftwareInventory.v1_2_3.SoftwareInventory",
  "Description": "ActiveBMC",
  "Id": "ActiveBMC",
  "Name": "ActiveBMC",
  "SoftwareId": "ActiveBMC",
  "Status": {
    "Health": "OK",
  },
  "State": "Enabled",
  "Updateable": true,
  "Version": "04.22.01.93"
}
```

- Response Code: 200

Output Description

For a description of the output returned when you query information about a specified updateable firmware resource of a server, refer to [Table 9-7](#).

Table 9-7 Output Descriptions for Querying Information About a Specified Updateable Firmware Resource

Field	Type	Description
-------	------	-------------

@odata.context	String	OData description of the updateable firmware resource.
@odata.id	String	Access path of the updateable firmware resource.
@odata.type	String	Type of updateable firmware resource.
Description	String	Description of the updateable firmware resource.
Id	String	ID of the updateable firmware resource.
Name	String	Name of the updateable firmware resource.
SoftwareId	String	Firmware ID.
Status	Object	Status of the specified UpdateService resources, including: ● Status: enabling status ● Health: health status
Version	String	Firmware version.
Updateable	Boolean	Whether the Update Service can update this software ● true ● false
VerAuxiliaryInfo	String	Auxiliary information about the version.

9.4 Updating Firmware

Function

Update the firmware of a server.

Syntax

- Operation Type: POST
- URL:
`https://device_ip/redfish/v1/UpdateService/Actions/UpdateService/upload`
- Request Header:

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

<pre>{ " O e m P a r a m e t e r s " : { "Im age Typ e": "BM C", "Ac tio n": "3" } " U p d a t e P a r a m e</pre>	
--	--

```

t
e
r
s
"
:
{
    "Targets":
    ["/redfish/v1/UpdateService/Firmwar
eInventory/BMC"]
    }
}

```

Parameters

For a description of the parameters for updating server firmware, refer to [Table 9-8](#).

Table 9-8 Parameter Descriptions for Updating Server Firmware

Field	Type	Description
UpdateFile	File	Firmware update file.
OemParameters	File	OEM parameter file in JSON format, including the following content: {"ImageType":"BMC"}
UpdateParameters	File	JSON file for parameters, including the following content: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/BMC"]} The content of UpdateParameters is not verified.
ImageType	String	Options:

Field	Type	Description
		● BMC ● BIOS ● EPLD ● FRU ● BOOT ● EXPANDER The file type is verified but not by file extension.

Action	String	Range: When ImageType is set to BMC: ● 1: Only the BMC BOOT is retained. ● 2: Only the BMC configuration is retained. ● 3: Both BMC BOOT and configuration are retained. ● 4: Neither BMC BOOT nor configuration is retained. Actions supported by the BMC: 1, 2, 3, and 4. When ImageType is set to BIOS: ● 3: NVRAM is retained. ● 4: NVRAM is not retained. Actions supported by the BIOS: 3 and 4. When ImageType is set to others, the Redfish interface does not parse the action setting.
Targets	Array	The active BMC or standby BMC is upgraded separately. They cannot be upgraded at the same time. The active BIOS or standby BIOS cannot be upgraded separately. They must be upgraded at the same time. ● Upgrade the active BMC: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/ActiveBMC"]} Upgrade the standby BMC: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/BackupBMC"]} ● The JSON parameters in the UpdateParameters file for upgrading the standby BIOS are as follows: {"Targets":["/redfish/v1/UpdateService/FirmwareInventory/BIOS"]}. The JSON parameters of the UpdateParameters file for upgrading both the active and standby BIOSs at the same time are as follows: {"Targets": ["/redfish/v1/UpdateService/FirmwareInventory/ActiveBIOS", "/redfish/v1/UpdateService/FirmwareInventory/BackupBIOS"]}

Usage Guidelines

None

Example

- Request Example:

```
POST https://device_ip/redfish/v1/UpdateService/Actions/UpdateService/upload
```

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234 Content-Type: multipart/form-data

- Request Message Body:

```
{
  "Oem": {
    "Parsa": {
      "ImageType": "BM",
      "Action": "3"
    }
  },
  "UpdateParameters": {
    "Targets": [
      "/redfish/v1/UpdateService/FirmwareInventory/BMC"
    ]
  }
}
```

- Response Example:


```
{
  "@odata.type":
"#UpdateService.v1_6_0.UpdateService",
  "Messages": [
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message":
"A new task /redfish/v1/TaskService/Tasks/1 was created.",
      "MessageArgs":
      [
"/redfish/v1/TaskService/Tasks/1"
      ],
      "MessageId": "Task.1.0.New",
      "Resolution": "None",
      "Severity": "OK"
    },
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message": "Device is preparing flash firmware for action
UpdateService.MultipartPush.",
      "MessageArgs":
      [
"UpdateService.MultipartPush"
      ],
      "MessageId":
"UpdateService.1.0.PrepareUpdate",
      "Resolution":
"None",
      "Severity": "OK"
    }
  ]
}
```

- Response Code: 202

Output Description

None

9.5 Querying Information About the Internal Firmware Resource Collection

Function

Query the information about the internal firmware resource collection.

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 the parameters for querying the information about the internal firmware resource collection, refer to [Table 9-9](#).

Table 9-9 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.
Parameter	Description	Value
auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .

Usage Guidelines

None

Example

- **Request Example:**

GET https://device_ip/redfish/v1/UpdateService/InsideFirmwareInventory

- **Request Header:**

X-Auth-Token: 8574621d21b84756218c7456821c234

- **Request Message Body:** None • **Response Example:**

```

{
  "@odata.context":
"/redfish/v1/$metadata#SoftwareInventoryCollection.SoftwareInventoryCollection",
"@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 the information about the internal firmware resource collection, refer to [Table 9-10](#).

Table 9-10 Output Descriptions for Querying Information About the Internal Firmware Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the internal firmware resource collection model.
@odata.id	Character string	Access path of the internal firmware resource collection.
@odata.type	Character string	Type of internal firmware resource collection.
Name	Character string	Name of the internal firmware resource collection.

Members@odata.count	Number	Number of internal firmware resources.
Members	Session List	-
@odata.id	Character string	Access path of an internal firmware resource.

9.6 Querying Information About a Specified Internal Firmware Resource

Function

Query the 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 the information about the specified internal firmware resource, refer to [Table 9-11](#).

Table 9-11 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	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
softid	ID of the specified firmware resource.	It can be obtained through 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.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",
  "Updateable": true
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query the information about the specified internal firmware resource, refer to [Table 9-12](#).

Table 9-12 Output Descriptions for Querying Information About the Specified Internal Firmware Resource

Field	Type	Description
@odata.context	Character string	OData description of the firmware resource model.
@odata.id	Character string	Access path of the firmware resource.
@odata.type	Character string	Firmware resource type.
Description	Character string	Firmware resource description.
Id	Character string	ID of the firmware resource.

Name	Character string	Name of the firmware resource.
SoftwareId	Character string	Firmware ID.
Status	Object	Status of the specified firmware resource. ● Status: enabling status ● Health: health status
InsideVersion	Character string	Internal firmware version.
Updateable	Boolean	Whether the firmware can be updated: ● true ● false

9.7 Updating Firmware Remotely

Function

Update the firmware of a server remotely.

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": imageuri,
  "TransferProtocol": protocol
}
```

Parameters

For a description of the parameters for remotely updating firmware, refer to [Table 9-13](#).

Table 9-13 Parameter Descriptions for Remotely Updating Firmware

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

auth_value	When executing this POST request, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
imageuri	Update package path.	Update package URL.
protocol	Protocol used to download the update package.	HTTPS
Oem	Vendor-defined network service.	-
Public	NETAS-defined service	-
FlashItem	Update package type.	Update package type, options: • BMC • BIOS • EPLD • FRU • BOOT • EXPANDER • VR • PSU
BMCFlash	BMC firmware update position.	BMC firmware update position. • ActiveBMC: The active BMC is updated. • BackupBMC: The standby BMC is updated. • Both: Both the active and standby BMC modules are updated.
BiosFlash	BIOS firmware update position.	BIOS firmware update position: • ActiveBios: The active BIOS is updated.
Parameter	Description	Value
		• BackupBios: The standby BIOS is updated. • Both:Both the active and standby BIOS modules are updated.
PreserveConf	Whether to retain configuration.	Specifies whether to retain the BMC or BIOS configuration when the update package type is set to BMC or BIOS.

Usage Guidelines

None.

Example

- Request Example:

POST https://device_ip/redfish/v1/UpdateService/Actions/UpdateService.SimpleUpdate

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234 Content-Type: application/json

- Request Message Body:

```
{
  "TransferProtocol": "HTTPS",
  "ImageURI":
    "https://10.10.10.10/bmc/
BMC_R5X00G5E_MI05102A_A6_R_V04.23.01.01T1_20230516085914.UBF",
  "Oem": {
    "Public": {
      "FlashItem": "BMC",
      "BMCFlash": "Flash1",
    }
  }
  "PreserveConf": true
}
```

- Response Example:

```
{
  "@odata.type":
    "#UpdateService.v1_6_0.UpdateService",
  "Messages": [
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message": "A new task /redfish/v1/TaskService/Tasks/1 was created.",
    }
  ]
}
```



```
      "MessageArgs": [
"/redfish/v1/TaskService/Tasks/1"
      ],
      "MessageId": "Task.1.0.New",
      "Resolution": "None",
"Severity": "OK"
    },
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message":
"Device is preparing flash firmware for action UpdateService.SimpleUpdate.",
      "MessageArgs": [
"UpdateService.SimpleUpdate"
      ],
      "MessageId":
"UpdateService.1.0.PrepareUpdate",
      "Resolution": "None",
"Severity": "OK"
    }
  ]
}
```

- Response code: 202

Output Description

None

Chapter 10

Operations on AccountService Resources

Table of Contents

Querying User Service Information.....365

Modifying User Service Information.....367

Querying Information About the User Resource Collection.....369

Querying Information About a Specified Account Resource.....371

Creating an Account.....373

Deleting an Account.....376

Modifying Information About a Specified Account..... 377

Querying Information About the Role Resource Collection..... 380

Querying Information About a Specified Role Resource..... 382

Querying Information About the LDAP Service Resource.....384

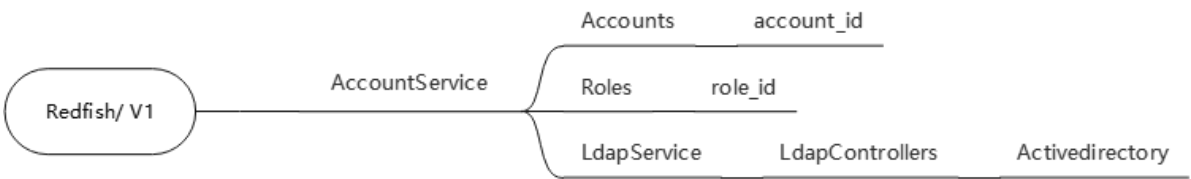
Querying Information About the Collection of LDAP Domain Controller Resources..... 386

Querying the Active Directory Information.....388

Modifying the Active Directory Information..... 391

Figure 10-1 shows the path requirements for the AccountService resources supported by NETA\$ servers

Figure 10-1 AccountService Resource Path Requirements



For a description of properties of AccountService resources and operations supported by the properties, refer to Table 10-1.

Table 10-1 Descriptions of AccountService Resources Properties

URL	Property	Description	Operation
-----	----------	-------------	-----------

/redfish/v1/AccountService	Id	ID of the AccountService resource.	GET
	Name	Name of the AccountService resource.	GET
	MinPasswordLength	Minimum password length.	GET
	MaxPasswordLength	Maximum password length.	GET
	AccountLockoutThreshold	Maximum number of incorrect password attempts.	GET
	AccountLockoutDuration	Account lockout duration after a user login failure.	GET
	AccountLockoutCounter-ResetAfter	Time after which account lockout counter is reset.	GET
	Roles	-	GET
	@odata.id	Access path of the role resource node.	GET
	Accounts	-	GET
	@odata.id	Access path of the account resource node.	GET/PATCH
	Status	Status of the specified resource, including: ● Status: enabling status ● Health: health status	GET
/redfish/v1/AccountService/Accounts	Name	Name of the account resource.	GET
	Members@odata.count	Number of account members.	GET
	Members	-	GET

/redfish/v1/AccountService/Accounts/account_id	Id	ID of the specified user resource.	GET
	Name	Name of the account resource.	GET
	UserName	Username of the account.	GET
	RoleId	Role resource ID in the account configuration.	GET
	Locked	Locked state of the account.	GET
	Enabled	Whether the account is enabled.	GET
	Links	Links to the user resource.	GET

URL	Property	Description	Operation
	Roles	Links to the roles corresponding to the user.	GET
/redfish/v1/AccountService/Accounts	Id	ID of a specified user resource.	POST
	Name	Resource name of an account.	POST
	UserName	Username of the account.	POST
	RoleId	Role resource ID in the account configuration.	POST
	Locked	Locked state of the account.	POST
	Enabled	Whether the account is enabled.	POST
	Links	Links to the user resource.	POST
	Roles	Links to the roles corresponding to the user.	POST
/redfish/v1/AccountService/Roles	Name	Name of the role resource.	GET

	Members@odata.count	Number of current roles.	GET
	Members	-	GET
/redfish/v1/AccountService/Roles/role_id	Id	ID of the specified role resource.	GET
	Name	Name of the specified role resource.	GET
	IsPredefined	Whether the specified role is pre-defined.	GET
	AssignedPrivileges	Privileges assigned to the specified role.	GET
	OemPrivileges	Customized privileges assigned to the specified role.	GET
/redfish/v1/AccountService/LdapService	Id	ID of the LDAP service resource.	GET
	Name	Name of the LDAP service resource.	GET
redfish/v1/AccountService/LdapService/Ldap-Controllers	Name	Name of the LDAP domain controller set.	GET
	Members	LDAP controller member list.	GET
/AccountService/LdapService/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
	GroupLoginInterface	Access permission.	GET/PATCH
	GroupRole	Role group permission.	GET/PATCH
	MemberId	Role group ID: 1–5	GET/PATCH

	GroupDomain	Group domain	GET/PATC H
--	-------------	--------------	---------------

10.1 Querying User Service Information

Function

Query the current user service information about a server, including the password length, the maximum number of incorrect password attempts, and the lockout duration.

Syntax

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

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

Parameter Descriptions

For a description of the parameters for querying the user service information, refer to [Table 10-2](#).

Table 10-2 Parameter Descriptions for Querying User Service Information

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

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/AccountService
- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234
- Request Message Body: None
- Response Example:

```

{
    "@odata.context":
"/redfish/v1/$metadata#AccountService.AccountService",
    "@odata.etag": "W/\"1593569280\"",
    "@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"
    },
    "AuthFailureLoggingThreshold": 3,
    "Description": "BMC User Accounts",
    "Id": "AccountService",
    "MaxPasswordLength": 16,

    "MinPasswordLength":
8,
    "Name":
"Account Service",
    "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 10-3](#).

Table 10-3 Output Descriptions for Querying User Service Information

Field	Type	Description
@odata.context	Character string	OData description of the AccountService resource model.

Field	Type	Description
@odata.id	Character string	Access path of the AccountService resource node.

@odata.type	Character string	Type of AccountService resource.
Id	Character string	ID of the AccountService resource.
Name	Character string	Name of the AccountService resource.
MinPasswordLength	Digit	Minimum password length.
MaxPasswordLength	Digit	Maximum password length.
AccountLockoutThreshold	Digit	Maximum number of incorrect password attempts, range: 1–10.
AccountLockoutDuration	Digit	Lockout duration after a login failure, range: 30–10000, in seconds.
AccountLockoutCounterResetAfter	Digit	Time after which account lockout counter is reset.
Roles	Role resources.	-
@odata.id	Character string	Access path of the role resource node.
Accounts	User resources.	-
@odata.id	Character string	Access path of the Account resource node.
Status	Object	Status of the specified resource, including: ● Status: enabling status ● Health: health status

10.2 Modifying User Service Information

Function

Modify the current user service information about a server, including the maximum number of incorrect password attempts, and the lockout duration.

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
}
```

→ [SSH administrator password modification](#):

```
{
  "Oem":{
    "Public":{
      "SSHAdministratorPassword": password
    }
  }
}
```

Parameter Descriptions

For a description of the parameters for modifying user service information, refer to [Table 10-4](#).

Table 10-4 Parameter Descriptions for Modifying User Service Information

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	Authentication parameters of the request message.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
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.	Range: 1–60, unit: minutes.
password	SSH administrator password .	8–64 characters.

Usage Guidelines

For a specified user, multiple properties in the request message body can be modified at the same time.

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/AccountService
```

- Request Header:

```
X-Auth-Token: 8574621d21b84756218c7456821c234 Content-Type:
application/json
```

- Request Message Body:

```
{
  "AccountLockoutThreshold":8,
  "AccountLockoutDuration": 3
}
```

→ SSH administrator password modification:

```
{
  "Oem": {
    "Public": {
      "SSHAdministratorPassword": "Superuser9!"
    }
  }
}
```

- Response Example: None
- Response Code: 204

Output Description

None

10.3 Querying Information About the User Resource Collection

Function

Query information about the user resource collection of a server.

Syntax

- Operation Type: GET
- URL: https://device_ip/redfish/v1/AccountService/Accounts
- Request Header:

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

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the user resource collection, refer to [Table 10-5](#).

Table 10-5 Parameter Descriptions for Querying Information About the User Resource Collection

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/Accounts
```

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
  "/redfish/v1/$metadata#ManagerAccountCollection.ManagerAccountCollection",
  "@odata.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 10-6](#).

Table 10-6 Output Descriptions for Querying Information About the User Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the account resource model.
@odata.id	Character string	Access path of the account resource node.
@odata.type	Character string	Type of account resource.
Name	Character string	Name of the account resource.
Members@odata.count	Digit	Number of account members.
Members	User List	-
@odata.id	Character string	Access path of a single account resource node.

10.4 Querying Information About a Specified Account Resource

Function

Query information about a specified account resource of a server.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/AccountService/Accounts/account_id`
 - Request Header:

```
X-Auth-Token: auth_value

```

- Request Message Body: None

Parameters

For a description of the parameters for querying information about the specified account resource, refer to [Table 10-7](#).

Table 10-7 Parameter Descriptions for Querying Information About the Specified Account Resource

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

- Status Code: 200

Output Description

a description of the output returned when you query information about the specified account resource, refer to [Table 10-8](#).

Table 10-8 Output Descriptions for Querying Information About the Specified Account Resource

Field	Type	Description
@odata.context	Character string	OData description of the specified account resource model.
@odata.id	Character string	Access path of the specified account resource node.
@odata.type	Character string	Type of the specified account resource.
Id	Character string	ID of the specified account resource.
Name	Character string	Name of the account resource.
UserName	Character string	Username of the account resource.
RoleId	Character string	Role resource ID in the account configuration.

Locked	Boolean	Locked state of the account resource.
Enabled	Boolean	Whether the account is enabled resource.
Links	Object	Links to the account resource.
Roles	Object	Links to the roles corresponding to the account resource.
@odata.id	Character string	Access path of the role corresponding to the account resource.

10.5 Creating an Account

Function

Create an account.

Syntax

- Operation Type: POST
- **URL:** `https://device_ip/redfish/v1/AccountService/Accounts`
- Request Header:

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

- Request Message Body:

```
{
  "UserName": name,
  "Password": password,
  "RoleId": role,
  "Id" : id
}
```

Parameters

For the parameter descriptions for creating an account, refer to [Table 10-9](#).

Table 10-9 Parameter Descriptions for Creating an Account

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
header_type	Format of the request message.	application/json

auth_value	When the post request is executed, the "X-Auth-Token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through / <i>redfish/v1/SessionService/Sessions</i> .
name	Username of the new account.	A string of 4–16 characters.
password	Password of the new account.	A string of 8–16 characters.
role	Role of the new account.	Available role types include: ● Administrator ● Operator ● User ● OEM1 ● OEM2 ● OEM3 ● OEM4
id	Account ID.	Character string, range: 2–16 characters.

Usage Guidelines

None

Example

- Request Example:

POST https://device_ip/redfish/v1/AccountService/Accounts

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234 Content-Type: application/json

- Request Message Body:

```
{
  "Id": "7",
  "UserName": "test77",
  "Password": "Superuser9!",
  "RoleId": "Administrator"
}
```

- Response Example:


```

{
  "@odata.context":
"/redfish/v1/$metadata#ManagerAccount.ManagerAccount",
  "@odata.id":
"/redfish/v1/AccountService/Accounts/7",
  "@odata.type":
"#ManagerAccount.v1_1_1.ManagerAccount",
  "Name": "User Account",
  "Enabled": true,
  "Id": "7",
  "Links": {
    "Roles": {
      "@odata.id":
"/redfish/v1/AccountService/Roles/Administrator"
    }
  },
  "Locked": false,
  "RoleId":
"Administrator",
  "UserName":
"test77"
}

```

- Response code: 201

Output Description

a description of the output returned when you create an account, refer to [Table 10-10](#).

Table 10-10 Output Descriptions for Creating an Account

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

Field	Type	Description
Id	Character string	ID of the specified user resource.
Name	Character string	Name of the account resource.
Enabled	Boolean	Whether the account is enabled.
Links	Object	Links to the account resource.

Roles	Object	Links to the roles corresponding to the account.
Locked	Boolean	Locked state of the account.
RoleId	Character string	Role name, including: • Administrator • Operator • User • OEM1 • OEM2 • OEM3 • OEM4
UserName	Character string	Username

10.6 Deleting an Account

Function

Delete a specified account.

Syntax

- Operation Type: DELETE
- URL: `https://device_ip/redfish/v1/AccountService/Accounts/account_id`
 - Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For a description of the parameters for deleting a specified account, refer to [Table 10-11](#).

Table 10-11 Parameter Descriptions for Deleting a Specified Account

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
account_id	Subscriber ID.	It can obtained by querying the account list.
Parameter	Description	Value

auth_value	When the DELETE request is executed, the "X-Auth-Token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <code>/redfish/v1/SessionService/Sessions</code> .
------------	--	---

Usage Guidelines

None

Example

- Request Example:

DELETE https://device_ip/redfish/v1/AccountService/Accounts/1

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

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

Output Description

None

10.7 Modifying Information About a Specified Account

Function

Modify the username, password, permission, lockout status, enabling status, and login interface of a specified account.

Syntax

- Operation Type: PATCH
- URL: `https://device_ip/redfish/v1/AccountService/Accounts/account_id`
 - Request Header:

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

- Request Message Body:

{
 "UserName":name,
 "Password":password,

```
"RoleId":role,
"Enabled": flag,
"Oem": {
    "Public": {
        "snmpAuthentication": authprotocol,
"snmpPrivacy": privprotocol
    }
}
```

Parameters

For the parameter descriptions for modifying information about the specified account, refer to [Table 10-12](#).

Table 10-12 Parameter Descriptions for Modifying Information About the Specified account

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	Authentication parameters of the request message.	It can be obtained by creating a session through / <i>redfish/v1/SessionService/Sessions</i> .
header_type	Format of the request message.	application/json
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.
username	Username of the new account.	A string of 4–16 characters.
password	Password of the new account.	The maximum length of the string is 20 characters.
role	Role of the new account.	Available role types include: ● Administrator ● Operator ● ReadOnly ● OEM1 ● OEM2 ● OEM3 ● OEM4
flag	Whether the account is enabled.	Range: ● true ● false

authprotocol	SNMPv3 authentication algorithm.	Character string, range: ● SHA
Parameter	Description	Value
		● MD5 ● SHA256 ● SHA384 ● SHA512
privprotocol	SNMPv3 encryption algorithm.	Character string, range: ● DES ● AES

Usage Guidelines

For a specified account, one or more properties in the requested message body can be modified at the same time.



Note

The Oem parameter is optional. If no Oem is added, this parameter is not modified.

Example

- Request Example:

```
PATCH https://device_ip/redfish/v1/AccountService/Accounts/account_id
```

- Request Header:

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

- Request Message Body:

```
{
  "UserName": "username",
  "Password": "Superuser9!",
  "RoleId": "Administrator",
  "Oem": {
    "Public": {
      "snmpAuthentication": "SHA",
      "snmpPrivacy": "DES"
    }
  }
}
```

- Response Example: None
- Response Code: 204

Output Description

None

10.8 Querying Information About the Role Resource Collection

Function

Query information about the role resource collection of a server.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/AccountService/Roles` • Request Header:

X-Auth-Token: auth_value

- Request Message Body: None

Parameters

For the parameter description for querying information about the role resource collection, refer to [Table 10-13](#).

Table 10-13 Parameter Descriptions for Querying Information About the Role Resource Collection

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

Usage Guidelines

None

Example

- Request Example:

GET https://device_ip/redfish/v1/AccountService/Roles

- Request Header:

X-Auth-Token: 8574621d21b84756218c7456821c234

- Request Message Body: None

- Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#RoleCollection.RoleCollection",
  "@odata.id":
"/redfish/v1/AccountService/Roles",
  "@odata.type":
"#RoleCollection.RoleCollection",
  "Name": "Roles Collection",
  "Members": [
    {
      "@odata.id":
"/redfish/v1/AccountService/Roles/Administrator"
    },
    {
      "@odata.id":
"/redfish/v1/AccountService/Roles/Operator"
    },
    {
      "@odata.id":
"/redfish/v1/AccountService/Roles/User"
    },
    {
      "@odata.id":
"/redfish/v1/AccountService/Roles/OEM1"
    },
    {
      "@odata.id":
"/redfish/v1/AccountService/Roles/OEM2"
    },
    {
      "@odata.id":
"/redfish/v1/AccountService/Roles/OEM3"
    },
    {
      "@odata.id":
"/redfish/v1/AccountService/Roles/OEM4"
    }
  ],
  "Members@odata.count": 7,
  "@odata.etag":
"W/\\"19189f29c96a0eb5de9656df36b84b4f\\""
}
```

- Status Code: 200

Output Description

a description of the output returned when you query information about the role resource collection, refer to [Table 10-14](#).

Table 10-14 Output Description for Querying Information About the Role Resource Collection

Field	Type	Description
@odata.context	Character string	OData description of the role resource model.

Field	Type	Description
@odata.id	Character string	Access path of the role resource node.
@odata.type	Character string	Type of role resource.
Name	Character string	Name of the role resource.
Members@odata.count	Digit	Number of role members.
Members	Object array	Session List
@odata.id	Character string	Access path of a single role resource node.

10.9 Querying Information About a Specified Role Resource

Function

Query information about a specified role resource of a server.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/AccountService/Roles/role_id`
 - Request Header:

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

Parameters

For a description of the parameters for querying information about the specified role resource, refer to Table 10-15.

Table 10-15 Parameter Descriptions for Querying Information About the Specified Role Resource

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

auth_value	X-Auth-Token value contained in Request Header in the GET request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
role_id	Role ID.	It can be obtained from the role resource collection.

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/Roles/Administrator
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context": "/redfish/v1/$metadata#Role.Role",
  "@odata.id": "/redfish/v1/AccountService/Roles/Administrator",
  "@odata.type": "#Role.v1_2_1.Role",
  "IsPredefined": true,
  "Name": "User Role",
  "Id": "Administrator",
  "AssignedPrivileges": [
    "ConfigureUsers",
    "ConfigureComponents",
    "ConfigureManager",
    "ConfigureSelf",
    "Login"
  ],
  "OemPrivileges": [
    "OEMSecureConfig",
    "OEMRemoteControl",
    "OEMTelecommunicationsMedium",
    "OEMPowerControl",
    "OEMDebugDiagnostics"
  ],
  "@odata.etag":
  "W/\"1dc3786b3603b7a1318c76fbada555ab\""
}
```

- Status Code: 200

Output Description

a description of the output returned when you query information about the specified role resource, refer to [Table 10-16](#).

Table 10-16 Output Descriptions for Querying Information About the Specified Role Resource

Field	Type	Description
@odata.context	Character string	OData description of the specified role resource model.
@odata.id	Character string	Access path of the specified role resource node.
@odata.type	Character string	Type of the specified role resource.
Id	Character string	ID of the specified role resource.
Name	Character string	Name of the specified role resource.
IsPredefined	Character string	Whether the specified role is pre-defined.
AssignedPrivileges	Array	Privileges assigned to the specified role.
OemPrivileges	Array	Customized privileges assigned to the specified role.

10.10 Querying Information About the LDAP Service Resource

Function

Query the [LDAP](#) about the LDAP service resource.

Syntax

- Operation Type: GET
- URL: `https://device_ip/redfish/v1/AccountService/LdapService`
 - Request Header:

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

Parameters

For a description of the parameters for querying the LDAP about the LDAP service resource, refer to [Table 10-17](#).

Table 10-17 Parameter Descriptions for Querying Information About the LDAP Service Resource

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/LdapService
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#AccountService.LdapService",
  "@odata.id": "/redfish/v1/AccountService/LdapService",
  "@odata.type": "#LdapCollection.LdapServiceCollection",
  "Id": "Ldap Service",
  "LdapControllers": [
    {
      "@odata.id":
        "/redfish/v1/AccountService/LdapService/LdapControllers"
    }
  ],
  "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 about the LDAP service resource, refer to [Table 10-18](#).

Table 10-18 Output Descriptions for Querying Information About the LDAP Service Resource

Field	Type	Description
@odata.context	Character string	OData description of the LDAP service resource model.
@odata.id	Character string	Access path of the LDAP service resource node.
@odata.type	Character string	Type of LDAP service resource.
Id	Character string	ID of the LDAP service resource.
Name	Character string	Name of the LDAP service resource.

Field	Type	Description
@odata.id	Character string	LDAP controller information.

10.11 Querying Information About the Collection of LDAP Domain Controller Resources

Function

Query information about the collection of LDAP domain controller resources.

Syntax

- Operation Type: GET
- URL:
`https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers`
- Request Header:

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

Parameters

For a description of the parameters for querying information about the collection of LDAP domain controller resources, refer to [Table 10-19](#).

Table 10-19 Parameter Descriptions for Querying Information About the Collection of LDAP Domain Controller Resources

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

auth_value	When the Get request is executed, the "x-auth-token" value must be carried in "Headers" for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions.</i>
------------	---	---

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers
```

- Request Header:

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

- Request Message Body: None
- Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#AccountService.LdapService.LdapControllers",
  "@odata.id":
"/redfish/v1/AccountService/LdapService/LdapControllers",
  "@odata.type":
"#AccountService.LdapService.LdapControllers.Activedirectory",
  "Members": [
    {
      "@odata.id":
"/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory"
    },
    {
      "@odata.id":
"/redfish/v1/AccountService/LdapService/LdapControllers/LDAP"
    }
  ],
  "Members@odata.count": 2,
  "Name": "Ldap Controller Collection"
}
```

- Status Code: 200

Output Description

For a description of the output returned when you query information about the collection of LDAP domain controller resources, refer to [Table 10-20](#).

Table 10-20 Output Descriptions for Querying Information About the Collection of LDAP Controller Resources

Field	Type	Description
@odata.context	Character string	OData description of the LDAP domain controller collection model.
@odata.id	Character string	Access path of the LDAP domain controller collection node.
@odata.type	Character string	Type of LDAP domain controller collection.
Name	Character string	Name of the LDAP domain controller collection.
Members	Array	LDAP controller member list.
@odata.id	Character string	ID of an LDAP controller member.

10.12 Querying the Active Directory Information

Function

Query the Active Directory information.

Syntax

- Operation Type: GET
- URL:
`https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory`
- Request Header:

x-auth-token:auth_value

- Request Message Body: None

Parameters

For a description of the parameters for querying the Active Directory information, refer to [Table 10-21](#).

Table 10-21 Parameter Descriptions for Querying the Active Directory Information

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

Usage Guidelines

None

Example

- Request Example:

```
GET https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory
```

- Request Header:

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

- Request Message Body: None • Response Example:

```
{
  "@odata.context":
    "/redfish/v1/$metadata#AccountService.LdapService.LdapControllers.Activedirectory",
```

```
"@odata.id":
"/redfish/v1/AccountService/LdapService/LdapControllers/Activedirectory",
"@odata.context": "#LdapCollection.LdapControllers.Activedirectory",
"ADAuthenticationEnable": true,      "ADRoleGroups": [
    {
        "GroupDomain": "",
        "GroupLoginInterface": [],
        "GroupName": "",
        "GroupRole": null,
        "MemberId": 0
    },
    {
        "GroupDomain": "",
        "GroupLoginInterface": [],
        "GroupName": "",
        "GroupRole": null,
        "MemberId": 1
    },
    {
        "GroupDomain": "",
        "GroupLoginInterface": [],
        "GroupName": "",
        "GroupRole": null,
        "MemberId": 2
    },
    {
        "GroupDomain": "",
        "GroupLoginInterface": [],
        "GroupName": "",
        "GroupRole": null,
        "MemberId": 3
    },
    {
        "GroupDomain": "",
        "GroupLoginInterface": [],
        "GroupName": "",
        "GroupRole": null,
        "MemberId": 4
    }
],
"ADSSLEnable": false,
"DomainControllerServerAddress1": "192.168.5.3",
"DomainControllerServerAddress2": null,
```



```

    "DomainControllerServerAddress3": null,
    "Name": "Activedirectory",
    "Password": null,
    "UserDomain": null,
    "UserName": null
  }

```

- Status Code: 200

Output Description

For a description of the output returned when you query the Active Directory information, refer to [Table 10-22](#).

Table 10-22 Output Descriptions for Querying the Active Directory Information

Field	Type	Description
@odata.context	Character string	OData description of the Active Directory information resource model.
@odata.id	Character string	Access path of Active Directory information resource node.
@odata.type	Character string	Type of Active Directory information resource.
Id	Character string	ID of the Active Directory information resource.
Name	Character string	Name of the Active Directory information resource.
Password	Object	Displayed as null.
ADAuthenticationEnable	Boolean	Whether Active Directory authentication is enabled.
ADSSLEnable	Boolean	Whether SSL encryption is enabled.
DomainControllerServerAddress1	Character string	Domain controller server address 1.
DomainControllerServerAddress2	Character string	Domain controller server address 2.
DomainControllerServerAddress3	Character string	Domain controller server address 3.
UserDomain	Character string	User domain.
ADRoleGroups	Object	AD role group.

GroupName	Character string	Group name.
GroupDomain	Character string	Group domain.
GroupLoginInterface	Object	Access permission: • KVM

Field	Type	Description
		• VMedia
GroupRole	Character string	Role group permission: • Administrator • Operator • ReadOnly
MemberId	Number	Role group ID: 1–5

10.13 Modifying the Active Directory Information

Function

Modify the Active Directory information.

Syntax

- Operation Type: PATCH
- URL:
`https://device_ip/redfish/v1/AccountService/LdapService/LdapControllers/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,
      "GroupName": GroupName_value,
      "GroupRole": GroupRole_value,
      "MemberId": MemberId_value
    }
  ]
}

```

Parameters

For a description of the parameters for modifying the Active Directory information, refer to [Table 10-23](#).

Table 10-23 Parameter Descriptions for Modifying the Active Directory Information

Parameter	Description	Value
device_ip	IP address for logging in to the device.	IPv4 or IPv6 address.
auth_value	X-Auth-Token value contained in Request Header in the PATCH request for authentication.	It can be obtained by creating a session through <i>/redfish/v1/SessionService/Sessions</i> .
ADAuthenticationEnable_value	Boolean	Whether Active Directory authentication is enabled. ● true: enabled. ● false: disabled.
DomainControllerServerAddress1_value	Character string	Domain controller server address 1.
DomainControllerServerAddress2_value	Character string	Domain controller server address 2.

DomainCon- trollerServerAddress3_value	Character string	Domain controller server address 3.
ADSSLEnable_value	Boolean	SSL encryption enabled: ● true ● false
Password_value	Character string	Password
UserDomain_value	Character string	User domain.
UserName_value	Character string	Username
ADRoleGroups	Object	Role group.
GroupDomain_value	Character string	Group domain.
GroupName_value	Character string	Group name. If this parameter is set to null, the role group is deleted.
GroupRole_value	Character string	Role group permission: ● Administrator ● Operator
Parameter	Description	Value
		● ReadOnly
MemberId_value	Number	Role group ID: 1–5

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",
      "GroupName": "bsp",
      "GroupRole": "ReadOnly",
      "MemberId": 1
    },
    {
      "GroupDomain": "exampdle.com",
      "GroupName": "testd",
      "GroupRole": "Administrator",
      "MemberId": 3
    }
  ]
}
```

- Response Example:

```
{
  "@odata.context":
"/redfish/v1/$metadata#AccountService.LdapService.LdapControllers.ActiveDirectory",
  "@odata.id":
"/redfish/v1/AccountService/LdapService/LdapControllers/ActiveDirectory",
}
```

```
"@odata.context":
"#LdapCollection.LdapControllers.Activedirectory",
"ADAuthenticationEnable": true,      "ADRoleGroups": [
    {
        "GroupDomain": "",
"GroupLoginInterface": [],
        "GroupName": "",
        "GroupRole": null,
"MemberId": 0
    },
    {
        "GroupDomain": "",
"GroupLoginInterface": [],
        "GroupName": "",
        "GroupRole": null,
"MemberId": 1
    },
    {
        "GroupDomain": "",
"GroupLoginInterface": [],
        "GroupName": "",
        "GroupRole": null,
"MemberId": 2
    },
    {
        "GroupDomain": "",
"GroupLoginInterface": [],
        "GroupName": "",
        "GroupRole": null,
"MemberId": 3
    },
    {
        "GroupDomain": "",
"GroupLoginInterface": [],
        "GroupName": "",
        "GroupRole": null,
"MemberId": 4
    }
],
"ADSSLEnable": false,
"DomainControllerServerAddress1": "192.168.5.3",
"DomainControllerServerAddress2": null,
"DomainControllerServerAddress3": null,
"Name": "Activedirectory",
```

```

    "Password": null,
    "UserDomain": null,
    "UserName": null
  }

```

- Status Code: 200

Output Description

For a description of the output returned when you modify the Active Directory information, refer to [Table 10-24](#).

Table 10-24 Output Descriptions for Modifying the Active Directory Information

Field	Type	Description
@odata.context	Character string	OData description of the Active Directory information resource model.
@odata.id	Character string	Access path of Active Directory information resource node.
@odata.type	Character string	Type of Active Directory information resource.
Id	Character string	ID of the Active Directory information resource.
Name	Character string	Name of the Active Directory information resource.
Password	Object	Displayed as null.
ADAuthenticationEnable	Boolean	Whether Active Directory authentication is enabled.
DomainControllerServerAddress1	Character string	Domain controller server address 1.
DomainControllerServerAddress2	Character string	Domain controller server address 2.
DomainControllerServerAddress3	Character string	Domain controller server address 3.
UserDomain	Character string	User domain.
ADRoleGroups	Object	AD role group.
GroupName	Character string	Group name.
GroupDomain	Character string	Group domain.

GroupLoginInterface	Object	Access permission: ● KVM ● VMedia
GroupRole	Character string	Role group permission: ● Administrator

Field	Type	Description
		● Operator ● ReadOnly
MemberId	Number	Role group ID: 1–5

Chapter 11

Redfish Installation and Use

Table of Contents

Environment Installation.....	397
Use Case.....	397

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.postman.com/>.
- Use the `httprequester-2.2-fx.xpi` plug-in for 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.



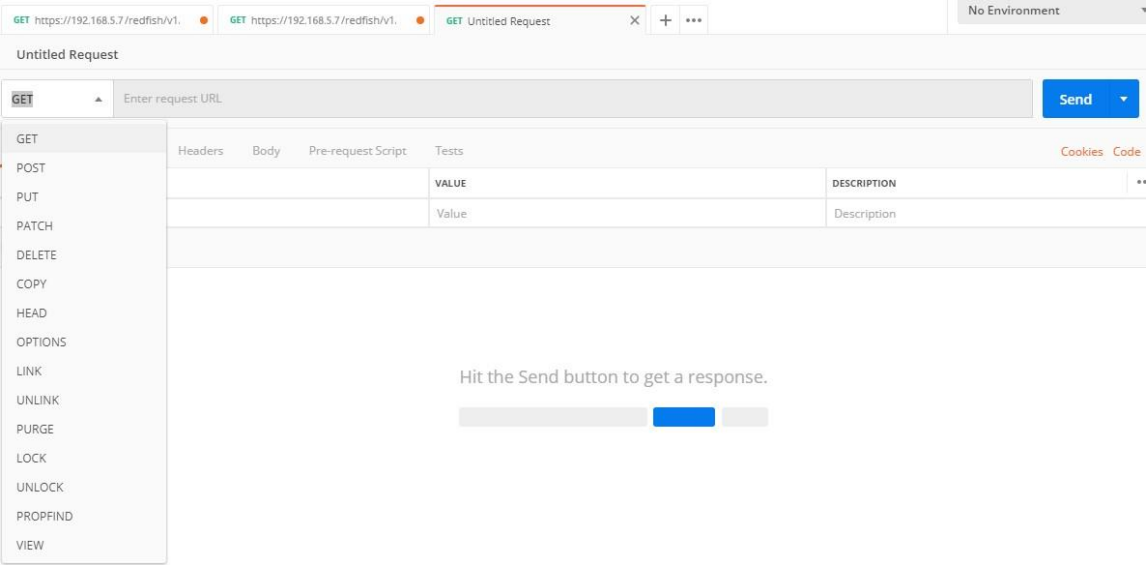
Note

For details on how to query the current root service resources, refer to [3.2 Querying the Current Root Service Resources](#).

Steps

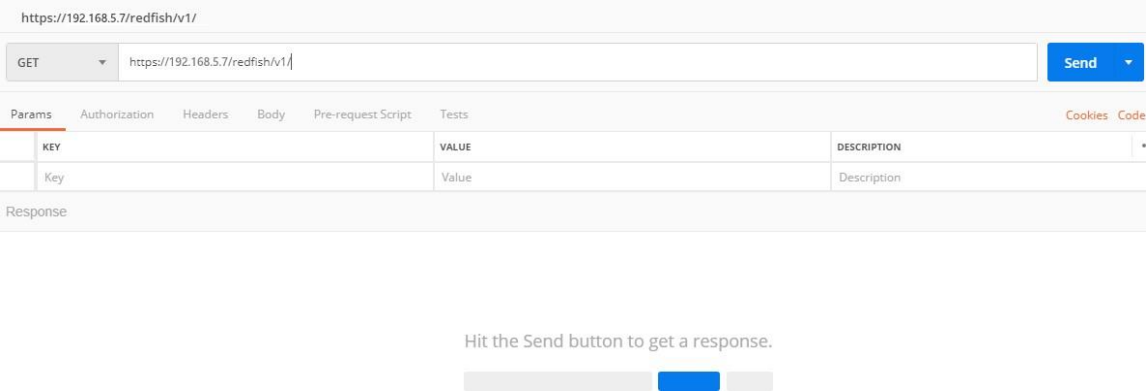
1. Open the Postman tool, create a request on the main page, and select a request action, see [Figure 11-1](#).

Figure 11-1 Selecting a Request Action



2. On the **Params** tab, set the **URL** of the Redfish interface, see 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

The screenshot shows the Redfish web interface. At the top, the URL bar displays `https://192.168.5.7/redfish/v1/`. Below the URL bar, the 'GET' method is selected, and the same URL is entered in the request line. A 'Send' button is visible on the right. The 'Authorization' tab is active, showing a dropdown menu for 'TYPE' with the following options: 'Inherit auth from parent', 'No Auth', 'Bearer Token', 'Basic Auth', 'Digest Auth', 'OAuth 1.0', 'OAuth 2.0', 'Hawk Authentication', 'AWS Signature', and 'NTLM Authentication [Beta]'. The main area of the interface displays the message: 'This request is not inheriting any authorization helper at the moment. Save it in a collection to use the parent's authorization helper.' At the bottom, a message says 'Hit the Send button to get a response.' with a 'Send' button.

4. On the **Authorization** tab, enter the BMC username and password, see [Figure 11-4](#).

Figure 11-4 Entering the BMC Username and Password

The screenshot shows the Redfish web interface with the 'Authorization' tab selected. The 'TYPE' dropdown is set to 'Basic Auth'. A message states: 'The authorization header will be automatically generated when you send the request. [Learn more about authorization](#)'. Below this is a 'Preview Request' button. To the right, the 'Username' field is filled with 'admin' and the 'Password' field is filled with '*****'. A 'Show Password' checkbox is present and unchecked. A warning message at the top of the form area says: 'Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)'. The 'Response' section at the bottom is empty.

5. Click **Send** to send a request through the Redfish interface, see [Figure 11-5](#).

Figure 11-5 Sending a Request

https://192.168.5.7/redfish/v1/

GEThttps://192.168.5.7/redfish/v1/

Send

ParamsAuthorizationHeaders (1)BodyPre-request ScriptTestsCookiesCode

TYPEBasic Auth

The authorization header will be automatically generated when you send the request. [Learn more about authorization](#)

Preview Request

Usernameadmin

Password*****

Show Password

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)

BodyCookiesHeaders (13)Test Results

Status: 200 OKTime: 331 msSize: 1.37 KB

PrettyRawPreviewJSON

```
1 {
2   "@odata.context": "/redfish/v1/$metadata#ServiceRoot.ServiceRoot",
3   "@odata.etag": "W/\"1558746422\"",
4   "@odata.id": "/redfish/v1/",
5   "@odata.type": "#ServiceRoot.v1_1_1.ServiceRoot",
6   "AccountService": {
7     "@odata.id": "/redfish/v1/AccountService"
8   },
9   "Chassis": {
10    "@odata.id": "/redfish/v1/Chassis"
11  },
12  "Description": "The service root for all Redfish requests on this host",
13  "EventService": {
14    "@odata.id": "/redfish/v1/EventService"
15  },
16  "Id": "RootService",
17  "Links": {
18    "Sessions": {
19      "@odata.id": "/redfish/v1/SessionService/Sessions"
20    }
21  }
22 }
```

Glossary

AD

- Active Directory

AHCI

- Advanced Host Controller Interface

API

- Application Program Interface

ARM

- Asynchronous Response Mode

BBU

- Battery Backup Unit

BDF

- Bus/Device/Function

BIOS

- Basic Input/Output System

BMC

- Baseboard Management Controller

BMC

- Baseboard Management Controller

CD

- Compact Disk

CIFS

- Common Internet File System

CPLD

- Complex Programmable Logic Device

CPU

- Central Processing Unit

CSRF

- Cross-Site Request Forgery

DDR

- Double Data Rate

DHCP

- Dynamic Host Configuration Protocol

DNS

- Domain Name System

EPLD

- Erasable Programmable Logic Device

FC

- Fiber Channel

FCoE

- Fibre Channel Over Ethernet

FPGA

- Field Programmable Gate Array

FRU

- Field Replaceable Unit

FTP

- File Transfer Protocol

GPU

- Graphics Processing Unit

HDD

- Hard Disk Drive

HDM

- Handoff Direction Message

HTTP

- Hypertext Transfer Protocol

HTTPS

- Hypertext Transfer Protocol Secure

I/O

- Input/Output

IB

- InfiniBand

ID

- Identification

IO

- Input & Output

IP

- Internet Protocol

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

LLDP

- Link Layer Discovery Protocol

MAC

- Media Access Control

MTU

- Maximum Transfer Unit

NFS

- Network File System

NTP

- Network Time Protocol

NVMe

- Non-Volatile Memory Express

OEM

- Original Equipment Manufacturer

OPA

- Optical Pre-Amplifier

OS

- Operating System

PCB

- Printed Circuit Board

PCIe

- Peripheral Component Interconnect Express

PSU

- Power Supervision Unit

PXE

- Preboot eXecution Environment

RAID

- Redundant Array of Independent Disks

RPM

- Rotations Per Minute

SAS

- Serial Attached SCSI

SATA

- Serial ATA

SEL

- System Event Log

SFTP

- Secure File Transfer Protocol

SMB

- Server Message Block

SMR

- Switching Mode Rectifier

SMTP

- Simple Message Transfer Protocol

SN

- Serial Number

SNMP

- Simple Network Management Protocol

SPI

- Serial Peripheral Interface

SSD

- Solid State Drive

SSDP

- Simple Service Discovery Protocol

SSH

- Secure Shell

SSL

- Secure Sockets Layer

TCP

- Transmission Control Protocol

UDP

- User Datagram Protocol

UHCI

- Universal Host Controller Interface

UID

- User Identifier

UID

- Unique Identifier

URI

- Uniform Resource Identifier

URL

- Uniform Resource Locator

USB

- Universal Serial Bus

UUID

- Universal Unique Identifier

VID

- VLAN Identifier

VLAN

- Virtual Local Area Network

VNC

- Virtual Network Computing

WWNN

- World Wide Node Name

WWPN

- World Wide Port Name

XML

- Extensible Markup Language

NETAŞ

- Zhongxing Telecommunications Equipment

iBMC

- intelligent Board Management

ControlleriSCSI

- Internet Small Computer System Interface