Unified Manager REST APIs

Active IQ Unified Manager

NetApp
March 26, 2025

Table of Contents

Unified Manager REST APIs . . . 1
- APIs for managing data centers . . . 1
- Gateway APIs . . . 5
  - Understanding the API Gateway tunneling . . . 7
  - Setting API scope . . . 8
- Administration APIs . . . 8
- Security APIs . . . 10
- Job objects API and asynchronous processes . . . 11
  - Asynchronous requests described using Job object . . . 11
  - Querying the Job object associated with an API request . . . 11
  - Steps in an asynchronous request . . . 11
  - Viewing Jobs . . . 12
- APIs for managing workloads . . . 12
  - Viewing storage workloads . . . 12
  - Managing access endpoints . . . 13
  - Managing Active Directory mapping . . . 14
  - Managing file shares . . . 15
  - Managing LUNs . . . 16
  - Managing Performance Service Levels . . . 18
  - Managing Storage Efficiency Policies . . . 19

Unified Manager REST APIs

The REST APIs for Active IQ Unified Manager are listed in this section, based on their categories.

You can view the online documentation page from your Unified Manager instance that includes the details of every REST API call. This document does not repeat the details of the online documentation. Each API call listed or described in this document includes only the information you need to locate the call on the documentation page. After locating a specific API call, you can review the complete details of that call, including the input parameters, output formats, HTTP status codes, and request processing type.

The following information is included for each API call within a workflow to help locate the call on the documentation page:

- Category

  The API calls are organized on the documentation page into functionally-related areas or categories. To locate a specific API call, scroll down to the bottom of the page, and then click the applicable API category.

- HTTP verb (call)

  The HTTP verb identifies the action performed on a resource. Each API call is executed through a single HTTP verb.

- Path

  The path determines the specific resource which the action uses to as a part of performing a call. The path string is appended to the core URL to form the complete URL identifying the resource.

APIs for managing data centers

The REST APIs under the `datacenter` category provide information about the clusters, nodes, aggregates, volumes, LUNs, fileshares, namespaces, and other elements in your data center. These APIs are available for querying, adding, deleting, or modifying the configuration in your data center.

Most of these APIs are GET calls that provide cross-cluster aggregation with filtering, sorting and pagination support. On running these APIs, they return data from the database. Therefore, the newly created-objects need to be discovered by the next acquisition cycle for appearing in the response.

If you want to query the details of a specific object, you need to enter the unique ID of that object to view its details. For example,

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-
2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

The CURL commands, examples, requests, and responses to the APIs, are available on your Swagger API interface. You can filter and order the results by specific parameters as indicated on Swagger. These APIs enable you to filter the results for specific storage objects, such as cluster, volume, or storage VM.

HTTP verb	Path	Description

GET	`/datacenter/cluster/clusters`
	
	`/datacenter/cluster/clusters/{key}`
		You can use this method to view the details of the ONTAP clusters across the data center.

GET	`/datacenter/cluster/nodes`
	
	`/datacenter/cluster/nodes/{key}`
		You can use this method to view the details of the nodes in the data center.

GET	`/datacenter/protocols/cifs/shares`
	
	`/datacenter/protocols/cifs/shares/{key}`
		You can use this method to view the details of the CIFS shares in the data center.

GET	`/datacenter/protocols/nfs/export-policies`
	
	`/datacenter/protocols/nfs/export-policies/{key}`
		You can use this method to view the details of the export policies for the supported NFS services.
		
		You can query the export policies for a cluster or storage VM and reuse the export policy key for provisioning NFS file shares. For more information about the assigning and reusing export policies on workloads, see “Provisioning CIFS and NFS file shares”.

HTTP verb	Path	Description
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	You can use this method to view the collection of aggregates in the entire data center for provisioning workloads on them or monitoring.
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	You can use this method to view the collection of LUNs in the entire data center.
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	You can use this method to view the details of all the QoS policies in the data center and apply the policies as required.
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	You can use this method to view the qtree details across the data center.
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	You can use this method to view the collection of volumes in the data center.

HTTP verb	Path	Description

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/protocols/san/igroups`
	
	`/datacenter/protocols/san/igroups/{key}`
		You can assign initiator groups (igroups) authorized to access particular LUN targets. If there is an existing igroup, you can assign it. You can also create igroups and assign them to the LUNs.
		
		You can use these methods to query, create, delete, and modify igroups respectively.
		
		Points to note:
		
		• `POST`: While creating an igroup, you can designate the storage VM on which you want to assign access.
		• `DELETE`: You need to provide the igroup key as an input parameter to delete a particular igroup. If you have already assigned an igroup to a LUN, you cannot delete that igroup.
		• `PATCH`: You need to provide the igroup key as an input parameter to modify a particular igroup. You must also enter the property that you want to update, along with its value.

HTTP verb	Path	Description

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/svm/svms`
	
	`/datacenter/svm/svms/{key}`
		You can use these methods to view, create, delete, and modify Storage Virtual Machines (storage VMs).
		
		Points to note:
		
		• `POST`: You must enter the storage VM object that you want to create as an input parameter. You can create a custom storage VM, and then assign required properties to it.
		
		ⓘ If you have enabled SLO-based workload provisioning on your environment, while creating the storage VM, ensure that it supports all of the protocols required for provisioning LUNs and file shares on them, for example, SMB/CIFS, NFS, FCP, and iSCSI. The provisioning workflows might fail if the storage VM does not support the required services. It is recommended that the services for the respective types of workloads are also enabled on the storage VM.
		
		• `DELETE`: You need to provide the storage VM key to delete a particular storage VM.
		
		ⓘ If you have enabled SLO-based workload provisioning on your environment, you cannot delete that storage VM on which storage workloads have been provisioned. When you delete a storage VM on which a CIFS/SMB server has been configured, this API also deletes the CIFS/SMB server, along with the local Active Directory configuration. However, the CIFS/SMB server name continues to be in the Active Directory configuration that you must delete manually from the Active Directory server.
		
		• `PATCH`: You need to provide the storage VM key to modify a particular storage VM. You also need to enter the properties that you want to update, along with their values.

Gateway APIs

The gateway APIs provide you with the advantage of using the Active IQ Unified Manager credentials to run ONTAP REST APIs and managing storage objects. These APIs are available when the API Gateway feature is enabled from the Unified Manager web UI.

Unified Manager REST APIs support only a select set of actions to be performed on the Unified Manager datasources, that is ONTAP clusters. You can avail the other features through ONTAP APIs. The gateway APIs allow Unified Manager to be a pass-through interface for tunneling all API requests to be performed on ONTAP clusters, without logging in to each data center cluster individually. It performs as a single point of management for running the APIs across the ONTAP clusters managed by your Unified Manager instance. The API Gateway

feature allows Unified Manager to be a single control plane from which you can manage multiple ONTAP clusters, without logging in to them individually. The gateway APIs enable you to remain logged in to Unified Manager and manage the ONTAP clusters by running ONTAP REST API operations.

All users can run a query by using the `GET` operation. Application Administrators can run all ONTAP REST operations.

The gateway acts as a proxy to tunnel the API requests by maintaining the header and body requests in the same format as in the ONTAP APIs. You can use your Unified Manager credentials and execute the specific operations to access and manage the ONTAP clusters without passing individual cluster credentials. It continues to manage the cluster authentication and cluster management, but redirects the API requests to run directly on the specific cluster. The response returned by the APIs is the same as the response returned by the respective ONTAP REST APIs executed directly from ONTAP.

HTTP verb	Path (URL)	Description
`GET`	`/gateways`	This GET method retrieves the list of all the clusters managed by Unified Manager that support ONTAP REST calls. You can verify the cluster details and choose to run other methods based on the cluster UUID or universal unique identifier (UUID). The gateway APIs retrieve only those clusters supported by ONTAP 9.5 or later, and added to Unified Manager over HTTPS.

HTTP verb	Path (URL)	Description

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
 	
`OPTIONS` (not available on Swagger)
 	
`HEAD` (not available on Swagger)
	`/gateways/{uuid}/{path}`
	
	The value for `{uuid}` must be replaced with the cluster UUID on which the REST operation is to be performed. Also, ensure that the UUID is of the a cluster supported by ONTAP 9.5 or later, and added to Unified Manager over HTTPS. `{path}` must be replaced by the ONTAP REST URL. You must remove `/api/` from the URL.
		This is a single point proxy API, supporting POST, DELETE, PATCH operations and GET for all the ONTAP REST APIs. No restrictions apply on any of the API as long as it is supported by ONTAP. The tunnelling or proxy functionality cannot be disabled.
		
		The `OPTIONS` method returns all the operations supported by an ONTAP REST API. For example, if an ONTAP API supports only the `GET` operation, running the `OPTIONS` method by using this gateway API returns `GET` as the response. This method is not supported on Swagger, but can be performed on other API tools.
		
		The `OPTIONS` method determines whether a resource is available. This operation can be used to view the metadata about a resource in the HTTP response headers. This method is not supported on Swagger, but can be performed on other API tools.

Understanding the API Gateway tunneling

The gateway APIs enable you to manage ONTAP objects through Unified Manager. Unified Manager manages the clusters and authentication details and redirects the requests to the ONTAP REST endpoint. The gateway API transforms the URL and Hypermedia as the Engine of Application State (HATEOAS) links in the header and response body with the API gateway base URL. The gateway API acts as the proxy base URL to which you append the ONTAP REST URL and execute the required ONTAP REST endpoint.

In this example, the gateway API (proxy base URL) is: `/gateways/{uuid}/`

The ONTAP API taken is: `/storage/volumes`. You need to add the ONTAP API REST URL as the value for the `path` parameter.

While adding the path, ensure that you have removed the “/” symbol at the beginning of the URL. For the API `/storage/volumes`, add `storage/volumes`.

The appended URL is: `/gateways/{uuid}/storage/volumes`

On running the `GET` operation, the generated URL is the following:
`GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes`

The `/api` tag of the ONTAP REST URL is removed in the appended URL and that for the gateway API is retained.

Sample cURL command

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes" -H "accept: application/hal+json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

The API returns the list of storage volumes in that cluster. The response format is the same as you receive when you run the same API from ONTAP. The status codes returned are the ONTAP REST status codes.

Setting API scope

All APIs have a context set within the scope of the cluster. APIs that operate on the basis of storage VMs also have the cluster as the scope, that is, the API operations are performed on a particular storage VM within a managed cluster. When you run the `/gateways/{uuid}/{path}` API, ensure that you enter the cluster UUID (Unified Manager datasource UUID) for the cluster on which you run the operation. For setting the context to a particular storage VM within that cluster, enter the storage VM key as the `X-Dot-SVM-UUID` parameter or the storage VM name as the `X-Dot-SVM-Name` parameter. The parameter is added as the filter in the string header and the operation is run within the scope of that storage VM inside that cluster.

Sample cURL command

```
curl -X GET "https://<hostname>/api/gateways/e4f33f90-f75f-11e8-9ed9-
00a098e3215f/storage/volume" -H "accept: application/hal+json" -H "X-Dot-
SVM-UUID: d9c33ec0-5b61-11e9-8760-00a098e3215f"
-H "Authorization: Basic <Base64EncodedCredentials>"
```

For more information about using ONTAP REST APIs, see ONTAP REST API Automation.

Administration APIs

You can use the APIs under the `administration` category to modify backup settings, verify the backup file information and cluster certificates, and also manage ONTAP clusters as Active IQ Unified Manager datasources.

You must have the Application Administrator role for running these operations. You can also use the Unified Manager web UI for configuring these settings.

HTTP verb	Path	Description
GET PATCH	/admin/backup-settings /admin/backup-settings	You can use the GET method to view the settings of the backup schedule configured in Unified Manager by default. You can verify the following: • Whether the schedule is enabled or disabled • Frequency of the backup scheduled (daily or weekly) • Time of the backup • Maximum number of backup files that should be retained in the application The time of the backup is in server time zone. The database backup settings are available on Unified Manager by default, and you cannot create a backup schedule. However, you can use the PATCH method to modify the default settings.
GET	/admin/backup-file-info	A backup dump file is generated every time the backup schedule is modified for Unified Manager. You can use this method to verify whether the backup file is generated according to the modified backup settings, and whether the information on the file matches the modified settings.
GET	/admin/datasource-certificate	You can use this method to view the datasource (cluster) certificate from the trust store. Validating the certificate is required before adding an ONTAP cluster as a Unified Manager datasource.

HTTP verb	Path	Description
GET POST PATCH DELETE	/admin/datasources/clusters /admin/datasources/clusters/{key}	You can use the GET method to retrieve the details of the datasources (ONTAP clusters) managed by Unified Manager. You can also add a new cluster to Unified Manager as a datasource. For adding a cluster, you must know its host name, user name, and password. For modifying and deleting a cluster managed as a datasource by Unified Manager, use the ONTAP cluster key.

Security APIs

You can use the APIs in the security category to control user access to selected cluster objects in Active IQ Unified Manager. You can add local users or database users. You can also add remote users or groups that belong to an authentication server. Based on the privileges of the roles that you assign to the users, they can manage the storage objects or view the data in Unified Manager.

You must have the Application Administrator role for running these operations. You can also use the Unified Manager web UI for configuring these settings.

The APIs under the security category use the users parameter, that is the user name, and not the key parameter as the unique identifier for the user entity.

HTTP verb	Path	Description
GET POST	/security/users /security/users	You can use these methods to get the details of users or add new user to Unified Manager. You can add specific roles to the users based on their user types. While adding users, you must provide passwords for the local user, maintenance user, and database user.

HTTP verb	Path	Description
GET PATCH DELETE	/security/users/{name}	The GET method enables you to retrieve all the details of a user, such as the name, email address, role, authorization type. The PATCH method enables you to update the details. The DELETE method enables you to remove the user.

Job objects API and asynchronous processes

The management-server category consists of the jobs API that provides information about the Jobs performed while running Active IQ Unified Manager APIs. you must know how asynchronous processing works using the Job object.

Some of the API calls, particularly those that are used for adding or modifying resources, can take longer to complete than other calls. Unified Manager processes these long-running requests asynchronously.

Asynchronous requests described using Job object

After making an API call that runs asynchronously, the HTTP response code 202 indicates the request has been successfully validated and accepted, but not yet completed. The request is processed as a background task which continues to run after the initial HTTP response to the client. The response includes the Job object anchoring the request, including its unique identifier.

Querying the Job object associated with an API request

The Job object returned in the HTTP response contains several properties. You can query the state property to determine if the request completed successfully. A Job object can be in one of the following states:

- NORMAL
- WARNING
- PARTIAL_FAILURES
- ERROR

There are two techniques you can use when polling a Job object to detect a terminal state for the task, either success or failure:

- Standard polling request: The current Job state is returned immediately.
- Long polling request: When the job state moves to NORMAL, ERROR, or PARTIAL_FAILURES.

Steps in an asynchronous request

You can use the following high-level procedure to complete an asynchronous API call:

1. Issue the asynchronous API call.
2. Receive an HTTP response 202 indicating successful acceptance of the request.

3. Extract the identifier for the Job object from the response body.
4. Within a loop, wait for the Job object to reach the terminal state `NORMAL`, `ERROR`, or `PARTIAL_FAILURES`.
5. Verify the terminal state of the Job and retrieve the Job result.

Viewing Jobs

In Active IQ Unified Manager, operations like adding and modifying resources are performed by synchronous and asynchronous API invocations. Invocations that are scheduled for asynchronous execution can be tracked by a Job object created for that invocation. Each Job object has a unique key for identification. Each Job object returns the Job object URI for you to access and track the progress of the job. You can use this API for retrieving the details of each execution.

You can query all of the Job objects. You can also use the Job key and Job object details to run the next set of operations on the resources.

View jobs

You can use this method to obtains a list of all of the Jobs. The response body consists of the Job details of all of the Jobs. You can also view the details of a particular Job object by specifying the Job key in the URI. The response body consists of the details that are identified by the Job key. In the response, the latest Job object is returned to the top. If you want to query a particular Job object, enter the Job ID of the job.

Category	HTTP verb	Path

management-server	GET	`/management-server/jobs`
		
		`/management-server/jobs/{key}`

APIs for managing workloads

The APIs described here cover various functions of storage administration, such as viewing storage workloads, creating LUNs and file shares, managing Performance Service Levels and Storage Efficiency Policies, and assigning the policies on storage workloads.

Viewing storage workloads

The APIs listed here enable you to view a consolidated list of storage workloads for all of the ONTAP clusters in your data center. The APIs also provide a summary view of the number of the storage workloads provisioned in your Active IQ Unified Manager environment, and their capacity and performance (IOPS) statistics.

View storage workloads

You can use the following method to view all the storage workloads in all the clusters in your data center. For information about filtering the response based on specific columns, see the API reference documentation

available in your Unified Manager instance.

Category	HTTP verb	Path
storage-provider	GET	`/storage-provider/workloads`

View storage workloads summary

You can use the following method to assess the used capacity, available capacity, used IOPS, available IOPS, and number of storage workloads managed by each Performance Service Level. The storage workloads displayed can be for any LUN, NFS file share, or CIFS share. The API provides a storage workloads overview, an overview of the storage workloads provisioned by the Unified Manager, a data center overview, an overview of the total, used, and available space and IOPS in the data center, in terms of the assigned Performance Service Levels. The information received in response to this API is used to populate the dashboard in the Unified Manager UI.

Category	HTTP verb	Path
storage-provider	GET	`/storage-provider/workloads-summary`

Managing access endpoints

You need to create access endpoints or logical interfaces (LIFs), which are required for provisioning Storage Virtual Machines (SVMs), LUNs, and file shares. You can view, create, modify, and delete the access endpoints for the SVMs, LUNs, or file shares in your Active IQ Unified Manager environment.

View access endpoints

You can view a list of the access endpoints in your Unified Manager environment by using the following method. To query a list of access endpoints of a particular SVM, LUN, or file share, you need to enter the unique identifier for the SVM, LUN, or file share. You can also enter the unique access endpoint key to retrieve the details of the particular access endpoint.

Category	HTTP verb	Path

storage-provider	GET	`/storage-provider/access-endpoints`
		
		`/storage-provider/access-endpoints/{key}`

Add access endpoints

You can create custom access endpoints and assign required properties to it. You must enter the details of the access endpoint that you want to create as the input parameters. You can use this API, or the System Manager or ONTAP CLI to create an access endpoint on each node. Both IPv4 and IPv6 addresses are supported for access endpoints creation.

You must configure your SVM with a minimum number of access endpoints per node for successful provisioning of LUNs and file shares. You should configure your SVM with at least two access endpoints per node, one supporting CIFS and/or NFS protocol, another supporting iSCSI or FCP protocol.

Category	HTTP verb	Path
storage-provider	POST	`/storage-provider/access-endpoints`

Delete access endpoints

You can delete a specific access endpoint by using the following method. You need to provide the access endpoint key as an input parameter to delete a particular access endpoint.

Category	HTTP verb	Path
storage-provider	DELETE	`/storage-provider/access-endpoints/{key}`

Modify access endpoints

You can modify an access endpoint and update its properties by using the following method. You need to provide the access endpoint key to modify a particular access endpoint. You also need to enter the property that you want to update, along with its value.

Category	HTTP verb	Path
storage-provider	PATCH	`/storage-provider/access-endpoints/{key}`

Managing Active Directory mapping

You can use the APIs listed here to manage Active Directory mappings on the SVM that are required for provisioning CIFS shares on the SVMs. Active Directory mappings need to be configured for mapping the SVMs with ONTAP.

View Active Directory mappings

You can view the configuration details of the Active Directory mappings for an SVM by using the following method. For viewing the Active Directory mappings on an SVM, you need to enter the SVM key. For querying the details of a particular mapping, you must enter the mapping key.

Category	HTTP verb	Path

storage-provider	GET	`/storage-provider/active-directories-mappings`
		
		`/storage-provider/active-directories-mappings/{key}`

Add Active Directory mapping

You can create Active Directory mappings on an SVM by using the following method. You must enter the mapping details as the input parameters.

Category	HTTP verb	Path
storage-provider	POST	`/storage-provider/active-directories-mappings`

Managing file shares

You can use the APIs listed here to view, add, and delete CIFS shares and NFS file shares. Using these APIs, you can also assign and modify the Performance Service Level and Storage Efficiency Policies for the file shares.

Before assigning storage, the virtual machine must have been created and provisioned with the supported protocols. Similarly, for assigning Storage Efficiency Policies to the file shares, the Storage Efficiency Policies must be created before creating the file shares.

View file shares

You can use the following method to view all of the storage workloads available in your Unified Manager environment. When you have added an ONTAP cluster as a datasource on Active IQ Unified Manager, the storage workloads for those clusters are automatically added to your Unified Manager instance. This API retrieves the all file shares automatically and manually added to your Unified Manager instance. You can view the details of a specific file share by running this API with the file share key.

Category	HTTP verb	Path

storage-provider	GET	`/storage-provider/file-shares`
		
		`/storage-provider/file-shares/{key}`

Add file shares

You can use the following method to add CIFS and NFS file shares in your SVM. You must enter the details of the file share that you want to create, as the input parameters. You cannot use this API for creating FlexGroups.

Category	HTTP verb	Path
storage-provider	POST	`/storage-provider/file-shares`

Depending on whether the access control list (ACL) parameters or the export policy parameters are provided, CIFS shares or NFS file shares are created. If you do not provide the values for the ACL parameters, CIFS shares are not created, and NFS shares are created by default, providing access to all.

Delete file shares

You can use the following method to delete a specific file share. You need to enter the file share key as an input parameter to delete a particular file share.

Category	HTTP verb	Path
storage-provider	DELETE	`/storage-provider/file-shares/{key}`

Modify file shares

You can use the following method to modify a file share and update its properties.

You need to provide the file share key to modify a particular file share. Additionally, you need to enter the property that you want to update, along with its value.

Note that you can update only one property at a single invocation of this API. For multiple updates, you need to run this API as many times.

Category	HTTP verb	Path
storage-provider	PATCH	`/storage-provider/file-shares/{key}`

Managing LUNs

You can use the APIs listed here to view, add, and delete LUNs on the Storage Virtual Machines (storage VMs). You can also assign and modify the Performance Service Level and Storage Efficiency Policies for the LUNs.

Before assigning storage, you must ensure that the SVM has been created and provisioned with the supported protocols. Similarly, for assigning Performance Service Levels to the LUNs, the Performance Service Levels must be created before creating the LUN.

View LUNs

You can use the following method to view all the LUNs in your Unified Manager environment. When you have added an ONTAP cluster as a datasource on Active IQ Unified Manager, the storage workloads for those

clusters are automatically added to your Unified Manager instance. This API retrieves the all LUNs automatically and manually added to your Unified Manager instance. You can view the details of a specific LUN by running this API with the LUN key.

Category	HTTP verb	Path

storage-provider	GET	`/storage-provider/luns`
		
		`/storage-provider/luns/{key}`

Add LUNs

You can use the following method to add LUNs to your SVMs.

Category	HTTP verb	Path
storage-provider	POST	`/storage-provider/luns`

In your cURL request, if you provide a value for the optional parameter `volume_name_tag` in the input, then that value is used while naming the volume during the LUN creation. This tag enables searching the volume easily. If you provide the volume key in the request, the tagging is skipped.

Delete LUNs

You can use the following method to delete a specific LUN. You need to provide the LUN key to delete a particular LUN.

If you have created a volume in ONTAP and then provisioned LUNs through Unified Manager on that volume, when you delete all of the LUNs by using this API, the volume also gets deleted from the ONTAP cluster.

Category	HTTP verb	Path
storage-provider	DELETE	`/storage-provider/luns/{key}`

Modify LUNs

You can use the following method to modify a LUN and update its properties. You need to provide the LUN key to modify a particular LUN. You also need to enter the LUN property that you want to update, along with its value. For updating LUN arrays by using this API, you should review the recommendations in “Recommendations for using the APIs”.

You can update only one property at a single invocation of this API. For multiple updates, you need to run this API as many times.

Category	HTTP verb	Path
storage-provider	PATCH	`/storage-provider/luns/{key}`

Managing Performance Service Levels

You can view, create, modify, and delete Performance Service Levels by using the storage provider APIs for on your Active IQ Unified Manager.

View Performance Service Levels

You can use the following method to view the Performance Service Levels for assigning them to storage workloads. The API lists all of the system-defined and user-created Performance Service Levels, and retrieves the attributes of all of the Performance Service Levels. If you want to query a specific Performance Service Level, you need to enter the unique ID of the Performance Service Level to retrieve its details.

Category	HTTP verb	Path

storage-provider	GET	`/storage-provider/performance-service-levels`
		
		`/storage-provider/performance-service-levels/{key}`

Add Performance Service Levels

You can use the following method to create custom Performance Service Levels and assign them to your storage workloads if the system-defined Performance Service Levels do not meet the required service level objectives (SLOs) for the storage workloads. Enter the details for the Performance Service Level that you want to create. For the IOPS properties, ensure that you enter valid range of values.

Category	HTTP verb	Path
storage-provider	POST	`/storage-provider/performance-service-levels`

Delete Performance Service Levels

You can use the following method to delete a specific Performance Service Level. You cannot delete a Performance Service Level if it is assigned to a workload, or if it is the only available Performance Service Level. You need to provide the unique ID of the Performance Service Level as an input parameter to delete a particular Performance Service Level.

Category	HTTP verb	Path
storage-provider	DELETE	`/storage-provider/performance-service-levels/{key}`

Modify Performance Service Levels

You can use the following method to modify a Performance Service Level and update its properties. You cannot modify a Performance Service Level that is system-defined or is assigned to a workload. You need to provide the unique ID of the to modify a particular Performance Service Level. You must also enter the IOPS property that you want to update, along with a valid value.

Category	HTTP verb	Path
storage-provider	PATCH	`/storage-provider/performance-service-levels/{key}`

Viewing aggregate capabilities based on Performance Service Levels

You can use the following method to query the aggregate capabilities based on Performance Service Levels. This API returns the list of aggregates available in your data center and indicates the capabilities in terms of the Performance Service Levels that can be supported in those aggregates. While provisioning workloads on a volume, you can view the capability of an aggregate to support a particular Performance Service Level, and provision workloads based on that capability. Your ability to specify the aggregate is available only when you are provisioning a workload by using APIs. This functionality is not available on the Unified Manager web UI.

Category	HTTP verb	Path

storage-provider	GET	`/storage-provider/aggregate-capabilities`
		
		`/storage-provider/aggregate-capabilities/{key}`

Managing Storage Efficiency Policies

You can view, create, modify, and delete Storage Efficiency Policies by using the storage provider APIs.

Note the following points:

- It is not mandatory to assign a Storage Efficiency Policy while creating a workload on Unified Manager.
- You cannot unassign a Storage Efficiency Policy from a workload after a policy is assigned to it.
- If a workload has some storage settings specified on ONTAP volumes, such as deduplication and compression, those settings can be overwritten by the settings specified in the Storage Efficiency Policy that you apply when you add the storage workloads on Unified Manager.

View Storage Efficiency Policies

You can use the following method to view the Storage Efficiency Policies before assigning them to storage workloads. This API lists all of the system-defined and user-created Storage Efficiency Policies, and retrieves the attributes of all of the Storage Efficiency Policies. If you want to query a specific Storage Efficiency Policy, you need to enter the unique ID of the policy to retrieve its details.

Category	HTTP verb	Path

storage-provider	GET	`/storage-provider/storage-efficiency-policies`
		
		`/storage-provider/storage-efficiency-policies/{key}`

Add Storage Efficiency Policies

You can use the following method to create custom Storage Efficiency Policies, and assign them to your storage workloads if the system-defined policies do not meet the provisioning requirements for your storage workloads. Enter the details of the Storage Efficiency Policy that you want to create, as input parameters.

Category	HTTP verb	Path
storage-provider	POST	`/storage-provider/storage-efficiency-policies`

Delete Storage Efficiency Policies

You can use the following method to delete a specific Storage Efficiency Policy. You cannot delete a Storage Efficiency Policy if it is assigned to a workload, or if it is the only available Storage Efficiency Policy. You need to provide the unique ID of the Storage Efficiency Policy as an input parameter to delete a particular Storage Efficiency Policy.

Category	HTTP verb	Path
storage-provider	DELETE	`/storage-provider/storage-efficiency-policies/{key}`

Modify Storage Efficiency Policies

You can use the following method to modify a Storage Efficiency Policy and update its properties. You cannot modify a Storage Efficiency Policy that is system-defined or is assigned to a workload. You need to provide the unique ID of the Storage Efficiency Policy to modify a particular Storage Efficiency Policy. Additionally, you need to provide the property that you want to update, along with its value.

Category	HTTP verb	Path
storage-provider	PATCH	`/storage-provider/storage-efficiency-policies/{key}`

Copyright information

Trademark information